В. Я. Ищейнов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

ТЕОРИЯ И ПРАКТИКА

DirectMEDIA

В. Я. Ищейнов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

ТЕОРИЯ И ПРАКТИКА

Учебное пособие

DirectMEDIA
Москва
Берлин
2020

УДК 004.056(075)
ББК 32.81я73+32.972.53я73
И98

Рецензенты:
С. М. Чудинов, доктор технических наук, профессор, научный консультант АО «НИИВК им. М. А. Кравцева»;
В. Т. Олейников, профессор, кандидат технических наук, старший научный сотрудник Академии ГПС МЧС России

Ищейнов, В. Я.
И98 Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. — Москва ; Берлин : Директ-Медиа, 2020. — 270 с.

ISBN 978-5-4499-0496-6

В учебном пособии рассмотрены основы общей теории информационной безопасности; методы и средства национальной безопасности Российской Федерации. Обобщены вопросы основ национальной безопасности в сфере информационной безопасности, рассмотрены информационные технологии и основные тенденции их развития, формы ведения информационных войн. Представлена система международной и региональной информационной безопасности.

Учебное пособие соответствует требованиям государственного стандарта образовательной программы подготовки специалистов высших учебных заведений по специальности 10.04.01 «Информационная безопасность».

Книга рассчитана на широкий круг читателей и, в первую очередь, на студентов высших учебных заведений, обучающихся в области информационной безопасности, а также преподавателей и специалистов, изучающих вопросы информационной безопасности и защиты информации.

УДК 004.056(075)
ББК32.81я73+32.972ю53я73

ISBN 978-5-4499-0496-6

Оглавление

Введение

Развитие информационно-телекоммуникационных технологий существенным образом затрагивает интересы государства, общества и личности, в связи с чем, является актуальным обеспечение их информационной безопасности.

Целью учебного пособия является рассмотрение базовых вопросов общей теории информационной безопасности для понимания и снижения рисков, угроз и уязвимостей.

Из широкого спектра задач рассмотрены основные, а именно:

– обеспечение информационной безопасности в современных условиях и основные факторы, влияющие на ее защиту;

– определение взаимосвязи национальных интересов и национальной безопасности;

– проведение анализа форм и методов ведения информационной войны;

– определение геополитической стратегии Российской Федерации в сфере информационной безопасности.

В учебном пособии рассмотрена теория информационной безопасности и национальной безопасности Российской Федерации, а также: типология, принципы, психология информационной безопасности. Обобщены вопросы основ национальной безопасности в сфере информационной безопасности, рассмотрены информационные технологии и основные тенденции развития, формы ведения информационной войны. Представлена система международной и региональной информационной безопасности, проведен анализ мировых соотношений информационных технологий в сфере информационной безопасности.

Книга рассчитана на широкий круг читателей, и в первую очередь на студентов, преподавателей и специалистов, изучающих вопросы информационной безопасности и защиты информации. В данной работе представлен обширный материал, который обобщен и систематизирован, что позволило его представить в виде основ общей теории информационной безопасности и использовать в качестве учебного пособия для студентов высших учебных заведений по специальности 10.04.01 «Информационная безопасность».

При написании учебного пособия был использован материал из работ авторов: А. И. Владимирова, В. А. Галатенко, В. А. Герасименко, Г. В. Емельянова, В. А. Конявского, Ю. М. Краковского, А. А. Малюка, А. В. Монайло, В. П. Петрова, С. В. Петрова, А. А. Позднякова, А. А. Стрельцова, Р. Хаббарда, А. А. Хорева, Л.Дж. Хоффмана, В. Н. Ясенева.

Глава 1
История вопроса и состояние проблемы

1.1. История вопроса

На заре своего развития человек, предупреждая своих современников об опасности или созывая на охоту, подавал сигналы криком или стуком. Звук — основа нашего речевого общения. Но если расстояние между собеседниками велико и силы голоса не хватает, требуются вспомогательные средства. Поэтому человек начал использовать «технику» — свистки, рога животных, факелы, костры, барабаны, гонги, а после изобретения пороха — ружья и ракеты. Появились специальные людигонцы, герольды, — которые переносили и передавали сообщения, оглашали народу волю владык. В Южной Италии кое-где по берегу моря до последнего времени сохранялись развалины сторожевых постов, с которых посредством колокольного звона передавались известия о приближении норманнов и сарацинов.

С незапамятных времен в качестве носителя информации применяется и свет. Первыми «системами» связи стали сторожевые посты, располагавшиеся вокруг поселений на специально построенных вышках или башнях, а иногда просто на деревьях. При приближении неприятеля зажигался костер тревоги. Увидев огонь, зажигали костер часовые на промежуточном посту, и неприятелю не удавалось застать жителей врасплох. Для гонцов создавались станции смены лошадей. Маяки и ракеты до сих пор несут свою «информационную службу» на море и в горах.

Необходимость передавать не только отдельные сигналы типа «тревога», но и различные сообщения привела к применению «кодов», когда разные сообщения различались, например, числом и расположением костров, числом и частотой свистков или ударов в барабан и т. п. Греки во втором веке до нашей эры использовали комбинации факелов для передачи сообщений «по буквам». На море широкое применение нашли сигнальные флаги различной формы и цвета, причем сообщение определяется не только самими флагами, но и их взаимным расположением, а также «семафор»-передача сообщений

изменением расположения рук с флажками (днем) или фонарями (ночью). Потребовались люди, знающие «язык» флагов или семафора, умеющие передавать и принимать переданные сообщения.

Однако огромным минусом такой коммуникации является то, что переданную информацию невозможно сохранить и обработать. Поэтому формы передачи информации постепенно совершенствовались. Сначала это были просто различные зарубки на деревьях и стенах пещер. Потом от серии примитивных рисунков человек постепенно переходит к клинописи и иероглифам, а затем — и к фонетическому письму буквами.

Аграрный период

Появление письменности отделяет первобытность от классической древности, с которой начинается современная история. Письменная информация отчуждается от своих создателей на протяжении веков и тысячелетий.

Самым древним образцом письменности считается дунайское протописьмо, нанесенное на тэртерийские таблички, найденные в 1961 г. в Румынии. Высеченные пиктограммы датируются 5500 г. до н.э. Следующими по древности выступают египетские иероглифы и месопотамская клинопись, которые уже существовали к 3000 г. до н.э. В Китае самые ранние свидетельства существования письменности датируются XIV в. до н.э., в Индии — III–II тысячелетиями до н. э.

Особое значение для эволюции информационной деятельности имело изобретение алфавита семитами Палестины и Сирии, от которого произошли все алфавиты прошлого и настоящего времени. Возникновение греческого алфавита относятся к XI в. до н. э.

Главной особенностью письменной информации является необходимость закреплять её на материальном носителе. На протяжении всей истории развития цивилизации человек искал наиболее оптимальные носители информации. Камень был первичным носителем информации почти во всех странах древности: в древнем Египте, Индии, Греции, Китае, Италии, на нем древние германцы высекали руны, а архивные служители раннего средневековья с помощью камня сохраняли свои записи от пожаров. Кости и панцири черепах использовались в

Египте, Месопотамии, Греции, Китае. Такие металлы, как железо золото, серебро, латунь, бронза были распространены для передачи информации по всему миру в качестве материала для различных предметов: монеты, посуда, музыкальные инструменты, оружие и т. п. Аналогично можно сказать и про глину, хотя классическая страна письма на глине — древняя Месопотамия. Дерево использовали для письма в древнем Египте и Месопотамии, Греции и Италии, особое значение имел бамбук в Китае. Кроме самой древесины широко использовалась и кора деревьев, особенно кора березы — береста, в Индии и древней Руси. В Непале, Малайзии и Индии традиционный материал для письма являлись пальмовые листья.

Мягкими носителями письма также были — различные ткани, папирус, кожа, пергамен и бумага. На тканях писали в древнем Египте, особенно на тканях, в которые заворачивали мумий, в Китае — не шелке, в Риме были широко известны «полотняные книги». Папирус был классическим материалом для фиксации информации в древнем Египте, кожа — в Персии, в Центральной Азии до изобретения бумаги, в Северной Америке, а также у евреев. Пергамен был дорогим материалом, использовавшимся в средние века в Германии и Франции. Бумага появилась в 105 году в Китае и получила широкое распространение по всему миру и по сей день.

В аграрный период одновременно с письмом стало развиваться ещё одно направление — почта. Также развитие почты связано с развитием дорог. Информацию необходимо было либо передать, либо хорошо спрятать, и величие стран напрямую зависело от того, как правители справлялись с этими задачами. Сначала по всему миру была распространена эстафетная почта, но это была сугубо государственная почта, которая не имела отношения к простым гражданам. Первая регулярная почтовая служба возникла в Ассирии. Персы организовали службу конных посыльных и установили на дороге из Суз в Сарды 11 почтовых станций (ок. 430–355 г. до н. э). Большое значение на развитие почты Китая и всего мира оказал Великий Шелковый путь. В распоряжении таньских императоров находилось 1297 почтовых станций на суше и 360 — на реках (618–907 гг. н. э). Однако лишь в Риме возникла подлинная государственная почтовая служба, что в значительной

степени объяснялось созданием знаменитой дорожной сети и необходимостью эффективно управлять государством с огромной территорией. Почта использовала как верховых гонцов, так и пеших, частные граждане использовали в качестве гонцов собственных рабов. При переходе к средним векам почта в основном исчезла, что объясняется плохим состоянием дорог, так как даже древние римские дороги не поддерживались в должном виде, а также небезопасным передвижением по дорогам.

Однако нельзя не сказать о нескольких видах почтовой связи, действовавших в Средние века. Так в Европе XI–XV веков, при раздробленности государственной власти, пересылку известий принимали на себя главным образом отдельные духовные и светские корпорации, которым было важно обмениваться новостями между собой. Это были, так называемые, монастырская почта и университетская почта. Монастырские курьеры поддерживали связь между отдельными монастырями и главной церковью Рима, между монашескими орденами и орденами их братствами. При университетах, куда учащиеся стекались из самых различных стран, также образовались корпорации профессиональных гонцов, пользовавшиеся разными привилегиями. В XII–XIII веке славились гонцы университетов в Болонье, Салерно, Неаполе, Монпелье, Тулузе, позднее — гонцы парижского университета Сорбонны.

Дальнейшее развитие общества, прежде всего торговли и ремёсел привело к появлению многочисленных и разнообразных служб посыльных и почт городов, обслуживавших купцов и ремесленников. Купеческая почта была заведена при крупных торговых домах, которые содержали собственных курьеров. В то же время единой государственной почты всё ещё не было. С развитием городских вольностей одним из важнейших средств сообщения в Средние века явился институт городских гонцов, который с XIV века существовал почти повсеместно, но особое развитие получил в крупных торговых центрах Германии и Италии.

Современная централизованная почта зародились с усилением государственной власти. Во Франции Людовик XI эдиктом 19 июня 1464 года учредил королевских курьеров. По всем его владения была раскинута сеть станций для перемены ло-

шадей; во главе все организации стоял grand maitre. Эта почта предназначалась исключительно для надобностей правительства; королевским курьерам под страхами смертной казни воспрещено было исполнять поручения частных лиц.

В России первое сообщение о системе почтовой связи на Руси относится к началу XVI века. Однако в начале VII века по всей стране уже существовала система ямов и Великий князь (царь Василий Шуйский) каждые восемь дней получал известия о том, что творится на границе и в других местах страны. Этот факт говорит нам о сложившейся почтовой системе в государстве.

Революционным событием в развитии человечества стало изобретение книгопечатания в 1450 году немцем Иоганном Гуттенбергом. Появилась возможность не только сохранять информацию, но и сделать ее массово-доступной. Грамотность становится массовым явлением. Все это ускорило рост науки и техники, помогло промышленной революции. Книги перешагнули границы стран, что способствовало началу создания общечеловеческой цивилизации.

Индустриальный период

Индустриальный период развития человечества охватывает период с 1776 г. по 1890 г. Его начало ознаменовало изобретение Дж. Уаттом парового двигателя. Индустриальный период — это промышленная революция, фабричная система, разделение труда, массовое производство, электричество. Все эти явления изменили социальную структуру общества, темп жизни людей, их взгляд на общество и самих себя. В это время появляются такие изобретения, как телеграф и телефон, которые становятся новыми и качественно другими средствами передачи информации. Они позволили передавать сведения почти мгновенно, на огромные расстояния и с небольшими затратами.

Первый электромагнитный телеграф создал российский ученый П. Л. Шиллинг в 1832 году, а также разработал оригинальный код, в котором каждой букве алфавита соответствовала определенная комбинация символов, которая могла проявляться черными и белыми кружками на телеграфном аппарате. Впоследствии электромагнитный телеграф был

построен в Германии — Карлом Гауссом и Вильгельмом Вебером (1833), в Великобритании — Куком и Уитоном (1837), а в США электромагнитный телеграф запатентован С. Морзе в 1837 году. Большой заслугой С.Морзе является изобретение телеграфного кода, где буквы алфавита были представлены комбинацией коротких и длинных сигналов — «точек» и «тире» (код Морзе).

Коммерческая эксплуатация электрического телеграфа впервые была начата в Лондоне в 1837 году. В России работы П. Л. Шиллинга, продолжил Б. С. Якоби, построивший в 1839 году пишущий телеграфный аппарат, а позднее, в 1850 году, — буквопечатающий телеграфный аппарат.

Кроме того, в 1843 году шотландский физик Александр Бэйн продемонстрировал и запатентовал собственную конструкцию электрического телеграфа, которая позволяла передавать изображения по проводам. Аппарат Бэйна считается первой примитивной факс-машиной.

В 1858 г. была установлена трансатлантическая телеграфная связь. Затем был проложен кабель в Африку, что позволило в 1870 году установить прямую телеграфную связь Лондон — Бомбей (через релейную станцию в Египте и на Мальте).

Телефон, наверное, основное средство связи начала XX века, родился значительно позже своего предшественника телеграфа. В 1861 году немецкий ученый Филипп Райс изобрел аппарат, который, как он сам объяснял, «наглядно демонстрировал принцип действия человеческого уха и переносил с помощью гальванического тока любые тона на любые расстояния». Прошло 15 лет и преподаватель школы для глухонемых Александр Грехем Белл на всемирной выставке в Филадельфии продемонстрировал первый электрический телефонный аппарат. Первым его можно назвать только условно, так как изобретатель Элиш Грей опоздал на два часа с заявкой на аналогичное изобретение.

Усовершенствованный Томасом Эдисоном аппарат стал бытовым средством связи в отличии от общественного телефона. Простота в обращении и быстрота развертывания сделало полевой телефон незаменимым для военных. В 1878 году открывается первая телефонная станция.

Таким образом, индустриальный период дал миру два новых важных средства передачи связи — телефон и телеграф.

Информационно-телекоммуникационный период

Информационно-телекоммуникационный период начался примерно в 1890-е годы, когда 7 мая 1895 г. А. С. Поповым было представлено его новое изобретение — радио.

Если в век промышленности определяющей теорией эпохи была формула Эйнштейна $E=mc^2$, то в век информации определяющей теорией эпохи стал закон Мура, который гласит, что информация устаревает каждые полтора года.

Можно выделить следующие признаки информационного общества:

— осознание обществом приоритетности информации перед другим продуктом деятельности человека;

— первоосновой всех направлений деятельности человека (экономической, производственной, политической, образовательной, научной, творческой, культурной и т. п.) является информация;

— информация является продуктом деятельности современного человека;

— информация в чистом виде (сама по себе) является предметом купли-продажи.

— равные возможности в доступе к информации всех слоев населения;

— безопасность информационного общества, информации;

— защита интеллектуальной собственности;

— взаимодействие всех структур государства и государств между собой на основе информационно-телекоммуникационных технологий (ИТКТ);

— управление информационным обществом со стороны государства, общественных организаций.

Итак, все эти признаки являются результатов развития средств передачи информации. Это не удивительно, потому что чуть больше чем за 100 лет человечество создало больше средств передачи информации, в том числе и массовых, чем за все свое существование. Это и радио, и телевидение, и сотовая связь, и интернет, и спутниковая связь, и др.

Как уже было сказано, радио было изобретено в 1895 г. На заседании физического отделения Русского физико-химического общества (РФХО) выступил преподаватель Минного офицерского класса Александр Степанович Попов с докладом «Об отношении металлических порошков к электрическим колебаниям.» Во время доклада А. С. Попов демонстрировал работу созданного им устройства, предназначенного для приема и регистрации электромагнитных волн. Это был первый в мире радиоприемник.

Современное электронное телевидение зародилось в Санкт-Петербурге в проекте преподавателя Технологического института Б. Л. Розинга. В 1907 г. он оформил патентные заявки в России, Германии и Англии на изобретение телевизионного устройства с электронно-лучевой трубкой (прототипом кинескопа), а 9 мая 1911 года продемонстрировал изображение на экране кинескопа.

Уже в 1928–1930 гг. в США и в ряде европейских стран началось ТВ вещание с помощь не электронных, а механических систем, позволяющих передавать лишь электромагнитные изображения. В начале 30-х годов на зарубежных выставках, а затем и в магазинах стали появляться телевизоры на кинескопах. Однако чёткость изображения оставалась низкой, так как на передающей стороне по-прежнему использовались механические развёртывающие устройства. Первым практически решил эту задачу В. К. Зворыкин, работавший в Американской радо корпорации (RCA). Ему удалось создать, кроме кинескопа, передающую трубку с накопителем зарядов, которую он навал иконоскопом (по-гречески «наблюдать изображение»).

Передача движущегося изображения при помощи электронно-лучевой трубки впервые в истории осуществлена 26 июля 1928 года в Ташкенте изобретателями Б. Грабовским и И. Белянским. Первый в истории телевизионный приемник назывался «телефотом».

Первая телевизионная станция WCFL вышла в эфир в Чикаго 12 июня 1928 года. А первые регулярные передачи черно-белого телевидения были начаты в Германии в 1934 году, которые велись без звука с 1929 года.

Еще одним важным элементом в развитии передатчиков информации создание спутниковой связи. 4 октября 1957 года в СССР был запущен первый в мире искусственный спутник земли. Ракета-носитель доставила спутник на заданную орбиту, наивысшая точка которого находилась на высоте около 10000 км. На нем были установлены 4 антенны и 2 радиопередатчика с источниками питания. Искусственные спутники Земли могут быть использованы в качестве: ретрансляционной станции для телевидения значительно расширяющей дальность действия передачи; радионавигационного маяка, для спутникового Интернет.

Сотовые системы были созданы для предоставления услуг беспроводной радиотелефонии связи в интересах большого числа абонентов (десять и более тысячи на территории одного города), они позволяют очень эффективно использовать частотный ресурс. Основными из стандартов сотовой связи являются — NMT и GSM — расшифровывают как Global System for Mobile Communications, а стандарт GSM и его версии приняты к использованию приблизительно в 80 странах мира. В России первая система сотовой связи появились только в 1991 годы.

Пейджинговые системы предназначены для обеспечения односторонней связи с абонентами путем передачи коротких сообщений в цифровой или алфавитно-цифровой форме.

Оптоволоконные линии связи. Глобальная информационная инфраструктура строится уже давно. Ее основной являются оптоволоконные кабельные линии, завоевавшие главенствующие позиции на мировых сетях связи, за истекшие четверть века. Такие магистрали уже опутали большую часть Земли, они проходят и по территории России, и по территории бывшего Советского Союза. Волоконно-оптические линии связи с высокой пропускной способностью, обеспечивают передачу сигналов всех видов (аналоговых и цифровых).

Internet — это общемировая совокупность сетей, связывающая между собой миллионы компьютеров. Зародышем была распределённая сеть ARPAnet, которая была создана в конце 60-х годов по заказу Министерства обороны США для связи между собой компьютеров этого министерства. Организации стали создавать собственные сети на тех принципах. Эти сети

стали объединяться между собой, образуя единую сеть с общим адресным пространством. Эта сеть и стала называться Internet. Internet дает возможность пользоваться такими средствами связи, как электронная почта (e-mail), IP-телефония и пр.

Бумага

В начале VII века способ изготовления бумаги становится известным в Корее и Японии. А еще через 150 лет, через военнопленных попадает к арабам. В VII веках производство бумаги осуществлялось в Средней Азии, Корее, Японии и других странах Азии. В VI–VIII веках бумага появилась в Европе, где вскоре заменила животный пергамент.

Звукозапись

С XVIII века начинается звукозапись. Революцией в деле хранения и передачи информации стало появление музыкальных шкатулок. До сих пор все носители информации были рассчитаны на единственное считывающее устройство — человеческий глаз. В шкатулке же мелодия записывалась не потоками знаков, а выступами вращающегося валика. Считывал ее специальный механизм. Для предварительной записи мелодии использовался металлический диск, на который нанесена глубокая спиральная канавка. В определенных местах канавки делаются точечные углубления — ямки, расположение которых соответствует мелодии. При вращении диска, приводимого в движение часовым пружинным механизмом, специальная металлическая игла скользит по канавке и «считывает» последовательность нанесенных точек. Игла скреплена с мембраной, которая при каждом попадании иглы в канавку издает звук.

В конце XIX века появляются фонограф и патефон. Механические музыкальные инструменты со сменяемыми валиками пользовались большим спросом до 30-х годов XX века. Но уже в 1877 году Томас Эдисон изобрел фонограф — прибор, записывающий звук на валики из олова или воска. А в 1887 году Эмиль Берлинер открыл способ массового тиражирования граммофонных пластинок.

Изобретения стало поразительным событием того времени; дальнейшим развитием фонографа стали граммофон и

патефон. Импульсом для создания Эдисоном подобного устройства стало желание зарегистрировать телефонные разговоры в своей лаборатории Менло Парк (Нью-Джерси, США).

С начала нашей эры по начало двадцатого века произошел большой рывок в эволюции материальных носителей информации — до XVIII века носители были в основном рассчитаны на зрительную передачу информации. С XVIII века теперь записанную информацию стало возможно воспринимать и на слух, не говоря уже о создании бумаги.

Магнитофон

В начале XX века продолжает совершенствоваться техника звукозаписи — появляется магнитофон. Его пластинки действовали подобно валикам шкатулок. Борозды направляли движение иглы и механически воздействовали на мембрану патефона. Но уже в 1900 году публике был впервые представлен магнитофон, в котором звук записывался путем намагничивания участков проволоки.

Перфокарты

С середины двадцатого века появляются перфокарты. Данные загружались при помощи перфокарт — картонных карточек с проделанными в них отверстиями. Информация записывалась и считывалась согласно определенным схемам, но в основе лежал двоичный код: наличие отверстия — 1, отсутствие — 0. Следующим на арену вышел жесткий диск. Случилось это в 1956 году, когда IBM начала продажи первой дисковой системы хранения данных — 305 RAMAC.

Эпоха магнитных лент

Немецкий инженер Фриц Пфлюмер создал магнитную пленку. Новый носитель состоял из тонкого слоя бумаги, покрытого порошком на основе оксида железа. Пфлюмер продал технологию компании AEG, которая разработала первое в мире записывающее и воспроизводящее устройство — Magnetophon. Изобретение тщательно скрывали до капитуляции Германии. Лишь в начале 1950-х магнитная пленка вырвалась за пределы страны. Инновацию подхватили звукозаписывающие и

телевизионные компании, которые стали использовать пленку для записи аудио и видео.

В мир компьютеров технология пришла в 1951 году, когда Eckert-Mauchly выпустила систему UNIVAC I. Первым делом компьютер попал в то самое бюро, с которого началась история IBM, — в бюро по переписи населения. Магнитная пленка, использовавшаяся в UNIVAC, хранила куда больше информации в сравнении с бумажными перфокартами (10 000 перфокарт = 1 бобине с пленкой). IBM не осталась в стороне и переключилась на новый тип носителя. Чтобы перевести данные с накопившихся перфокарт, Eckert-Mauchly и IBM представили автоматические преобразователи.

Со временем бобины с пленкой обернули в пластиковые коробки, именно в таком виде «кассеты» дошли до наших дней. Пленка стала стандартом де-факто для записи данных, видео и музыки.

Настал 1967 год; руководство IBM поручило одному из инженеров разработать быстрый и компактный носитель, чтобы рассылать клиентам обновления софта. Команда Дэвида Ноубла разработала гибкий 8-дюймовый (20 см) диск объемом 80 Кб с возможностью одноразовой записи. Изделие было хрупким и притягивало много пыли. Доработанную версию упаковали в ткань, запечатали в пластик и назвали FD23. Разработка получила название «флоппи» или «дискета» (пластиковая упаковка была тонкая и гибкая, носитель как бы «хлопал крыльями», когда его несли в руках или трясли им в воздухе — отсюда и название *floppy*, от английского слова *flop* — хлопать). Дисководами для чтения дискет начали оборудовать компьютеры, но путь к успеху оказался непростым. Дисковод стоил наравне с самим компьютером, многие продолжали использовать пленочные кассеты.

Флэш-память

Первый вариант флеш-памяти (Flash Erase EEPROM) был разработан в 1984 году компанией Toshiba. Четырьмя годами позже подобное решение информационного носителя было представлено и компанией Intel. Накопители на основе флеш-памяти называют твердотельными, т. к. они не имеют движущихся частей. Это повысило надежность флеш-памяти по сравнению с другими носителями.

Первыми флеш-накопителями были карты ATA Flash. Они изготавливались в виде PC Card со встроенным ATA контроллером. Потом начали выходить все новые и новые стандарты флеш-карт. Такие, как Compact Flash TypeII (CF II) — выпущены в 1994 году компанией SanDisk, представляют собой модификацию PC Card.

В 2001 году появляется USB-flash, эта карта состоит из защитного колпачка и собственно накопителя с USB-разъемом (внутри него размещаются одна или две микросхемы флеш-памяти и USB-контроллер), которые снабжены средствами защиты от незаконного копирования.

Технологии не стоят на месте. В сфере оптических накопителей большие перспективы ожидают диски AO-DVD (Articulated Optical Digital Versatile Disc), работа над которыми кипит в недрах компании Iomega.

В основе разработки лежит идея использования наноструктур — участков диска с размерами меньшими, чем длина волны лазерного излучения. При этом сами участки могут располагаться под разными углами наклона.

1.2. Состояние проблемы

Проблема информационной безопасности во все времена являлась актуальной несмотря на то, что решалась различными методами и способами, и в других масштабах. В настоящее время вопросы информационной безопасности приобрели огромное значение, как для граждан, общества, так и для государства.

Перемещение больших массивов информации через границы государств стало сложившейся реальностью. Имеющиеся в глобальной информационной сети базы данных, к сожалению, не защищены полностью от негативных воздействий.

Развитие теории информационной безопасности в настоящее время связано с учетом новых обстоятельств, характерных для современного периода развития информатизации общества.

Во-первых, так как все большую актуальность приобретает не только защита информации, но и защита людей и технических (главным образом, электронных) систем от разрушающего воздействия информации, то формируется задача

обеспечения информационной безопасности как органической совокупности задач защиты информации и защиты от информации.

Во-вторых, с самого начала регулярного использования автоматизированных технологий обработки информации актуальность задачи обеспечения требуемого качества информации возрастает, а сама задача усложняется. Следовательно, обеспечение информационной безопасности невозможно без учета задач обеспечения качества информации.

В-третьих, решение задач защиты информации, задач защиты от информации и обеспечения качества информации обуславливает эффективность деятельности объектов. В свою очередь, учет задач управления информацией необходим при формировании, поддержке и использовании концепции информационного обеспечения деятельности объектов.

В-четвертых, серьезное внимание на новом этапе развития теории защиты информации должно быть уделено совершенствованию научно-методического базиса и инструментальных средств, обеспечивающих решение любых возникающих задач на регулярной основе в органической связи с решением проблем информационной безопасности, информационных технологий, информатизации общества.

Таким образом, вышеизложенное позволяет выделить следующие наиболее острые проблемы развития теории и практики информационной безопасности, а именно:

1. Создание теоретических основ и формирование научно-методического базиса, позволяющих адекватно описывать процессы в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов (информационные угрозы).

2. Разработка научно-обоснованных нормативно-методических документов по обеспечению информационной безопасности на базе исследования и классификации угроз информации и выработки стандартов требований к защите.

3. Стандартизация подходов к созданию систем защиты информации и рационализации схем и структур управления защитой на объектовом, региональном и государственном уровне.

Контрольные вопросы

1. Перечислите способы передачи информации в различные периоды развития общества.

2. Назовите основные способы записи информации и устройства ее хранения.

3. Назовите различные методы передачи информации.

4. Чем характерен современный период развития информационного общества?

Глава 2
Основы информационной безопасности

2.1. Сущностные основы теории информационной безопасности

2.1.1. Информация и ее природа

Термин «информация» в настоящее время часто употребляется и широко распространено. Трудно найти такую область знаний, где бы он не применялся. Огромные информационные потоки буквально захлестнули людей. Объем научных знаний, по оценке специалистов, удваивается каждые пять лет.

До начала индустриального общества, определение сути информации оставалось прерогативой философов. В XX веке вопросами теории информации стали заниматься науки — кибернетика и информатика.

Понятие «информация» (*informatio* — разъяснение, осведомление изложение) является одним из основных, ключевых понятий в науке, в социуме.

Согласно традиционной философской точке зрения, информация существует независимо от человека и является свойством материи. Она рассматривается как отражение объектов материального мира, в частности, отражение организованности или упорядоченности кибернетических объектов.

Согласно нетрадиционной точке зрения информация трактуется как неравенство микро и макромира вселенной (информация — первична, а материя — вторична). Информация существует независимо от нас и проявляется в триедином процессе фундаментального взаимодействия: энергии, движения и массы в пространстве и во времени.

Сформулированные к настоящему времени строгие научные определения концентрируют внимание на одном из основных аспектов этого многозначного понятия — соотношения информации и материи.

Природа информации определяется отражением объективных закономерностей материального мира. Отражение — воздействие одной материальной системы на другую, при котором устанавливается некоторое соответствие между одной

(отражаемой) и другой (отраженной) системами. Отражение определяет диалектическую связь между двумя объектами — источником и приемником информации.

Раскрытие природы информации через понятие разнообразия и ее трактовки, как отраженного разнообразия, представляется достаточным основанием для тезиса об объективности информации. Информация многолика, разнообразна, может существовать в различных видах, формах и категориях, способна многократно переходить из одной ее формы в другую, может теряться, восстанавливаться и разрушаться.

Информация является отдельной самостоятельной субстанцией и подчиняется своим специфическим законам и правилам. Любое взаимодействие между объектами (объект — нечто устойчивое во времени и ограниченное в пространстве), в процессе которого один приобретает некоторую субстанцию, а другой ее не теряет, называется информационным взаимодействием.

В науке и социуме понятие информации трактуется поразному:

— любая сущность, которая вызывает изменения в некоторой информационно — логической, состоящей из данных, знаний, абстракций и т.п., модели системы **(математика, системный анализ)**;

— сообщения, полученные системой из внешнего мира в процессе адиативного управления, приспособления **(теория управления, кибернетика)**;

— отрицание энтропии, отражение мира хаоса в системе **(термодинамика)**;

— связи, устраивающие неопределенность в системе **(теория информации)**;

— вероятность выбора в системе **(теория вероятностей)**;

— отражение разнообразия в системе **(физиология, биокибернетика)**;

— отражение материи, атрибут сознания, «интеллекта» системы **(философия).**

По определению Н. Винера информация — обозначение содержания, полученное нами из внешнего мира в процессе приспособления к нему нас и наших чувств.

Выше перечисленные трактовки информации приводят к выводу, что понятие «информация» — практически не формализуемое и не структурируемое понятие.

Считается, что информация — некоторая последовательность (упорядоченность) сведений, знаний, которые актуализируемы (получаемы, передаваемы, преобразуемы, снимаемы или регистрируемы) с помощью некоторых знаков (символьного, образного, жестового, звукового типа). Это приращение, развитие, актуализация знаний, возникающее в процессе целеполагающей интеллектуальной деятельности человека.

Никакая информация, никакое знание не появляются сразу — этому предшествуют этапы накопления, осмысления, систематизации опытных знаний. Знание — продукт такого процесса. Мышление — необходимый атрибут этого процесса.

Однако, возможно и внезапное «озарение» человека какой либо информацией.

Формы и классификация информации

Информация может существовать в пассивной (не актуализируемой) и активной (актуализируемой) форме.

Информацию, по отношению к окружающему миру можно представить как: входная, выходная и внутренняя информация.

Информацию можно классифицировать по следующим признакам:

— стадии использования (первичная, вторичная);

— полноте (избыточности, достаточности, недостаточности);

— отношению к цели системы (синтаксическая, семантическая, прагматическая);

— отношению к элементам системы (статическая, динамическая);

— отношению к структуре системы (структурная, относительная);

— отношению к управлению системой (управляющая, преобразующая, советующая, смешанная);

— отношению к территории распространения;

— доступности;

— характеру использования.

Возможны следующие свойства информации: полнота, актуальность, ясность, адекватность, достоверность, информативность, массовость, защищенность, доступность, ценность.

Информация может быть получена следующими методами: эмпирическим, теоретическим и эмпирико-теоретическим. Эмпирические методы — наблюдение, сравнение, измерение, эксперимент. Эмпирико-теоретические методы — абстрагирование, анализ, синтез, индукция, дедукция, эвристика, мониторинг. Теоретические методы — идеализация, формализация, аксиоматизация, виртуализация.

Информация разделяется на виды по следующим критериям:

1. По способу восприятия:

— визуальная, актуальная, тактильная, обонятельная, вкусовая.

2. По форме представления:

— текстовая, числовая, графическая, звуковая, когнитивная.

3. По назначению:

— массовая, личная, конфиденциальная, секретная.

4. По истинности:

— истинная, ложная.

Таким образом можно сделать следующий вывод о природе информации: информация связана с разнообразием, различием и с отражением, т. е. информация — это разнообразие, которое один объект содержит о другом объекте (в процессе их взаимодействия). Следовательно, информация выражает свойство материи, которое является всеобщим.

2.1.2. Общие понятия теории информационной безопасности

Любая область теории и практики базируется на строгом понятийном аппарате. Формирование более полного перечня терминов, их определение и интерпретация связана с тем, чтобы обеспечивалось однозначное понимание каждого из них, первостепенное значение имеет и для основ информационной безопасности.

Множество понятий и терминов информационной безопасности отражает широкий спектр отличительных существенных свойств, признаков и отношений, присущих данному

специфическому виду безопасности. Выделяют три группы терминов теории информационной безопасности. Рассмотрим перечень терминов, входящих в каждую группу.

Термины, определяющие предметную научную основу информационной безопасности.

К этой группе относятся термины, которые используются во многих областях знаний и являются однозначными, семантически унифицированными и стилистически нейтральными. Информация, коммуникация, конфликт, воздействие, угроза, опасность, безопасность, система.

Термины этой группы отвечают требованиям однозначности и устойчивости, т.е. эти термины однозначно употребляются в одной области знаний и сохраняют свой особый смысл в каждой другой области знаний, а также являются общепризнанными т.к. они употребляются в обиходе. Однако термину «информация» присуще специфическое свойство: в разных областях знаний, и даже в одной области знания он может характеризовать предмет, явление, процесс и их свойства, и отношения одновременно.

Термины, определяющие предметную основу информационной безопасности.

Ко второй группе относятся термины, обозначающие понятия и их соотношение с другими понятиями в пределах информационной безопасности как специальной сферы или области знаний. К таковым относятся: информатика, информатизация, информационная система, информационные технологии, информационные процессы, информационной объект, информационный ресурс, информационная инфраструктура, информационная сфера, информационный потенциал.

Термины, определяющие характер деятельности по обеспечению информационной безопасности.

К третьей группе относятся термины, служащие обозначениями характерных для этой сферы предметов, явлений, процессов, их свойств и отношений (в том числе сил, средств и методов их использования при решении задач обеспечения информационной безопасности). Термины этой группы обозначают широкий круг понятий различного уровня: от техни-

ческого канала утечки информации до информационного противоборства. К ним относятся: информационное противоборство, информационное превосходство, информационная безопасность, угрозы информационной безопасности, обеспечение информационной безопасности, система обеспечения информационной безопасности, информационная защищенность, безопасность информации, защита информации, объект защиты информации, носитель информации, доступ к информации, доступность информации, целостность информации, конфиденциальность информации, несанкционированный доступ к информации, утечка информации, канал утечки информации, канал передачи информации, воздействие на информацию, информационно-психологическое воздействие, информационно-психологическая сфера.

Важной специфической особенностью терминологической системы информационной безопасности является ее тесная связь с правовой лексикой. Это следствие того факта, что информационная безопасность давно перестала быть технической дисциплиной, частью информатики. В связи с этим выработка единообразия в терминологии по проблеме обеспечения информационной безопасности создает предпосылки для целенаправленного развития всех работ по теории информационной безопасности и методологии защиты информации.

Определение информационной безопасности в свете информационных проблем современного общества

Известно, что каждое явление, процесс, объект имеет внутреннее содержание и внешнее выражение. Только сочетание этих составляющих дает полное представление о предмете исследования и возможных направлениях использования его результатов.

Сложность освещения проблемы обеспечения информационной безопасности связана с отсутствием до настоящего времени общепринятого толкования терминов, используемых для описания данной предметной области. В связи с этим для определения понятия информационной безопасности необходимо рассмотреть базовое ключевое понятие «безопасность».

Безопасность как общенаучная категория может быть определена как некоторое состояние рассматриваемой системы,

при котором последняя, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой ее функционирование не создает угроз для элементов самой системы и внешней среды. При таком определении мерой безопасности системы являются:

• с точки зрения способности противостоять дестабилизирующему воздействию внешних и внутренних угроз — степень (уровень) сохранения системой своей структуры, технологии и эффективности функционирования при воздействии дестабилизирующих факторов;

• с точки зрения отсутствия угроз для элементов системы и внешней среды — степень (уровень) возможности (или отсутствия возможности) появления таких дестабилизирующих факторов, которые могут представлять угрозу элементам самой системы или внешней среде.

Интерпретация данных формулировок приводит к следующему определению информационной безопасности:

Информационная безопасность — такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой — ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

В Доктрине информационной безопасности Российской Федерации записано, что информационная безопасность — это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечивается реализация конституционных прав и свобод жизни граждан, суверенитет, территориальная целостность и устойчивость социально — экономического развития Российской Федерации, оборона и безопасность государства.

Ориентиром в направлении поиска путей решения проблем информационной безопасности может служить информация.

Информация как непременный компонент любой организованной системы, с одной стороны, легко уязвима (т. е. весьма доступна для дестабилизирующего воздействия большого числа разноплановых угроз), а с другой — сама может быть источником большого числа разноплановых угроз, как

для элементов самой системы, так и для внешней среды. Отсюда, обеспечение информационной безопасности в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении трех составляющих проблем:

– защите находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации;

– защите элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз;

– защите внешней среды от информационных угроз со стороны рассматриваемой системы.

В соответствии с изложенным общая схема обеспечения информационной безопасности может быть представлена на рисунке 1.

Таким образом, развитие теории информационной безопасности обусловливается основными направлениями развития защиты информации как первой составляющей общей проблемы информационной безопасности, с другой, — изучением и разработкой второй составляющей информационной безопасности — защиты от информации.

Вкратце акцентируем внимание на сложность решения второй составляющей проблемы информационной безопасности.

Необходимо отметить, что проблема защиты от информации существенно сложнее проблемы защиты информации в силу многообразности информационных угроз, воздействие которых не всегда очевидно. Предотвращение и нейтрализация таковых требуют как технических решений, так и организационно-правовых и политических на внутригосударственном, межгосударственном и международном уровнях.

В свою очередь, отличительной особенностью проблемы защиты людей от информации, состоит в том, что ее решение будет носить преимущественно гуманитарный характер, в то время как решения по защите от информации технических средств и систем, так же как и по защите информации, носят технический характер и поддаются строгой структуризации.

Рис. 1. Общая схема обеспечения информационной безопасности

Основные составляющие информационной безопасности

Информационная безопасность многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

С методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов.

В обеспечении информационной безопасности нуждаются столь разные субъекты информационных отношений, таких как:

- государство в целом или отдельные органы и организации;
- общественные или коммерческие организации (объединения), предприятия (юридические лица);
- отдельные граждане (физические лица).

Весь спектр интересов субъектов, связанных с использованием информации, можно разделить на следующие категории: обеспечение доступности, целостности и конфиден-

циальности ресурсов информационной среды и поддерживающей инфраструктуры.

Иногда в число основных составляющих ИБ включают защиту от несанкционированного копирования информации, но, как нам видится, это слишком специфический аспект с сомнительными шансами на успех, поэтому мы не станем его выделять.

Поясним понятия доступности, целостности и конфиденциальности.

Доступность — это возможность за приемлемое время получить требуемую информационную услугу.

Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность — это защита от несанкционированного доступа к информации.

В качестве основных информационных ресурсов в дальнейшем будем рассматривать информационные системы и средства коммуникации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, принято выделять ее как важнейший элемент информационной безопасности.

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий). Средства контроля динамической целостности применяются в частности при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Конфиденциальность — самый проработанный аспект информационной безопасности. Но практическая реализация мер по обеспечению конфиденциальности современных информационных систем имеет в России серьезные трудности. Во-первых, сведения о технических каналах утечки информации

являются закрытыми. Большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные и технические проблемы.

2.1.3. Системы обеспечения информационной безопасности

Информационная сфера современного мира настолько глобальна, что ее аспекты отражаются в любой деятельности людей: будь то социальная, техническая или политическая сферы.

Актуальность проблемы в современных условиях определяется следующими основными факторами:

— обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование;

— расширением сферы использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, высокими темпами увеличения парка средств вычислительной техники и связи;

— повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности;

— вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса;

— концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях;

— количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;

— отношением к информации, как к товару, переходом к рыночным отношениям в области предоставления информа-

ционных услуг с присущей им конкуренцией и промышленным шпионажем;

— многообразием видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации;

— ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими нежелательных программно-математических воздействий на системы обработки информации;

— увеличением потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (возрастанием уязвимости различных затрагиваемых субъектов);

— развитием рыночных отношений (в области разработки, поставки, обслуживания вычислительной техникой, разработки программных средств, в том числе средств защиты).

Изменился подход и к самому понятию «информация». Этот термин все чаще используется для обозначения особого товара, стоимость которого зачастую превосходит стоимость вычислительной системы, в рамках которой он существует. Осуществляется переход к рыночным отношениям в области создания и предоставления информационных услуг.

Прежде всего, необходимо разобраться, что такое безопасность информационных технологий, определить *что (кого), от чего (от кого), почему (зачем) и как (в какой степени и какими средствами) надо защищать.* Только получив четкие ответы на данные вопросы, можно правильно сформулировать общие требования к системе обеспечения информационной безопасности и переходить к обсуждению вопросов построения соответствующих систем зашиты.

Определимся, что субъект это:

— *государство* (в целом или отдельные его органы и организации);

— общественные или коммерческие организации (объединения) и предприятия *(юридических лиц);*

— отдельные граждане *(физические лица).*

В процессе своей деятельности субъекты могут находиться друг с другом в разного рода отношениях, в том числе, касающихся вопросов получения, хранения, обработки, распространения и использования определенной информации. Такие

отношения между субъектами будем называть *информационными отношениями,* а самих участвующих в них субъектов — *субъектами информационных отношений.*

Для обеспечения законных прав необходимо постоянно поддерживать следующие свойства информации и систем ее обработки:

— *доступность информации* — такое свойство системы (инфраструктуры, средств и технологии обработки, в которой циркулирует информация), которое характеризует ее способность обеспечивать своевременный доступ субъектов к интересующей их информации и соответствующим автоматизированным службам (готовность к обслуживанию поступающих от субъектов) запросов всегда, когда в обращении к ним возникает необходимость;

— *целостность информации* — такое свойство информации, которое заключается в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);

— *конфиденциальность информации* — характеристика (свойство) информации, которая указывает на необходимость введения ограничений на ряд субъектов, имеющих доступ к данной информации, и обеспечиваемую способностью системы (инфраструктуры) сохранять указанную информацию в тайне от субъектов, не имеющих прав на доступ к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

Отсюда следует, что в качестве *объектов, подлежащих защите* в целях обеспечения безопасности субъектов информационных отношений, должны рассматриваться: информация, любые ее носители (отдельные компоненты АС и АС в целом) и процессы обработки (передачи).

Следовательно, термин *«безопасность информации»* нужно понимать как *защищенность* информации от нежелательного для соответствующих субъектов информационных отношений ее разглашения (нарушения конфиденциальности), искажения или утраты (нарушения целостности, фальсификации) или снижения степени доступности информации, а

также незаконного ее тиражирования (неправомерного использования).

Безопасность любого компонента (ресурса) АС складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность компонента (ресурса) АС заключается в том, что он доступен только тем субъектам (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента (ресурса) АС предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

Доступность компонента (ресурса) АС означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.

Структура и основные функции государственной системы защиты информации от ее утечки по техническим каналам и организация работ по защите информации определены в *«Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам»,* утвержденном Постановлением Правительства от 15 сентября 1993 г. № 912-51.

Этим Положением предусматривается, что мероприятия по защите информации, обрабатываемой техническими средствами, являются составной частью управленческой, научной и производственной деятельности учреждений и предприятий и осуществляются во взаимосвязи с другими мерами по обеспечению установленного федеральными законами *«Об информации, информационных технологиях и защите информации»* и *«О государственной тайне»* комплекса мер по защите сведений, составляющих государственную и иные виды тайн.

Основными задачами государственной системы защиты информации являются:

— проведение единой технической политики, организация и координация работ по защите информации в оборонной,

экономической, политической, научно-технической и других сферах деятельности;

— исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных специальных программно-технических воздействий на информацию с целью ее разрушения, уничтожения, искажения или блокирования в процессе обработки, передачи и хранения;

— принятие в пределах компетенции нормативно-правовых актов, регулирующих отношения в области защиты информации;

— общая организация сил, создание средств защиты информации и средств контроля эффективности ее защиты;

— контроль за проведением работ по защите информации в органах государственного управления, объединениях, на предприятиях, в организациях и учреждениях (независимо от форм собственности).

Необходимой составляющей государственной системы обеспечения информационной безопасности являются Государственные стандарты и другие нормативно-технические и методические документы по безопасности информации, утвержденные федеральными органами государственного управления в соответствии с их компетенцией, и определяющие нормы защищенности информации и требования в различных направлениях защиты информации.

Угрозы безопасности информации, АС и субъектов информационных отношений

Под *угрозой* (вообще) обычно понимают потенциально возможное событие, процесс или явление, которое может (воздействуя на что-либо) привести к нанесению ущерба чьим-либо интересам.

Угрозой интересам субъектов информационных отношений будем называть потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

Нарушением безопасности (просто нарушением или атакой) будем называть реализацию угрозы безопасности.

По способам осуществления противодействия угрозам безопасности все меры защиты информации, ее носителей и систем ее обработки подразделяются на:

– правовые (законодательные);

– морально-этические;

– технологические;

– организационные (административные и процедурные);

– физические;

– технические (аппаратурные и программные).

Правовые (законодательные)

К правовым мерам защиты относятся действующие в стране законы, указы и другие нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

Морально-этические

К морально-этическим мерам защиты относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как требования нормативных актов, однако, их несоблюдение ведет обычно к падению авторитета или престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т. п.), так и писаные, то есть оформленные в некоторый свод (устав, кодекс чести и т. п.) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах пользователей и обслуживающего персонала АС.

Технологические

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные обычно на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т. п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии разрешений от нескольких должностных лиц, процедур проверки соответствия реквизитов исходящих и входящих сообщений в системах коммутации сообщений.

Организационные

Организационные меры зашиты — это меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Меры физической защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. К данному типу относятся также меры и средства контроля физической целостности компонентов АС (пломбы, наклейки и т.п.).

Меры технической защиты

Технические меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

Основной задачей системы защиты является обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов (ресурсов) АС соответствующими множеству значимых угроз, методами и средствами.

Обеспечение информационной безопасности — это непрерывный процесс, основное содержание которого составляет управление — управление людьми, рисками, ресурсами, средствами защиты и т.п. Люди — обслуживающий персонал и конечные пользователи АС являются неотъемлемой частью автоматизированной (то есть *«человеко-машинной»)* системы. От того, каким образом они реализуют свои функции в системе, существенно зависит не только ее функциональность (эффективность решения задач), но и ее безопасность.

Для того, чтобы обеспечить безопасность информационных систем, нужно знать, кто является субъектами, влияющими на состояние информационной безопасности:

— *сотрудники структурных подразделений* (конечных пользователей АС), решающие свои функциональные задачи с применением средств автоматизации;

— *программисты,* осуществляющие разработку (приобретение и адаптацию) необходимых прикладных программ (задач) для автоматизации деятельности сотрудников организации;

— *сотрудники подразделения внедрения и сопровождения ПО,* обеспечивающие нормальное функционирование и установленный порядок инсталляции и модификации прикладных программ (задач);

— *сотрудники подразделения эксплуатации ТС,* обеспечивающие нормальную работу и обслуживание технических средств обработки и передачи информации и системного программного обеспечения;

— *системные администраторы* штатных средств защиты (ОС, СУБД и т. п.);

— *сотрудники подразделения защиты информации,* оценивающие состояние информационной безопасности, определяющих требования к системе защиты, разрабатывающие организационно-распорядительные документы по вопросам ОИБ (аналитиков), внедряющие и администрирующие специализированные дополнительные средства защиты (администраторов безопасности);

— *руководители организации,* определяющие цели и задачи функционирования АС, направления ее развития, принимающие стратегические решения по вопросам безопасности и утверждающих основные документы, регламентирующие порядок безопасной обработки и использования защищаемой информации сотрудниками организации.

Кроме того, на информационную безопасность организации могут оказывать влияние *посторонние лица* и сторонние организации, предпринимающие попытки вмешательства в процесс нормального функционирования АС или несанкционированного доступа к информации как локально, так и удаленно.

Таким образом, организационную структуру системы обеспечения информационной безопасности АС организации можно представить в виде, совокупности следующих уровней:

— уровень 1 — Руководство организации;

— уровень 2 — Подразделение ОИБ;

— уровень 3 — Администраторы штатных и дополнительных средств защиты;

— уровень 4 — Ответственные за ОИБ в подразделениях (на технологических участках);

— уровень 5 — Конечные пользователи и обслуживающий персонал.

Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты

Организационные меры являются той основой, которая объединяет различные меры защиты в единую систему. Они включают:

— разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;

— мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде (по необходимости);

— периодически проводимые (через определенное время) мероприятия;

— постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

К разовым мероприятиям относят:

— мероприятия по созданию нормативно-методологической базы (разработка концепции и других руководящих документов) защиты АС;

— мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АС (исключение возможности тайного проникновения в помещения, исключение возможности установки прослушивающей аппаратуры и т. п.);

— мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых технических и программных средств, документирование и т. п.);

— проведение спецпроверок применяемых в АС средств вычислительной техники и проведение мероприятий по защите информации от утечки по каналам побочных электромагнитных излучений и наводок;

— выявление наиболее вероятных угроз для данной АС, выявление уязвимых мест процессов обработки информации и каналов доступа к ней, оценка возможного ущерба, вызванного нарушением безопасности информации, разработку адекватных требований по основным направлениям защиты);

— организация охраны и надежного пропускного режима;

— определение порядка проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ на рабочих местах защищенной системы (кто обладает правом разрешения таких действий).

К периодически проводимым мероприятиям относят:

— распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);

— анализ системных журналов (журналов регистрации), принятие мер по обнаруженным нарушениям правил работы;

— пересмотр правил разграничения доступа пользователей к ресурсам АС организации;

— осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты и разработка

необходимых мер по совершенствованию (пересмотру состава и построения) системы защиты.

К мероприятиям, проводимым по необходимости, относят:

— мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;

— мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения (санкционирование, рассмотрение и утверждение изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т. п.);

— проверка поступающего оборудования, предназначенного для обработки закрытой информации, на наличие специально внедренных закладных устройств, инструментальный контроль технических средств на наличие побочных электромагнитные излучения и наводок;

— оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи;

— мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т. д.).

Постоянно проводимые мероприятия включают:

— мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АС (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности СВТ, носителей информации и т. п.);

— мероприятия по непрерывной поддержке функционирования и управления (администрирования) используемыми средствами защиты;

— организацию явного и скрытого контроля за работой пользователей и персонала системы;

— контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй, функционирования, обслуживания и ремонта АС;

— постоянно (силами службы безопасности) и периодически (с привлечением сторонних специалистов) осуществ-

ляемый анализ состояния и оценка эффективности мер и применяемых средств защиты.

На основе утвержденной системы организационно-распорядительных документов подразделения выполняют следующие основные действия:

— определяют критерии, по которым различные АРМ относятся к той или иной категории по требуемой степени защищенности, и оформляет их в виде «Положения об определении требований по защите (категорировании) ресурсов»;

— определяют типовые конфигурации и настройки программно-аппаратных средств защиты информации для АРМ различных категорий (требуемых степеней защищенности);

— по заявкам руководителей подразделений (используя формуляры АРМ и формуляры задач) проводят анализ возможности решения (а также совмещения) указанных задач на конкретных АРМ (с точки зрения обеспечения безопасности) и принимают решение об отнесении АРМ к той или иной группе по степени защищенности;

— совместно с отделом технического обслуживания Управления автоматизации проводят работы по установке на АРМ программно-аппаратных средств защиты информации;

— согласовывают и утверждают предписания на эксплуатацию АРМ (формуляры АРМ), подготовленные в подразделениях организации;

— обеспечивают проведение необходимых дополнительных специальных мероприятий по обеспечению безопасности информации;

— определяют организацию, методики и средства контроля эффективности противодействия попыткам несанкционированного доступа к информации (НСД) и незаконного вмешательства в процесс функционирования АС.

2.2.Типология информационной безопасности

2.2.1.Виды угроз

Под угрозами информационной безопасности понимается потенциальная возможность нарушения ее следующих основных, качественных характеристик (свойств):

– конфиденциальности (разглашение, утечка) сведений, составляющих государственную, служебную или коммерческую тайну, а также персональных данных;

– работоспособности (дезорганизация работы) программно-технических комплексов, блокирование информации, нарушение технологических процессов обработки информации, срыв своевременного решения выполняемых задач;

– целостности и достоверности информационных, программных и других ресурсов, а также фальсификации (подделка) документов.

Каждое государство защищает свои информационные ресурсы, которые можно представить в виде следующих групп:

– свободно распространяемую информацию;

– информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях, т. е. информацию с ограниченным доступом;

– информацию, которая в соответствии с федеральным законодательством подлежит представлению или распространению;

– информацию, представление которой в Российской Федерации ограничивается или запрещается.

В монографии Л. Дж. Хоффмана «Современные методы защиты информации» были выделены 5 групп различных угроз:

– хищение носителей;

– запоминание или копирование информации;

– несанкционированное подключение к аппаратуре;

– несанкционированный доступ к ресурсам ЭВМ;

– перехват побочных излучений и наводок.

В книге предпринята попытка классификации угроз по источнику возможной опасности:

– человек,

– аппаратура;

– программа.

К группе угроз, в реализации которых основную роль играет человек, отнесены: хищение носителей, чтение информации с экрана, чтение информации с распечаток.

К группе, где основным средством выступает аппаратура: подключение к устройствам, перехват излучений.

К группе, где основное средство программа — несанкционированный программный доступ, программное дешифрование зашифрованных данных, программное копирование информации с носителей.

Аналогичный подход предлагается и группой авторов учебных пособий по защите информации от несанкционированного доступа.

Ими выделено три класса угроз:

— природные (стихийные бедствия, магнитные бури, радиоактивное излучение и наводки);

— технические (отключение или колебания напряжения сети электропитания, отказы и сбои аппаратно-программных средств, электромагнитные излучения и наводки, утечки через каналы связи);

— созданные людьми, причем в последнем случае различают непреднамеренные и преднамеренные действия различных категорий лиц.

В руководящем документе Гостехкомиссии России «Концепция защиты средств вычислительной техники в АС от НСД к информации» введено понятие модели нарушителя в автоматизированной системе обработки данных. В качестве такового рассматривается субъект, имеющий доступ к работе со штатными средствами АС.

Согласно «Специальные требования и рекомендации по технической защите конфиденциальной информации» различают 4 уровня возможностей внутреннего нарушителя, которые увеличиваются от уровня к уровню.

Первый уровень — возможность запуска программ из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень — возможность создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень — возможность получения управления функционированием системы, а также воздействия на базовое программное обеспечение, состав и конфигурацию оборудования.

Четвертый уровень — определяется возможностью проектирования, установки и ремонта средств электронно-вычислительной техники, вплоть до включения в их состав

собственных технических и программных средств с новыми функциями по обработке информации.

Еще один вид источников угроз безопасности информации, связанный с ее хищением, достаточно подробно классифицирован в монографии С. П. Расторгуева «Программные методы защиты информации в компьютерах и сетях». Автор выделяет четыре способа хищения информации:

— по каналам побочных электромагнитных излучений;

— посредством негласного копирования, причем выделено две разновидности копирования: «ручное» вывод информации на печать или на экран оператором) и «вирусное» — вывод информации с помощью встроенной в ЭВМ радиозакладки;

— хищение носителей информации;

— хищение персональной ЭВМ.

В монографии В. А. Герасименко «Защита информации в автоматизированных системах обработки данных» предпринята попытка системной классификации угроз информации исходя из целей ее защиты.

Таким образом, можно провести следующую классификацию:

— по отношению источника угрозы к АС (внешние и внутренние угрозы);

— по виду источника угрозы (физические — отражают физические действия на систему; логические — средства, при помощи которых человек получает доступ к логической информации системы; коммуникационные — относятся к процессам передачи данных по линиям связи; человеческие — являются наиболее трудно контролируемыми и непосредственно связанными с физическими и логическими угрозами);

— по степени злого умысла (случайные и преднамеренные) и т. д.;

— по способам их воздействия.

Преднамеренные угрозы, в свою очередь, могут быть подразделены на активные (несанкционированная модификация данных или программ) и пассивные (несанкционированное копирование данных или программ).

Такая классификация (поддерживается подавляющим большинством специалистов) предусматривает подразделение

угроз на информационные, программно-математические, физические и организационные.

Информационные угрозы реализуются в виде:

— нарушения адресности и своевременности информационного обмена;

— противозаконного сбора и использования информации;

— осуществления несанкционированного доступа к информационным ресурсам и их противоправного использования;

— хищения информационных ресурсов из банков и баз данных;

— нарушения технологии обработки информации.

Программно-математические угрозы реализуются в виде:

— внедрения в аппаратные и программные изделия компонентов, реализующих функции, не описанные в документации на эти изделия;

— разработки и распространения программ, нарушающих нормальное функционирование информационных систем или их систем защиты информации.

Физические угрозы реализуются в виде:

— уничтожения, повреждения, радиоэлектронного подавления или разрушения средств и систем обработки информации, телекоммуникации и связи;

— уничтожения, повреждения, разрушения или хищения машинных и других носителей информации;

— хищения программных или аппаратных ключей и средств криптографической защиты информации;

— перехвата информации в технических каналах связи и телекоммуникационных системах;

— внедрения электронных устройств перехвата информации в технические средства связи и телекоммуникационные системы, а также в служебные помещения;

— перехвата, дешифрования и навязывания ложной информации в сетях передачи данных и линиях связи;

— воздействия на парольно-ключевые системы защиты средств обработки и передачи информации.

Организационные угрозы реализуются в виде:

— невыполнения требований законодательства в информационной сфере;

— противоправной закупки несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникации и связи.

Учитывая важность вопроса классификации угроз безопасности информации и существование в этой области большого числа различных подходов, необходимо провести системный анализ данной проблемы.

Из предыдущего изложения следует, что к настоящему времени известно большое количество разноплановых угроз безопасности информации различного происхождения. Различными авторами предлагается целый ряд подходов к их классификации. При этом в качестве критериев деления множества угроз на классы используются виды порождаемых опасностей, степень злого умысла, источники проявления угроз и т. д. Все многообразие предлагаемых классификаций с помощью подходов, предложенных В. А. Герасименко, на основе методов системного анализа может быть сведено к некоторой системной классификации, таблица 1.

Таблица 1. **Классификация угроз информации**

Параметры классификаций	**Значения параметров**	**Содержание значения параметров**
1. Виды угроз. Целевая направленность	1.1. Физическая целостность	Уничтожение
	1.2. Логическая структура	Искажение структуры
	1.3. Содержание	Несанкционированная модификация
	1.4. Конфиденциальность	Несанкционированное получение
	1.5. Право собственности	Присвоение чужого права
2. Природа происхождения	2.1. Случайности	Отказы, сбои, ошибки, стихийные бедствия, побочные влияния
	3.2. Преднамеренная	Злоумышленные действия людей
3. Предпосылки появления	3.1. Объективные	Количественная недостаточность элементов системы.

	3.2. Субъективные	Качественная недостаточность элементов системы Разведывательные органы иностранных государств, промышленный шпионаж, уголовные элементы, недобросовестные сотрудники, хакеры, фишеры, спамеры, операторы зомби-сетей, создатели шпионского, злонамеренного ПО, террористы
4. Источники угроз	4.1. Люди	Посторонние лица, пользователи, персонал
	4.2. Технические устройства	Технические устройства регистрации, передачи, хранения, переработки, выдачи
	4.3. Модели, алгоритмы, программы	Общего назначения, прикладные, вспомогательные
	4.4. Технологические схемы обработки	Ручные, интерактивные, внутри машинные, сетевые.
	4.5. Внешняя среда	Состояние атмосферы, побочные шумы, побочные сигналы

2.2.2. Средства защиты информации

Защита информации — комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостность, доступность и, если нужно, конфиденциальность информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных). «Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию».

Основными критериями оценки надежности защиты информации являются политика безопасности и гарантированность.

Политика безопасности, являясь активным компонентом защиты (включает в себя анализ возможных угроз и выбор соответствующих мер противодействия), отображает тот набор законов, правил и норм поведения, которым пользуется конкретная организация при обработке, защите и распространении информации.

Выбор конкретных механизмов обеспечения безопасности системы производится в соответствии с сформулированной политикой безопасности.

Гарантированность, являясь пассивным элементом защиты, отображает меру доверия, которое может быть оказано архитектуре и реализации системы (другими словами, показывает, насколько корректно выбраны механизмы, обеспечивающие безопасность системы).

В надежной системе должны регистрироваться все происходящие события, касающиеся безопасности (должен использоваться механизм подотчетности протоколирования, дополняющийся анализом заполненной информации, то есть аудитом).

1. Угрозы информации

Под угрозами информации**,** понимаются потенциальные или реально возможные действия по отношению к информационной сфере, приводящие к несанкционированным изменениям свойств информации (конфиденциальность, доступность, достоверность, целостность).

По конечному проявлению можно выделить следующие угрозы информации:

1. Ознакомление
2. Модификация
3. Уничтожение
4. Блокирование

Ознакомление. Ознакомление с конфиденциальной информацией может проходить различными путями и способами, при этом существенным, является отсутствие изменений самой информации.

Нарушение конфиденциальности или секретности информации связано с ознакомлением с ней тех лиц, для которых она не предназначалась. Какая информация является конфиденциальной или секретной решает собственник или владелец

этой информации. Они же определяют круг лиц, имеющих доступ к ней. Нарушение конфиденциальности информации может произойти путем *ознакомления* с ней лицами, не имеющими на то права и несанкционированной *модификации* грифа секретности.

Модификация. Модификация информации направлена на изменение таких свойств как *конфиденциальность, достоверность, целостность,* при этом подразумевается изменение состава и содержания сведений. Модификация информации не подразумевает ее полное уничтожение.

Уничтожение. Уничтожение информации направлено, как правило, на целостность информации и приводит к ее полному разрушению. *Нарушение целостности информации* заключается в утере информации. При утере информации она пропадает безвозвратно и не может быть восстановлена никакими средствами. Утеря может произойти из-за разрушения или уничтожения носителя информации или его пропажи, из-за стирания информации на носителях с многократной записью, из-за пропадания питания в устройствах с энергозависимой памятью. При уничтожении информации нарушается также свойство ***доступности*** информации.

Блокирование. Блокирование информации приводит к потере доступа к ней, т. е. к ***недоступности*** информации. Доступность информации заключается в том, что субъект, имеющей право на ее использование, должен иметь возможность на своевременное ее получение в удобном для него виде. При потере доступа к информации она по-прежнему существует, но воспользоваться ею нельзя. То есть субъект не может с ней ознакомиться, скопировать, передать другому субъекту или представить в виде удобном для использования.

Потеря доступа может быть связана с отсутствием или неисправностью некоторого оборудования автоматизированных систем (АС), отсутствием какого-либо специалиста или недостаточной его квалификацией, отсутствием или неработоспособностью какого-то программного средства, использованием ресурсов АС для обработки посторонней информации, выходом из строя систем обеспечения АС и др. Так как информация не утеряна, то доступ к ней может быть получен после устранения причин потери доступа.

Перечисленные угрозы информации могут проявляться в виде комплекса последовательных и параллельных реализаций. Реализация угроз информации, связанная с нарушением свойств информации приводит к нарушению режима управления и в конечном итоге к моральным и (или) материальным потерям.

2. Направления защиты информации

Направления обеспечения информационной безопасности — это нормативно-правовые категории, ориентированные на обеспечение комплексной защиты информации от внутренних и внешних угроз.

Учитывая практику обеспечения информационной безопасности, можно выделить следующие направления защиты информации:

– *правовая защита* — это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

– *организационная защита* — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям;

– *инженерно-техническая защита* — это использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности.

По характеру угроз защитные действия ориентированы на защиту информации от разглашения, утечки и несанкционированного доступа. По способам действий их можно подразделить на предупреждение, выявление, обнаружение, пресечение и восстановление ущерба или иных убытков. По охвату защитные действия могут быть ориентированы на территорию, здание, помещение, аппаратуру или отдельные элементы аппаратуры.

Рассмотрим каждое направление подробнее.

Правовая защита

Понятие «право» определяет совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Правовая защита информации признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном уровне правовая защита регулируется государственными и ведомственными актами. В Российской Федерации такими правилами являются Конституция, законы Российской Федерации, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Что касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, издаваемыми ведомствами, организациями и предприятиями, действующими в рамках определенных структур.

В литературе приводится такая структура правовых актов, ориентированных на правовую защиту информации.

Первый блок — конституционное законодательство. Нормы, касающиеся вопросов информатизации и защиты информации, входят в него как составные элементы.

Второй блок — общие законы, кодексы, которые включают нормы по вопросам информатизации и информационной безопасности.

Третий блок — законы об организации управления, касающиеся отдельных структур хозяйства, экономики, системы государственных органов и определяющие их статус. Они включают отдельные нормы по вопросам защиты информации. Наряду с общими вопросами информационного обеспечения и защиты информации конкретного органа эти нормы должны устанавливать его обязанности по формированию, актуализации и безопасности информации, представляющей общегосударственный интерес.

Четвертый блок — специальные законы, полностью относящиеся к конкретным сферам отношений, отраслям хозяйства, процессам. Именно состав и содержание этого блока законов и создает специальное законодательство как основу правового обеспечения информационной безопасности.

Пятый блок — законодательство субъектов Российской Федерации, касающееся защиты информации.

Шестой блок — подзаконные нормативные акты по защите информации.

Седьмой блок — это правоохранительное законодательство России, содержащее нормы об ответственности за правонарушения в сфере информатизации.

Таким образом, правовая защита информации обеспечивается нормативно-законодательными актами, представляющими собой по уровню иерархическую систему от Конституции РФ до функциональных обязанностей и контракта отдельного конкретного исполнителя, определяющих перечень сведений, подлежащих охране, и меры ответственности за их разглашение.

Одним из новых направлений правовой защиты является страховое обеспечение. Оно предназначено для защиты собственника информации и средств ее обработки как от традиционных угроз (кражи, стихийные бедствия), так и от угроз, возникающих в ходе работы с информацией. К ним относятся разглашение, утечка и несанкционированный доступ к конфиденциальной информации.

В основе российского страхового законодательства лежит Закон РФ «Об организации страхового дела в Российской Федерации». Он призван гарантировать защиту интересов страхователей, определять единые положения по организации страхования и принципы государственного регулирования страховой деятельности.

Опираясь на государственные правовые акты и учитывая ведомственные интересы на уровне конкретного предприятия (фирмы, организации), разрабатываются собственные нормативно-правовые документы, ориентированные на обеспечение информационной безопасности.

К таким документам относятся:

— Положение о сохранении конфиденциальной информации;

— Перечень сведений, составляющих конфиденциальную информацию;

— Инструкция о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию;

— Положение о специальном делопроизводстве и документообороте;

— Перечень сведений, разрешенных к опубликованию в открытой печати;

— Положение о работе с иностранными фирмами и их представителями;

— Обязательство сотрудника о сохранении конфиденциальной информации;

— Памятка сотруднику о сохранении коммерческой тайны.

Указанные нормативные акты направлены на предупреждение случаев неправомерного оглашения (разглашения) секретов на правовой основе и в случае их нарушения должны приниматься соответствующие меры воздействия.

В зависимости от характера информации, ее доступности для заинтересованных потребителей, а также экономической целесообразности конкретных защитных мер могут быть избраны следующие формы защиты информации:

— патентование;

— авторское право;

— признание сведений конфиденциальными;

— товарные знаки;

— применение норм обязательственного права.

Реализация правовых норм и актов, ориентированных на защиту информации на организационном уровне, опирается на те или иные организационно-правовые формы, к числу которых относятся соблюдение конфиденциальности работ и действий, договоры (соглашения) и различные формы обязательного права.

Конфиденциальность — это форма обращения со сведениями, составляющими коммерческую тайну, на основе организационных мероприятий, исключающих неправомерное овладение такими сведениями.

Договоры — это соглашения сторон (двух и более лиц) об установлении, изменении или прекращении взаимных обязательств.

Обязательство — гражданское правоотношение, в силу которого одна сторона (должник) обязана совершить в пользу другой стороны определенные действия.

Правовое регулирование необходимо для совершенствования механизма предупреждения противоправных действий по отношению к информационным ресурсам, для уточнения и закрепления задач и полномочий отдельных субъектов в сфере

предпринимательской деятельности, охраны прав и законных интересов граждан и организаций.

Анализ законодательства, регулирующего деятельность субъектов в сфере информационной безопасности, показывает наличие определенных недостатков. Существующие правовые нормы разбросаны по различным нормативным актам, издававшимся в разное время, в разных условиях и на разных уровнях. Действующее законодательство не систематизировано, что создает большие трудности в его использовании на практике.

Правовые меры обеспечения безопасности и защиты информации являются основой порядка деятельности и поведения сотрудников предприятия и определяют меры их ответственности за нарушение установленных норм.

Организационная защита

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

— организацию охраны, режима, работу с кадрами, с документами;

— использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, кото-

рые исключали бы (или по крайней мере сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

К основным организационным мероприятиям можно отнести:

— организацию режима и охраны. Их цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.;

— организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

— организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение;

— организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

— организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;

— организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Одним из важнейших организационных мероприятий является создание специальных штатных служб защиты информации в закрытых информационных системах в виде

администратора безопасности сети и администратора распределенных баз и банков данных, содержащих сведения конфиденциального характера.

Организационные мероприятия должны четко планироваться, направляться и осуществляться какой-то организационной структурой, каким-то специально созданным для этих целей структурным подразделением, укомплектованным соответствующими специалистами по безопасности предпринимательской деятельности и защите информации.

Как правило, таким структурным подразделением является служба безопасности предприятия (фирмы, организации), на которую возлагаются следующие общие функции:

— организация и обеспечение охраны персонала, материальных и финансовых ценностей и защиты конфиденциальной информации;

— обеспечение пропускного и внутриобъектового режима на территории, в зданиях и помещениях, контроль соблюдения требований режима сотрудниками, смежниками, партнерами и посетителями;

— руководство работами по правовому и организационному регулированию отношений по защите информации;

— участие в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты информации, а также положений о подразделениях, трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;

— разработка и осуществление совместно с другими подразделениями мероприятий по обеспечению работы с документами, содержащими конфиденциальные сведения; при всех видах работ организация и контроль выполнения требований «Инструкции по защите конфиденциальной информации»;

— изучение всех сторон производственной, коммерческой, финансовой и другой деятельности для выявления и последующего противодействия любым попыткам нанесения ущерба; ведения учета и анализа нарушений режима безопасности, накопление и анализ данных о злоумышленных устремлениях конкурентной и других организаций, о деятельности предприятия и его клиентов, партнеров, смежников;

— организация и проведение служебных расследований по фактам разглашения сведений, утрат документов, утечки конфиденциальной информации и других нарушений безопасности предприятия;

— разработка, ведение, обновление и пополнение «Перечня сведений конфиденциального характера» и других нормативных актов, регламентирующих порядок обеспечения безопасности и защиты информации;

— обеспечение строгого выполнения требований нормативных документов по защите производственных секретов предприятия;

— осуществление руководства службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и другими структурами в части оговоренных в договорах условий по защите конфиденциальной информации;

— организация и регулярное проведение учета сотрудников предприятия и службы безопасности по всем направлениям защиты информации и обеспечения безопасности производственной деятельности;

— ведение учета и строгого контроля выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации и каналами проникновения к источникам охраняемых секретов;

— обеспечение проведения всех необходимых мероприятий по пресечению попыток нанесения морального и материального ущерба со стороны внутренних и внешних угроз;

— поддержание контактов с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне) и оказания взаимной помощи в кризисных ситуациях.

Служба безопасности является самостоятельной организационной единицей предприятия, подчиняющейся непосредственно руководителю предприятия. Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности.

Организационные меры являются решающим звеном формирования и реализации комплексной защиты информации и создания системы безопасности предприятия.

Инженерно-техническая защита

С развитием техники и технологий окружающая нас информация стремительно возрастает и человек уже не в силах хранить ее в собственной памяти. На помощь к нему приходят современные средства хранения информации, информационные системы. Но сохраняя информацию, на каком либо носителе мы подвергаем себя опасности вероятного доступа третьих лиц. Поэтому информационная безопасность не только становиться обязательной, но и выступает как одна из важнейших характеристик информационной системы.

Во многих системах безопасности отведена первостепенная роль фактору безопасности. Большинство современных предприятий, занимающихся бизнесом в любой сфере деятельности, занимаются вопросами обеспечения безопасности своей информации.

В защите нуждается только та информация, которая имеет цену, а ценной она становится, когда ее обладатель может получить какую либо выгоду: материальную, политическую или моральную.

Поэтому, информация как категория, имеющая стоимость, защищается ее собственником или государством от лиц или организаций, пытающихся завладеть ею любыми способами. В связи с этим складывается тенденция, что чем выше уровень секретности информации, тем выше и уровень ее защиты, а значит, тем больше средств затрачивается на защиту.

Высокой эффективностью защиты информации можно определить как совокупность следующих факторов: своевременность, активность, непрерывность, комплексность. Очень важно проводить профилактические защитные мероприятия комплексно, то есть гарантировать нейтрализацию всех потенциально опасных каналов утечки информации. Необходимо иметь в виду, что один открытый канал утечки информации может свести на нет эффективность все системы защиты.

Теория инженерно-технической защиты информации описывает основные принципы, средства и методы обеспечения информационной безопасности объектов. Она включает в себя следующее: систему защиты информации; оценку угроз; принцип построения системы защиты информации.

Инженерно — техническая защита состоит из таких компонентов, как специальные органы, технические средства и

мероприятия по их использованию для защиты конфиденциальной информации.

Постоянная и эффективная техническая защита информационных ресурсов является обязательной составляющей комплексной системы обеспечения информационной безопасности и способствует оптимизации финансовых расходов на организацию защиты информации. Техническая защита информации предполагает целый комплекс мероприятий по защите информации от несанкционированного доступа по различным видам каналов, а также исключения специальных воздействий на нее, таких как, уничтожение, искажение или блокирование доступа.

Основными целями и задачами технической защиты являются:

— защита носителей информации от полного уничтожения в результате различных природных и техногенных воздействий;

— предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения;

— предотвращение утечки информации по различным техническим каналам.

При проектировании систем технической защиты необходимо соблюдать следующие принципы:

— непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности;

— многозональность и многорубежность защиты, задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности;

— избирательность в выборе первоочередности защиты наиболее важной информации;

— интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности;

— создание централизованной службы безопасности в интегрируемых системах.

По своему функциональному назначению средства инженерно-технической защиты подразделяются на следующие группы:

— инженерные средства, представляющие собой различные сооружения и устройства, предотвращающие физическое проникновение злоумышленников на защищаемые объекты;

— аппаратные средства, представляющие собой измерительные приборы и устройства, программно-аппаратные комплексы, предназначенные для выявления каналов утечки информации, оценки их характеристик по защите информации;

— программные комплексы и средства системы защиты информации в информационных системах различного назначения и в основных средствах обработки данных;

— криптографические средства защиты компьютерной информации, передаваемой по открытым каналам передачи данных и сетям связи.

В концепции инженерно-технической защиты информации кроме целей и задач системы безопасности, определяются принципы ее организации и функционирования; правовые основы; виды угроз и ресурсы, подлежащие защите, а также основные направления разработки системы безопасности.

К основным целям защиты информации относятся: предотвращение утечки, утраты, хищения, искажения, подделки информации и применение других несанкционированных негативных воздействий.

Разработка и создание новой системы защиты, а также оценка эффективности существующей системы безопасности объекта начинается с анализа наиболее возможных угроз и оценки их реального появления. Для получения данных такого рода, необходимо произвести обследование объекта на наличие уязвимостей в защите, а также учесть особенности расположения, инженерных конструкций, коммуникаций и т. п.

При рассмотрении вероятных угроз объекту нельзя забывать про угрозу безопасности здоровья персонала; угрозу целости и сохранности оборудования и материальных ценностей; безопасности информации и сохранность государственной или иной тайны.

При проектировании защиты в комплексную систему должно вписываться все разнообразие возможных информационных угроз. Так как она должна обеспечивать надежное перекрытие всех опасных каналов утечки информации.

Эффективность всей системы защиты от утечки информации по техническим каналам оценивается разнообразными критериями, которые определяются физической природой информационного сигнала, но чаще всего по соотношению «сигнал/шум».

Все способы защиты, согласно руководящим документам, делятся на две группы — скрытие и дезинформация.

К группе скрытие относятся:

— пассивное скрытие, заключающееся в исключении или значительном затруднении обнаружения объектов;

— активное скрытие, заключающееся в создании техническими средствами разведки маскирующих шумовых помех различной физической природы и ложной обстановки по физическим полям;

— специальная защита, заключающаяся в скремблировании телефонных переговоров, кодировании цифровой информации криптографическими методами, программные методы модификации информации.

К группе дезинформации относятся:

— техническая дезинформация;

— имитация;

— легендирование.

На вооружении промышленных шпионов, недобросовестных конкурентов и просто злоумышленников находятся самые разнообразные средства проникновения на объекты противоправных интересов и получения конфиденциальной информации. В этих условиях в интересах обеспечения информационной безопасности необходимы адекватные по ориентации, функциональному назначению и другим характеристикам технические средства защиты охраняемых секретов.

Инженерно-техническая защита (ИТЗ) по определению — это совокупность специальных органов, технических средств и мероприятий, по их использованию в интересах защиты конфиденциальной информации.

Многообразие целей, задач, объектов защиты и проводимых мероприятий предполагает рассмотрение некоторой системы классификации средств по виду, ориентации и другим характеристикам.

Многообразие классификационных характеристик позволяет рассматривать инженерно-технические средства по

объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны службы безопасности.

По функциональному назначению средства инженерно-технической защиты классифицируются на следующие группы:

— физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств и финансов и информации от противоправных воздействий;

— аппаратные средства. Сюда входят приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность. Основная задача аппаратных средств — обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности;

— программные средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных;

— криптографические средства — это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Аппаратные средства и методы защиты распространены достаточно широко.

Физические средства защиты — это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Эти средства применяются для решения следующих задач:

— охраны территории предприятия и наблюдения за ней;

— охраны зданий, внутренних помещений и контроль за ними;

— охраны оборудования, продукции, финансов и информации;

— осуществления контролируемого доступа в здания и помещения.

Все физические средства защиты объектов можно разделить на три категории: средства предупреждения, средства обнаружения и системы ликвидации угроз.

Физические средства являются первой преградой для злоумышленника при реализации им заходовых методов доступа.

Аппаратные средства защиты

К аппаратным средствам защиты информации относятся самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации.

Аппаратные средства защиты информации применяются для решения следующих задач:

— проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;

— выявление каналов утечки информации на разных объектах и в помещениях;

— локализация каналов утечки информации;

— поиск и обнаружение средств промышленного шпионажа;

— противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

По функциональному назначению аппаратные средства могут быть классифицированы на средства обнаружения, средства поиска и детальных измерений, средства активного и пассивного противодействия. При этом по своим техническим возможностям средства защиты информации могут быть общего назначения, рассчитанные на использование непрофессионалами с целью получения предварительных (общих) оценок, и профессиональные комплексы, позволяющие проводить тщательный поиск, обнаружение и прецизионные измерения всех характеристик средств промышленного шпионажа.

Аппаратные средства защиты информации — это различные технические устройства, системы и сооружения, предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа.

Программные средства защиты

Системы защиты компьютера от чужого вторжения весьма разнообразны и могут быть классифицированы на такие группы, как:

— средства собственной защиты, предусмотренные общим программным обеспечением;

— средства защиты в составе вычислительной системы;

— средства защиты с запросом информации;

— средства активной защиты;

— средства пассивной защиты и др.

Можно выделить следующие направления использования программ для обеспечения безопасности конфиденциальной информации такие как:

— защита информации от несанкционированного доступа;

— защита информации от копирования;

— защита программ от копирования;

— защита программ от вирусов;

— защита информации от вирусов;

— программная защита каналов связи.

Программная защита информации — это система специальных программ, включаемых в состав программного обеспечения, реализующих функции защиты информации.

Криптографические средства защиты

Криптография как средство защиты (закрытия) информации приобретает все более важное значение в мире коммерческой деятельности.

Криптография имеет достаточно давнюю историю. Вначале она применялась, главным образом, в области военной и дипломатической связи. Теперь она необходима в производственной и коммерческой деятельности. Криптография включает в себя несколько разделов современной математики, а также специальные отрасли физики, радиоэлектроники, связи и некоторых других смежных отраслей. Ее задачей является преобразование математическими методами передаваемого по каналам связи секретного сообщения, телефонного разговора или компьютерных данных таким образом, что они становятся совершенно непонятными для посторонних лиц.

Криптография должна обеспечить такую защиту секретной (или любой другой) информации, что даже в случае ее перехвата посторонними лицами и обработки любыми способами с использованием самых быстродействующих ЭВМ и последних достижений науки и техники она не должна быть дешифрована в течение нескольких десятков лет. Для такого преобразования информации используются различные шифровальные средства — такие, как средства шифрования документов, в том числе и портативного исполнения, средства шифрования речи (телефонных и радиопереговоров), средства шифрования телеграфных сообщений и передачи данных.

2.2.3. Системы защиты информации

Проблема защиты информации на сегодняшний день является одной из важнейших проблем современности. Если еще несколько лет назад задача защиты информации могла быть решена с помощью организационных мер и программных средств, то появление интернета, персональных компьютеров, спутниковой связи существенно обострило проблему защиты информации.

Система защиты информации — совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Классификация систем защиты информации

В качестве классификационного признака для систем защиты можно выбрать их функциональные свойства. На основе этого признака выделяются системы:

— без схем защиты;

— с полной защитой;

— с единой схемой защиты;

— с программируемой схемой защиты;

— системы с засекречиванием.

В некоторых системах отсутствует механизм, препятствующий пользователю в доступе к какой-либо информации, хранящейся в системе. Характерно, что большинство наиболее распространенных и широко применяемых за рубежом систем обработки информации (СОД) с пакетной обработкой не имеют механизма защиты. Однако такие системы содержат обычно развитый аппарат обнаружения и предотвращения ошибок, гарантирующий исключение разрушений режима функционирования.

В системах с полной защитой обеспечивается взаимная изоляция пользователей, нарушаемая только для информации общего пользования (например, библиотеки общего пользования). В отдельных системах средства работы с библиотеками общего пользования позволяют включить в них информацию пользователей, которая тоже становится общим достоянием.

В системах с единой схемой защиты для каждого файла создается список авторизованных пользователей. Кроме того, применительно к каждому файлу указываются разрешаемые режимы его использования: чтение, запись или выполнение, если этот файл является программой. Основные концепции защиты здесь довольно просты, однако их реализация довольно сложная.

В системах с программируемой схемой защиты предусматривается механизм защиты данных с учетом специфических требований пользователя, например, ограничение календарного времени работы системы, доступ только к средним значениям файла данных, локальная защита отдельных элементов массива данных и т. д. В таких системах пользователь должен иметь возможность выделить защищаемые объ-

екты и подсистемы. Защищаемая подсистема представляет собой совокупность программ и данных, правом доступа к которым наделены лишь входящие в подсистему программы. Обращение к этим программам возможно, в свою очередь, только в заранее ограниченных точках. Таким образом, программы подсистемы контролируют доступ к защищаемым объектам. Подобный механизм защиты с различными модификациями реализован только в наиболее совершенных СОД.

В системах с засекречиванием решаются не вопросы ограничения доступа программ к информации, а осуществляется контроль над дальнейшим использованием полученной информации. Например, в системе использования грифов секретности на документах гриф служит уведомлением о мере контроля. В СОД эта схема защиты используется редко. Отличительная особенность рассмотренных схем защиты — их динамичность, т. е. возможность ввода и изменения правил доступа к данным в процессе работы системы. Однако, обеспечение динамичности схем защиты значительно усложняет их реализацию.

Системы защиты информации на предприятии

Для создания и использования системы защиты на микроуровне необходимо хорошо знать сведения внешнего, внутреннего и специального назначения.

Сведения внешнего назначения — данные об окружении предприятия с точки зрения его безопасности.

Сведения внутреннего назначения — понятие о предприятии (персонале, оборудовании, промышленном производстве и т.д.).

Сведения специального назначения — это также все данные о предприятии, но с учетом особенностей его производства.

Система включает в себя следующие данные, составляющие коммерческую тайну:

— любые относящиеся к такой тайне;

— о количестве сотрудников, допущенных к тайне;

— о возможных каналах утечки такой информации;

— о том, какие меры для сохранения коммерческой тайны предпринимаются;

— о несанкционированном доступе к данным извне;

— о доле информированности о сведениях, относящихся к коммерческой тайне, сторонних лиц и организаций, а также о попытках получить такие сведения;

— о финансовых затратах на обеспечение коммерческой тайны.

Для полноценного функционирования всей системы безопасности проводится следующая работа:

— идентифицируются тайны;

— организуется защита тайны в подразделениях;

— отслеживается состояние защищенности коммерческой тайны;

— решается вопрос об изменении или снятии грифа секретности с технологии, производства, изделий, документов;

— оформляются допуски сотрудников, работающих со сведениями, составляющими коммерческую тайну;

— оценивается объем данных, характеризующих тайну, который может быть раскрыт представителям иной фирмы в интересах предприятия;

— расследуются факты утечки данных;

— локализуются возможные последствия утечки;

— оказывается помощь правоохранительным органам в расследовании дел, связанных с интересами фирмы.

Большой интерес с точки зрения системы защиты информации на предприятии может представлять и иная информация об организации — финансово-экономического характера касающаяся производственной деятельности, о международной и торгово-экономической деятельности, о научно-исследовательской деятельности.

К тому же для защиты отдельной предпринимательской структуры необходимы данные о следующих организациях и лицах:

— о деловых партнерах;

— о предприятиях-конкурентах;

— об организациях, которые располагают коммерческой тайной в той же или подобных сферах деятельности;

— об организациях и группировках, которые наносят ущерб предпринимательской деятельности;

— об организациях, в которых работали ранее действующие сотрудники и т. п.

Для специалистов, занимающихся системой защиты информации на предприятии, особое значение имеет информация о следующих категориях физических лиц:

— о сотрудниках, опыт и знания которых имеют определяющее значение для эффективной деятельности;

— о бывших работниках;

— о руководителях организаций-партнеров;

— о сотрудниках организаций-партнеров, которые осуществляли контакт с сотрудниками;

— о лицах, имеющих дружеские и иные связи с сотрудниками.

Деятельность специалистов, работающих в системе защиты информации на предприятии, начинается еще при приеме нового сотрудника, которого проверяют по степени надежности (оценивается уровень общей культуры, индивидуальные качества, опыт работы с секретной информацией), степень проявления к нему интереса со стороны конкурентов или преступного мира, способность противостоять покушениям на безопасность предприятия.

Для профилактики защиты информации на предприятии следует распространять сведения среди сотрудников о формах и методах обеспечения безопасности соответствующей деятельности, о конкретных фактах пресечения попыток причинения ущерба безопасности и поощрения сотрудников, которые предотвратили таковые попытки. Данная работа способствует повышению дисциплины труда, поднятию уровня культуры работы с секретными документами и обеспечивает высокое качество ежедневной деятельности предприятия с учетом требований безопасности.

Вся эта деятельность обеспечивает безопасную работу любого предприятия и составляет основу системы защиты информации на предприятии.

Комплексная система защиты информации

Комплексный (системный) подход к построению любой системы включает в себя: прежде всего, изучение объекта внедряемой системы; оценку угроз безопасности объекта; анализ средств, которыми будем оперировать при построении системы; оценку экономической целесообразности; изучение самой системы, ее свойств, принципов работы и возможность

увеличения ее эффективности; соотношение всех внутренних и внешних факторов; возможность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца.

Комплексный (системный) подход — это принцип рассмотрения проекта, при котором анализируется система в целом, а не ее отдельные части. Его задачей является оптимизация всей системы в совокупности, а не улучшение эффективности отдельных частей. Это объясняется тем, что, как показывает практика, улучшение одних параметров часто приводит к ухудшению других, поэтому необходимо стараться обеспечить баланс противоречий требований и характеристик.

Комплексный (системный) подход не рекомендует приступать к созданию системы до тех пор, пока не определены следующие ее компоненты:

1. Входные элементы. Это те элементы, для обработки которых создается система. В качестве входных элементов выступают виды угроз безопасности, возможные на данном объекте.

2. Ресурсы. Это средства, которые обеспечивают создание и функционирование системы (например, материальные затраты, энергопотребление, допустимые размеры и т. д.). Обычно рекомендуется четко определять виды и допустимое потребление каждого вида ресурса, как в процессе создания системы, так и в ходе ее эксплуатации.

3. Окружающая среда. Следует помнить, что любая реальная система всегда взаимодействует с другими системами, каждый объект связан с другими объектами. Очень важно установить границы области других систем, не подчиняющихся руководителю данного предприятия и не входящих в сферу его ответственности.

Характерным примером важности решения этой задачи является распределение функций по защите информации, передаваемой сигналами в кабельной линии, проходящей по территориям различных объектов. Как бы ни устанавливались границы системы, нельзя игнорировать ее взаимодействие с окружающей средой, ибо в этом случае принятые решения могут оказаться бессмысленными. Это справедливо как для границ защищаемого объекта, так и для границ системы защиты.

4. *Назначение и функции.* Для каждой системы должна быть сформулирована цель, к которой она (система) стремится. Эта цель может быть описана как назначение системы, как ее функция. Чем точнее и конкретнее указано назначение или перечислены функции системы, тем быстрее и правильнее можно выбрать лучший вариант ее построения. Так, например, цель, сформулированная в самом общем виде как обеспечение безопасности объекта, заставит рассматривать варианты создания глобальной системы защиты. Если уточнить ее, определив, например, как обеспечение безопасности информации, передаваемой по каналам связи внутри здания, то круг возможных решений существенно сузится. Следует иметь в виду, что, как правило, глобальная цель достигается через достижение множества менее общих локальных целей (подцелей). Построение такого «дерева целей» значительно облегчает, ускоряет и удешевляет процесс создания системы.

5. *Критерий эффективности.* Необходимо всегда рассматривать несколько путей, ведущих к цели, в частности нескольких вариантов построения системы, обеспечивающей заданные цели функционирования. Для того чтобы оценить, какой из путей лучше, необходимо иметь инструмент сравнения — критерий эффективности. Он должен: характеризовать качество реализации заданных функций; учитывать затраты ресурсов, необходимых для выполнения функционального назначения системы; иметь ясный и однозначный физический смысл; быть связанным с основными характеристиками системы и допускать количественную оценку на всех этапах создания системы.

Таким образом, учитывая многообразие потенциальных угроз информации на предприятии, сложность его структуры, а также участие человека в технологическом процессе обработки информации, цели защиты информации могут быть достигнуты только путем создания системы защиты информации (СЗИ) на основе комплексного подхода.

Назначение комплексной системы защиты информации

Главная цель создания системы защиты информации — это ее надежность. СЗИ — организованная совокупность объек-

тов и субъектов ЗИ, используемых методов и средств защиты, а также осуществляемых защитных мероприятий.

Но компоненты ЗИ, с одной стороны, являются составной частью системы, с другой — сами организуют систему, осуществляя защитные мероприятия.

Поскольку система может быть определена как совокупность взаимосвязанных элементов, то назначение СЗИ состоит в том, чтобы объединить все составляющие защиты в единое целое, в котором каждый компонент, выполняя свою функцию, одновременно обеспечивает выполнение функций другими компонентами и связан с ними логически и технологически.

Надежность защиты информации прямо пропорциональна системности, т. е. при несогласованности между собой отдельных составляющих риск «проколов» в технологии защиты увеличивается.

Во-первых, необходимость комплексных решений состоит в объединении в одно целое локальных СЗИ, при этом они должны функционировать в единой «связке». В качестве локальных СЗИ могут быть рассмотрены, например, виды защиты информации (правовая, организационная, инженерно-техническая).

Во-вторых, необходимость комплексных решений обусловлена назначением самой системы. Система должна объединить логически и технологически все составляющие защиты. Но из ее сферы выпадают вопросы полноты этих составляющих, она не учитывает всех факторов, которые оказывают или могут оказывать влияние на качество защиты. Например, система включает в себя какие-то объекты защиты, а все они включены или нет — это уже вне пределов системы.

Поэтому качество, надежность защиты зависят не только от видов составляющих системы, но и от их полноты, которая обеспечивается при учете всех факторов и обстоятельств, влияющих на защиту. Именно полнота всех составляющих системы защиты, базирующаяся на анализе таких факторов и обстоятельств, является вторым назначением комплексности.

При этом должны учитываться все параметры уязвимости информации, потенциально возможные угрозы ее безопасности, охватываться все необходимые объекты защиты, использоваться все возможные виды, методы и средства защи-

ты и необходимые для защиты кадровые ресурсы, осуществляться все вытекающие из целей и задач защиты мероприятия.

В-третьих, только при комплексном подходе система может обеспечивать безопасность всей совокупности информации, подлежащей защите, и при любых обстоятельствах. Это означает, что должны защищаться все носители информации, во всех компонентах ее сбора, хранения, передачи и использования, во все время и при всех режимах функционирования систем обработки информации.

В то же время комплексность не исключает, а, наоборот, предполагает дифференцированный подход к защите информации, в зависимости от состава ее носителей, видов тайны, к которым отнесена информация, степени ее конфиденциальности, средств хранения и обработки, форм и условии проявления уязвимости, каналов и методов несанкционированного доступа к информации.

Таким образом, значимость комплексного подхода к защите информации состоит:

— в интеграции локальных систем защиты;

— в обеспечении полноты всех составляющих системы защиты;

— в обеспечении всеохватности защиты информации.

Исходя из этого, можно сформулировать следующее определение:

«Комплексная система защиты информации — система, полно и всесторонне охватывающая все предметы, процессы и факторы, которые обеспечивают безопасность всей защищаемой информации».

Принципы построения комплексной системы защиты информации

При построении любой системы необходимо определить принципы, в соответствии с которыми она будет построена. КСЗИ — сложная система, функционирующая, как правило, в условиях неопределенности, требующая значительных материальных затрат. Поэтому определение основных принципов КСЗИ позволит определить основные подходы к ее построению.

Принцип законности заключается в соответствии принимаемых мер законодательству РФ о защите информации, а в

случае отсутствия соответствующих законов — другим государственным нормативным документам по защите.

В соответствии с принципом полноты защищаемой информации защите подлежит не только информация, составляющая государственную, коммерческую или служебную тайну, но и та часть несекретной информации, утрата которой может нанести ущерб ее собственнику либо владельцу. Реализация этого принципа позволяет обеспечить и охрану интеллектуальной собственности.

Принцип обоснованности защиты информации заключается в установлении путем экспертной оценки целесообразности засекречивания и защиты той или другой информации, вероятных экономических и других последствий такой защиты исходя из баланса жизненно важных интересов государства, общества и граждан. Это, в свою очередь, позволяет расходовать средства на защиту только той информации, утрата или утечка которой может нанести действительный ущерб ее владельцу.

Принцип создания специализированных подразделений по защите информации заключается в том, что такие подразделения являются непременным условием организации комплексной защиты, поскольку только специализированные службы способны должным образом разрабатывать и внедрять защитные мероприятия и осуществлять контроль за их выполнением.

Принцип участия в защите информации всех соприкасающихся с нею лиц исходит из того, что защита информации является служебной обязанностью каждого лица, имеющего по роду выполняемой работы отношение к защищаемой информации, и такое участие дает возможность повысить качество защиты.

Принцип персональной ответственности за защиту информации требует, чтобы каждое лицо персонально отвечало за сохранность и неразглашение вверенной ему защищаемой информации, а за утрату или распространение такой информации оно несет уголовную, административную или иную ответственность.

Принцип наличия и использования всех необходимых правил и средств для защиты заключается в том, что КСЗИ

требует, с одной стороны, участия в ней руководства предприятия и специальной службы защиты информации и всех исполнителей, работающих с защищаемой информацией, с другой стороны, использования различных организационных форм и методов защиты, с третьей стороны, наличие необходимых материально-технических ресурсов, включая технические средства защиты.

Принцип превентивности принимаемых мер по защите информации предполагает априорное опережающее заблаговременное принятие мер по защите до начала разработки или получения информации. Из этого принципа вытекает, в частности, необходимость разработки защищенных информационных технологий.

Среди рассмотренных принципов едва ли можно выделить более, или менее важные. А при построении КСЗИ важно использовать их в совокупности.

Комплексная система защиты информации обеспечивает исполнение требований нормативных правовых актов Российской Федерации в сфере защиты информации:

— Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологий и о защите информации»;

— Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

— Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

— Приказ Федеральной Службы по техническому и экспортному контролю (ФСТЭК России) от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

— Приказ Федеральной Службы по техническому и экспортному контролю (ФСТЭК России) от 11.02 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

— иные нормативно-правовые акты в сфере защиты информации.

Оценка эффективности систем защиты программного обеспечения

Системы защиты ПО широко распространены и находятся в постоянном развитии, благодаря расширению рынка ПО и телекоммуникационных технологий. Необходимость использования систем защиты (СЗ) ПО обусловлена рядом проблем, среди которых следует выделить:

— незаконное использование алгоритмов, являющихся интеллектуальной собственностью автора, при написании аналогов продукта (промышленный шпионаж);

— несанкционированное использование ПО (кража и копирование);

— несанкционированная модификация ПО с целью внедрения программных злоупотреблений;

— незаконное распространение и сбыт ПО (пиратство).

Системы защиты ПО по методу установки можно подразделить на системы:

— устанавливаемые на скомпилированные модули ПО;

— встраиваемые в исходный код ПО до компиляции;

— комбинированные.

Системы первого типа наиболее удобны для производителя ПО, так как легко можно защитить уже полностью готовое и оттестированное ПО (обычно процесс установки защиты максимально автоматизирован и сводится к указанию имени защищаемого файла и нажатию «Enter»), а потому и наиболее популярны. В то же время стойкость этих систем достаточно низка (в зависимости от принципа действия СЗ), так как для обхода защиты достаточно определить точку завершения работы «конверта» защиты и передачи управления защищенной программе, а затем принудительно ее сохранить в незащищенном виде.

Системы второго типа неудобны для производителя ПО, так как возникает необходимость обучать персонал работе с программным интерфейсом (API) системы защиты с вытекающими отсюда денежными и временными затратами. Кроме того, усложняется процесс тестирования ПО и снижается его

надежность, так как кроме самого ПО ошибки может содержать API системы защиты или процедуры, его использующие. Но такие системы являются более стойкими к атакам, потому что здесь исчезает четкая граница между системой защиты и как таковым ПО.

Для защиты ПО используется ряд методов, таких как:

Алгоритмы запутывания — используются хаотические переходы в разные части кода, внедрение ложных процедур — «пустышек», холостые циклы, искажение количества реальных параметров процедур ПО, разброс участков кода по разным областям ОЗУ и т.п.

Алгоритмы мутации — создаются таблицы соответствия операндов — синонимов и замена их друг на друга при каждом запуске программы по определенной схеме или случайным образом, случайные изменения структуры программы.

Алгоритмы компрессии данных — программа упаковывается, а затем распаковывается по мере выполнения.

Алгоритмы шифрования данных — программа шифруется, а затем расшифровывается по мере выполнения.

Вычисление сложных математических выражений в процессе отработки механизма защиты — элементы логики защиты зависят от результата вычисления значения какой-либо формулы или группы формул.

Методы затруднения дизассемблирования — используются различные приемы, направленные на предотвращение дизассемблирования в пакетном режиме.

Методы затруднения отладки — используются различные приемы, направленные на усложнение отладки программы.

Эмуляция процессоров и операционных систем — создается виртуальный процессор и/или операционная система (не обязательно реально существующие) и программа-переводчик из системы команд IBM в систему команд созданного процессора или ОС, после такого перевода ПО может выполняться только при помощи эмулятора, что резко затрудняет исследование алгоритма ПО.

Нестандартные методы работы с аппаратным обеспечением — модули системы защиты обращаются к аппаратуре ЭВМ, минуя процедуры операционной системы, и используют малоизвестные или недокументированные её возможности.

Государственная система защиты информации

Государственную систему защиты информации образуют:

— Федеральная служба по техническому и экспортному контролю (ФСТЭК России) и ее центральный аппарат;

— ФСБ, МО, СВР, МВД, их структурные подразделения по защите информации;

— структурные и межотраслевые подразделения по защите информации органов государственной власти;

— специальные центры ФСТЭК России;

— организации по защите информации органов государственной власти;

— головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские учреждения;

— предприятия оборонных отраслей промышленности, их подразделения по защите информации;

— предприятия, специализирующиеся на проведении работ в области защиты информации;

— аттестация объектов ТСОИ по требованиям защиты информации;

— вузы, институты по подготовке и переподготовке специалистов в области защиты информации.

ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

— обеспечения безопасности информации в ключевых системах информационной инфраструктуры;

— противодействия иностранным техническим разведкам;

— обеспечения защиты информации, содержащей государственную тайну криптографическими способами;

— предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней;

— предотвращения специальных воздействий на информацию (ее носители) с целью ее добывания, уничтожения, искажения и блокирования доступа к ней.

Руководство деятельностью ФСТЭК России осуществляет президент РФ.

Непосредственное руководство работами по защите информации осуществляют руководители органов государственной власти и их заместители.

В органе государственной власти могут создаваться технические комиссии, межотраслевые советы.

Головные и ведущие НИИ органов государственной власти разрабатывают научные основы и концепции, проекты нормативно-технических и методических документов по защите информации. На них возлагается разработка и корректировка моделей иностранных технических разведок.

Предприятия, занимающиеся деятельностью в области защиты информации, должны получить лицензию на этот вид деятельности. Лицензии выдаются ФСТЭК России, ФСБ, СВР в соответствии с их компетенцией и по представлению органа государственной власти.

Организация работ по защите информации возлагается на руководителей организаций. Для методического руководства и контроля за обеспечением защиты информации может быть создано подразделение по защите информации или назначен ответственный за безопасность информации.

Разработка системы ЗИ производится подразделением по технической защите информации или ответственным за это направление во взаимодействии с разработчиками и ответственными за эксплуатацию объектов ТСОИ. Для проведения работ по созданию системы ЗИ могут привлекаться на договорной основе специализированные предприятия, имеющие соответствующие лицензии.

Работы по созданию системы ЗИ проводятся в три этапа.

На I этапе разрабатывается техническое задание на создание СЗИ:

— вводится запрет на обработку секретной (служебной) информации на всех объектах ТСОИ до принятия необходимых мер защиты;

— назначаются ответственные за организацию и проведение работ по созданию системы защиты информации;

— определяются подразделения или отдельные специалисты, непосредственно участвующие в проведении указанных работ, сроки введения в эксплуатацию системы ЗИ;

— проводится анализ возможных технических каналов утечки секретной информации;

— разрабатывается перечень защищаемых объектов технических средств обработки информации (ТСОИ);

— проводится категорирование основных технических средств и систем (ОТСС), а также выделенных помещений (ВП);

— определяется класс защищенности автоматизированных систем, участвующих в обработке секретных (служебных) данных;

— определяется контролируемая зона (КЗ);

— оцениваются возможности средств иностранных технических разведок (ИТР) и других источников угроз;

— обосновывается необходимость привлечения специализированных предприятий для создания системы защиты информации;

— разрабатывается техническое задание (ТЗ) на создание СЗИ.

Разработка технических проектов на установку и монтаж ТСОИ производится проектными организациями, имеющими лицензию ФСТЭК.

На II этапе:

— разрабатывается перечень организационных и технических мероприятий по защите объектов ТСОИ в соответствии с требованиями ТЗ;

— определяется состав серийно выпускаемых в защищенном исполнении ТСОИ, сертифицированных средств защиты информации, а также состав технических средств, подвергаемых специальным исследованиям и проверке; разрабатываются технические паспорта на объекты ТСОИ и инструкции по обеспечению безопасности информации на этапе эксплуатации технических средств.

На III этапе осуществляются:

— проведение специальных исследований и специальной проверки импортных ОТСС, а также импортных вспомогательных технических средств и систем (ВТСС), установленных в выделенных помещениях;

— размещение и монтаж технических средств, входящих в состав объектов ТСОИ;

— разработка и реализация разрешительной системы доступа к средствам вычислительной техники и автоматизированным системам, участвующим в обработке секретной (служебной) информации;

— приемосдаточные испытания системы защиты информации по результатам ее опытной эксплуатации;

— аттестация объектов ТСОИ по требованиям защиты информации.

2.3. Принципы, законы, право и психология информационной безопасности

2.3.1. О принципах информационной безопасности

В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:

— целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;

— конфиденциальность информации;

— доступность информации для всех авторизованных пользователей.

Построение системы обеспечения безопасности информации в АС и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

— законности;
— системности;
— комплексности;
— непрерывности;
— своевременности;
— разумной достаточности;
— персональной ответственности;
— разделения функций;
— минимизации полномочий;
— взаимодействия и сотрудничества;
— гибкости системы защиты;
— открытости алгоритмов и механизмов защиты;
— простоты применения средств защиты;
— научной обоснованности и технической реализуемости;
— специализации и профессионализма;
— взаимодействия и координации;
— обязательности контроля.

Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности информации в АС в соответствии с действующим законодательством в области информации, информатизации и защиты информации, других нормативных актов по безопасности, утвержденных органами государственной власти в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.

Системность

Системный подход к защите информации в АС предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности в АС.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только

всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами.

Одним из наиболее укрепленных рубежей призваны быть средства защиты, реализованные на уровне СВТ в силу того, что ОС — это та часть компьютерной системы, которая управляет использованием всех ее ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

Непрерывность защиты

Защита информации — не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а *непрерывный целенаправленный процесс,* предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т. п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по

комплексной защите АС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки АС в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования АС и ее системы защиты с учетом изменений в методах и средствах перехвата информации и воздействия на компоненты АС, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

Разделение функций

Принцип разделения функций требует, чтобы ни один сотрудник организации не имел полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Все такие операции должны быть разделены на части, и их выполнение должно быть поручено различным сотрудникам. Кроме того, необходимо предпринимать специальные меры по недопущения сговора и разграничению ответственности между этими сотрудниками.

Разумная достаточность (экономическая целесообразность, сопоставимость возможного ущерба и затрат)

Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы АС, в которой эта информация циркулирует. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в

обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Персональная ответственность

Предполагает ответственность за обеспечение безопасности информации и системы ее обработки каждым сотрудником в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, в каком это необходимо сотруднику для выполнения его должностных обязанностей.

Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделении. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений обеспечения безопасности информации.

Гибкость системы защиты

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на

уже работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости системы защиты избавляет владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления. Это, однако, не означает, что информация о конкретной системе защиты должна быть общедоступна.

Простота применения средств защиты

Механизмы зашиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т. д.).

Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственные лицензии на право оказания услуг в этой области.

Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными сотрудниками (специалистами подразделений обеспечения безопасности информации).

Взаимодействие и координация

Предполагают осуществление мер обеспечения безопасности информации на основе взаимодействия всех заинтересованных министерств и ведомств, предприятий и организаций при разработке и функционировании АС и ее системы защиты информации, специализированных предприятий и организаций в области защиты информации, привлеченных для разработки системы защиты информации в АС, координации их усилий для достижения поставленных целей ФСТЭК России.

Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства зашиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации, и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

2.3.2. О законах по информационной безопасности

Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей; статья 42 — право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; статья 29 — право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

В Гражданском кодексе Российской Федерации фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

В УК РФ по вопросу информационной безопасности содержится три статьи:

— статья 272. Неправомерный доступ к компьютерной информации;

— статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;

— статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Первая имеет дело с посягательствами на конфиденциальность, вторая — с вредоносным ПО, третья — с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Для банковской и коммерческой тайны существует статья 183 УК РФ.

Основные законы в сфере информационной безопасности.

Базовым актом информационного законодательства Российской Федерации является Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. N 149-ФЗ (ред. от 01.05.2019). В нем законодательно закрепляется право граждан, организаций и государства на информацию, устанавливаются их основные права и обязанности, правовой режим обработки и использования информации, порядок обеспечения информационной безопасности и гарантии реализации прав и ответственности субъектов информационных отношений.

Основная цель закона состоит в совершенствовании правовой основы отношений в области формирования и использования информационных ресурсов, в области информатизации с учетом возрастающей роли информации в обновлении производственного, научного, организационного и управленческого потенциалов страны, в решении вопроса о включении России в мировое сообщество. Сфера действия Закона охватывает отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации (ст. 1).

Согласно закону «Об информации, информационных технологиях и о защите информации» (ст. 3), правовое регулирование отношений в данной сфере основывается на следующих принципах:

— свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

— установление ограничений доступа к информации только федеральными законами; открытость информации о деятельности государственных органов и органов местного самоуправления;

— равноправие языков народов Российской Федерации при создании информационных систем;

— достоверность информации и своевременность ее предоставления; неприкасаемость частной жизни;

— недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими.

Законом «Об информации, информационных технологиях и о защите информации» (ст. 5) вся информация в зависимости от порядка ее предоставления и распространения подразделяется на следующие группы:

— информация, свободно распространяемая;

— информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях;

— информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

— информация, распространение которой в Российской Федерации ограничивается или запрещается.

Согласно закону, обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование (ст. 6). Обладатель информации обязан соблюдать права и законные интересы иных лиц, принимать меры по защите информации, ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Закон определяет порядок государственного регулирования в сфере применения информационных технологий (ст. 12), использования информационно-телекоммуникационных сетей (ст. 15) и защиты информации (ст.16), а также ответственность за правонарушения в сфере информации, информационных технологий и защиты информации (ст. 17).

Со дня вступления в силу данного Федерального закона признаны утратившими силу Федеральный закон от 20 февраля 1995 г. «Об информации, информатизации и защите информации» и ряд других законодательных актов (ст. 18).

Национальное законодательство, призванное регулировать отношения в сфере информатизации и обеспечения информационной безопасности, включает в себя ряд других действующих законодательных актов.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Федеральном законе «О государственной тайне» от 21.07.1993 N 5485-1 (ред. от 08.11.2011). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Закон РФ «О средствах массовой информации» принят 27 декабря 1991 г. (в редакции от 01.09.2013). В ст. 1 закона записано, что свобода массовой информации в РФ не подлежит ограничениям, за исключением случаев, предусмотренных законодательством о средствах массовой информации. Не подлежат также ограничениям поиск, получение, производство и распространение массовой информации, учреждение средств массовой информации, владение, пользование и распоряжение ими, изготовление, приобретение, хранение и эксплуатация технических устройств и оборудования, сырья и материалов, предназначенных для производства и распространения продукции средств массовой информации.

В законе прямо указывается, что цензура массовой информации, а также создание и финансирование организаций, учреждений, органов или должностей, в задачи или функции которых входит осуществление цензуры массовой информации, не допускается. В ст. 4 закона говорится о недопустимости злоупотребления средствами массовой информации в целях совершения уголовно наказуемых деяний:

— разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну;

— призыва к захвату власти, насильственному изменению конституционного строя и целостности государства;

— разжигания национальной, классовой, социальной, религиозной нетерпимости или розни, пропаганды войны;

— распространения передач, пропагандирующих порнографию, культ насилия и жестокости.

Федеральный закон РФ «О безопасности» N 390-ФЗ принят 28 декабря 2010 г. Он пришел на смену Федеральному закону РФ «О безопасности» N 2446-I , принятому 5 марта 1992 г. Новый закон является базовым в области защиты жизненно важных интересов государства, однако он дает более общие трактовки понятий по сравнению с предыдущим законом. В частности, из нового закона убрана трактовка понятия информационная безопасность.

В ст. 13 Закона «О безопасности» указывается, что Совет Безопасности РФ, являющийся конституционным органом, осуществляющим подготовку решений Президента РФ в соответствующей области, осуществляет свою деятельность в сфере государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности. В законе имеется положение о том, что в функции Совета, в частности, входит рассмотрение вопросов информационной безопасности, обеспечения стабильности и правопорядка. Таким образом, Совет безопасности является ответственным за состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних угроз.

Закон РФ «О связи» №126 -ФЗ от 07.07.2003 г. Сфера действия этого закона распространяется на отношения, связанные с деятельностью по предоставлению услуг и выполнению работ в области связи, в осуществлении которых участвуют органы государственной власти, операторы связи, отдельные должностные лица, а также пользователи связи. Закон устанавливает правовую основу деятельности в области связи, осуществляемой под юрисдикцией Российской Федерации (федеральная связь), определяет полномочия органов государственной власти по регулированию указанной деятельности, а также права и обязанности физических и юридических лиц, участвующих в указанной деятельности или пользующихся

услугами связи. Отдельная глава закона посвящена регулированию отношений в области управления связью, регулированию использования радиочастотного спектра и орбитальных позиций спутников связи, управлению сетями связи при чрезвычайных ситуациях и в условиях чрезвычайного положения. Законом определено, что к федеральной связи относятся все сети и сооружения электрической и почтовой связи на территории Российской Федерации (за исключением внутрипроизводственных и технологических сетей связи).

Закон РФ «Об авторском праве и смежных правах» вступил в силу 3 августа 1993 г. (в настоящее время Закон действует в редакции 2004 г.). Предметом регулирования закона, в частности, являются отношения, возникающие в связи с созданием и использованием произведений науки, литературы (включая программы для ЭВМ), которые являются результатом творческой деятельности, независимо от назначения и достоинства произведения, а также способа его выражения. Источниками регулирования являются не только законы Российской Федерации и принимаемые на их основе законодательные акты субъектов Российской Федерации, но и международные договоры, в которых участвует Россия. Если международным договором, в котором участвует Российская Федерация, установлены иные правила, чем те, которые содержатся в Законе, то применяются правила международного договора. К основным понятиям закона относятся, в числе прочих, понятия программы для ЭВМ и базы данных, записи программы в память ЭВМ, а также понятие контрафактных экземпляров произведений. Законом определено, что программы для ЭВМ являются объектами авторского права, нарушение которого влечет гражданскую, уголовную и административную ответственность в соответствии с законодательством Российской Федерации.

Закон «Об органах федеральной службы безопасности Российской Федерации», принятый 10 апреля 1995 г. (ред. от 02.07.2013 г.), и Закон «О внешней разведке» от 10 января 1996 г. (ред. от 08.12.2011 г.) в части, касающейся добывания, обработки разведывательной информации и защиты государственной тайны, имеют много общего.

Для достижения целей разведывательной деятельности и получения специальной информации органы Федеральной

службы безопасности (ФСБ) и Службы внешней разведки (СВР) используют методы и средства в соответствии с федеральными законами. В ст. 20 Закона «Об органах федеральной службы безопасности Российской Федерации» указано, что хранение в информационных системах сведений о физических и юридических лицах не является основанием для принятия мер, ограничивающих права названных лиц. Законом «О внешней разведке» регламентируется деятельность подразделений и частей радиоразведки, которые обеспечивают и ведут разведывательную деятельность в сфере шифрованной, засекреченной и иных видов специальной связи.

В Федеральных законах «О государственной охране» от 27.05.1996 N 57-ФЗ (ред. от 02.07.2013) и «О Федеральной фельдъегерской связи» N 67-ФЗ от 17.12.1994 (ред. от 02.07.2013) определены права и обязанности соответствующих служб в сфере сбора, получения, охраны, защиты и доставки информации.

Юридическое закрепление информационных отношений, возникающих в сфере деятельности органов внутренних дел, регулируются Федеральным законом «Об оперативно-розыскной деятельности» от 12.08.1995 N 144-ФЗ (ред. от 02.11.2013). В соответствии с законом оперативные подразделения органов внутренних дел получили широкие возможности по сбору информации «о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации» (ст. 2). В ст. 6 закона приведен перечень оперативно-розыскных мероприятий, в ходе проведения которых для получения необходимых сведений «используются информационные системы, видео- и аудиозаписи, кино- и фотосъемки, а также другие технические и иные средства, не наносящие ущерб жизни и здоровью людей и не причиняющие вред окружающей среде».

Федеральный закон «Об оперативно-розыскной деятельности» допускает ограничения конституционных прав граждан при проведении оперативно-розыскных мероприятий только с разрешения суда на основании мотивированного постановления одного из руководителей органа — субъекта оперативно-розыскной деятельности.

В Законе «Об основах государственной службы» определены права, обязанности и ограничения, накладываемые на государственных служащих, в том числе и в области информационного обмена. Так, ст. 11 закона запрещает государственным служащим использовать в неслужебных целях средства информационного обеспечения и служебную информацию.

Законодательное регулирование прав граждан на благоприятную окружающую среду и достоверную информацию о ее состоянии нашло отражение в Федеральном законе «О радиационной безопасности населения» N 3-ФЗ, принятом 9 января 1996 г. (ред. от 19.07.2011). В соответствии со ст. 23 закона граждане и общественные организации получили право на объективную информацию о радиационной обстановке и принимаемых мерах безопасности от тех организаций, которые осуществляют деятельность с применением источников ионизирующего излучения. Кроме того, согласно ст. 6 закона, субъекты Российской Федерации уполномочены информировать граждан о радиационной обстановке на соответствующей территории.

Важнейшим документом в сфере информационной политики, который был принят в России и реализуется в настоящее время, является Доктрина информационной безопасности.

Доктрина информационной безопасности Российской Федерации, утвержденная Указом № 646 от 5.12.2016 года Президента Российской Федерации В. В. Путиным, является базовым концептуальным документом, который определяет основные направления обеспечения одного из ключевых направлений безопасности российского государства. В Доктрине отмечается, что информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Доктрина информационной безопасности служит основой:

— для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по

совершенствованию системы обеспечения информационной безопасности и является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683, а также других документов стратегического планирования в указанной сфере.

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности любого государства. Национальная безопасность Российской Федерации также существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать, учитывая, в частности, усиливающиеся угрозы со стороны террористов, приверженцев любой экстремальной идеи и других деструктивных общественных сил.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности. Решение этой проблемы является первостепенным для дальнейшей разработки доктринальных основ обеспечения информационной безопасности.

Таким образом можно сделать вывод, что современному государству, просто необходимо создавать систему обеспечения информационной безопасности, опирающуюся на комплекс нормативных правовых актов, которая позволит предупреждать и противодействовать реализации имеющихся угроз информационной безопасности, а также выявлять и принимать меры против уже объективно реализовавшихся угроз.

При этом следует подчеркнуть, что на сегодняшний день осуществление этих задач наталкивается на целый ряд проблем, связанных, в первую очередь, с недостатком финансирования государственной информационной политики Российской Федерации за рубежом. Еще одной проблемой является недостаток профессиональных специалистов, которые способны эффективно решать информационные задачи за

пределами России. И, наконец, еще одной составляющей указанного комплекса проблем является слабая теоретическая разработка основ современной российской политики в указанной сфере.

2.3.3. О праве по информационной безопасности

Вопросы, связанные с информационным законодательством требуют внимания государства к ряду направлений деятельности в области информатизации. Можно отметить из них наиболее очевидные.

Формирование информационных ресурсов и развитие информационной деятельности — деятельности, непосредственно связанной со сбором, хранением, обработкой, передачей информации в самых разных организационных формах (документированная, звуковая, световая, цифровая и т. п.); деятельности по созданию средств обработки информации в электронном виде — создание программ, программного обеспечения и иных средств работы с информацией и ее транспортировкой (коммуникацией) по каналам связи, сетям в соответствии с типами организации информационных систем и сетей на основе современных технических и технологических достижений; управление качеством информационных технологий (достоверность, полнота, неуязвимость передаваемой информации и создание средств ее защиты в системах информационной безопасности); организация рынка информационных технологий. Все эти направления могут быть объединены в блок формирования специальной отрасли информатики, объединяющей проблемы создания, производства и использования средств информатизации, информационных технологий в широком понимании.

Вторым крупным блоком в системе государственного управления является деятельность по организации применения средств информатизации и информационных ресурсов в самых разных сферах социального развития.

Здесь сосредоточены проблемы информатизации экономики, экологии, здравоохранения, любых отраслей производства, науки, образования, культурно-просветительской деятельности, формирования и использования соответствующих видов и форм информационных ресурсов. Сюда же входят

проблемы региональной и отраслевой информатизации и формирование специальных отраслей государственного управления в данной сфере.

Пока на уровне системы федеральных органов исполнительной власти функционирует федеральный орган, непосредственно выполняющий функции государственного управления — это Министерство связи и информатизации Российской Федерации. Кроме того, действуют специализированные государственные органы, ориентированные на организацию и использование отдельных массивов информационного ресурса. Это Архивная служба Российской Федерации, органы федеральной статистики. Большое внимание информационным проблемам уделяет Совет Безопасности Российской Федерации.

Данное направление охватывает процессы информатизации деятельности органов государственной власти и местного самоуправления и их взаимодействия. Деятельность органов государственной власти законодательных, исполнительных, правоохранительных — может быть продуктивной и эффективной при условии применения информационных технологий в работе аппарата каждого органа и в системе взаимодействия различных органов между собой.

Следующий блок в сфере государственного управления в области информационных технологий является деятельность каждого из ведомств и государственных организаций, которые самостоятельно и с учетом своих потребностей обеспечивают процессы информационного обеспечения своей деятельности. При отсутствии должной координации на уровне федерации это направление деятельности подвержено местничеству и заканчивается неоправданной тратой средств, несовместимостью средств информатизации, в том числе и информационных технологий в едином пространстве страны.

Поддержка процессов информатизации во всех секторах хозяйства и культуры страны, во всех сферах социального развития и жизнеобеспечения; привлечение населения к новым методам работы с информацией на основе воспитания информационной культуры, переподготовки кадров и массового обучения молодого поколения работе в новых условиях. Здесь сосредоточены организационно-правовые проблемы

обеспечения реализации права на информацию различных субъектов, разрешение конфликтов в области формирования и использования информационных технологий.

Все обозначенные направления государственного управления в области информационных технологий реализуются на основе создания и применения соответствующих законов и иных правовых актов, введения обязательных государственных стандартов, методик и правил.

Правовые проблемы информационной безопасности

Законом РФ «О безопасности» безопасность определяется как состояние защищенности жизненно важных интересов личности, общества и государства.

Жизненно важные интересы определяются законодателем как совокупность потребностей, удовлетворение которых обеспечивает существование и возможности прогрессивного развития личности, общества, государства, а угроза безопасности — как совокупность условии и факторов, создающих опасность жизненно важным интересам личности, общества, государства. И, наконец, обеспечение безопасности — проведение единой государственной политики в этой сфере и система мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства, направленных на выявление и предупреждение угроз.

Федеральным законом «Об участии в международном информационном обмене» определено понятие информационной безопасности как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

На основании Федерального закона «Об информации, информационных технологиях и о защите информации» целями защиты информационной сферы являются:

— предотвращение утечки, хищения, утраты, искажения, подделки информации;

— предотвращение угроз безопасности личности, общества, государства;

— предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию,

блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

— защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

— сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

— обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

В результате сопоставительного анализа области информационной безопасности информационной сферы с учетом положений Доктрины информационной безопасности и норм информационного законодательства в этой области можно выделить три основных направления правовой защиты объектов в информационной сфере (правового обеспечения информационной безопасности).

1. Первое направление. Обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации.

2. Второе направление. Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее — критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время.

Развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также

совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности.

Доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры.

Содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

3. *Третье направление*. Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Правовая защита интересов личности, общества, государства от угроз воздействия недоброкачественной информации, от нарушения порядка распространения информации

Правовую основу первого направления правового обеспечения информационной безопасности составляют следующие информационно-правовые нормы Конституции Российской Федерации.

«Статья 29

5. Гарантируется свобода массовой информации. Цензура запрещается».

Законодатель имеет в виду, что свобода массовой информации и запрет цензуры дают возможность создавать и распространять достоверную, своевременную, объективную,

т.е. доброкачественную информацию, при которой должно быть исключено распространение вредной и опасной информации. Именно такие требования с точки зрения информационной безопасности должны применяться при формировании института массовой информации, учитываться при подготовке нормативных правовых актов в рамках этого института.

«Статья 41

3. Сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом».

Эта норма прямого действия защищает личность и общество от сокрытия опасной информации.

«Статья 29

2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства».

Ответственность за распространение недоброкачественной информации, за нарушения порядка распространения информации предусматривается нормами УК РФ. Это клевета (ст. 129), оскорбление (ст. 130), воспрепятствование законной профессиональной деятельности журналистов (ст. 144), заведомо ложная реклама (ст. 182), злоупотребления при выпуске ценных бумаг (эмиссии) (ст. 185), заведомо ложное сообщение об акте терроризма (ст. 207), сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (ст. 237), незаконное распространение порнографических материалов или предметов (ст. 242), публичные призывы к насильственному изменению конституционного строя РФ (ст. 280), возбуждение национальной, расовой или религиозной вражды (ст. 282), публичные призывы к развязыванию агрессивной войны (ст. 354).

Нормы об ответственности за административные правонарушения содержатся в Кодексе Российской Федерации об административных правонарушениях. Это, например, нарушение установленного порядка опубликования документов, связанных с подготовкой и проведением выборов, референдумов,

нарушение правил проведения предвыборной агитации, агитации при проведении референдума в периодических печатных изданиях и на каналах организаций, осуществляющих теле- и (или) радиовещание, изготовление или распространение анонимных агитационных материалов, не предоставление или не опубликование отчета, сведений о поступлении и расходовании средств на подготовку и проведение выборов, референдума, не предоставление сведений об итогах голосования, нарушение порядка изготовления и распространения продукции средства массовой информации.

Таким образом, защита от воздействия недоброкачественной информации сосредоточена главным образом в нормах законодательства о средствах массовой информации, нормах Уголовного кодекса РФ и КоАП.

Правовая защита информации, информационных ресурсов и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц

Правовую основу второго направления информационной безопасности составляют следующие информационные конституционные нормы.

«Статья 29

4. Перечень сведений, составляющих государственную тайну, определяется федеральным законом».

Конституция Российской Федерации охраняет личную тайну, информацию о личности или персональные данные от вмешательства посторонних лиц.

«Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений...».

При этом прямо запрещается кому бы то ни было собирать информацию о любом гражданине без его на то согласия.

«Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются».

Конституцией Российской Федерации запрещается также получать иную информацию от любого гражданина без его

добровольного на то согласия или убеждать его отказаться от предоставленной ранее информации.

Законом предусматривается защита прав субъектов в сфере информационных процессов и информатизации.

Статья 15.2. Порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

(введена Федеральным законом от 02.07.2013 N 187-ФЗ)

1. Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», объектов авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемых в таких сетях, или информации, необходимой для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без его разрешения или иного законного основания, вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такие объекты или информацию, на основании вступившего в силу судебного акта. Форма указанного заявления утверждается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней:

1) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети «Интернет», указанного информационного ресурса, обслуживающего владельца сайта в сети «Интернет», на котором размещена информация, содер-

жащая объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания;

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

2) направляет провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в электронном виде уведомление на русском и английском языках о нарушении исключительных прав на объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», с указанием наименования произведения, его автора, правообладателя, доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети «Интернет», на котором размещена информация, содержащая объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания, а также указателей страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию, и с требованием принять меры по ограничению доступа к такой информации;

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в соответствующей информационной системе.

3. В течение одного рабочего дня с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно ограничить доступ к незаконно размещенной информации.

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

4. В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного в пункте 1 части 2 настоящей статьи лица уведомления о необходимости ограничить доступ к незаконно размещенной информации владелец информационного ресурса обязан удалить незаконно размещенную информацию или принять меры по ограничению доступа к ней. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи.

(часть 4 в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

5. В случае непринятия провайдером хостинга или иным указанным в пункте 1 части 2 настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в частях 3 и 4 настоящей статьи, доменное имя сайта в сети «Интернет», его сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать информацию, содержащую объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, и размещенную без разрешения правообладателя или иного законного основания, а также иные сведения об этом сайте и информация направляются по системе взаимодействия операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сайту в сети "Интернет", или к размещенной на нем информации.

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

6. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней со дня получения судебного акта об отмене ограничения доступа к информационному ресурсу, содержащему объекты авторских и (или)

смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без разрешения правообладателя или иного законного основания, уведомляет провайдера хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо и операторов связи об отмене мер по ограничению доступа к данному информационному ресурсу. В течение одного рабочего дня со дня получения от указанного федерального органа исполнительной власти уведомления об отмене мер по ограничению доступа к информационному ресурсу провайдер хостинга обязан проинформировать об этом владельца информационного ресурса и уведомить о возможности снятия ограничения доступа.

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

7. В течение суток с момента получения по системе взаимодействия сведений об информационном ресурсе, содержащем объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые используются без разрешения правообладателя или иного законного основания, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан ограничить доступ к незаконно размещенной информации в соответствии с вступившим в законную силу судебным актом. В случае отсутствия у оператора связи технической возможности ограничить доступ к незаконно размещенной информации оператор связи обязан ограничить доступ к такому информационному ресурсу.

(часть 7 в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

8. Порядок функционирования информационной системы взаимодействия устанавливается федеральным органом

исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

9. Предусмотренный настоящей статьей порядок не применяется к информации, подлежащей включению в реестр в соответствии со статьей 15.1 настоящего Федерального закона.

Статья 15.3. Порядок ограничения доступа к информации, распространяемой с нарушением закона

(введена Федеральным законом от 28.12.2013 N 398-ФЗ)

1. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, включая случай поступления уведомления о распространении такой информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители направляют требование в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании обращения, указанного в части 1 настоящей статьи, незамедлительно:

1) направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу, в том числе к сайту в сети «Интернет», или к информации, размещенной на нем и содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка. Данное требование должно содержать доменное имя сайта в

сети «Интернет», сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать такую информацию;

2) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети «Интернет», указанного информационного ресурса, обслуживающего владельца сайта в сети «Интернет», на котором размещена информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка;

3) направляет провайдеру хостинга или иному указанному в пункте 2 настоящей части лицу уведомление в электронном виде на русском и английском языках о нарушении порядка распространения информации с указанием доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети «Интернет», на котором размещена информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, а также указателей страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию, и с требованием принять меры по удалению такой информации;

4) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 2 настоящей части лицу в соответствующей информационной системе.

3. После получения по системе взаимодействия требования федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан незамедлительно ограничить доступ к информационному ресурсу, в том числе к сайту в сети «Интернет», или к информации, размещенной на нем и содержащей призывы к массовым беспорядкам, осуществлению экстремистской

деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка.

4. В течение суток с момента получения уведомления, указанного в пункте 3 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 2 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить информацию, содержащую призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка.

5. В случае, если владелец информационного ресурса удалил информацию, содержащую призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, он направляет уведомление об этом в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Такое уведомление может быть направлено также в электронном виде.

6. После получения уведомления, указанного в части 5 настоящей статьи, и проверки его достоверности федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, обязан незамедлительно уведомить по системе взаимодействия оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», о возобновлении доступа к информационному ресурсу, в том числе к сайту в сети «Интернет».

7. После получения уведомления, указанного в части 6 настоящей статьи, оператор связи незамедлительно возобновляет доступ к информационному ресурсу, в том числе к сайту в сети «Интернет».

Статья 15.4. Порядок ограничения доступа к информационному ресурсу организатора распространения информации в сети «Интернет»

(введена Федеральным законом от 05.05.2014 N 97-ФЗ)

1. В случае установленного вступившим в законную силу постановлением по делу об административном правонарушении неисполнения организатором распространения информации в сети «Интернет» обязанностей, предусмотренных статьей 10.1 настоящего Федерального закона, в его адрес (адрес его филиала или представительства) уполномоченным федеральным органом исполнительной власти направляется уведомление, в котором указывается срок исполнения таких обязанностей, составляющий не менее чем пятнадцать дней.

2. В случае неисполнения организатором распространения информации в сети «Интернет» в указанный в уведомлении срок обязанностей, предусмотренных статьей 10.1 настоящего Федерального закона, доступ к информационным системам и (или) программам для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» и функционирование которых обеспечивается данным организатором, до исполнения таких обязанностей ограничивается оператором связи, оказывающим услуги по предоставлению доступа к сети «Интернет», на основании вступившего в законную силу решения суда или решения уполномоченного федерального органа исполнительной власти.

3. Порядок взаимодействия уполномоченного федерального органа исполнительной власти с организатором распространения информации в сети «Интернет», порядок направления указанного в части 1 настоящей статьи уведомления, порядок ограничения и возобновления доступа к указанным в части 2 настоящей статьи информационным системам и (или) программам и порядок информирования граждан (физических лиц) о таком ограничении устанавливаются Правительством Российской Федерации.

Статья 15.5. Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных

(введена Федеральным законом от 21.07.2014 N 242-ФЗ)

1. В целях ограничения доступа к информации в сети «Интернет», обрабатываемой с нарушением законодательства

Российской Федерации в области персональных данных, создается автоматизированная информационная система «Реестр нарушителей прав субъектов персональных данных» (далее — реестр нарушителей).

2. В реестр нарушителей включаются:

1) доменные имена и (или) указатели страниц сайтов в сети «Интернет», содержащих информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных;

2) сетевые адреса, позволяющие идентифицировать сайты в сети «Интернет», содержащие информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных;

3) указание на вступивший в законную силу судебный акт;

4) информация об устранении нарушения законодательства Российской Федерации в области персональных данных;

5) дата направления операторам связи данных об информационном ресурсе для ограничения доступа к этому ресурсу.

3. Создание, формирование и ведение реестра нарушителей осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации.

4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в соответствии с критериями, определенными Правительством Российской Федерации, может привлечь к формированию и ведению реестра нарушителей оператора такого реестра — организацию, зарегистрированную на территории Российской Федерации.

5. Основанием для включения в реестр нарушителей информации, указанной в части 2 настоящей статьи, является вступивший в законную силу судебный акт.

6. Субъект персональных данных вправе обратиться в федеральный орган исполнительной власти, осуществляющий

функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, на основании вступившего в законную силу судебного акта. Форма указанного заявления утверждается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

7. В течение трех рабочих дней со дня получения вступившего в законную силу судебного акта федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании указанного решения суда:

1) определяет провайдера хостинга или иное лицо, обеспечивающее обработку информации в информационно-телекоммуникационной сети, в том числе в сети «Интернет», с нарушением законодательства Российской Федерации в области персональных данных;

2) направляет провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в электронном виде уведомление на русском и английском языках о нарушении законодательства Российской Федерации в области персональных данных с информацией о вступившем в законную силу судебном акте, доменном имени и сетевом адресе, позволяющих идентифицировать сайт в сети «Интернет», на котором осуществляется обработка информации с нарушением законодательства Российской Федерации в области персональных данных, а также об указателях страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию, и с требованием принять меры по устранению нарушения законодательства Российской Федерации в области персональных данных, указанные в решении суда;

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в реестре нарушителей.

8. В течение одного рабочего дня с момента получения уведомления, указанного в пункте 2 части 7 настоящей статьи, провайдер хостинга или иное указанное в пункте 1 части 7 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно принять меры по устранению нарушения законодательства Российской Федерации в области персональных данных, указанного в уведомлении, или принять меры по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных.

9. В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного в пункте 1 части 7 настоящей статьи лица уведомления о необходимости устранения нарушения законодательства Российской Федерации в области персональных данных владелец информационного ресурса обязан принять меры по устранению указанного в уведомлении нарушения. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в пункте 1 части 7 настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления, указанного в пункте 2 части 7 настоящей статьи.

10. В случае непринятия провайдером хостинга или иным указанным в пункте 1 части 7 настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в частях 8 и 9 настоящей статьи, доменное имя сайта в сети «Интернет», его сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных, а также иные сведения об этом сайте и информация направляются по автоматизированной информационной системе операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сетевому адресу, доменному имени, указателю страниц сайта в сети «Интернет».

11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств

массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра нарушителей исключает из такого реестра доменное имя, указатель страницы сайта в сети «Интернет» или сетевой адрес, позволяющие идентифицировать сайт в сети «Интернет», на основании обращения владельца сайта в сети «Интернет», провайдера хостинга или оператора связи не позднее чем в течение трех дней со дня такого обращения после принятия мер по устранению нарушения законодательства Российской Федерации в области персональных данных или на основании вступившего в законную силу решения суда об отмене ранее принятого судебного акта.

12. Порядок взаимодействия оператора реестра нарушителей с провайдером хостинга и порядок получения доступа к содержащейся в таком реестре информации оператором связи устанавливаются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

Статья 15.6. Порядок ограничения доступа к сайтам в сети «Интернет», на которых неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»

(введена Федеральным законом от 24.11.2014 N 364-ФЗ)

1. В течение суток с момента поступления по системе взаимодействия в адрес федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, вступившего в законную силу соответствующего решения Московского городского суда указанный орган направляет операторам связи по системе взаимодействия требование о принятии мер по постоянному ограничению доступа к сайту в сети «Интернет», на котором неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием

информационно-телекоммуникационных сетей, в том числе сети «Интернет».

2. В течение суток с момента получения указанного в части 1 настоящей статьи требования оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан ограничить доступ к соответствующему сайту в сети «Интернет». Снятие ограничения доступа к такому сайту в сети «Интернет» не допускается.

3. Сведения о сайтах в сети «Интернет», доступ к которым ограничен на основании решения Московского городского суда, размещаются на официальном сайте федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в информационно-телекоммуникационной сети «Интернет».

Федеральным законом «Об информации, информационных технологиях и о защите информации» предусматриваются права и обязанности субъектов в области защиты информации.

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

(п. 7 введен Федеральным законом от 21.07.2014 N 242-ФЗ)

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Третье направление

Защита информации ограниченного доступа регулируются нормами: института государственной тайны, института коммерческой тайны, института персональных данных, а также нормами защиты других видов тайн.

По третьему направлению Конституция РФ защищает от угроз информационной безопасности следующие информационные права и свободы.

«Статья 29

Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом»

«Статья 33

1. Граждане Российской Федерации имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления».

«Статья 29

2. Каждому гарантируется свобода мысли и слова».

«Статья 44

1. Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

2. Каждый имеет право на участие в культурной жизни и пользование учреждениями культуры, на доступ к культурным ценностям».

«Статья 29

3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них».

Защита информационных прав и свобод обеспечивается нормами институтов интеллектуальной собственности, института документированной информации, УК РФ, КоАП РФ, ГК РФ.

Примеры норм УК РФ: клевета (ст. 129), оскорбление (ст. 130), нарушение неприкосновенности частной жизни (ст. 137), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138), отказ в предоставлении гражданину информации (ст. 140),

нарушение авторских и смежных прав (ст. 146), отказ в предоставлении гражданину информации (ст. 140), нарушение изобретательских и патентных прав (ст. 147), воспрепятствование осуществлению права на свободу совести и вероисповеданий (ст. 148), разглашение тайны усыновления (удочерения) (ст. 155).

Примеры норм КоАП РФ: воспрепятствование осуществлению гражданином Российской Федерации своих избирательных прав либо работе избирательной комиссии; распространение ложных сведений о кандидате; нарушение прав члена избирательной комиссии (комиссии по проведению референдума), наблюдателя или иностранного (международного) наблюдателя; нарушение права граждан на ознакомление со списком избирателей; нарушение условий проведения предвыборной агитации через средства массовой информации; изготовление или распространение анонимных агитационных материалов.

Примеры норм ГК РФ: компенсация морального вреда (ст. 151), защита чести, достоинства и деловой репутации (ст. 152).

Заключая рассмотрение правовых проблем информационной безопасности, отметим, что информационную безопасность можно рассматривать как аспект или ракурс изучения и формирования системы информационного права, подготовки и совершенствования норм и нормативных правовых актов этой отрасли. Используя результаты исследования в области информационной безопасности, законодатель и исследователь отрасли информационного права получают дополнительные возможности совершенствования средств и механизмов правовой защиты информационной безопасности в информационной сфере. Тем самым существенно повышаются качество и эффективность правового регулирования отношений в информационной сфере.

В этой связи структура правового регулирования отношений в области информационной безопасности как бы повторяет структуру самого информационного законодательства, акцентируя внимание на вопросах защищенности объектов правового регулирования, исходя из требований информационной безопасности. В итоге можно построить

некоторую модель основных направлений защиты объектов информационной сферы и институтов информационного законодательства, с помощью нормативных предписаний которых решается проблема правового обеспечения защиты их информационной безопасности. Правовое регулирование информационной безопасности формируется на базе информационных правоотношений, охватывающих все направления деятельности субъектов информационной сферы. Они охватывают все области информационной сферы, всех субъектов и объектов правоотношений.

Объекты правоотношений в области информационной безопасности — это духовность, нравственность и интеллектуальность личности и общества, права и свободы личности в информационной сфере; демократический строй, знания и духовные ценности общества; конституционный строй, суверенитет и территориальная целостность государства.

Субъектами правоотношений в области информационной безопасности выступают личность, государство, органы законодательной, исполнительной и судебных властей, система обеспечения безопасности, Совет Безопасности РФ, граждане.

Поведение субъектов в данной области определяются предписаниями законов и других нормативных правовых актов в порядке осуществления их прав и обязанностей, направленных на обеспечение защищенности объектов правоотношений.

Права и обязанности субъектов задаются нормами законов и иных нормативных правовых актов, устанавливающих правила поведения субъектов в порядке защиты объектов правоотношений, контроля и надзора за обеспечением информационной безопасности. Здесь же вводятся ограничения информационных прав и свобод в порядке защиты интересов граждан, общества, государства. При формировании норм права, установления прав и обязанностей применяются методы конституционного, административного и гражданского права.

Ответственность за правонарушения в информационной сфере устанавливается в порядке: защиты нравственности и духовности личности, общества, государства от воздействия недоброкачественной, ложной информации и дезинформации; защиты личности в условиях информатизации; защиты

информации и информационных ресурсов от несанкционированного доступа (гражданско-правовая, административно-правовая, уголовно-правовая ответственность). Особенности установления ответственности за правонарушения в среде трансграничных информационных сетей, в том числе в Интернет основываются на особенностях и юридических свойствах информации, информационных технологий и средств их обеспечения.

Правовые механизмы защиты жизненно важных интересов личности, общества, государства должны разрабатываться и внедряться в каждой из областей информационной сферы.

1. Область поиска, получения и потребления информации.

Объекты правоотношений: духовность и нравственность гражданина, общества, государства (от воздействия недостоверной, ложной, вредной информации); информационные права и свободы человека и гражданина (право на получение и использование информации); честь и достоинство гражданина (в связи с созданием и распространением недостоверной информации или несанкционированным распространением личной информации о нем).

Субъекты правоотношений: человек и гражданин, потребитель информации, редакция.

2. Область создания (производство) исходной и производной информации.

Объекты правоотношений: информация как интеллектуальная собственность; документированная информация как интеллектуальная и вещная собственность.

Субъекты правоотношений: человек и гражданин, авторы, пользователи исключительных прав, издатели, потребители информации, органы государственной власти и местного самоуправления, органы и системы обеспечения защиты объектов информационной безопасности.

3. Область формирования информационных ресурсов, подготовки и предоставления пользователям информационных продуктов, информационных услуг.

Объекты правоотношений: право авторства и собственности на информационные ресурсы; информационные ресурсы на всех видах носителей, в том числе содержащие информацию ограниченного доступа.

Субъекты правоотношений: человек и гражданин, автор, пользователь, потребитель, участники самостоятельного оборота информации.

4. Область создания и применения информационных систем, технологий и средств их обеспечения.

Объекты правоотношений: автоматизированные информационные системы, базы и банки данных, другие информационные технологии, средства обеспечения этих объектов.

При этом, прежде всего, должны защищаться:

— права авторов и собственников информационных систем и технологий, средств их обеспечения;

— машинные носители с информацией; базы данных (знаний) в составе автоматизированных информационных систем и их сетей от несанкционированного доступа;

— программные средства в составе ЭВМ, их сетей, информационные системы и их сети от несанкционированного доступа;

— информационные технологии и средства их обеспечения.

Субъекты правоотношений: создатели, производители, заказчики, исполнители.

2.3.4. О психологии информационной безопасности

Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

а) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

г) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

Безопасность является важнейшим критерием оценки стабильности систем социальных, политических, экономических, информационных, психологических отношений современного общества.

Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства. В настоящее время существует полемика относительно подходов к обеспечению безопасности. Различные источники по проблемам безопасности трактуют ее по-разному. В одних, безопасность — это качество какой-либо системы, определяющее ее возможность и способность к самосохранению. В других — это система гарантий, обеспечивающих устойчивое развитие и защиту от внутренних и внешних угроз. Рядом экспертов также высказывается мнение, согласно которому за основу следует брать состояние защищенности собственно личности, общества и государства, а не их интересов.

В целом в различных отраслях научного знания понятие безопасности трактуется исходя из особенностей его рассмотрения специалистами соответствующего профиля. Так, в юридической науке безопасность рассматривается как система установленных законами правовых гарантий защищенности личности и общества. С психологической точки зрения понятие «безопасность» раскрывается как ощущение, восприятие и переживание потребности в защите жизненно важных потребностей и интересов людей. В философии безопасность характеризуется как состояние, тенденции развития и условия жизнедеятельности социума, его структур, институтов и установлений, при которых обеспечивается сохранение их качественной определенности, оптимальное соотношение свободы и

необходимости. В политологической трактовке безопасность — это свойство определенной системы и результат деятельности ряда систем и органов государства, а также сам процесс деятельности, направленный на достижение поставленных задач по обеспечению защищенности личности, общества и государства. Также в политологии безопасность может определяться как состояние защищенности материального мира и человеческого общества от негативного воздействия различного рода.

На уровне обыденного сознания понятие «безопасность» определяется как отсутствие опасности, состояние, при котором не угрожает опасность, есть защита от опасности, т. е. как отсутствие угрозы.

В юридической и политической литературе выделяют такие понятия, как безопасность личности, общества (как всего общества в целом, так и отдельных его составляющих) и государства. В наиболее общем плане можно утверждать, что безопасность общества и безопасность государства — это безопасность социальных систем или, в случае рассмотрения социально-политической и информационно-психологической составляющих безопасности — безопасность системы социальных, политических, информационно-психологических отношений общества. Личность, в силу своей принципиальной физической неделимости, не может входить в категорию социальных систем и ее безопасность требует специального рассмотрения.

Как представляется, безопасность является для социальной системы главным условием ее интенсивного развития и прогресса. Следовательно, именно интенсивные процессы развития системы свидетельствуют о том, что система находится в состоянии безопасности и способна выделять на свое развитие достаточно ресурсов, которые в иных, менее благоприятных для системы, условиях тратились бы на защиту от активности источников угроз. Поэтому в данном исследовании мы будем придерживаться следующего определения безопасности.

Безопасность системы социально-политических отношений общества — такое состояние системы социально-политических отношений, в котором социальная система способна успешно, устойчиво и непрерывно развиваться в условиях интенсивного воздействия внешних и внутренних фак-

торов, оказывающих на систему как стабилизирующее, так и деструктивное воздействие.

Признаками безопасности системы являются характеристики (показатели) процесса ее развития, а именно:

— успешность развития системы, т.е. приобретение системой новых качеств в оптимальные (с точки зрения непрерывности процесса развития системы) сроки с минимальными затратами материальных и интеллектуальных ресурсов;

— непрерывность процесса развития системы;

— устойчивость процесса развития системы по отношению к воздействию внешних деструктивных факторов и процессов;

— необратимость процесса развития системы, т.е. приобретение в процессе развития новых качеств, ранее в системе отсутствовавших;

— интенсивность процесса развития системы, т.е. способность системы поддерживать методами внутреннего регулирования необходимый темп (интенсивность) собственного развития для приобретения системой новых качеств, имеющих для нее жизненно важное значение (в первую очередь — качеств, обеспечивающих дальнейшее развитие системы).

Безопасность социальной системы достигается при следующих условиях:

— при установлении состояния динамического равновесия между факторами, дестабилизирующими систему, и факторами, оказывающими на систему стабилизирующее воздействие;

— при доминировании в пространстве возникновения конфликтов, не представляющих угрозу для системы;

— при постоянном, непрерывном, систематическом выявлении, подавлении или локализации активности источников угроз;

— при способности системы динамично изменяться под влиянием внешних и внутренних факторов таким образом, что скорость ответной реакции источников угроз на эти изменения была существенно ниже, чем скорость изменений, происходящих в системе;

— при способности системы редуцировать внешние и внутренние угрозы безопасности до уровня институциональных конфликтов.

Информационно-психологическая безопасность системы социально-политических отношений общества — такое состояние системы информационно-психологических отношений, в котором система способна успешно, устойчиво и непрерывно развиваться в условиях интенсивного воздействия внешних и внутренних факторов, оказывающих на систему как стабилизирующее, так и деструктивное информационно-психологическое воздействие.

Информационно-психологическая безопасность системы социально-политических отношений общества в условиях угрозы внешнего управления — такое состояние системы, в котором система способна успешно, устойчиво и непрерывно развиваться в условиях применения субъектами информационного противоборства по отношению к системе технологий тайного манипулятивного управления.

Информационно-психологическая безопасность системы социально-политических отношений общества в условиях информационно-психологической агрессии — такое состояние системы, в котором система способна успешно, устойчиво и непрерывно развиваться при информационно-психологической агрессии со стороны участников информационного противоборства.

Информационно-психологическая безопасность системы социально-политических отношений общества в условиях информационно-психологической войны — такое состояние системы, в котором система способна успешно, устойчиво и непрерывно развиваться в условиях использования иностранными государствами и иными участниками информационного противоборства арсенала сил, средств и методов информационно-психологической войны в политических целях.

Государство, как специальная политическая надстройка общества — это социальная система и важнейшая составляющая системы социально-политических отношений общества, которая развивается вместе с обществом, часть отношений которого она регулирует. Следовательно, в условиях интенсивного развития системы социальных отношений государство вынуждено изменяться, и целью таких изменений является сохранение или даже увеличение эффективности государственного управления в изменяющихся условиях.

Контрольные вопросы

1. Информационно-психологическая безопасность.
2. Источники угроз интересам общества.
3. Источники угроз интересам человека.
4. Источники угроз интересам государства.
5. Понятие: информационные ресурсы. Информационные ресурсы общества, государства, мировые информационные ресурсы.
6. Понятие, сущность, цели и значение защиты информации.
7. Задачи и значение обеспечения безопасности информации. Виды защищаемой информации.
8. Основные понятия информационной безопасности. Методы, обеспечивающие безопасность информации.
9. Основные составляющие информационной безопасности.
10. Меры защиты от угроз безопасности.
11. Информация как основной объект информационной сферы и системы права.
12. Информационное право. Роль и место в системе права Российской Федерации.
13. О структуре и составе информационного законодательства
14. Область информационных технологий и средств их обеспечения в Интернет.
15. Скрытие информации в технических средствах.
16. Скрытие речевой информации в каналах связи.
17. Концепция и методы инженерно-технической защиты информации; методы и средства инженерной защиты и технической охраны объектов.
18. Основные организационные и технические меры по защите информации.
19. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.

Глава 3
Теория информационной безопасности и национальной стратегии России

3.1. О национальной стратегии информационной безопасности России

3.1.1. О национальной культуре и национальной стратегии информационной безопасности России

Информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти.

Увеличение добавленной стоимости в экономике происходит сегодня в значительной мере за счет интеллектуальной деятельности, повышения технологического уровня производства и распространения современных информационных и телекоммуникационных технологий.

Существующие хозяйственные системы интегрируются в экономику знаний. Переход от индустриального к постиндустриальному обществу существенно усиливает роль интеллектуальных факторов производства.

Международный опыт показывает, что высокие технологии, в том числе информационные и телекоммуникационные, уже стали локомотивом социально-экономического развития многих стран мира, а обеспечение гарантированного свободного доступа граждан к информации — одной из важнейших задач государств.

Динамика показателей развития информационной и телекоммуникационной инфраструктуры и высоких технологий в России не позволяет рассчитывать на существенные изменения в ближайшем будущем без совместных целенаправленных усилий органов государственной власти, бизнеса и гражданского общества. Необходимо уже в среднесрочной перспективе реализовать имеющийся культурный, образовательный и научно-технологический потенциал страны и обеспечить Российской

Федерации достойное место среди лидеров глобального информационного общества.

Обеспечение национальной безопасности страны не может сводиться только лишь к укреплению обороноспособности и обеспечению эффективности специальных структур, охраняющих ее государственные и общественные интересы. Фундаментом такой безопасности являются экономическая независимость, сохранение страной, ее народом самобытной культуры, сознание самоценности последней и основанного на этом чувства собственного достоинства. Страна может многое потерять в материальном плане, но она способна возродиться, пока сохраняет свой духовный, культурно-интеллектуальный потенциал.

В декабре 2015 г. Указом № 683 Президента РФ была утверждена «Стратегия национальной безопасности Российской Федерации». В ней, в качестве целей обеспечения национальной безопасности в сфере культуры названы: сохранение и приумножение традиционных российских духовно-нравственных ценностей как основы российского общества, воспитание детей и молодежи в духе гражданственности; сохранение и развитие общероссийской идентичности народов российской Федерации, единого культурного пространства страны; повышение роли России в мировом гуманитарном и культурном пространстве.

Главной задачей следовало бы считать использование культурной политики как инструмента для создания качественно лучшего общества, где каждый может свободно развивать свои способности и таланты. Реализация этой задачи невозможна без демократизации культуры в целом и поддержки национальных культур как формы выражения национального самосознания. Последнее является одним из важнейших аспектов культурной политики Российской Федерации.

Совершенно очевидна целесообразность и необходимость поддержки культуры и как формы выражения национального самосознания, и как средства воспитания и просвещения широких слоев населения, особенно культурного и эстетического воспитания подрастающего поколения, поскольку от него зависит будущее и культуры, и общества.

Появление новых технологий воспроизведения видео— и аудиопродукции способствовало тому, что сфера потребления культуры все больше стала перемещаться в дом, в связи с чем ряд объектов правового регулирования в сфере культуры требует особенно пристального внимания. Сюда можно отнести, прежде всего, те сферы культурной деятельности, которые в силу присущей им возможности массового охвата населения в наибольшей степени способны воздействовать на сознание людей.

Неизбежно встает проблема контроля за качеством культурных услуг, общей направленности программ и информации, получаемых гражданами через средства массовой информации. Уже существующее здесь законодательство, как показала практика, требует дальнейшего совершенствования, целью которого должно быть создание политически независимых культурных организаций и советов, осуществляющих такой контроль в интересах всего общества, контроль, связанный с порицанием со стороны части общества, не имеющей ничего общего с политической цензурой недавнего исторического прошлого.

Угрозами национальной безопасности в области культуры являются размывание традиционных российских духовно-нравственных ценностей и ослабление единства многонационального народа Российской Федерации путем внешней культурной и информационной экспансии (включая распространение низкокачественной продукции массовой культуры), пропаганды вседозволенности и насилия, расовой, национальной и религиозной нетерпимости, а также снижение роли русского языка в мире, качества его преподавания в России и за рубежом, попытки фальсификации российской и мировой истории, противоправные посягательства на объекты культуры.

Для достижения стратегических целей обеспечения национальной безопасности в области культуры реализуются государственная культурная политика и государственная национальная политика, которые направлены на укрепление и приумножение традиционных российских духовно-нравственных ценностей, обеспечение национальной, религиозной, расовой терпимости, на воспитание взаимного уважения народов Российской Федерации, а также на развитие

межнациональных и межрегиональных культурных связей. Усиливается координация деятельности заинтересованных федеральных органов исполнительной власти и Российской академии наук по реализации государственной культурной политики.

Особое значение для укрепления национальной безопасности в области культуры имеет проведение государственной политики по реализации функции русского языка как государственного языка Российской Федерации, средства обеспечения государственной целостности страны и межнационального общения народов Российской Федерации, основы развития интеграционных процессов на постсоветском пространстве и средства удовлетворения языковых и культурных потребностей соотечественников за рубежом. Россия реализует программы поддержки изучения русского языка и культуры в государствах — участниках Содружества Независимых Государств для ускорения процессов евразийской интеграции.

Разработанная Советом Безопасности Российской Федерации национальная Стратегия информационного развития общества в России, представляет собой политический документ, который закрепляет цель, принципы и основные направления государственной политики в области использования и развития информационных и телекоммуникационных технологий, науки, образования и культуры для продвижения страны на пути к информационному обществу.

В настоящей Стратегии закрепляются цель, задачи, принципы и основные направления государственной политики в области использования и развития информационных и телекоммуникационных технологий, науки, образования и культуры для продвижения страны по пути формирования и развития информационного общества.

Данный документ является основой для подготовки и уточнения доктринальных, концептуальных, программных и иных документов, определяющих цели и направления деятельности органов государственной власти, а также принципы и механизмы их взаимодействия с организациями и гражданами в области развития информационного общества в Российской Федерации.

В Стратегии информационного развития общества учтены основные положения Окинавской хартии глобального

информационного общества, Декларации принципов построения информационного общества, Плана действий Тунисского обязательства и других международных документов, принятых на Всемирной встрече на высшем уровне по вопросам развития информационного общества.

Наиболее полно вопросы национальной информационной безопасности отражены в новой редакции Доктрины информационной безопасности Российской Федерации.

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

В соответствии с Доктриной основными информационными угрозами и негативными факторами, влияющими на состояние информационной безопасности Российской Федерации являются:

— Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности. При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

— Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении

российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

— Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий. Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации.

Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.

Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

— Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

— Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с

использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

— Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.

— Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

— Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

— Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий,

низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы.

— Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.

Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.

Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

3.2. Основы национальной стратеги России

3.2.1. Стратегическая матрица нации

Для России важнейшим историческим, цивилизационным фактором является как данность, что она является матрицей, своей особенной христианской православной белой цивилизации, что накладывает на Россию особые обязательств, связанные с ее предназначением вечно быть основой и опорой этой цивилизации.

Основой стратегической матрицы нации является сама нация, ее историческая ментальность, а также ее «жизненное пространство» как историческое место развития, образ жизни и ареал расселения, а также пространства контролируемые нацией.

В целом основными носителями стратегической матрицы нации являются:

— качество и мощь коренного этноса (титульной нации);

— национальные ценности и мощь национальной культуры;

— образ жизни нации, принимаемый ее большинством как «достойный и правильный»;

— наличие и освоенность достигнутого исторического пространств;

— ресурсная, научная и технологическая самодостаточность;

— военная самодостаточность нации;

— дееспособное национальное управление, имеющее «идею» управления, т. е. национальную стратегию развития и безопасности;

— глобальные информационные ресурсы.

Таким образом, стратегическая матрица нации есть все то, что и делает нацию нацией в качестве объекта и субъекта собственной культуры и истории, дает ей свою собственную, самобытную, неповторимую и однозначную идентификацию и делает ее частью культуры и истории человечества, определяет ее место и роль в мире.

С утратой, «размыванием» или катастрофическим сокращение (развалом, обвалом) «стратегической матрицы» или даже одной из составляющих, вопрос о какой — либо национальной стратегии развития и даже выживании самой нации можно считать снятым.

Поэтому безопасность (сбережение) и развитие стратегической матрицы нации (как совокупность всех ее составляющих), является главной задачей и главной целью национальной стратегии и текущей политики России. Можно констатировать, что в современном мире национальная культура великой державы может считаться цивилизационным оружием.

Россия как цивилизация и великая держава может существовать при условии экспансии своих цивилизационных начал.

Также очевидно, что дальнейшее строительство национальных информационных систем должно осуществляться с учетом этих факторов.

Информационная безопасность самих национальных информационных систем должна удовлетворять требованиям целостности, конфиденциальности, защищенности и надежности, что является не только проблемой технологий, но и проблемой управления самими системами и их информационными ресурсами.

Эффективность защиты национальных информационных систем определяет безопасность управления и инфраструктуру государства в целом. Управление социумом есть исключительно управление информационное, т. е. осуществляется за счет национального информационного ресурса, через информационные сети.

3.2.2. Народ — как позиция

Исходя их исторического опыта развития человечества, можно сделать вывод о том, что в истории человечества главную и окончательную роль играет народ.

Раскрытие рассматриваемой темы неизбежно приводит нас к стратегии формирования национального бытия, базирующегося на исторических основах нашей государственности, и к другим политическим практикам, способным обеспечить развитие России и не допустить национального краха.

Народ — как основа стратегической матрицы нации, это главный субъект перманентной войны за свое выживание, существование и историческое будущее, а значит, главный субъект стратегических действий по изменению реальности своего национального бытия — всегда должен иметь собственную позицию как основу обозначения собственной силы, а также для его обороны или экспансии.

Народ являет собой определенную социальную целостность, которая может быть определена в качестве национальной идентичности как частоты социума, так или иначе имеющей свое (общественное) мнение, а значит, способной

иметь свое представление о собственной сущности, как свою позицию относительно собственного бытия, истории и своего будущего.

Абсолютной аксиомой нашего национального бытия должны стать утверждения:

1. Народ является основной и стратегической матрицей России как великой державы, а государство является только инструментом нации по управлению национальным бытием в целях благосостояния самой нации.

2. Ценности и интересы нации всегда абсолютны и значимы, чем любые запросы государства, и государство обязано следовать за интересами нации.

Основные задачи общества состоят в том, чтобы вырабатывать приоритеты собственного развития и в том, чтобы заставить свое государство руководствоваться ценностями общества.

Также необходимо и важно, чтобы нация — общество, как основатель своего государства и его матрица сформировало и добилось официального признания: своих исторических национальных ценностных основ, как основ своего жизнеустроения и государственности, а также определило и заставило сделать обязательным для исполнения систему обязанностей государства, общества и личности, как основы и рамки функционирования своего социума и государства.

3.2.3. Государство — как основа стратегической позиции

Стратегическая цель государств есть намечаемый результат действий государства стратегического масштаба, достижение которого приводит к коренным позитивным изменениям качества (и международного статуса) самого государства и создает предпосылки усиленного (безопасного) национального развития.

Стратегические действия — некая совокупность согласованных и взаимоувязанных по цели, задачам, месту и времени внутренних и внешних действий (усилий и акций) государства, проводимых по единому замыслу и плану для достижения стратегических целей государства.

Важнейшим геостратегическим фактором успеха России, как государства, является обеспечение безопасности ее стратегической матрицы, основой которой является мощь ее коренного этноса.

На сегодняшний день стратегическими задачами России являются:

1. Выживание России как государства, отдельной цивилизации и суперэтноса.

2. Возвращение России роли и статуса одной из ведущих великих держав и возможность свободно оперировать в геополитическом поле, что подразумевает обеспечение своей успешности и исторической вечности.

Государство должно опираться на национальную стратегическую матрицу.

3.2.4. Информационная сфера нации и ее безопасность

Правовое регулирование общественных отношений, связанных с информацией, происходит в информационной сфере. Информационная сфера — это сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

В информационной сфере происходят информационные процессы — процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации. Помимо перечисленных определений, данном законодателем, к информационным процессам необходимо также отнести процессы создания и применения информационных систем, информационных технологий и средств их обеспечения.

Общественные отношения, возникающие в информационной сфере при осуществлении информационных процессов, называются информационными отношениями. Деятельность по осуществлению информационных процессов называется информационной деятельностью.

Рассматривая информационные отношения, необходимо отметить, что, несмотря на всю их разнообразность, они происходят между составными частями информационной сферы.

Область создания и применения средств и механизмов информационной безопасности обеспечивает защиту информации в других областях. Область создания и применения

информационных технологий и средств их обеспечения осуществляет создание механизмов информационной безопасности и формирование информационных ресурсов, информационных продуктов, оказание информационных услуг.

Субъектом разных областей может выступать одно и то же лицо одновременно. Субъектами могут быть как физические, так и юридические лица. В отдельных случаях субъектом является государство и территориальные образования. Одна и та же организация может одновременно создавать новую информацию, разрабатывать информационные технологии и на их основе формировать из созданной информации информационный продукт, оказывать информационные услуги. Область создания и применения средств и механизмов информационной безопасности является обеспечивающей для всех остальных областей и предназначена для создания инструментов обеспечения информационной безопасности. Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

На основе национальных интересов России в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности. Наиболее тесно данная область взаимодействует с областью создания и применения информационных технологий и средств их обеспечения, а также с областью формирования информационных ресурсов, создания информационных продуктов, предоставления информационных услуг. В каждой области информационной сферы средства и механизмы информационной безопасности решают различные задачи.

Субъектами данной области являются лица, обеспечивающие защиту, и лица, нуждающиеся в этой защите. Защита прав и интересов касается всех субъектов информационной сферы. Что же касается субъектов, обеспечивающих защиту, то они подразделяются на три вида: специализированные государственные организации, юридические лица, оказывающие данные услуги в соответствии с договором, и структурные подразделения в составе самой организации.

Специализированные государственные организации обеспечивают защиту государственной тайны и правовое регулирование в данной области информационной сферы. Данные организации защищают информационную безопасность государства и общества в целом. К ним относятся правоохранительные органы и федеральные органы власти.

Юридические лица, оказывающие договорные услуги по защите информации, обеспечивают защиту коммерческой и служебной тайн. Они также создают новое программное обеспечение и технические средства для защиты информации. Данные субъекты осуществляют свою деятельность на коммерческой основе и оказывают услуги всем остальным субъектам информационной сферы. Отдельно необходимо выделить субъекты, обеспечивающие защиту авторских и смежных прав в информационной сфере. К ним относятся издатели, компьютерные фирмы и другие субъекты, осуществляющие гражданский оборот информации.

Структурные подразделения в составе организаций обеспечивают защиту информации ограниченного доступа, закупают и используют специальное оборудование и программное обеспечение, осуществляют другие мероприятия. Именно структурные подразделения осуществляют большую часть действий по защите информации и обеспечивают информационную безопасность вместе с государственными органами.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы.

Информационная сфера на современном этапе представляет собой совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность

Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

3.2.5. Национальные интересы и национальная безопасность

В российской истории термин «национальная безопасность» впервые был использован в 1995 году в Федеральном законе «Об информации, информатизации и о защите информации». Свое дальнейшее развитие понятие «национальная безопасность» получило в Послании по национальной безопасности Президента Российской Федерации Федеральному собранию от 13 июня 1996 года: «…национальная безопасность понимается как состояние защищенности национальных интересов от внутренних и внешних угроз, обеспечивающее прогрессивное развитие личности, общества и государства».

Национальными интересами на долгосрочную перспективу являются:

— укрепление обороны страны, обеспечение незыблемости конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации;

— укрепление национального согласия, политической и социальной стабильности, развитие демократических институтов, совершенствование механизмов взаимодействия государства и гражданского общества;

— повышение качества жизни, укрепление здоровья населения, обеспечение стабильного демографического развития страны;

— сохранение и развитие культуры, традиционных российских духовно-нравственных ценностей;

— повышение конкурентоспособности национальной экономики;

— закрепление за Российской Федерацией статуса одной из лидирующих мировых держав, деятельность которой на-

правлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях полицентричного мира.

Обеспечение национальных интересов осуществляется посредством реализации следующих стратегических национальных приоритетов:

— оборона страны;

— государственная и общественная безопасность;

— повышение качества жизни российских граждан;

— экономический рост;

— наука, технологии и образование;

— здравоохранение;

— культура;

— экология живых систем и рациональное природопользование;

— стратегическая стабильность и равноправное стратегическое партнерство.

Национальная безопасность как система представляет собой совокупность связей и отношений, характеризующих такое состояние личности, общества и государства, при котором обеспечиваются устойчивое, стабильное существование, удовлетворение и реализация жизненных потребностей, способность к эффективному парированию внутренних и внешних угроз, саморазвитию и прогрессу. С позиции системного подхода можно согласиться с мнением ряда российских исследователей, считающих понятия «национальная безопасность» и «система обеспечения национальной безопасности» близкими по содержанию, обозначающими одноуровневую с национальной безопасностью систему, призванную обеспечить ее существование и развитие.

Безопасность выступает как деятельность, содержание которой формируется в процессе разрешения противоречия между объективной реальностью, заключающей в себе элементы угроз жизнедеятельности хозяйствующих субъектов, и разумными потребностями индивидов, социальных групп и общностей, стремящихся предотвратить эти угрозы, локализовать их и устранить негативные последствия, создаваемые ими. Таким образом, объектом безопасности как деятельности являются угрозы в виде экономических, военных, экологических,

национальных, а конкретными носителями этих угроз являются природные, социальные, общественные процессы.

Виды безопасности

Безопасность имеет многоуровневый характер. В экономике, например, как основе стабильности функционирования государства выделяют следующие **уровни безопасности**:

— индивида (личность),
— фирмы;
— региона;
— страны;
— мирового хозяйства.

В современных условиях резкое возрастание нестабильности затрагивает интересы всех хозяйствующих субъектов. В России негативные процессы, связанные с переходом на рыночные методы хозяйствования, привели к обострению всех типов противоречий в народном хозяйстве:

— экономических;
— социальных;
— экологических;
— правовых;
— национальных и т. д.

Состояние национальной безопасности напрямую зависит от степени реализации стратегических национальных приоритетов и эффективности функционирования системы обеспечения национальной безопасности. А именно.

В сфере **экономики** сокращение исследований в отраслях, обеспечивающих научно-технический прогресс, вызывает противоречие между имеющимся научно-технологическим потенциалом и возможностями его реализации. В результате происходит отток высококвалифицированных кадров за рубеж, разрушается научно-технический потенциал и нарастает опасность деградации наукоемких производств.

В сфере **территориальной организации** производства. Сокращение внутреннего валового продукта и экономическая дезинтеграция усиливают сепаратистские настроения ряда субъектов Российской Федерации. В результате нарастают противоречия, с одной стороны, между отдельными регионами; с другой — между регионами и центром. Это ведет к ослаблению единого экономического пространства, России, нарушению ее федеративного устройства.

В **социальной** сфере. Дифференциация и глубокое расслоение общества на узкий круг богатых и преобладающую массу малообеспеченных граждан, а также ослабление системы государственного регулирования и контроля порождают имущественные противоречия, которые способствуют росту преступности и криминализации общественных отношений.

На международном уровне интересы государства в различных сферах пересекаются с интересами других стран и на этой основе возникают конфликтные ситуации. Преодоление их вызывает необходимость создания системы международной безопасности.

Международная безопасность — это такое состояние системы международных и военно-политических отношений, которое гарантирует безопасность каждой стране, ее функционированию как целостной системы, исключает угрозу возникновения военных конфликтов и обеспечивает разрешение возникающих противоречий путем принятия определенных соглашений без нарушения суверенитета и целостности. Внешняя и внутриполитическая деятельность каждой страны строится с учетом объективно существующих национальных интересов, возникновения потенциально возможных угроз этим интересам и необходимостью противодействия этим угрозам.

Рассмотрим понятие «национальная сила».

Национальная сила государства характеризуется экономической мощью страны, ее природно-географическими возможностями по наращиванию экономического и оборонного потенциала, а также обладанием военной и экономической властью, способной оказывать силовое давление на другие страны.

Индекс «комплексной национальной силы» государства разработан японскими учеными по заказу Национального управления экономического планирования. По определению японских ученых, этот индекс включает три составные части:

— во-первых, «способность вносить вклад в международное сообщество», которая содержит финансово-экономические и научно-технические возможности государства создавать и развивать международные социальные и экономические проекты;

— во-вторых, «способность к выживанию» в кризисных и экстремальных условиях, которая определяется географическим

положением, численностью населения, природными ресурсами, экономической и оборонной мощью государства;

— в-третьих, оценка потенциала «возможного силового давления», которая характеризуется как способность государства навязывать свои решения другим странам, подчиняя их поведение собственным интересам.

Государство оценивается как находящееся в состоянии безопасности, если оно не приносит в жертву свои национальные интересы и если оно, ориентируясь на собственные национальные цели, способно отстоять эти цели путем политических, экономических, социально-психологических, военных и других действий.

В Стратегии национальной безопасности Российской Федерации сделан вывод о том, что угроза национальным интересам России — совокупность условий и факторов, создающая прямую или косвенную возможность нанесения ущерба национальным интересам.

будут представлять:

— односторонний силовой подход в международных отношениях;

— противоречия между основными участниками мировой политики;

— угроза распространения оружия массового уничтожения и его попадания в руки террористов;

— совершенствование форм противоправной деятельности в кибернетической области и в сфере высоких технологий.

Кроме того, усилится глобальное информационное противоборство.

Краткий анализ основных вызовов и угроз безопасности Российской Федерации в условиях современного глобального мира показывает, что существенную роль в их природе и содержании играет военная составляющая.

Угрозами военной безопасности России является превосходство ряда ведущих зарубежных стран в развитии высокотехнологичных средств ведения вооруженной борьбы, формирование в одностороннем порядке глобальной системы противоракетной обороны и милитаризации околоземного космического пространства.

Военная безопасность

Стратегическими целями обороны страны являются создание условий для мирного и динамичного социально-экономического развития Российской Федерации, обеспечение ее военной безопасности.

Достижение стратегических целей обороны страны осуществляется в рамках реализации военной политики путем стратегического сдерживания и предотвращения военных конфликтов, совершенствования военной организации государства, форм и способов применения Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, повышения мобилизационной готовности Российской Федерации и готовности сил и средств. Основные положения военной политики и задачи военно-экономического обеспечения обороны страны, военные опасности и военные угрозы определяются Военной доктриной Российской Федерации.

В целях обеспечения стратегического сдерживания и предотвращения военных конфликтов разрабатываются и реализуются взаимосвязанные политические, военные, военно-технические, дипломатические, экономические, информационные и иные меры, направленные на предотвращение применения военной силы в отношении России, защиту ее суверенитета и территориальной целостности. Стратегическое сдерживание и предотвращение военных конфликтов осуществляются путем поддержания потенциала ядерного сдерживания на достаточном уровне, а Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов в заданной степени готовности к боевому применению.

Совершенствование военной организации государства осуществляется на основе своевременного выявления существующих и перспективных военных опасностей и военных угроз, сбалансированного развития компонентов военной организации, наращивания оборонного потенциала, оснащения Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов современными вооружением, военной и специальной техникой, инновационного развития оборонно-промышленного комплекса Российской Федерации.

Совершенствование форм и способов применения Вооруженных Сил Российской Федерации, других войск, воинских

формирований и органов предусматривает своевременный учет тенденций изменения характера современных войн и вооруженных конфликтов, создание условий для наиболее полной реализации боевых возможностей войск (сил), выработку требований к перспективным формированиям и новым средствам вооруженной борьбы.

Повышение мобилизационной готовности Российской Федерации осуществляется путем совершенствования планирования мер по обеспечению мобилизационной подготовки и мобилизации в Российской Федерации и их реализации в необходимом объеме, своевременного обновления и поддержания на достаточном уровне военно-технического потенциала военной организации государства.

Важнейшими направлениями совершенствования мобилизационной подготовки являются подготовка экономики Российской Федерации, экономики субъектов Российской Федерации, экономики муниципальных образований, подготовка органов государственной власти, органов местного самоуправления и организаций, Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов к выполнению задач в соответствии с их предназначением и удовлетворению потребностей государства и нужд населения в военное время.

Готовность сил и средств гражданской обороны обеспечивается заблаговременно путем проведения мероприятий по подготовке к защите и по защите населения, материальных и культурных ценностей на территории Российской Федерации от опасностей, возникающих при военных конфликтах или вследствие этих конфликтов, а также при чрезвычайных ситуациях природного и техногенного характера. Обеспечение обороны страны осуществляется на основании принципов рациональной достаточности и эффективности, в том числе путем применения методов и средств невоенного реагирования, механизмов дипломатии и миротворчества, расширения международного военного и военно-технического сотрудничества, контроля над вооружением и использования других международно-правовых инструментов.

Прогнозы развития военно-политической обстановки в мире на среднесрочный период, предпринятые российскими

исследователями, показывают, что вблизи границ России активизируется противоборство за доступ к природным, энергетическим, научно-техническим, людским и другим ресурсам на постсоветском пространстве, а также за расширение возможностей, в том числе легальных, по их использованию. В так называемых цветных революциях в Грузии, Украине и Киргизии вмешательство Запада парализовало военно-политическое руководство этих стран, обеспечив их подчинение указаниям западных посольств.

Для организации управляющего информационного воздействия на руководителей независимых государств используется весь арсенал инновационных средств и технологий.

Информационный терроризм стал неотъемлемым атрибутом глобального информационного общества. Его можно считать проявлением крайнего экстремизма в информационной сфере, направленным на достижение политических целей через выдвижение отдельными лицами или организованной группой лиц требований к властным структурам, которые не могут быть удовлетворены в рамках существующего правового поля.

В отечественной литературе достаточно подробно исследован вопрос о потенциальных угрозах национальной безопасности России, включая ее военную составляющую, а также факторы, способствующие возникновению таких угроз.

Первая группа — включает потенциальные угрозы, имеющие геополитическую природу и несущие опасность геополитическим интересам нашей страны, ее геополитическому положению и статусу в мировом сообществе. Они также направлены против территориальной целостности и независимости внешней политики Российской державы.

Вторая группа — состоит из потенциальных угроз, имеющих геоэкономическое измерение и способных нанести ущерб фундаментальным экономическим интересам России, ослабить ее позиции в международных экономических отношениях, создать затруднения для поступательного роста экономического потенциала нашей страны, повышения благосостояния народа и укрепления обороноспособности страны.

Третья группа — это потенциальные угрозы в энергетической и ресурсной сферах, которые могут создавать препятствия

развитию Российской Федерации как мировой энергетической державы, выражаться в претензиях иностранных государств на природные богатства нашей страны, на ее колоссальную базу естественных ресурсов.

Четвертая группа — это потенциальные угрозы, непосредственно имеющие военный характер. Устранение подобных угроз связано с недопущением ситуаций, при которых могла бы быть совершена военная агрессия в отношении Российской Федерации или нападение на ее воинские контингенты и граждан, находящихся за пределами нашего государства.

При исследовании первой группы возможных угроз нашей национальной безопасности, имеющих геополитический характер, следует рассмотреть наиболее существенные факторы, обусловливающие возрастание опасностей жизненно важным интересам Российской Федерации.

В качестве таких факторов могут выступать:

— действия государств, направленные на нарушение целостности Российской Федерации (в том числе с использованием межэтнических, межконфессиональных и других внутренних противоречий) и на удовлетворение территориальных претензий к Российской Федерации со ссылками в отдельных случаях на отсутствие четкого договорно-правового оформления межгосударственных границ;

— действия других стран, направленные на подрыв и сдерживание интеграционных процессов в рамках СНГ, ослабление связей Российской Федерации со странами Центральной, Восточной Европы и Балтии, а также с другими государствами в районах традиционного сотрудничества, приобретающие все более скоординированный характер;

— нарушения прав и свобод русскоязычного населения и граждан Российской Федерации, проживающих в сопредельных государствах, приводящие к нарастанию напряженности и неуправляемым миграционным процессам;

— политика двойных стандартов, проводимая определенными силами за рубежом, которые, заявляя на словах о необходимости обеспечения стабильности в Российской Федерации, в действительности стремятся сделать все от них зависящее, чтобы не допустить этого и тем самым снизить значимость Российской Федерации в решении ключевых про-

блем мирового сообщества и деятельности международных организаций.

Оценивая угрозы геополитического характера, становится очевидным объективная тенденция к расширению в мире конфликтного пространства и, что крайне опасно, его распространению на зону жизненно важных интересов России.

Вторая из рассматриваемых групп угроз включает опасности геоэкономического характера. К данной группе следует отнести следующие основные угрозы:

— стремление ведущих западных стран ослабить экономическую самостоятельность Российской Федерации и закрепить за ней роль поставщика топливно-сырьевых ресурсов для мировой экономики и источника квалифицированной, но дешевой рабочей силы;

— попытки ограничить присутствие России на зарубежных рынках (в том числе на рынке вооружений), а также действия по ее вытеснению с них;

— действия «партнеров», направленные на сохранение ограничений на доступ Российской Федерации к передовым технологиям, создание препятствий для полноправного участия России в международных финансово-экономических и торговых структурах и организациях.

К третьей, из рассматриваемых групп, отнесены угрозы в энергетической и ресурсной сферах.

Специалисты предсказывают быстрое развитие мировой энергетики в первой половине XXI столетия. Согласно оценкам экспертов в ближайшие пятнадцать лет глобальное энергопотребление может возрасти на одну треть, что представляет собой очень высокий рост. При этом спрос в мире на газ будет опережать спрос на нефть. Так, по мнению аналитиков, к 2020 году потребление газа в мировой экономике может вырасти на 60 процентов, а нефти на 42 процента. Однако роль нефти до 2017 года останется ведущей в мировом энергоснабжении. Из этого источника будет обеспечиваться 40 процентов энергопотребления. Соответственно 28 процентов будет приходиться на природный газ, 20 процентов на уголь, 7 процентов на возобновляемые источники и 5 процентов на ядерную энергетику.

В данной связи аналитики отмечают, что в ближайшее время наша страна как обладатель основных мировых

топливно-энергетических ресурсов будет подвергаться сильнейшему геополитическому давлению со стороны стран потребителей. Такое давление согласно прогнозам российских исследователей может осуществляться в следующих наиболее вероятных формах:

— выдвижение новых территориальных претензий к Российской Федерации и заявлений по типу, которые сделали в начале 2007 года бывшая тогда Госсекретарем США Кондолиза Райс и Мадлен Олбрайт (также занимавшая в свое время указанный пост), о том, что в Сибири настолько большие запасы ресурсов, что они принадлежат не России, а миру;

— попытки игнорировать (ущемлять) интересы Российской Федерации в решении проблем международной безопасности, противодействия ее укреплению как одного из влиятельных центров многополюсного мира;

— разжигание новых очагов вооруженных конфликтов, прежде всего вблизи границ Российской Федерации и границ ее союзников (Ближний Восток, Центральная Азия, Кавказ, Балканы) и уже имеется такой очаг на Украине;

— проведение всевозможного рода тайных, подрывных, разведывательных и пропагандистских операций для взятия под контроль добычу и распределение топливно-энергетических ресурсов;

— создание (наращивание) группировок войск (сил), ведущих к нарушению сложившегося баланса сил вблизи границ Российской Федерации и границ ее союзников, а также на прилегающих к их территории морях и уже делается в странах Балтии и бывших странах Варшавского договора — Польша, Румыния.

— расширение влияния Североатлантического альянса, стремление закрепиться на постсоветском пространстве, а также попытки использовать совокупную военную мощь НАТО для оказания военно-политического давления и получения уступок в доступе к топливно-энергетическим ресурсам;

— ввод иностранных войск в нарушение Устава ООН на территорию сопредельных с Российской Федерацией и дружественных ей государств (создание военных баз и размещение группировок войск на территориях бывших республик СССР).

В четвертую из рассматриваемых нами групп объединены потенциальные угрозы, непосредственно имеющие военный характер.

К основным внешним военным угрозам многие российские исследователи, как правило, относят следующие:

— развертывание группировок сил и средств, имеющих целью военное нападение на Россию или ее союзников;

— территориальные претензии к Российской Федерации, угрозы политического или силового отторжения от нее отдельных территорий;

— осуществление государствами, организациями и движениями программ по созданию оружия массового поражения;

— вмешательство во внутренние дела Российской Федерации со стороны иностранных государств или организаций, поддерживаемых иностранными государствами;

— демонстрация военной силы вблизи границ России, проведение учений с провокационными целями;

— наличие вблизи границ Российской Федерации или границ ее союзников очагов вооруженных конфликтов, угрожающих их безопасности;

— нестабильность, слабость государственных институтов в приграничных странах;

— наращивание группировок войск, ведущее к нарушению сложившегося баланса сил вблизи границ Российской Федерации или границ ее союзников и прилегающих к их территории морских водах;

— расширение военных блоков и союзов в ущерб военной безопасности Российской Федерации или ее союзников;

— деятельность международных радикальных группировок, усиление позиций исламского экстремизма вблизи российских границ;

— ввод иностранных войск (без согласия Российской Федерации и санкции Совета Безопасности ООН) на территории сопредельных и дружественных Российской Федерации государств;

— вооруженные провокации, включая нападения на военные объекты Российской Федерации, расположенные на территории зарубежных государств, а также на объекты и сооружения на государственной границе Российской Федерации или границах ее союзников;

— действия, препятствующие работе российских систем государственного и военного управления, обеспечению функционирования стратегических ядерных сил, предупреждению о ракетном нападении, противоракетной обороне, контролю космического пространства и обеспечению боевой устойчивости войск;

— действия, затрудняющие доступ России к стратегически важным транспортным коммуникациям;

— дискриминация, подавление прав, свобод и законных интересов граждан Российской Федерации в зарубежных государствах;

— распространение оборудования, технологий и компонентов, используемых для изготовления ядерного и других видов оружия массового поражения, а также технологий двойного назначения, которые могут использоваться для создания оружия массового поражения и средств его доставки.

Составной частью военной угрозы национальной безопасности Российской Федерации является угроза из воздушно-космического пространства.

Следует отметить, что превращение средств борьбы в воздушно-космическом пространстве в главное оружие современных войн и их интенсивное развитие ведущими зарубежными странами свидетельствует об объективном нарастании этого вида угроз.

Для Российской Федерации опасность угроз из воздушно-космического пространства в известной мере усугубляется особенностями ее геостратегического положения и рядом факторов военно-географического плана, основными среди которых являются:

— большая протяженность границ, площадь территории, низкая плотность размещения объектов вооруженных сил, экономики и инфраструктуры;

— наличие критически важных объектов стратегических ядерных сил, топливно-энергетического комплекса и других потенциально опасных объектов;

— сложность создания достаточного информационного воздействия на важнейших направлениях;

— наличие анклавов (Калининградская область), а также удаленных и труднодоступных районов (Приморье, Сахалин, Камчатка);

— расположение мест добычи и переработки стратегически жизненно важных сырьевых ресурсов в отдаленных труднодоступных районах.

Национальные интересы

Категория «национальные интересы» — одна из наиболее распространенных, и в то же время трудно поддающихся точному определению. Особенно трудно это сделать ныне, поскольку данное понятие широко используется различными политическими силами утилитарно-идеологически как своего рода освящение предлагаемых программ и курсов действия. «Национальные интересы» понимаются как некое олицетворение высших ценностей и целей государства, сообщества, общественного движения. Столь общее определение, естественно, поддается неоднозначным толкованиям, что и происходит в реальной политике и в ее идеологических отражениях.

Национальные интересы можно понимать по-разному. Г. Моргентау определяет их как долговременные, жизненно важные для всей нации выражения общности. В таком случае национальные интересы воплощаются в стремлении представителей одной нации к объединению на основе общности культуры, т.е. языка, семейных, религиозных, моральных, этических традиций и обычаев на основе общей политической системы, общей политики.

Национальный интерес определяется как:

1. Национальный интерес — объективная данность. Он основан, во-первых, на своеобразии геополитического положения государства и связанных с ним особенностях геоэкономического и социокультурного развития; во-вторых, опосредуется особенностями человеческой природы.

2. Государственные деятели обязаны исходить из того, что хорошая политика — это рациональная политика, опирающаяся на правильно понятый национальный интерес. База такой политики — четко выстроенный имидж государства, через который происходит восприятие национального интереса.

3. Национальный интерес кардинально отличается от общественного интереса. Национальные интересы обеспечиваются внешней политикой, а общественные — внутренней. Они не должны ни противопоставляться, ни сливаться.

Национальные интересы делятся на постоянные и преходящие. Постоянные интересы являются основополагающими и включают в себя:

— защиту территории, населения, государственных институтов от внешней опасности;

— развитие внешней торговли;

— обеспечение роста инвестиций;

— защита частного капитала за границей;

— взаимоотношения с союзниками;

— выбор внешнего курса.

К преходящим национальным интересам он отнес:

— интересы выживания нации и государства;

— безопасность и благосостояние общества;

— периферийные, локальные интересы.

Для России к числу важнейших национальных интересов на современном этапе обычно относят:

— предотвращение угроз по всему спектру — главный национальный интерес России;

— территориальная целостность страны;

— сохранение гражданского мира, свободы и прав;

— интересы России в политической сфере, которые обусловлены геостратегическим положением;

— экономические интересы России, которые формулируются как совершенствование концепции национальной экономической безопасности.

Существует различная классификация национальных интересов России. Можно отнести к нашим постоянным интересам:

— братские, дружеские, очень тесные отношения между этносами внутри российской нации;

— обеспечение единства российской территории, российской нации;

— создание и поддержание условий для развития и роста, а не упадка нации, роста ее экономики, науки, культуры;

— всестороннее развитие человека: интеллектуальное и нравственное, индивидуальное и социальное;

— развитие отношений с соседними странами, в первую очередь государствами СНГ;

— поддержание мира, решение глобальных проблем, с которыми столкнулось человечество.

К преходящим интересам России на данном этапе ее развития можно отнести:

— обеспечение интересов русскоязычного населения в странах СНГ;

— укрепление стратегического союза с Арменией и Казахстаном, позволяющего России контролировать Закавказье и Среднюю Азию;

— улучшение отношений с соседними странами (Китай, Монголия, Финляндия, страны Балтии, Средней Азии и др.).

Исходя из географического принципа, национальные интересы России могут быть дифференцированы по следующим группам:

— национальные интересы на территории России;

— интересы России внутри СНГ;

— национальные интересы России в различных регионах мира;

— глобальные интересы России.

Национальные приоритеты

Национальные приоритеты — это первоочередные интересы национальной безопасности для данного периода времени. Комплекс национальных интересов начал формироваться в России в перестроечный период лишь в 1994 г. В экономической литературе высказываются разные подходы определения приоритетов. Это во многом зависит от соотношения экономики и политики, объективного и субъективного. Возьмем, к примеру, преобразование экономической сферы. Если при выборе приоритетов за основу берется политика, то неизбежно экономическое обоснование отодвигается на второй план. Выбор приоритетов приобретает субъективную направленность. Формула выбора приоритетов принимает вид: «политика-экономика». При использовании экономического подхода выбор приоритетов осуществляется путем всестороннего экономического расчета, который приобретает объективную направленность, а формула будет выглядеть как «экономика-политика».

Так, в начале 1990-х гг. важнейшим приоритетом России и восточноевропейских стран являлась приватизация как способ повышения эффективности. В России определяющим

условием приватизации была передача государственной собственности в частную, которая, как правило, осуществлялась в кратчайшие сроки вне зависимости от эффективности, и как итог превращение предприятия в объект фондовых спекуляций, а не в объект эффективных капитальных вложений. Политика превалировала над экономикой. В Восточной Германии в процессе приватизации в качестве исходного принималось инвестирование и на этой основе повышение эффективности и конкурентоспособности путем внедрения новых технологий, недопущение разрушения предприятий. В результате там нет инфляции, идет рост производства, сохраняется стабильность, национальное хозяйство целиком управляемое и регулируемое. Аналогичный подход, как известно, проводится и в Китае, где также решают задачу крупномасштабной модернизации.

При выборе национальных приоритетов в России включаются духовные и культурные ценности; экономическое направление; направление, связанное с сохранением независимости, суверенитета и территориальной целостности страны; проблемы правового характера.

Наиболее полно, на наш взгляд, национальные приоритеты России сформулированы в работе: «Основы экономической безопасности: государство, регион, предприятие, личность», под ред. Е. А. Олейникова. Такими приоритетами являются:

— формирование у нации системы подлинных духовных и культурных ценностей, основанных на истории, традиции и православии;

— сохранение независимости, суверенитета и территориальной целостности страны, ее духовного и культурного наследия, активное противодействие «деидеологизаторам» государственности;

— защита свободы и прав граждан, их безопасность и обеспечение высокого жизненного уровня не как абстрактных либеральных ценностей, а как обязанности Государства перед Нацией;

— возрождение политического развития государства, основанного на национальной идее, идущего в унисон с передовыми тенденциями в развитии человеческой цивилизации и подлинными общечеловеческими ценностями;

— возрождение и развитие национальной экономики, укрепление социальной стабильности в стране на базе новейших достижений науки и техники, поддержка отечественного производителя;

— восстановление внешнеэкономических связей и сотрудничества в соответствии с уровнем и стандартами, существующими между высокоразвитыми государствами;

— обеспечение доступа государства к внешним источникам ресурсов, рынкам, свободы торговли, мореплавания и воздушных сообщений на равных с другими государствами мира условиях;

— ликвидация преступности и правонарушений как угроз национальной безопасности;

— развитие образования, науки и культуры как основы будущего процветания России;

— экономическая безопасность, которая может быть только преимущественно национальной, а не компрадорской (т. е. осуществляющей посредничество между иностранным капиталом и рынком экономики отсталой страны), ориентированной на развитие наукоемких производств и отечественных технологий;

— создание подлинной системы национальной безопасности, обеспечивающей защиту интересов России в мире.

3.3. Государство, информационная безопасность и информационные технологии: основные тенденции

3.3.1. Государство и информационная безопасность

В конце XX века, когда современные информационные технологии интенсивно внедряются во все сферы жизни и деятельности общества, национальная безопасность начинает напрямую зависеть от наличия необходимой и достаточной для ее обеспечения информации. Стремительное развитие информационных технологий все быстрее приближает нас к тому времени, когда значительная часть информационного ресурса страны будет содержаться в электронной форме. Такое положение обязывает искать эффективные и рациональные пути получения, обработки, использования информации, обеспечения ее

сохранности. Последнее приобретает особую важность, так как от сохранности информации, ее полноты все более зависимыми оказываются стабильность в обществе, обеспечение прав и свобод граждан, правопорядок и даже сохранение ценностей государства, вплоть до его целостности, сохранение устоев и традиций нации, ее самоидентификации.

Иными словами существует объективная потребность, как отдельных индивидов, так и социальных групп, государства, общества в целом в информации, т. е. в надежном, эффективном и своевременном осуществлении информационного обеспечения. Можно утверждать, что информационное обеспечение является не только неотъемлемой частью системы национальной безопасности, но и важнейшим условием ее функционирования.

В самом общем виде информационное обеспечение всегда представляет собой специфическую деятельность, которая направлена на подготовку и доведение информации до ее потребителей. Сбор (добыча), переработка, хранение и представление информации представляют собой информационный процесс, который присущ всегда при осуществлении информационного обеспечения применительно к любой сфере или области человеческой деятельности. Однако, чтобы дать определение информационного обеспечения национальной безопасности, следует выяснить его характерные черты, обусловленные спецификой сферы национальной безопасности. Важной чертой информационного обеспечения национальной безопасности служит то, что оно реализуется в строгом соответствии с информационными потребностями субъектов национальной безопасности. Только в этом случае могут быть созданы условия для эффективной деятельности соответствующих информационных структур и их работников по обеспечению информацией нуждающихся в ней потребителей.

В принципе информационное обеспечение национальной безопасности сводится к тому, чтобы субъекты обеспечения национальной безопасности своевременно получали нужную им достоверную и полную информацию о реализации национальных интересов и угрозах им в необходимом и достаточном количестве и удобной форме. Выступая как самостоятельный процесс, информационное обеспечение национальной безо-

пасности имеет свои цели и задачи. В рассматриваемом контексте информационное обеспечение как условие надежного функционирования системы обеспечения безопасности личности, общества и государства — это сбор (добыча) и представление информации, а также установление коммуникаций, открывающих возможность свободной циркуляции широкого и сбалансированного распространения информации, гарантирующих разнообразие источников информации, свободный доступ к ним и обеспечение прав человека в информационной сфере. Цель информационного обеспечения национальной безопасности достигается через решение конкретных задач в информационной сфере. Среди них:

— достижение наиболее полного и своевременного представления информации ее потребителям в сфере национальной безопасности;

— широкомасштабное информационное взаимодействие по выявлению источников опасности и угроз на различных уровнях безопасности;

— улучшение распространения, доступа и обмена информацией по источникам опасности и угроз на различных уровнях безопасности;

— совершенствование распространения, доступа и обмена информацией по вопросам сотрудничества в обеспечении национальной, коллективной и глобальной безопасности;

— формирование общественного мнения (международного и внутри страны) по проблемам обеспечения национальной безопасности;

— изменение стиля работы информационных структур и специалистов.

Цели и задачи определяют специфику содержания информационного обеспечения национальной безопасности, а также требования предъявляемые к нему. Специфика, в свою очередь, проявляется в функциях, т. е. в той роли, которая отводится процессу представления информации на различных этапах обеспечения национальной безопасности.

Далеко не одинаково проявляются функции информационного обеспечения национальной безопасности в различных государствах с различными политическими режимами. В государствах с демократическими режимами имеются необходимые

условия для наиболее полной реализации функций информационного обеспечения во всех сферах, в том числе и национальной безопасности. И совсем другое дело — осуществление информационного обеспечения в условиях полного или частичного табу государственных органов на циркулирование информации. Поэтому представляется необходимым остановиться на общих моментах функционирования, не вдаваясь в детальный анализ осуществления информационного обеспечения национальной безопасности при различных политических режимах.

Следует подчеркнуть, что в отечественной научной литературе функции, выполняемые информационным обеспечением национальной безопасности, оказались неисследованными. Такое положение требует, применяя метод аналогий, осуществить выделение функций с учетом особенностей осуществления информационного обеспечения в сфере национальной безопасности. Представляется, что последние детерминированы самим процессом обеспечения национальной безопасности.

Информационное обеспечение национальной безопасности осуществляется так же с помощью определенных форм и методов деятельности.

В отечественной науке и практике выработано большое разнообразие форм и методов (систем) информационного обеспечения. Информационное обеспечение функционирует в двух основных режимах — текущего информирования и справочного обеспечения. В их основе лежат соответственно две основные структурные составляющие информационной потребности — потребности в текущей информации, позволяющей постоянно отслеживать изменения в сфере национальной безопасности и потребности в разовой, ретроспективной информации, необходимой для решения конкретных задач в этой сфере. При этом разница между этими режимами довольно условна. Виды, формы и способы информационного обеспечения национальной безопасности образуют тот инструментарий, посредством которого силы информационного обеспечения решают весь комплекс задач по наиболее полному удовлетворению информационных потребностей субъектов национальной безопасности.

Выбор тех или иных видов, форм и способов информационного обеспечения зависит от целого ряда факторов, как об-

щего, так и частного характера. Факторы общего характера определяют, прежде всего, существующую в стране систему доведения информации до различных категорий потребителей. К числу таковых можно отнести: существующий политический режим, наличие и развитость демократических норм и ценностей, возможности имеющиеся в распоряжении государства и общества информационных служб, количество и профессиональную квалификацию работников информационной сферы, уровень информатизации и использования передовых информационных технологий.

Факторы частного характера образуют информационную ситуацию, в которой протекает процесс обеспечения национальной безопасности. Это, прежде всего, характер возмущающих воздействий, создающих угрозы национальным интересам, степень их опасности для системы обеспечения национальной безопасности, то есть, их значимость, «удельный вес» в спектре всех опасностей, имеющееся время на подготовку необходимой информации, а также наличие и состав источников информации.

3.3.2. Стратегические цели и основные направления обеспечения информационной безопасности

В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;

г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв

исторических основ и патриотических традиций, связанных с защитой Отечества.

Стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры.

Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение

безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;

д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

е) повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

ж) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

з) совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;

и) повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

Стратегическими целями обеспечения информационной безопасности в экономической сфере являются сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности.

Основными направлениями обеспечения информационной безопасности в экономической сфере являются:

а) инновационное развитие отрасли информационных технологий и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте, в структуре экспорта страны;

б) ликвидация зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет создания, развития и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе;

в) повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности, разработку, производство и эксплуатацию средств обеспечения информационной безопасности, оказывающих услуги в области обеспечения информационной безопасности, в том числе за счет создания благоприятных условий для осуществления деятельности на территории Российской Федерации;

г) развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на мировой рынок.

Стратегической целью обеспечения информационной безопасности в области науки, технологий и образования является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности.

Основными направлениями обеспечения информационной безопасности в области науки, технологий и образования являются:

а) достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;

б) создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

в) проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;

г) развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

д) обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

Стратегической целью обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

Основными направлениями обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства являются:

а) защита суверенитета Российской Федерации в информационном пространстве посредством осуществления самостоятельной и независимой политики, направленной на реализацию национальных интересов в информационной сфере;

б) участие в формировании системы международной информационной безопасности, обеспечивающей эффективное противодействие использованию информационных технологий в военно-политических целях, противоречащих международному праву, а также в террористических, экстремистских, криминальных и иных противоправных целях;

в) создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;

г) продвижение в рамках деятельности международных организаций позиции Российской Федерации, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере;

д) развитие национальной системы управления российским сегментом сети «Интернет».

В целом Российская Федерация, наряду с другими странами, находится в состоянии кризиса традиционных политических коммуникаций. Об этом говорит низкая политическая активность граждан. В ситуации, когда нынешний избиратель всё больше и больше удаляется от политической надстройки общества (которая состоит из органов власти, политических

объединений и прочих политических структур) — та, в свою очередь, вынуждена использовать альтернативные методы коммуникаций, дабы поддерживать связь с электоратом. Среди них, увеличивает свои позиции сеть Интернет.

Интернет, как средство массовой информации, обладает целым рядом значительных преимуществ перед традиционными каналами массовой коммуникации, заключающимся, в самых общих чертах, в следующих параметрах: дешевизна, доступность, быстрота, интерактивность, глобальность, избирательность и др. Появление сетевых СМИ привело к значительному изменению стиля политической журналистики и появлению, так называемой, журналистики в стиле «онлайн». Интернет СМИ являются наиболее распространенным источником политической информации в сети.

В современной России Интернет используется в качестве вспомогательного средства политической коммуникации ввиду серьезных ограничений. С одной стороны, ограничения связаны с фундаментальными характеристиками российской интернет-аудитории. С другой стороны, одной из основных преград в широком распространении интернет-технологий в России является сложившийся стереотип Интернета, как легкодоступного средства размещения непроверенной информации или компрометирующих данных.

Говоря об информационном обеспечении безопасности, связанном с функционированием сетевых коммуникаций и, прежде всего, Интернет, как новой формы коммуникации, целесообразно отметить одновременно как позитивные, так и негативные их свойства.

Первое. Электронные сети обеспечивают возможность не только массовой, но также межличностной и групповой коммуникации. В истории средств коммуникации есть примеры, когда одна технология обеспечивала коммуникацию всех трех уровней. Достаточно вспомнить радио как средство межличностной (диалог по рации), групповой (использование определенной частоты каким-либо ведомством) и массовой (традиционные радиостанции) коммуникации. Принципиальное различие радио и Интернета в нашем контексте состоит в том, что в первом случае различные уровни коммуникации разделены и не смешиваются, тогда, как во втором случае

пользователь сети может одновременно выступать как субъект и межличностной, и групповой, и массовой коммуникации. Кроме того, как подчеркивают специалисты, появление и распространение Интернета стимулирует в современном информационном обществе новые социокультурные процессы, главными из которых, как представляется, являются особые качества общения — открытость, искренность, возможность ухода от традиционного для средств массовой информации желания воздействовать, влиять, воспитывать.

Второе. Интернет с его особыми возможностями обратной связи с воспринимающей стороной и даже стиранием граней между распространителем и получателем информации может в корне изменить все масс-медиа процессы. Открытость, массовость, интимность — все это здесь не противоречия, а синонимы, характеризующие новое качество общения людей. Нет границ, нет пространства, нет цензуры, нет ограничений в визуальном самовыражении, полная и абсолютная анонимность, сочетаемая с аналогичной открытостью, возможностью самому выбирать источник информации и возможность мгновенного отзыва на происходящее.

Бесконечное количество возможностей поиска и выбора обеспечивает каждому пользователю Интернета равноправное и полноценное общение, при котором достигается взаимопонимание мотивов и целей собеседников, то есть подлинный диалог. В связи с этим можно говорить не только о социальной значимости самой сети Интернет, но и социальной значимости любых двунаправленных вариантов общения с прозрачностью и искренностью «разговора».

Третье. Сегодня становится вполне очевидным, что Интернет может оказаться не только средством обмена информацией, диалогического общения и развлечения, но и, как все другие СМИ, использоваться как средство влияния, воздействия. В настоящее время число его пользователей в России, как и во всем мире, растет лавинообразно. Все большее число фирм, предприятий, институтов, школ подключаются к «всемирной паутине». Число пользователей «домашнего» Интернета также все время растет (хотя позволить его могут далеко не все — здесь доминирует материальный принцип), охватывая

едва ли не самую дееспособную часть современного российского общества (как правило, от 15 до 35 лет).

Четвертое. Поскольку специфика сети Интернет обеспечивает любому ее пользователю возможность стать коммуникатором, имеющим неограниченную аудиторию, а самому при этом оставаться персоной анонимной, в крайнем случае, пользующейся псевдонимом, естественен бурный всплеск социальной активности, находящей свое отражение во многих сайтах. Ожидать, что люди, получившие доступ к коммуникации, не воспользуются возможностью высказаться по принципиально значимым для себя и для общества проблемам, не станут искать варианты самоутверждения, было бы наивно.

В последнее время в Интернете появилось огромное количество предложений всевозможных российских коммерческих фирм о продаже самых разнообразных баз данных, содержащих информацию, являющуюся собственностью государственных структур. Этот факт свидетельствует о том, что информационные ресурсы российского государства не защищены должным образом ни в правовом, ни в техническом плане. В этой связи должно быть уточнено понятие собственности на информационные ресурсы и все механизмы обеспечения соответствующих прав собственности. Необходимо также обеспечить правовую защиту конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

Актуализация проблемы защиты информационного пространства и его влияния на информационную безопасность непосредственно связана с существующими реальными и потенциальными угрозами и вызовами безопасности государства, уровень и масштабы которых в последнее десятилетие многократно возросли и приобрели крайне опасный характер.

Информационный век приносит много новых вопросов, которыми должны заняться законодательная и исполнительные власти, — среди них онлайновая безопасность и удостоверение личности, конфиденциальность и защита данных, юрисдикция в киберпространстве и налогообложение электронной коммерции, правовые аспекты коммуникационного общения и ответственность за киберпреступления.

Информационное обеспечение безопасности, как процесс неизбежно приведет к усилению гуманитарно-нравственных начал в отношениях между государствами и народами, а также между социальными группами внутри отдельных государств. Это в значительной степени относится к современной России, у которой ещё велик традиционно-исторический потенциал нерастраченной духовности, но в то же время существует острый дефицит цивилизованной и нравственно богатой идеологии, недостаточность и неразвитость информационной составляющей безопасного существования и развития.

3.3.3. Государство и информационное воздействие

На современном этапе мирового развития возрастает роль информационной сферы и информационных ресурсов. Превращаясь в один из главных факторов жизни общества, они все более активно влияют на состояние политической, экономической, оборонной, личной, имущественной и других составляющих безопасности.

Сотрудничество и соперничество государств из традиционной материальной сферы все более отчетливо смещаются в информационную область.

Современные информационные технологии существенно меняют не только структуру отношений, но и образ жизни людей, их мышление, механизмы функционирования семьи, общественных институтов, органов власти и в целом государства. Они становятся действенным фактором развития личности и общества. В то же время широкое распространение некоторых информационных технологий сопровождается появлением ряда новых угроз конституционным правам и свободам граждан, формированию здоровья, полноценной духовной жизни. Эти технологии уже используются для целей экономики, торговли, рекламы, политической борьбы, оказывая порой разрушительное воздействие на психику людей.

Информационное воздействие становится главным рычагом управления людьми, все больше заменяя физическое воздействие, тысячелетиями считавшееся основным средством управления.

Естественно, одной из главных составляющих национальной, общественной и личной безопасности становится информационная безопасность.

Средства и методы информационного воздействия. Понятие информационной сферы

Информация необходима каждому как условие и как средство существования человека в обществе. И поэтому так же нуждается в защите, как среда обитания, пища и все остальные элементы жизнедеятельности.

Стремительное нарастание возможностей оперативного обмена информацией является великим достижением цивилизации. Однако это достижение в определенных условиях или при неправильном использовании может перерасти в беду.

Если у человека нет информационного взаимодействия с социальной средой, то его личность деградирует. В то же время, информационные технологии являются фактором влияния дезинформации огромных масс людей путем сообщения ложных сведений, создавая информационную сферу.

Информационная сфера в соответствии с новой Доктриной информационной безопасности Российской Федерации является совокупностью информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет»), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Исходя из чего информационная сфера формируется из:

1. Технических средств и информационных технологий.
2. Информационной инфраструктуры.
3. Субъектов информационного воздействия.
4. Общественных отношений, базирующихся на формировании, передаче, распространении и хранении информации.

Информационное противоборство и информационная война

Информационное противоборство — комплексное взаимное информационное воздействие противоборствующих сторон друг на друга, способное привести к принятию благоприятных для инициатора воздействия решений либо вывести

из строя информационную инфраструктуру противника. Методы противоборства: радиоэлектронная борьба, компьютерные атаки, воздействия на мировоззренческом уровнях, вброс дезинформации.

Более острая стадия информационного противоборства — информационная война. Этот термин имеет два значения:

1. Воздействие на гражданское население и/или военнослужащих другого государства путём распространения определённой информации. Термин «информационно-психологическая война» появился в русском языке из словаря военных кругов США. Перевод этого термина («information and psychological warfare») с английского языка может звучать и как «информационное противоборство», и как «информационная, психологическая война», в зависимости от контекста конкретного официального документа или научной публикации. В этом смысле также используется термин психологическая война — психологическое воздействие на гражданское население и (или) военнослужащих другого государства с целью достижения политических или чисто военных целей.

2. Целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем.

Основными целями и задачами информационной войны являются:

1. Информационное обеспечение боевых действий, политики и экономики.

2. Психологическое воздействие на личный состав вооруженных сил и население страны.

3. Хакерское воздействие на информационные системы противника.

4. Подавление радиоэлектронных систем противника.

5. Подавление и уничтожение систем связи и управления противника.

Информационно-технические и информационно-психологические операции широко используются в наступательных и оборонительных целях.

Информационные операции

Одной из основных составляющих частей информационной войны является информационная операция, которая классифицируется на:

1. Информационно-психологические операции.
2. Информационно-технические операции.
3. Наступательные информационные операции.
4. Оборонительные информационные операции.

При наступательных целях используется:

1. Уничтожение информационной инфраструктуры противника.
2. Дезинформация противника.
3. Атаки на информационно-телекоммуникационные структуры противника.
4. Стратегическая маскировка замысла.

Для оборонительных целей используется:

1. Физическая защита информационно-телекоммуникационной инфраструктуры.
2. Подавление, блокировка средств массовой информации противника.
3. Контрпропаганда.
4. Контрдезинформация.
5. Радиоэлектронная борьба.
6. Оперативная и стратегическая маскировка ключевых объектов инфраструктуры.

Информационное оружие

В информационных войнах используются специальные методы воздействия, как, например, информационное оружие.

Информационное оружие — комплекс специальной информации и информационно-телекоммуникационных технологий, создаваемых для деструктивного воздействия, в первую очередь, на армию и гражданское население, а затем, на информационно-телекоммуникационные системы государства.

Основная цель информационной войны и использование информационного оружия — это поражение противника.

Основными задачами использования информационного оружия являются:

1. Дезинформация граждан об исторических корнях, о государственно-политической системе.

2. Провоцирование политической напряженности, поддержка внесистемной оппозиции.

3. Создание атмосферы бездуховности и безнравственности.

4. Подрыв международных позиций государства.

5. Разрушение системы управления войсками, вооружением и военной техникой, а также ключевыми объектами экономики.

Средства и методы информационного воздействия на сознание человека

В конце XX века активно формировались все новые факторы, расширяющие возможности информационного воздействия на человека и более полного управления его поведением. Наряду с появлением принципиально новых технических средств массового информирования людей и глобализацией информационных потоков к числу таких факторов следует отнести бурное развитие поведенческих наук, используемых для разработки эффективных методов и технологий манипуляции сознанием граждан, их отношением к происходящему в окружающем мире.

В настоящее время существуют целые научные дисциплины о том, как управлять поведением человека, коллектива, общества. К ним относятся современные варианты психотерапии, теория рекламы, суггестология, нейролингвистическое программирование, дианетика и т. п. Получил свое теоретическое обоснование гипноз, и были сделаны попытки перенесения методов гипнотического воздействия с отдельного индивидуума на коллективы и целые человеческие сообщества. Все это было невозможно 40–50 лет назад из-за отсутствия эффективных средств массовой информации и научно обоснованных алгоритмов управления социумом.

Нейролингвистическое программирование

В основе концепции ***нейролингвистического программирования (НЛП)*** лежит убеждение, что нашу психику можно уподобить компьютеру, в котором восприятие и обработка информации осуществляется по определенным заданным программам. Первичная информация в ней воспринимается,

структурируется, осмысливается и оценивается на основе внутреннего опыта, состоящего из мыслей, убеждений, ценностей, эмоциональных переживаний, памяти. Один из принципов НЛП: *сознание и тело — части одной управляемой системы.*

Вторым основанием НЛП является убеждение, что можно соединить в единое целое две системы: первую сигнальную систему (система условно-рефлекторных связей, формирующихся в коре больших полушарий головного мозга животных и человека при воздействии конкретных раздражителей: свет, звук, боль) и вторую сигнальную систему (обычная человеческая речь).

Поэтому словосочетание «нейролингвистическое программирование» включает в себя три понятия:

— «нейро» — то, что происходит в мозге и центральной нервной системе;

— «лингвистическое» — то, какими словами мы пользуемся, и как это влияет на наше восприятие внешнего мира и взаимодействие с ним;

— «программирование» — процесс, который позволяет самому человеку (или тому, кто его программирует) решить, как он будет мыслить, чувствовать и говорить.

Специалисты по НЛП работают с так называемыми словесными «якорями», то есть программами, которые незаметно для пациента вводятся в его мозг в виде слов и вызывают проявление того или иного типа поведения. НЛП — это современный вариант кодирования (или перекодирования) психики.

Территория и карты. Один из базовых постулатов НЛП гласит: у человека есть индивидуальный образ мира, его карта. Этот образ всегда субъективен и не тождествен реальности. Он формируется за счет фильтрации внешней информации с помощью языка, личного опыта (персональной истории), особенностей перцептивной системы (специфики работы органов чувств, анализаторов) и, в конечном счете, образует ментальную карту (или психологическую) человека.

Территория — это громадный мир вокруг нас, все события и вещи в нем; тогда как карта — наша модель, наше представление об этом мире.

Ментальная карта — это символическое представление (не обязательно адекватное) в нашей психике реальности, все-

го внешнего и внутреннего мира, это присущая каждому человеку субъективная модель реальности, тех или иных ее фрагментов. Мы воспринимаем мир в ходе повседневного опыта с помощью органов чувств, мозга и языковых систем, посредством которых осмысливается реальность. Первичный материал всегда богаче, чем отображающая его ментальная карта. Поэтому результаты нашего восприятия подобны карте, которая представляет мир, но не копирует его. У всех людей свои, специфические карты, или субъективные модели мира. И они в большей степени, чем сама действительность, определяют то, как мы интерпретируем окружающий мир, реагируем на его сигналы, какой смысл придаем своему поведению.

Нейролингвистические программы определяют, что и как мы воспринимаем и интерпретируем. От их характера и совершенства непосредственно зависят восприятие и обработка информации, образ мышления, ощущения, действия и жизнь вообще. Программы, имеющиеся у разных людей, существенно отличаются не только с точки зрения субъективных ощущений, но и с точки зрения эффективности решения жизненных проблем. Поэтому разные люди неодинаково воспринимают одни и те же события и даже слова и по-разному реагируют на них.

Столь важная роль ментальных карт (программ) в восприятии и отборе стимулов делает их одним из ключевых звеньев в управлении психикой. Они как бы предопределяют и программируют наше общее восприятие и общую реакцию на мир. На протяжении многих тысячелетий ментальные карты формировались преимущественно стихийно с помощью традиционных институтов социализации: семьи, церкви, школы и т. д. В конце XX века стало возможным, как считают создатели НЛП, целенаправленно в сравнительно короткий промежуток времени формировать или по крайней мере существенно изменять наши «программы». Этим, собственно, и занимается нейролингвистическое программирование. Следовательно, НЛП можно рассматривать как процесс анализа и преобразования структуры субъективного опыта человека, обучения его новым формам реагирования на внешние и внутренние стимулы путем модификации старых «программ» или замены их на новые.

Фильтры восприятия — еще одно понятие НЛП. Способности человеческого восприятия ограничены, и нам приходится

выбирать наиболее важное, а все остальное — отсеивать. Поэтому в определенном смысле НЛП — это также наука о фильтрах нашего восприятия, о том, что для конкретного человека важно, а что он отсеивает. Мы не можем видеть или слышать абсолютно все, что нас окружает, мы выбираем то, что нам кажется более важным и интересным, или то, что нам ближе и роднее. Как говорится, что ищем, то и находим.

Все техники НЛП построены на реорганизации информационных процессов человека, создании новых психологических «карт» и фильтров восприятия и, как следствие, изменении в нужную сторону его взаимодействия с реальным миром. Причем изменению подлежит не только поведение индивида, но и внутренние установки, оценочные критерии, весь процесс мышления и принятия жизненных решений.

НЛП стремится манипулировать человеческим сознанием путем подбора кодовых фраз, слов, звукосочетаний, изображений и прочей атрибутики. Цель — пробраться к потаенным инстинктам, чувствам и желаниям ни о чем не подозревающей «жертвы» в обход разума и заставить ее совершать поступки под диктовку навязанных установок.

В ходе программирования учитывается эффект, который раздельно производят на человека:

— слова и их смысловое содержание;

— голос, его интонация и тембр;

— поза, мимика и жесты говорящего.

Пропорции их воздействия выглядят следующим образом:

55 % этого воздействия занимает «язык тела» (позы, движения, мимика), около 38 % — голос (тон, интонации, ритм, тембр) и только 7 % — собственно слова, их смысл. Цифры показывают, что мы должны быть в курсе возможностей вербального и невербального управления нашим поведением, уметь распознавать и адекватно реагировать на различные формы воздействия.

Дианетика как метод и технология манипулирования человеком

Создатель ***дианетики*** — американский писатель-фантаст Р. Хаббард. Начало новому методу было положено изданной им

в 1950 г. книгой «Дианетика» (подзаголовок — «Современная наука душевного здоровья»), ставшей позднее руководством по применению технологии очищения и рационализации психики человека.

Последователи Р. Хаббарда утверждают, что их методика позволяет проникнуть сквозь плотную завесу времени и выяснить, какие события прошлого явились причиной сегодняшних бед человека. Суть *дианетической терапии* заключается в том, чтобы провести индивида через сохранившиеся в подсознании «критические точки» и путем их повторного переживания излечиться от связанных с ними недугов.

В этом и состоит технология данной терапии, процесс которой называют *одитингом,* а того, кто его проводит, — *одитором.* Пациент с помощью одитора как бы «проживает», находясь в особом состоянии, всю свою жизнь с момента зачатия, натыкается на «болевые точки» и неоднократно их переживает — до тех пор, пока накопленная в них негативная энергия не разрядится полностью. В итоге человек получает свободный от былых кошмаров и комплексов, «чистый», разум. И только разум! Все иное — чувства, эмоции, переживания, влечения и т. п. — ему теперь не нужны.

Дианетика — это наука о Разуме и мышлении. Для нее человеческий ум — «превосходная вычислительная машина», «отлично построенный компьютер». В освобождении от всех других волнительных для человека особенностей психики эта наука видит залог вечно счастливой жизни. Р. Хаббард был убежден: «В сегодняшнем мире нет ни одной проблемы, которая не могла бы быть разрешена одним только разумом».

С точки зрения инженерно-компьютерного понимания человека дианетика перекликается с НЛП. Новейшие методики призваны обеспечить возможность работать с человеком как с машиной. Но для этого необходимо избавить его от всего собственно человеческого — способности и потребности переживать, любить, сострадать, поступать «по совести». Оставить только очищенный разум. Тогда человек станет прекрасным природным компьютером, и им можно будет без каких-либо проблем управлять (манипулировать), вводя программы и нажимая на клавиши (или меняя интонации голоса). Таков в своей глубине замысел и дианетики, и НЛП.

Сайентология

Идеологической вершиной дианетики стала созданная Р. Хаббардом на ее основе прикладная, фактически религиозная, философия — сайентология.

Руководствуясь своей философией, последователи дианетики готовы переделать внутренний мир миллионов людей, структуры власти и государства. Сайентологи почти открыто действуют, собирая любую информацию, связанную с исполнительными органами власти, структурами правопорядка, средствами массовой информации, с деятельностью основных религиозных конфессий, а также иными организациями, имеющими влияние в обществе или оказывающими какое-либо воздействие на принятие государственных решений — например, банки, профсоюзы, крупные предприятия.

В соответствии с заветами Р. Хаббарда сайентологи стремятся продвинуть на ключевые посты любых структур и организаций своих людей или добиться сочувствия своим идеям от лиц, нужные посты уже занимающих. При необходимости сайентологи прибегают к подкупу, шантажу, прямым угрозам.

Внушение и гипноз

Внушение — один из наиболее распространенных и важнейших методов манипулирования сознанием человека. Оно представляет собой преимущественно скрытое воздействие на подсознание и отчасти сознание индивида с целью изменения его общего состояния и отдельных характеристик психики — установок, ценностей, убеждений и т. п.

Внушение осуществляется с помощью слов, взглядов, жестов, образов и других средств передачи информации. В зависимости от средств воздействия выделяются два основных вида внушения:

— вербальное — с помощью речи;

— невербальное — посредством жестов, определенных форм поведения, создаваемых образов и т. п.

При внушении с помощью речи главное воздействие на внушаемого чаще всего оказывает не значение слов и предложений, не логическая аргументация, а построение речи, ее форма, источник и сопутствующая ей паравербальная информация: интонация, громкость, темп, дикция, образность и т. п.

Внушение может быть прямым и косвенным. Прямое внушение характеризуется открытостью влияния, четкой формулировкой требований, непосредственной направленностью на конкретного индивида.

Косвенное внушение в большей мере относится к методам манипулирования и обычно является составной частью манипуляционных акций. Оно осуществляется без прямых требований, с помощью опосредованного воздействия, путем намеков, незаконченных фраз. В этом случае более широко используется паравербальная информация.

Внушение неодинаково действует на разных людей. Это действие зависит также от состояния, в котором находится человек, и его возраста. Наиболее восприимчивы к внушению люди эмоционально неустойчивые, впечатлительные, имеющие неуравновешенную нервную систему, а также находящиеся в ослабленном, переутомленном или встревоженном, растерянном состоянии, неоформившиеся в возрастном и личностном отношениях.

По мнению ряда авторов, многовековое воздействие цивилизационной культуры стабилизирует нервную систему человека и снижает влияние внушения на его психику. Поэтому более восприимчивы к внушению, в частности, представители традиционных сообществ и народов стран «третьего мира», не прошедших длительную цивилизационную эволюцию.

Внушение основано на некритичности восприятия и предполагает, как правило, неспособность внушаемого сознательно контролировать поток поступающей информации. Необходимым условием внушающего воздействия является авторитетность источника информации.

Факторы эффективности внушения. В современной литературе к числу таких факторов чаще всего относят:

— личные качества субъекта внушения (суггестора), наличие у него соответствующих способностей, личное обаяние, уверенность в себе, чувство внутреннего превосходства, авторитетность, а также знание техник внушения и умение их использовать;

— личные качества и состояние объекта внушения. Более внушаемым человека делают тревожность, неуверенность, робость, низкая самооценка, впечатлительность, повышенная

эмоциональность, ограниченный жизненный опыт и конкретное состояние, определяющее восприимчивость к внушению;

— отношения между субъектом и объектом внушения. Успеху способствуют взаимное доверие и уважение, а также способности первого подстроиться (подключиться) к внутреннему миру объекта общения и «вести» его в нужном направлении;

— ситуация, уровень личностной значимости происходящего для объекта внушения, дефицит времени, неожиданность;

— конструкция сообщений в ходе процесса внушения. Наиболее эффективны сообщения, имеющие образную форму и даже кажущиеся бессмысленными, но способные непосредственно обращаться к подсознательному уровню человеческой психики.

Как показывает практика, за счет сочетания ярких, красочных образов, эмоциональных комментариев и т.п. сообщения суггестора способны достигать бессознательных уровней психики без какого-либо адекватного рационального осмысления, вызывая при этом определенные чувства и поведенческие реакции. Для усиления возможностей внушающего воздействия речевые сообщения могут сопровождаться видеозаписями, движениями, музыкой и т. п. Внушение может проводиться в состоянии бодрствования или гипнотического сна.

Гипноз — это внушаемый сон. Существуют различные стадии гипноза, различающиеся по тонусу коры головного мозга, ее активности, глубине транса.

Само слово «гипноз» появилось в середине XIX века, но состояния, которые оно обозначает, наблюдались еще у истоков цивилизации. Уже в те времена использование данного состояния было связано как с лечебным эффектом и появлением, в частности, «чудесных исцелений», так и с попытками поставить его на службу личным и кастовым интересам отдельных групп людей, особенно служителей религиозных культов.

В одном древнем папирусе, который египтологи рассматривают как копию с еще более раннего утерянного текста, есть следующая запись: «Принеси опрятную и очищенную лампу, наполни ее лучшим ароматным маслом и повесь ее на клин из куска лаврового дерева на стене, расположенной с внутренней стороны. Затем поставь перед ней мальчика. Погрузи его в сон твоей рукой и зажги лампу. Произнеси над ним слова заклина-

ний до семи раз. Снова разбуди его и спроси так: «Что видел ты?» Ответит он: «Да! Я видел богов вокруг лампы». Тогда будут говорить ему боги все, о чем их будут спрашивать».

Налицо описание одного из вариантов гипнотического навязывания человеку определенных представлений и попытки управления его мыслями через эти представления.

В современной практике гипноз широко используется в медицине, педагогике, спорте, промышленности, искусстве и других сферах человеческой деятельности:

— как метод лечения, прежде всего психических расстройств;

— как метод извлечения «забытой» информации;

— как метод программирования психики и управления человеком через скрытое навязывание ему определенных представлений, намерений, моделей поведения.

Не менее вероятно его использование в преступных целях, а также для решения определенных задач в ходе любого информационного противостояния. Гипноз особенно привлекателен для разного рода манипуляторов и мошенников. Он позволяет отключить разум и критическое мышление, быстро, без использования каких-либо аргументов записывать в мозг человека определенную информацию, закладывать те или иные эмоционально-поведенческие установки и таким образом предопределять его будущее поведение.

Эффективность гипноза, как и любого внушения, прежде всего зависит от психологических особенностей пациента, его состояния в данный момент, а также от личных возможностей и умения гипнотизера.

В современной психотерапии различают две группы методов введения в гипноз как в особое состояние сознания:

— методы многократно повторяющегося воздействия монотонными раздражителями на различные анализаторы (органы чувств);

— шоковые методы, при которых особое состояние сознания вызывается внезапным действием сильного раздражителя (вспышка света, сильный звук, слабый удар электрического тока), сопровождаемого категорическим приказом (например, «Спать!»).

Издавна для введения людей в транс (слабая форма гипноза) используется музыка. Звуковое и ритмическое воздействие

лежит в основе любой религиозно-мистической системы. У древних и современных народов бой барабанов, ритмичные танцы и песнопения являются средством введения людей в транс и повышения эффективности сопутствующего словесного внушения.

Средства манипуляции человеческим сознанием

К числу средств, используемых при реализации вышерассмотренных методов манипуляции человеческим сознанием, можно отнести:

— средства массовой информации (радио, пресса, телевидение, Интернет);

— агитационно-пропагандистские и учебные материалы (видеокассеты, электронные и печатные учебники, энциклопедии, наглядные пособия, рекламную продукцию и др.);

— произведения литературы (художественной, научно-технической, общественно-политической, публицистической, специальной) и искусства (в том числе различных направлений массовой культуры);

— энергоинформационные средства (специальные генераторы, передающие устройства и излучатели электромагнитных волн и импульсов, радиоэлектронные приборы и др.);

— лингвистические средства (языковые единицы, «специальную» терминологию, обороты речи, имеющие семантическую неоднозначность при переводе на другие языки и др.);

— психотропные средства (особым образом структурированные лекарства, психофармакологические и психодислептические препараты, транквилизаторы, антидепрессанты, галлюциногены, наркотики, алкоголь и др.);

— личное индивидуальное и групповое общение (учебное, профессиональное, деловое, семейное, повседневное и др.).

В России литература всегда была важнейшим средством духовного и нравственного воспитания подрастающих поколений, приобщения молодежи к возвышенным мыслям и романтике. Увы, и литература не избежала пагубных тенденций и используется разными силами как средство манипуляции сознанием людей.

Книжный рынок заполнен произведениями, кодирующими читателя на либерально-потребительский, свободный от социальных обязанностей стиль жизни. За яркими обложками

можно найти скрытую пропаганду наркотического «расширения» сознания, изобилие неформальной лексики, порнографические сцены, смакование актов насилия, рекламу товарных брендов, алкоголя и табака. Прямо или косвенно такой информацией наполнены многие романы, детективы, новомодные исторические творения, утратившая элементы научности фантастика.

Приемы и методы защиты от манипулирования

Для защиты от манипулирования необходимо знать не только его методы и средства, но и ряд общих условий, расширяющих возможности воздействия на психику человека.

Обработка человека всегда начинается с ослабления или отключения его способности сопротивляться. Это — первый этап и главнейшая задача для любого манипуляционного метода: и для НЛП, и для дианетики, и для гипноза. На данном этапе могут использоваться самые разные приемы и эффекты, помогающие удивить, поразить, «сбить с толку» человека. Вполне годится здесь и скрытое энергоинформационное воздействие или легкое наркотическое опьянение, маскируемое обрядовыми напитками, благовониями. Главное — заморочить человеку голову настолько, чтобы он разрешил себе измениться.

Этот принцип далеко не нов. Его знали еще христианские миссионеры средних веков. Огромные храмы, органная музыка, изобилие цветов. Цель состояла в том, чтобы нарушить душевное равновесие и внутренний покой человека, обеспокоить его, ослабить существующие стереотипы и шаблоны представлений. В таком состоянии человек готов прислушаться к любому мнению, принять любую, кажущуюся спасительной установку.

И сегодня человек, находящийся в состоянии удивления, восхищения, внутреннего распутья или возмущения, — самая удобная жертва не только для гипнотизеров, специалистов НЛП и дианетики, но и для религиозных сектантов и политических демагогов.

Еще одно важное условие, на которое следует обращать внимание, связано с речью манипулятора. Мы привыкли в любой речи прежде всего улавливать ее логику и смысл. Однако в большинстве методов на нас скрытно воздействуют интонации,

жесты, позы, мимика, движения рук и выражения глаз, эмоциональные переходы и т. п. Именно эти эффекты адресованы нашему подсознанию, которое, как известно, обычно побеждает сознание. И устоять против такого воздействия (вспомним автора «Властелина колец») может «только твердейшая воля и устремленная мысль», разумная установка на «спасительное недоверие» к обещаниям счастья и богатства.

Метод самовнушения. Если манипуляции подвержен психологически издерганный человек, то защитой от нее будет своевременное улучшение и, по возможности, постоянное поддержание хорошего психического самочувствия. Сегодня самовнушение, медитация является одним из основных методов внутренней саморегуляции и восстановления психического равновесия. Человек, использующий данный метод, должен сформировать индивидуальное словесное утверждение, направленное на регуляцию собственного состояния. Формулировки должны быть простыми, утвердительными, позитивно окрашенными: «Мой страх (моя наивность) полностью исчезает»; «Я спокоен, уравновешен, способен анализировать ситуацию»; «Мой организм способен вырабатывать вещества, которые помогут сохранить спокойствие и увидеть ложь, нечестные помыслы мошенника» и т.п. Словесные формулировки наиболее эффективны при мысленном проговаривании в ходе воздействия манипулятора.

3.3.4. Формы ведения информационной борьбы

Можно говорить о том, что на современном этапе развития общества в большинстве стран наблюдается так называемая «*информатизация*» — организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, предприятий, организаций, государства, всех структур общества на основе организации информационных ресурсов с использованием перспективных информационных технологий.

При этом нередко возникает проблема обеспечения *безопасности информации* — защиты информации от случайного или преднамеренного доступа лиц, не имеющих на это права, ее получения, раскрытия, модификации или разрушения — как

на уровне отдельных предприятий (и даже их структурных подразделений), так и на уровне государства в целом.

При этом обеспечение информационной безопасности может происходить самыми разными способами. Иногда при возникновении прямого конфликта интересов, который не может быть решен «мирно» или силы не считают данный способ достаточно приемлемым для себя, возникает процесс так называемой *информационной борьбы* — особой формы борьбы двух и более сторон, предусматривающей использование специальных политических, экономических, дипломатических, военных и иных методов, способов и средств воздействия на информационную среду противостоящей стороны в интересах достижения поставленных целей.

Суть информационной борьбы

Итак, рассмотрим информационную борьбу более подробно.

Само ее появление, как особого вида противоборства сторон, представляется достаточно логичным: в современном мире, с его постепенным переходом к информационному обществу, возрастающей ролью информации и возникающей необходимостью обеспечивать ее безопасность.

При этом информационная борьба условно делится на две составные части:

— определенное воздействие на информационную среду противника (с использованием специальных средств);

— обеспечение собственной информационной безопасности.

Отсюда можно сделать вывод о том, что главной целью информационной борьбы является обеспечение собственной информационной безопасности и максимальное снижение информационной безопасности противника.

Составными элементами цели, в свою очередь, является ряд задач, наиболее важными из которых являются:

— разработка общей стратегии ведения информационной борьбы;

— разработка плана мероприятий по обеспечению собственной информационной безопасности и ее непосредственному укреплению;

— разработка плана подрыва информационной безопасности соперника с минимальными затратами для себя;

— поражение объектов информационной среды противника.

При этом отбору задач должно уделяться достаточно времени и внимания, потому что чрезмерное их количество (переоценивание противника) и количество недостаточное (недооценивание сил противника) вполне может привести к поражению в информационной борьбе.

При этом в отличие от иных видов борьбы, в частности, прямого военного столкновения, информационная борьба ведет постоянно, даже в мирное время (в военное время — усиливается). При этом масштаб ведения борьбы может сильно варьироваться: от конкретного объекта информатизации до государства в целом.

Таким образом, можно говорить о необходимости специальной подготовки к ведению информационной борьбы — как в плане сбора необходимых, в особенности числе человеческих ресурсов, так и в плане разработки своеобразного плана ведения борьбы.

Исследователи выделяют четыре этапа развития информационного противоборства:

1. Первый этап (этап древности) — информационное обеспечение боевых и повстанческих движений.

Противоборствующие стороны «пытались использовать средства духовного воздействия, чтобы ослабить дух и боевую мощь противника, а также поднять боевой дух своих войск». Основным средством доведения информации выступал человек, объектом воздействия выступала психика его врагов или союзников (в зависимости от целей информационного воздействия). Формы ведения были строго ограничены вербальными технологиями и включали в себя: выступления ораторов, распространение слухов, прямую дезинформацию, аресты, убийства ораторов и т.д.

2. Второй этап — «бумажный»

Начался с появления письменности и распространения грамотности среди населения. Характеризуется появлением новых форм ведения информационного противоборства (в частности — листовок, используемых до сих пор).

3. Третий этап — возникновение принципиально новых носителей информации.

Появление фотографии, изобретение телеграфа, телефона, радио и кино значительно расширили спектр средств и форм ведения информационного противоборства. Стало возможным оказание оперативного, долгосрочного, избирательного, массового и иных видов воздействия на человеческое сознание. Однако психика противника перестала быть единственным объектом для информационных атак: воздействие стало производиться и на информационно-технические системы и комплексы (например, подавлялось радиовещание на территории противника). Именно в этот период зародились так называемые «информационные войны» — особая форма ведения информационной борьбы.

4. Четвертый этап — современный.

Начался в результате принципиально важных изменений всех сфер человеческой деятельности связанных с изобретением персональных компьютеров и компьютерных сетей разной степени охвата, телекоммуникационных сетей. Именно компьютерные носители стали основными, важнейшим же средством ведения борьбы стали вышеозначенные сети. Появилась уникальная особенность оказывать информационное воздействие максимально скрытно, без привязки к конкретным персоналиям, а иногда — и к воздействующему в целом.

Среди принципов ведения информационной борьбы на современном этапе развития можно выделить следующие:

— соответствие целей и задач, поставленных в информационной борьбе основополагающим политическим целям (приемлемо на уровне государств);

— заблаговременная подготовка ресурсов, сил и средств для ведения информационной борьбы;

— сосредоточение нужных средств в нужном месте (рациональное их применение, четкое соответствие выбранной цели и задачам);

— высокая активность и решительность в проведении запланированных мероприятий (позволяет «опередить» соперника);

— внезапность (неожиданно для соперника, в том числе путем маскировки или дезинформации).

Содержание информационной борьбы достаточно индивидуально в каждом конкретном случае и в значительной мере

зависит от политических, экономических, духовных и иных факторов, влияющих на каждую из сторон информационного противоборства. Исходя из данных факторов формируются цели, задачи, выбираются средства ведения. В свою очередь количество и качество выбранных средств определяет формы и способы информационной борьбы, а также ее итоговую эффективность.

Существуют различные классификации форм ведения информационной борьбы, а именно:

1. Информационная акция.
2. Информационная атака.
3. Информационный удар.
4. Информационная операция.
5. Информационная кампания.
6. Информационная война.

Информационная акция

Информационная акция является одной из основных и наиболее распространенных форм ведения информационной борьбы. В ряде источником упоминается под названием «информационное мероприятие».

Информационная акция представляет собой ограниченное в пространстве и во времени информационное воздействие на конкретной информационный объект или группу объектов противника, а также защиту от воздействия со стороны враждующей стороны конфликта (поступающего как в ответ на уже свершенные действия, либо действия превентивные).

Информационная акция не отличается масштабностью распространения, чаще всего длится весьма ограниченное время: в среднем от несколько минут или часов до нескольких недель.

Объектом информационной акции выступают:

— отдельные представители из населения страны-соперника;

— отдельные социальные группы людей, группы, отобранные по критерию, напрямую или косвенно связанные с желаемой целью акции;

— конкретные информационные объекты соперника (в том числе телекоммуникационные и радиоэлектронные центры);

— отдельные элементы инфраструктуры информационных объектов соперника.

Под воздействием в данном контексте понимается, во-первых, непосредственное применение различных видов информационного оружия, воздействие на элементы информационного пространства противника доступными и заранее выбранными для этого средствами, а во-вторых — согласованное по целям, задачам, месту и времени мероприятие по воздействию выбранных средств на информацию и информационные (отдельные) объекты противника.

В качестве возможного результата среднестатистической информационной акции могут бы названы следующие последствия для страны-противника:

— дезориентация и дезинформация отдельных персоналий и групп населения;

— нанесение ущерба морально-нравственному климату в обществе;

— нанесение ущерба информационным объектам.

Информационная атака

Информационная атака также является достаточно распространенной формой ведения информационной борьбы.

Под данным термином стоит понимать однократное информационное и/или физическое воздействие на одиночный информационный объект противника, т.е. совокупность неких действий, приводящих к нарушению информационной безопасности информационной системы противника.

Целями информационной атаки могут быть самые разнообразные объекты информационной среды противника, в том числе:

— крупные серверы;

— рабочие станции пользователей;

— телекоммуникационное оборудование.

Жизненный цикл информационной атаки также может быть уникальным, с рядом присущих только ему особенностей, в каждом конкретном случае, но в общем смысле включает в себя:

1. Рекогнисцировку.

Сбор информации об объекте атаки (типе и версии (Операционная Система), списке зарегистрированных в системе пользователей, сведения об используемом в системе

программном обеспечении), планирование конкретных мероприятий вторжения.

2. Вторжение.

Получение несанкционированного доступа к серверам противника, хранящим информацию.

3. Атакующее действие.

Практическая реализация целей и задач конкретной информационной атаки. Нередко включает в себе маскирование или удаление внешних следов атаки, своего присутствия в чужой информационной системе.

4. Развитие атаки.

Расширение объектов атаки (как поиск новых, так и внедрение в иные информационные части уже затронутых).

В целом можно говорить о том, что любая атака основана на наличии в любой современной информационной системе определенных уязвимых мест. Это могут быть ошибки при конфигурации сетевых служб, ошибки в программном обеспечении, использование «слабых» паролей, отсутствие необходимых средств защиты и даже ошибки руководства информационного объекта в проведении политики защиты данных, в особенности — конфиденциальных.

Результатом успешной атаки могут стать:

— несанкционированный доступ противника к закрытой информации, находящейся в пределах информационной системы;

— удаление или модифицирование хранящихся на серверах противника данных;

— нарушение работоспособности информационной системы.

При этом можно заметить определенное сходство информационных атак с вышеназванными информационными акциями, однако, эти две формы информационной борьбы не полностью тождественны друг другу. Так, атака подразумевает именно враждебное вторжение в информационную среду противника, тогда как акция может быть мероприятием более «мирным», направленным на укрепление собственной информационной безопасности. При этом информационная акция может быть направлена на широкий круг объектов, в то время как атака подразумевает информационное воздействие на

единичный объект. Информационная акция направлена, прежде всего, на человека (или группы людей) и человеческую психику, тогда как атака — на технические объекты, в частности, из системы коммуникаций. Наконец информационная акция чаще всего имеет больший масштаб и является более протяженной во времени.

Информационный удар

Под информационным ударом принято понимать некую совокупность информационных атак, четко согласованных между собой и преследующих одну и ту же главную цель. В свою очередь целью является поражение одного или нескольких важных элементов систем противника, а также получение информационного превосходства над противником.

При этом достаточно распространенным средством достижения цели информационного удара является негативизация выбранного объекта противника как путем прямой дезинформации и подмены данных, так и путем распространения слухов и иных методов.

Информационные удары чаще всего кратковременны, массированы, направлены на ключевые объекты противника. При этом характерной особенностью ударов является сочетание информационной атаки с прямым физическим воздействием на ключевые объекты информатизации противника.

Объектами, которые чаще всего подвергаются информационным ударам, можно назвать следующие:

— элементы информационной инфраструктуры противника;

— системы телекоммуникации;

— системы управления (военного и гражданского);

— важнейшие информационные средства противника.

Информационные удары нередко применяются до начала военных действий или в период их зарождения. Так, нередко проводится подавление радиоэлектронных и телекоммуникационных средств противника, подкрепленное физическим уничтожением ключевых объектов и инфраструктуры с применением специальных видов вооружения.

Соответственно, логичным результатом информационного удара могут быть следующие последствия для сил противника:

— повреждение и захват радио и телекоммуникационных средств;

— физическое уничтожение объектов информатизации;

— дестабилизация связи между отдельными частями сил;

— дезинформирование, подрыв морального настроя сил.

Информационная операция

Информационная операция является более крупным элементов информационной борьбы, чем все названные ранее. При этом она же считается основной формой ведения информационной борьбы.

В строгом смысле слова она представляет собой сложную совокупность информационных атак, акций и ударов с общими целями, задачами, объектами информационного воздействия и временем проведения. Осуществляются как последовательно, по заранее определенному и разработанному специалистами плану мероприятий по ведению информационной борьбы, так и одновременно, взаимодополняя друг друга.

Проводится как в мирное, так и в военное время: в первом случае воздействие ведется, в первую очередь, на психику отдельных групп населения противника с целью создать у них определенное представление о той или иной сфере жизни оппонента, во втором же, на первый план выходит дестабилизация и дезорганизация системы государственного и военного управления противника.

В целом информационные операции могут преследовать следующие задачи:

— дезорганизация сил противника;

— уничтожение информационной инфраструктуры;

— достижение состояние информационного превосходства над противником;

— создание благоприятных информационных условий для действий своих сил;

— обеспечение собственной информационной безопасности.

Объектами информационных операций, в свою очередь, выступают:

— население страны-соперника (социальные группы; лица, занимающие ключевые государственные посты; руководство страны; личный состав вооруженных сил);

— система государственного и военного управления страны-противника (а также отдельные ее элементы и различные их совокупности);

Характерной особенностью информационных операций является их относительно немалая длительность — от нескольких недель до нескольких месяцев.

Большинство информационных операций включают в себе техническую и психологическую составляющую, которые могут быть скоординированы и использоваться на равных условиях одновременно.

На основании этого критерия ряд исследователей выделяют особый подвид информационных операций — информационно-психологические операции.

В целом для успешного проведения информационной операции необходимо:

— предварительное изучение информационной среды противника, в том числе типичных морально-нравственных установок населения;

— выбор достаточно популярного, удобного и надежного канала связи для ведения информационного воздействия;

— непосредственный захват заранее выбранного канала связи и проведение запланированного информационного воздействия.

Однако говорить об их существовании в реальной практике ведения информационной борьбы представляется достаточно затруднительным, ведь любая информационная операция, на современно этапе, предполагает не только воздействие на психику и психологию, но и на ряд технических коммуникаций и средств.

Информационная кампания

Информационная кампания, как форма информационного противоборства также представляет собой совокупность ряда операций, мероприятий и иных видов деятельности, связанных общими целями, задачами и средствами их достижения. Может быть совокупностью информационных акций, атак, ударов и операций в самых различных комбинациях.

При этом информационные кампании носят массовый характер, могут разрабатываться и воплощаться сразу в

нескольких направлениях — по территориальному (в отдельно взятых регионах) или тематическому (по областям деятельности) признакам. При этом для непосредственной разработки нередко привлекают не только специалистов в сфере защиты информации, но и экспертов в той области знаний, на которую рассчитано воздействие, или же экспертов по выбранному региону страны-противника. Это позволяет составить не только более детальный план мероприятий, но и учесть характерные особенности взятого для разработки вопроса, что, в конечном счете, позитивно влияет на итоговую эффективность информационной кампании.

Информационные кампании, в силу своей сложности, масштабности и длительности, достаточно затратны в плане денежных, человеческих и иных ресурсов, поэтому их проведением чаще занимаются органы власти конкретного государства, а не конкретная организация или заинтересованная группа лиц.

Главной целью проведения информационной кампании является способствование проведению заявленной национальной политики государства, а также с целью всесторонней, полной и своевременной защиты собственных национальных интересов. При этом в ряде случаев задачей может становиться взятие полного контроля над внутренней и/или внешней политикой противника.

Примечательно, что в данном случае объект информационного воздействия заметно укрупняется и уже не представляет собой отдельные группы населения противника или его технико-информационные объекты. Объектом информационной кампании становится государство-противник в целом.

Информационные кампании в большинстве своем носят долговременный и перманентный характер. При этом воздействие во многом не имеет той интенсивности, что вышеназванные формы, и может то уменьшаться, то усиливаться — в зависимости от намеченного плана, возникающих обстоятельств, политических, экономических, духовных и иных факторов, влияющих на обе стороны противоборства.

Информационная война как особая разновидность информационной борьбы

Говоря об информационном противоборстве на современном этапе развития человеческого общества нельзя не затронуть тему так называемых «информационных войн».

В целом не все исследователи рассматривают информационную войну как одну из форм ведения информационной борьбы. В общем смысле слова информационная война представляет собой широкомасштабную информационную борьбу с применением способов и средств информационного воздействия на противника в интересах достижения целей воздействующей стороны.

Структурно можно разделить информационную войну на две крупных разновидности:

— информационно-психологическое (психологическую) войну;

— информационно-техническую войну.

Главными объектами воздействия сил противника становятся уже не государство в целом, его руководящие чины и не случайно выбранные социальные группы среди населения, а, в первую очередь, личный состав вооруженных сил, системы формирования общественного мнения и принятия решений — для информационно-психологической войны, и информационно-технические системы (связи, управления, телекоммуникации, радиоэлектроники, компьютерные) — для информационно-технической войны.

Информационная война может проводиться как по всем сферам деятельности государства-противника в целом, так и по отдельным направлениям, сферам его существования. Например, исключительно в политике, экономике, в военной сфере, в сфере социальных отношений, духовной жизни, и, в особенности, в сфере идеологии.

Цель информационной войны — дезориентировать, дезинформировать противника, подорвать моральный дух, а в ряде случаев — и моральные установки, его вооруженных сил.

При этом, как и любая другая война, информационная предполагает работу по двум основным направлениям:

— наступление — проведение плана мероприятий по подрыву информационной безопасности соперника;

— оборона — проведение ряда мероприятий по оказанию противодействия действия противника.

И наступательная, и оборонительные части информационной войны должны проводиться одновременно и на всем протяжении информационных военных действий.

Непосредственное воздействие на силы противника производится путем применения так называемого «информационного оружия», к которому может относиться:

— средства высокоточного местоопределения оборудования (по излучению в электромагнитном спектре), распознания, наведения и непосредственного огневого поражения;

— средства воздействия на радиоэлектронное оборудование и энергопитание для временного или необратимого вывода из строя элементов, либо систем целиком;

— средства воздействия на программный ресурс электронных управляющих модулей посредством использования специальных программных средств, в том числе изменяющих алгоритм их функционирования;

— средства пропаганды и дезинформации для модификации информации систем управления, создания искаженной картины текущей ситуации, изменения ценностей и нравственных ориентиров населения, нанесения конкретного ущерба духовно-нравственной жизни общества государства-противника;

— психотронное оружие, предназначенное специально для прямого воздействия на психику и подсознание человека и групп людей в целях снижения и/или подавления воли, зомбирования, временного или постоянного выхода из строя.

В целом информационная война ведется на двух уровнях:

— тактическом — при котором информационное военное воздействие носит весьма ограниченный характер, прежде всего — по времени, и служит неким сопровождением, а иногда и отвлекающим маневром при информационной операции.

— стратегическом — при котором информационное военное воздействие носит массовый характер и длится гораздо дольше (до нескольких лет и даже нескольких десятков лет, а иногда — постоянно) с целью постепенно внедрения в страну-противника очерченных ценностей, интересов, часто — своего видения мира.

Таким образом, можно говорить о том, что информационная война, с одной стороны, имеет ряд сходных черт с другими формами ведения информационной борьбы (объект воздействия — индивидуальное и коллективное сознание людей; цель — внедрение нужных ценностей и установок; искажение фактов во имя цели), а с другой — обладает характерными особенностями (использование жестких методов борьбы, в том числе психоактивного оружия, шантажа, запугивания, подкупов; сочетание принципов наступательности и обороны) и, следовательно, не может быть однозначно отнесена в одной их типичных форм ведения информационной борьбы.

В целом можно говорить о том, что на современном этапе разработано и активно используется сразу несколько форм ведения информационной борьбы. Назвать одну из них худшей или лучшей нельзя, ведь выбор формы, в конечно итоге, зависит от обстоятельств и факторов, присущих конкретной практической ситуации.

3.3.5. Организационные основы обеспечения информационной безопасности

Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких от-

ношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

а) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

г) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также

организаций, осуществляющих образовательную деятельность в данной области.

Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

б) совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

Контрольные вопросы

1. Роль информации в жизни личности, общества, государства.
2. Область создания и применения средств и механизмов информационной безопасности.
3. Информационное правоотношение информационных ресурсов, информационных продуктов, информационных услуг.
4. Информационно-правовые нормы Конституции Российской Федерации.
5. Государственная политика в области создания информационных систем, информационных технологий и средств их обеспечения.
6. Основные направления правового регулирования информационных отношений в Интернет.
7. Стратегия информационной безопасности и ее цели.
8. Концепции национальной безопасности РФ.

9. Назовите основные цели государства в области обеспечения информационной информации.

10. Какие государственные органы занимаются вопросом обеспечения безопасности информации и какие задачи они решают?

11. Назовите основные положения Доктрины информационной безопасности РФ.

12. Структура правового регулирования отношений в области информационной безопасности.

Глава 4
Государство и геополитическая стратегия

4.1. Информационная безопасность и общество

4.1.1. Информационная безопасность и политика

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Так постепенно защита экономической информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации; даже принимаются федеральные законы о защите информации, которые рассматривают проблемы защиты информации и задачи защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности Российской Федерации — хранения конфиденциальной информации имеет особое значение. К таким информационным системам можно отнести, например, военные, спецслужбы, банковские или ключевые системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным для защиты информации в информационных системах.

Информационная безопасность государства — состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Информационная безопасность — это процесс обеспечения конфиденциальности, целостности и доступности информации.

1. Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям.

2. Целостность: обеспечение достоверности и полноты информации и методов ее обработки.

3. Доступность: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Информационная безопасность — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.

Безопасность информации (данных) — состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Безопасность информации (при применении информационных технологий) — состояние защищённости информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

Безопасность автоматизированной информационной системы — состояние защищённости автоматизированной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчётность и подлинность её ресурсов.

Информационная безопасность — защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Поддерживающая инфраструктура — системы электро-, тепло-, водо-, газоснабжения, системы кондиционирования и т. д., а также обслуживающий персонал. Неприемлемый ущерб — ущерб, которым нельзя пренебречь.

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

— конфиденциальность — состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право;

— целостность — избежание несанкционированной модификации информации;

— доступность — избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

— неотказуемость или апеллируемость — способность удостоверять имевшее место действие или событие так, что эти события или действия не могли быть позже отвергнуты;

— подотчётность — обеспечение идентификации субъекта доступа и регистрации его действий;

— достоверность — свойство соответствия предусмотренному поведению или результату;

— аутентичность или подлинность — свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

— акты федерального законодательства;

— международные договоры РФ;

— конституция РФ;

— законы федерального уровня (включая федеральные конституционные законы, кодексы);

— указы Президента РФ;

— постановления правительства РФ;

— нормативные правовые акты федеральных министерств и ведомств;

— нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

К нормативно-методическим документам можно отнести:

— методические документы государственных органов России:

— доктрина информационной безопасности РФ;

— руководящие документы ФСТЭК (Гостехкомиссии России);

— приказы ФСБ;

— стандарты информационной безопасности, из которых выделяют: международные стандарты; государственные (национальные) стандарты РФ; рекомендации по стандартизации; методические указания;

Государственные органы РФ, контролирующие деятельность в области защиты информации:

— Комитет Государственной думы по безопасности;

— Совет Безопасности России;

— Федеральная служба по техническому и экспортному контролю (ФСТЭК России);

— Федеральная служба безопасности Российской Федерации (ФСБ России);

— Федеральная служба охраны Российской Федерации (ФСО России);

— Служба внешней разведки Российской Федерации (СВР России);

— Министерство обороны Российской Федерации (Минобороны России);

— Министерство внутренних дел Российской Федерации (МВД России);

— Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);

— службы, организующие защиту информации на уровне предприятия;

— служба экономической безопасности;
— служба безопасности персонала (режимный отдел);
— кадровая служба;
— служба информационной безопасности.

Организационно-технические и режимные меры и методы

Для описания технологии защиты информации конкретной информационной системы обычно строится так называемая Политика информационной безопасности или Политика безопасности рассматриваемой информационной системы.

Политика безопасности (информации в организации) — совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Политика безопасности информационно-телекоммуникационных технологий — правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и её информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию.

Для построения Политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы:

— защита объектов информационной системы;
— защита процессов, процедур и программ обработки информации;
— защита каналов связи (акустические, инфракрасные, проводные, радиоканалы и др.);
— подавление побочных электромагнитных излучений;
— управление системой защиты.

При этом по каждому из перечисленных выше направлений Политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

— определение информационных и технических ресурсов, подлежащих защите;
— выявление полного множества потенциально возможных угроз и каналов утечки информации;
— проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

— определение требований к системе защиты;

— осуществление выбора средств защиты информации и их характеристик;

— внедрение и организация использования выбранных мер, способов и средств защиты;

— осуществление контроля целостности и управление системой защиты.

Политика информационной безопасности оформляется в виде документированных требований на информационную систему. Документы обычно разделяют по уровням описания (детализации) процесса защиты.

Документы верхнего уровня Политики информационной безопасности отражают позицию организации к деятельности в области защиты информации, её стремление соответствовать государственным, международным требованиям и стандартам в этой области. Подобные документы могут называться «Концепция ИБ», «Регламент управления ИБ», «Политика ИБ», «Технический стандарт ИБ» и т. п. Область распространения документов верхнего уровня обычно не ограничивается, однако данные документы могут выпускаться и в двух редакциях — для внешнего и внутреннего использования.

Согласно ГОСТ Р ИСО/МЭК 17799–2005, на верхнем уровне Политики информационной безопасности должны быть оформлены следующие документы: «Концепция обеспечения ИБ», «Правила допустимого использования ресурсов информационной системы».

К среднему уровню относят документы, касающиеся отдельных аспектов информационной безопасности. Это требования на создание и эксплуатацию средств защиты информации, организацию информационных и бизнес-процессов организации по конкретному направлению защиты информации. Например: Безопасности данных, Безопасности коммуникаций, Использования средств криптографической защиты, Контентная фильтрация и т. п. Подобные документы обычно издаются в виде внутренних технических и организационных политик (стандартов) организации. Все документы среднего уровня политики информационной безопасности конфиденциальны.

В политику информационной безопасности нижнего уровня входят регламенты работ, руководства по

администрированию, инструкции по эксплуатации отдельных сервисов информационной безопасности.

Государственная политика обеспечения информационной безопасности Российской Федерации

Государственная политика обеспечения информационной безопасности РФ определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере. Государственная политика обеспечения информационной безопасности РФ основывается на следующих основных принципах:

— соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ;

— открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;

— правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

— приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Для того, чтобы сформировать и определить политику информационной безопасности, понадобятся следующие исходные данные:

— необходимо определить информацию, которая подлежит защите, и создать перечень сведений конфиденциального характера, в соответствии с защищаемой информацией;

— определить топологии средств автоматизации (физической и логической)

— необходимо описать административную структуру и категории зарегистрированных пользователей, описать технологию обработки информации и выделить потенциальных субъектов и объектов доступа;

— определить угрозы безопасности информации и создать модель нарушителя;

— обнаружить и описать известные угроз и уязвимости;

— расположить угрозы по убыванию уровня риска (провести анализ рисков).

Так, например, для организации необходимо описать общую характеристику и специализацию организации (наименование организации, специализация, род деятельности, решаемые задачи, характер и объем работ, расположение угроз по убыванию уровня риска).

Необходимо описать организационно-штатную структуру организации (отделы и отделения организации, наименования отделов, решаемые задачи, общая технологическая схема функционирования подразделений).

Так же составляется общее описание рабочего процесса, технологическая схема операций при выполнении рабочего процесса, интенсивность, с которой выполняется рабочий процесс, технологические ограничения, средства контроля и критерии качества результатов рабочего процесса, перечень проблемных вопросов подразделений по обеспечению защиты информации.

Необходимо так же знать следующее:

Используемые в организации средства вычислительной техники и программное обеспечение:

— сведения об используемых СВТ (описание аппаратных средств, коммуникационного оборудования удаленного доступа);

— сведения об используемом общем ПО (наименование и назначение, фирма разработчик, аппаратные требования, размещение);

— сведения об используемом специальном ПО (наименование и назначение, фирма разработчик, аппаратные требования, функциональные возможности, размещение).

Организацию и структуру информационных потоков и их взаимодействие:

— топология ЛВС;

— схема коммуникационных связей;

— структура и состав потоков данных (перечень входных информационных объектов и их источники, перечень выходных информационных объектов и их получатели, перечень внутренних информационных объектов);

— организация хранения данных.

Общую характеристику автоматизированных систем организации;

— расположение ЛВС;

— технические и программные средства ЛВС (физическая среда передачи, используемые протоколы, операционные системы, серверы баз данных, места хранения конфиденциальных данных, средства защиты информации);

— технические и программные средства доступа к ЛВС из сетей общего доступа;

— принадлежность и типы каналов связи;

— сетевые протоколы удаленного доступа;

Угрозы информационной безопасности

— сведения о распределении обязанностей и инструкциях по обработке и защите информации;

— вероятные угрозы (угроза, ее вероятность и возможный ущерб);

— применяемые меры защиты (организационные меры, средства защиты ОС, средства защиты, встроенные в ПО, специализированные средства защиты).

В итоге создается, документ «Политика информационной безопасности организации», который определяет:

— само понятие информационной безопасности и ее основных составляющих и используемых понятий;

— цели и принципы информационной безопасности;

— разъяснение политики безопасности, принципов, стандартов и требований к ее соблюдению (основные направления, способы и требования по обеспечению безопасности информа-

ции, выполнение правовых и договорных требований, требования к обучению персонала правилам безопасности, политику предупреждения и обнаружения вирусов, политику обеспечения бесперебойной работы организации).

Для обеспечения ИТ-безопасности в организации, следует придерживаться следующих правил, инструкций:

— правила парольной защиты;

— правила защиты от вирусов и злонамеренного программного обеспечения;

— требования по контролю за физическим доступом;

— требования по физической защите оборудования;

— инструкция по безопасному уничтожению информации или оборудования;

— инструкция по безопасности рабочего места (документов на рабочем столе и на экране монитора);

— правила осуществления локального и удаленного доступа;

— требования резервного сохранения информации;

— требования мониторинга;

— требования при обращении с носителями данных;

— требования по проверке прав пользователей;

— правила использования системных утилит;

— правила удаленной работы мобильных пользователей;

— распределение ответственности при обеспечении безопасности;

— правила контроля вносимых изменений.

Как уже было сказано, под политикой информационной безопасности понимается многоуровневая система документов, имеющих различное назначение и область применения. Наиболее эффективным методом выстраивания иерархии документов, составляющих политику информационной безопасности, представляется использование 4-уровневой модели.

Система документов, составляющих политику информационной безопасности

Документы 1-го уровня

Единственным документом 1-го уровня является Общая политика информационной безопасности или иначе Концепция информационной безопасности. Данный документ должен

отражать общие подходы и требования, и являться основой для создания всей структуры документов.

Общая политика информационной безопасности в общем случае должна включать:

— определение понятия информационной безопасности, основных целей и области действия;

— стратегические подходы и принципы обеспечения информационной безопасности;

— отраслевые и законодательные требования;

— определение основных ролей и ответственности по обеспечению информационной безопасности;

— подходы к проведению мероприятий по анализу и обработке рисков информационной безопасности;

— ссылки на другие документы, содержащие более детальные разъяснения положений политики информационной безопасности (частные политики ИБ);

— санкции в случае нарушения требований политики.

Документы 2-го уровня

К документам 2-го уровня относятся частные политики ИБ и корпоративные стандарты. Частные политики призваны детализировать требования общей политики в рамках определенной области такой, как, например, антивирусная защита или контроль физического доступа.

Корпоративные стандарты выдвигают требования к определенным операциям, защитным системам. В качестве примера можно привести:

— корпоративный стандарт резервного копирования — описывает применяемые средства резервного копирования, порядок хранения и утилизации резервных копий;

— корпоративный стандарт беспроводной связи — выдвигает требования к подключению и использованию беспроводных сетей (протоколы шифрования, методы аутентификации, настройки рабочих станций и др.).

Документы 3-го уровня

К документам 3-го уровня относятся процедуры и инструкции. Процедуры представляют собой документированное описание процесса, относящегося к той или иной области информационной безопасности, например:

— процедура предоставления доступа к сетевым ресурсам;

— процедура выполнения резервного копирования;

— процедура реагирования на инциденты ИБ.

Инструкции в свою очередь дополняют процедуры детальным описанием каждого шага по выполнению той или иной задачи и могут предназначаться как техническому персоналу, так и рядовым пользователям.

Документы 4-го уровня

Документами 4-го уровня являются разного рода рабочие формы, журналы, заявки, протоколы и другие формы документов, используемые в рамках выполнения тех или иных процедур и являющиеся отражением (и подтверждением) выполнения той или иной деятельности. Примерами документов 4-го уровня являются:

— форма заявки на предоставление доступа к сетевым ресурсам;

— форма журнала регистрации инцидентов ИБ;

— форма отчета о проведении оценки уязвимости сетевых ресурсов.

Разработка и внедрение документов, составляющих политику информационной безопасности, как и любой другой проект, имеющий общеорганизационное значение. Руководство должно отвечать за отслеживание выполнения работ, выделение необходимых ресурсов (людских, денежных и пр.), а также за утверждение разработанных документов.

Непосредственно самой разработкой, как правило, занимается либо специально созданная для этой цели группа, либо приглашенная консалтинговая организация.

4.1.2. Роль силовых структур в системе защиты информации

Под силовыми структурами обычно понимают государственные органы, созданные с целью защиты национальных интересов и безопасности как внутри страны, так и на международной арене.

На протяжении всей истории России проблема безопасности государства постоянно находилась в центре внимания. Для реализации такой безопасности использовались различные методы, которые находили свое отражение, как в законодательстве, так и в создании специальных органов, целью

которых было своевременное выявление и предотвращение любых действий против господствующего строя.

Структура силовых органов Российской Федерации

Это, прежде всего, Министерство внутренних дел (МВД России) — федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел.

Его структура представлена территориальными управлениями по субъектам Российской Федерации и федеральными округами, в которых существует вертикальное подчинение центральному аппарату.

Следующим по важности органом является Федеральная служба безопасности (ФСБ России) — федеральный орган исполнительной власти Российской Федерации, спецслужба, осуществляющий в пределах своих полномочий решение задач по обеспечению безопасности Российской Федерации. Руководство деятельностью ФСБ России осуществляется Президентом Российской Федерации.

Его структура представлена:

— территориальными управлениями по субъектам РФ;

— управлениями и отделами в вооруженных силах (особыми управлениями в пограничных округах);

— «ситуативными органами» в иных организациях.

Генеральная прокуратура — это единая федеральная централизованная система органов, осуществляющих от имени Российской Федерации надзор за соблюдением Конституции Российской Федерации и исполнением законов, действующих на её территории. Прокуратура Российской Федерации выполняет и иные функции, установленные федеральными законами. Полномочия, организация и порядок деятельности прокуратуры Российской Федерации определяются федеральным законом «О прокуратуре Российской Федерации». Прокуратура осуществляет свои полномочия независимо от органов государственной (законодательной, исполнительной, судебной) власти и не относится ни к одной из ветвей власти.

Его структура представлена:

— управлениями Генпрокуратуры по федеральным округам;

— прокуратурами субъектов РФ, городов, районов;

— главной военной прокуратурой с собственным центральным аппаратом и прокуратурами по военным округам и гарнизонам;

— специализированными прокуратурами в субъектах РФ (природоохранными, по надзору за исправительными учреждениями и т. д.).

Следственный комитет — это следственный орган в Российской Федерации, образованный в 2011 году.

Его структура представлена:

— следственными управлениями по федеральным округам;

— правовым управлением;

— военным следственным управлением;

— управлениями по защите государственной тайны, физической защите.

Министерство юстиции — это орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, в том числе:

— в сфере исполнения уголовных наказаний;

— регистрации некоммерческих организаций, включая отделения международных организаций и иностранных некоммерческих неправительственных организаций, общественные объединения, политические партии и религиозные организации, в сфере адвокатуры, нотариата, государственной регистрации актов гражданского состояния;

— обеспечения установленного порядка деятельности судов и исполнения судебных актов и актов других органов;

— правоприменительные функции и функции по контролю и надзору в сфере регистрации некоммерческих организаций, включая отделения международных организаций и иностранных некоммерческих неправительственных организаций, общественные объединения, политические партии и религиозные организации, в сфере адвокатуры, нотариата, государственной регистрации актов гражданского состояния.

Его структура представлена:

— территориальными управлениями и отделами по федеральным округам и субъектам РФ;

— отделами во всех субъектах РФ.

Федеральная служба по контролю за оборотом наркотиков — это федеральная служба Российской Федерации, находящаяся в непосредственном ведении Президента России. Главная цель деятельности ФСКН — борьба с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров, а также контроль за соблюдением установленных норм при их легальном обороте.

Его структура представлена:

— территориальными управлениями и отделами по федеральным округам и субъектам РФ.

Федеральная служба охраны — это федеральный орган исполнительной власти Российской Федерации, спецслужба, осуществляющий функции по выработке государственной политики, нормативно-правовому регулированию, контролю и надзору в сфере государственной охраны, президентской, правительственной и иных видов специальной связи и информации, предоставляемых федеральным органам государственной власти, органам государственной власти субъектов Российской Федерации и другим государственным органам.

Его структура представлена:

— органами, функционирующими применительно к объектам особой государственной охраны.

Главное разведывательное управление — спецслужба, орган внешней разведки Министерства обороны Российской Федерации, центральный орган управления военной разведкой в Вооружённых Силах Российской Федерации. Является исполнительным органом и органом военного управления других военных организаций (Минобороны России и Генерального штаба Вооруженных Сил Российской Федерации); в свою очередь имеет исполнительные органы в составе органов военного управления, иных органов и подведомственных организаций; является государственным учреждением.

Служба внешней разведки — это основной орган внешней разведки Российской Федерации, спецслужба.

Его структура представлена:

— оперативными и аналитическими управлениями: экономической, разведки, контрразведки, анализа и обработки информации, оперативной техники, «ситуационными» оперативными отделами.

Цели и задачи, поставленные перед силовыми структурами

Министерство внутренних дел в своей деятельности руководствуется ФЗ от 07.02.2011 г. № 3-ФЗ «О полиции», где в статье 2 четко прописаны цели и задачи, которым должно служить данное министерство:

1. Деятельность полиции осуществляется по следующим основным направлениям:

— защита личности, общества, государства от противоправных посягательств;

— предупреждение и пресечение преступлений и административных правонарушений;

— выявление и раскрытие преступлений, производство дознания по уголовным делам;

— розыск лиц;

— производство по делам об административных правонарушениях, исполнение административных наказаний;

— обеспечение правопорядка в общественных местах;

— обеспечение безопасности дорожного движения;

— контроль за соблюдением законодательства Российской Федерации в области оборота оружия;

— контроль за соблюдением законодательства Российской Федерации в области частной детективной (сыскной) и охранной деятельности;

— охрана имущества и объектов, в том числе на договорной основе;

— государственная защита потерпевших, свидетелей и иных участников уголовного судопроизводства, судей, прокуроров, следователей, должностных лиц правоохранительных и контролирующих органов, а также других защищаемых лиц;

— осуществление экспертно-криминалистической деятельности.

Федеральная служба безопасности в своей деятельности руководствуется «Положением о Федеральной службе безопасности Российской Федерации», которое утверждено Указом Президента РФ № 960 от 11.08.2003. Во второй части Положения представлены основные задачи ФСБ:

— управление органами и войсками, а также организация их деятельности;

— информирование Президента Российской Федерации, Председателя Правительства Российской Федерации, а также

по их поручениям — федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации об угрозах безопасности Российской Федерации;

— организация выявления, предупреждения и пресечения разведывательной и иной деятельности специальных служб и организаций иностранных государств, отдельных лиц, направленной на нанесение ущерба безопасности Российской Федерации;

— координация осуществляемых федеральными органами исполнительной власти контрразведывательных мероприятий и мер по обеспечению собственной безопасности;

— организация выявления, предупреждения, пресечения и раскрытия преступлений, осуществление досудебного производства по которым отнесено к ведению органов и войск;

— организация во взаимодействии с федеральными органами государственной власти борьбы с организованной преступностью, коррупцией, контрабандой, легализацией преступных доходов, незаконной миграцией, незаконным оборотом оружия, боеприпасов, взрывчатых и отравляющих веществ, наркотических средств и психотропных веществ, специальных технических средств, предназначенных для негласного получения информации, а также противодействия экстремистской деятельности, в том числе деятельности незаконных вооруженных формирований, преступных сообществ и групп, отдельных лиц и общественных объединений, ставящих своей целью организацию вооруженного мятежа, насильственное изменение конституционного строя Российской Федерации, насильственный захват или насильственное удержание власти;

— обеспечение борьбы с террористической и диверсионной деятельностью;

— осуществление в пределах своих полномочий разведывательной деятельности;

— организация в пределах своих полномочий и во взаимодействии с органами внешней разведки Российской Федерации добывания и обработки разведывательной информации;

— организация осуществления мер, отнесенных федеральным законодательством к полномочиям федерального ор-

гана исполнительной власти, уполномоченного в области защиты и охраны государственной границы;

— обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям, осуществляющим техническую разведку;

— обеспечение производства по делам об административных правонарушениях, рассмотрение которых отнесено Кодексом Российской Федерации об административных правонарушениях к ведению органов и войск;

— организация оказания содействия федеральным органам государственной власти и органами государственной власти субъектов Российской Федерации в реализации мер, осуществляемых в интересах обеспечения безопасности Российской Федерации, повышения ее экономического, научно-технического и оборонного потенциала;

— формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности;

— организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом.

Генеральная прокуратура. В ФЗ «О прокуратуре РФ» говорится, что Генеральная прокуратура является органом «обеспечения верховенства закона, единства и укрепления законности, защиты прав и свобод человека и гражданина, а также охраняемых законом интересов общества и государства».

Следственный комитет. В статье 1, подпункт 4 ФЗ от 28.12.2010 № 403-ФЗ «О следственном комитете РФ» говорится об основных задачах:

— оперативное и качественное расследование преступлений в соответствии с последовательностью, установленной уголовно процессуальным законодательством Российской Федерации;

— обеспечение законности при приеме, регистрации, проверке сообщений о преступлениях, возбуждении уголовных дел, производстве предварительного расследования, а также защита прав и свобод человека и гражданина;

— осуществление процессуального контроля деятельности следственных органов Следственного комитета и их должностных лиц;

— организация и осуществление в пределах своих полномочий выявления обстоятельств, способствующих совершению преступлений, принятие мер по устранению таких обстоятельств;

— осуществление в пределах своих полномочий международного сотрудничества в сфере уголовного судопроизводства;

— разработка мер по реализации государственной политики в сфере исполнения законодательства Российской Федерации об уголовном судопроизводстве;

— совершенствование нормативно-правового регулирования в установленной сфере деятельности;

— определение порядка формирования и представления статистических отчетов и отчетности о следственной работе, процессуальном контроле.

Министерство юстиции. Основными целями являются:

— повышение уровня защиты прав и законных интересов граждан и организаций;

— улучшение качества исполнения судебных решений, актов иных органов и приговоров.

Федеральная служба по контролю за оборотом наркотиков, основными целями и задачами которой являются:

— обеспечение в пределах своей компетенции контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров и осуществление мер по противодействию их незаконному обороту;

— выявление, предупреждение, пресечение, раскрытие и предварительное расследование преступлений, отнесенных законодательством Российской Федерации к подследственности органов ФСКН;

— координация деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по противодействию незаконному обороту наркотических средств, психотропных веществ и их прекурсоров;

— участие в разработке и реализации государственной политики в области оборота наркотических средств, психо-

тропных веществ и их прекурсоров, а также противодействия их незаконному обороту;

— создание и ведение единого банка данных по вопросам, касающимся оборота наркотических средств, психотропных веществ и их прекурсоров, а также противодействия их незаконному обороту;

— осуществление в соответствии с международными договорами Российской Федерации взаимодействия и информационного обмена с международными организациями и компетентными органами иностранных государств в области противодействия незаконному обороту наркотических средств, психотропных веществ и их прекурсоров, а также представление интересов Российской Федерации в международных организациях по вопросам противодействия незаконному обороту наркотических средств, психотропных веществ и их прекурсоров.

Основные цели ФСКН России являются:

— принятие мер по стабилизации наркоситуации;

— создание условий для приостановления роста злоупотребления наркотиками и их незаконного оборота;

— поэтапное сокращение наркотизации населения и связанной с ней преступности.

Федеральная служба охраны в своей деятельности руководствуется «Положением о Федеральной службе охраны Российской Федерации», утвержденным Указом Президента РФ от 07.08.2004 № 1013.

Основными задачами ФСО являются:

— обеспечение безопасности объектов государственной охраны в местах их постоянного и временного пребывания и на трассах проезда;

— прогнозирование и выявление угрозы жизненно важным интересам объектов государственной охраны, осуществление комплекса мер по предотвращению этой угрозы;

— предупреждение, выявление и пресечение противоправных посягательств на объекты государственной охраны и охраняемые объекты;

— предупреждение, выявление и пресечение преступлений и иных правонарушений на охраняемых объектах, в местах постоянного и временного пребывания объектов государственной охраны и на трассах их проезда;

— защита охраняемых объектов;

— участие в пределах своих полномочий в борьбе с терроризмом;

— организация и обеспечение эксплуатации, безопасности, совершенствования специальной связи и информации, предоставляемых государственным органам;

— участие в разработке и реализации мер по обеспечению информационной безопасности Российской Федерации, противодействию техническим разведкам и защите сведений, составляющих государственную тайну;

— осуществление государственной политики в области правовой информатизации Российской Федерации и координация работ, производимых в этой сфере;

— информационно-технологическое и информационно-аналитическое обеспечение государственных органов, техническое обслуживание и программное сопровождение информационно-телекоммуникационных систем и ситуационных центров, а также информационное обеспечение управления государством в военное время и при чрезвычайных ситуациях;

— обеспечение собственной безопасности.

Главное управление.

Главное управление Генерального штаба Вооруженных Сил Российской Федерации является органом внешней разведки Министерства обороны Российской Федерации и центральным органом разведки Вооруженных Сил Российской Федерации. Правовую основу разведывательной деятельности Главного управления составляют Конституция Российской Федерации, Федеральные законы «О внешней разведке», «Об обороне» и «О безопасности» и иные нормативные правовые акты федеральных органов государственной власти, касающиеся внешней разведки Российской Федерации.

Главное управление решает задачи в военной, военно-политической, военно-технической, военно-экономической и экологической сферах.

Целями разведывательной деятельности являются:

— обеспечение Президента РФ, Федерального Собрания, Правительства РФ, Министра обороны РФ, начальника Генерального штаба Вооруженных Сил РФ разведывательной информацией, необходимой им для принятия решений в

политической, экономической, оборонной, научно-технической и экологической областях;

— обеспечение условий, способствующих успешной реализации политики Российской Федерации в сфере обороны и безопасности;

— содействие экономическому развитию, научно-техническому прогрессу страны и военно-техническому обеспечению безопасности Российской Федерации.

Служба внешней разведки.

СВР осуществляет разведывательную деятельность в целях:

— обеспечения Президента Российской Федерации, Федерального Собрания и Правительства разведывательной информацией, необходимой им для принятия решений в политической, экономической, военно-стратегической, научно-технической и экологической областях;

— обеспечения условий, способствующих успешной реализации политики Российской Федерации в сфере безопасности;

— содействия экономическому развитию, научно-техническому прогрессу страны и военно-техническому обеспечению безопасности Российской Федерации.

Системы защиты информации в силовых структурах

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Существует ряд мероприятий по обеспечению защиты информации в силовых структурах, которая составляет государственную тайну.

Мобильный комплекс видеоконференцсвязи

Предназначен для:

— подразделений специального назначения (спецназ);

— военных поисково-спасательных служб.

Возможности:

— цифровая передача аудио и видеосигнала от участников на месте проведения работ в ситуационный центр;

— организация дуплексной аудиосвязи работников в зоне их действия с ситуационным центром, посредством мобильного модуля связи;

— организация видеосвязи между участниками проведения работ;

— возможность функционирования до 6 участников, находящихся на месте проведения работ в одной сети комплекса видеоконференцсвязи. В зависимости от пожеланий заказчика, количество участников в сети может быть увеличено;

— связь работников с ситуационным центром на расстоянии до 1000 м в прямой видимости и до 400 м в условиях городской застройки;

— блок источника питания позволяет проводить регистрацию аудио и видео информации с места происшествия в течение 4 часов посредством индивидуальных регистраторов;

— сбор информации о положении участников проведения работ на местности, его физиологическом состоянии, а также состоянии окружающей среды.

Назначение:

— обеспечение эффективности межведомственного взаимодействия за счет высококачественной аудио и видеосвязи между бойцами и штабом;

— повышение безопасности проводимых операций;

— повышение оперативности принятия коллективных решений как между бойцами внутри зоны действия комплекса ВКС, так и между бойцом и штабом;

— поддержка связи в таких районах, где другие каналы связи дают сбой посредством организованного спутникового канала связи.

Автоматизация деятельности служб

Назначение и цели:

— своевременное выявление фактов чрезвычайных ситуаций или подозрений на них, предупреждение возникновения чрезвычайных ситуаций, оперативное пресечение совершения преступлений;

— обеспечение безопасности населения;

— визуальное наблюдение объектов и контроль ситуации;

— анализ и хранение данных о происшествиях и преступлениях;

— принятие оперативных мер, контроль и управление действиями при возникновении нештатных ситуаций;

— восстановления хода событий на основе записанных видеоматериалов;

— обеспечение сознание системы единого мониторинга подвижных сил и средств оперативных и аварийных служб и системы их управления;

— создание эффективного взаимодействия и механизмов партнерства органов государственной власти, специальных служб, частного бизнеса и граждан в вопросах безопасности;

— обеспечение личной безопасности и безопасности общества в целом, антитеррористической защищенности населения и различных объектов;

— повышение оперативности взаимодействия правоохранительных органов с органами государственной, исполнительной власти и населением;

— обеспечение повышенных мер безопасности в местах массового скопления людей;

— повышение эффективности оперативно-служебной деятельности подразделений охраны общественного порядка и обеспечения общественной безопасности;

— повышение раскрываемости преступлений, совершенных в местах массового скопления людей;

— своевременное выявление нарушений общественного порядка (преступлений и иных правонарушений), нештатных ситуаций (чрезвычайных происшествий, нарушений деятельности транспортной инфраструктуры, объектов жизнеобеспечения и т. п.);

— обеспечение взаимодействия между ГУ МВД, Правительством муниципального объекта, городами и районами, а также территориальными подразделениями.

Системы периметрной охраны

Периметрная охрана играет важную роль в системе контроля доступа. Используется такой вид охраны в основном для крупных объектов: военных и секретных объектов, объектов государственной важности, границы государства, а также для предприятий и складских помещений промышленного типа.

Биометрический контроль доступа к объектам

Применение биометрического контроля доступа становится более распространенным в современных системах

безопасности. Основным достоинством биометрической идентификации человека является то, что она обеспечивает высокий уровень безопасности, так как фальсифицировать биометрические характеристики очень сложно, а в некоторых видах биометрических методик невозможно, например, таких как рисунок вен.

Применение биометрических технологий для силовых структур определяется наличием зон с ограниченным доступом в связи с повышенной безопасностью, например, силовые структуры, обеспечивающие информационную безопасность страны или отдельных регионов, или службы исполнения наказаний, тюрьмы и исправительные колонны.

Системы видеонаблюдения

Системы видеонаблюдения занимают важное место в обеспечении безопасности. Главная функция видеонаблюдения это постоянный контроль над территорией, а также обнаружение посторонних предметов, например, переброшенных через ограждение объекта.

Защита информации

К защите конфиденциальной информации всегда подходили с высоким приоритетом, и с каждым днем требования к этой задаче растут. Совокупность технико-инженерных, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, которые используются в том числе и для предотвращения утечки, и для обеспечения безопасности информации — все это средства защиты информации.

В сфере информационной безопасности применяют:

— аудит информационной безопасности;

— построение системы защиты информации/ персональных данных;

— разработка политик по обеспечению информационной безопасности;

— развертывание средств защиты в информационной сети организации;

— разработка и внедрение системы управления идентификацией и аутентификацией;

— обеспечение сетевой безопасности передачи данных с применением криптографических средств защиты информации;

— внедрение средств антивирусной защиты и средств защиты электронной почты от спама и других угроз.

4.2. Геополитическая стратегия России в сфере информационной безопасности

4.2.1. О мировом соотношении информационных технологий в сфере информационной безопасности

Развитие и широкое применение информационных технологий (ИТ) всеми слоями общества является глобальной тенденцией мирового развития. Использование ИТ имеет решающее значение для повышения уровня жизни граждан и конкурентоспособности национальной экономики, расширения возможностей ее интеграции в мировую экономическую систему, роста эффективности государственного управления и местного самоуправления.

Для России опережающее развитие отрасли ИТ является особенно важным, так как позволяет внести значительный вклад в удвоение валового внутреннего продукта, содействовать ликвидации сырьевой зависимости российской экономики и успешной реализации осуществляемой в стране программы реформ в социальной сфере и в области государственного управления. Широкое применение ИТ в других отраслях выводит их на качественно иной уровень развития за счет внедрения информационных технологий, позволяет повысить в них производительность труда и, в свою очередь, ускорить темпы роста. Таким образом, развивающаяся отрасль ИТ является необходимым условием экономического подъема.

В мире складывается глобальное информационное общество, единство которого обеспечено современными технологиями. Стратегической задачей России на данном историческом этапе является полномасштабное вхождение в это общество в качестве его полноправного участника — при сохранении политической независимости, национальной самобытности и культурных традиций.

Сегодня в России наблюдаются высокие темпы роста отрасли ИТ, однако, при невысоком стартовом уровне ее развития. По уровню использования ИТ в экономике, государственном управлении и общественной жизни Россия пока

отстает не только от лидеров мирового прогресса, но и от стран Центральной и Восточной Европы. Для того чтобы войти в группу государств с развитой отраслью ИТ, необходимо сохранить высокие темпы роста до 2020 года и далее. При отсутствии последовательных действий со стороны государства, темпы роста отрасли неизбежно замедлятся, и отставание сохранится.

В то же время, примеры других государств показывают, что при проведении последовательной программы поддержки отрасли ИТ возможно в течение нескольких лет совершить рывок в развитии. России нужна четкая, скоординированная программа действий по развитию отрасли ИТ, выполнение которой позволит сохранить темпы роста отрасли и выйти на качественно новый уровень развития. Необходимо определить возможные конкурентные преимущества России в области ИТ на мировом рынке, наиболее перспективные области развития, идентифицировать существующие барьеры, мешающие отрасли развиваться, и предусмотреть действия по их преодолению.

Структура отрасли ИТ

Под сектором ИТ понимается совокупность трех сегментов: услуг ИТ (включая аутсорсинг бизнес процессов), программного обеспечения, производство и продажа ИТ-оборудования (персональных компьютеров, серверов, периферийных устройств и пр.)

Такой классификации придерживаются международных организации и аналитические агентства. Отрасль ИТ не включает телекоммуникационное оборудование, а также услуги по предоставлению информации.

Анализ состояния рынка ИТ

Общемировые тенденции. Отрасль ИТ является одной из наиболее динамично развивающихся отраслей в мир за последние 2010–2015 г. доходы отрасли росли в среднем на 10 процентов в год, при среднем темпе ВВП как роста экономики 3–4 процента, что привело к увеличению доли отрасли как в развитых так и развивающихся стран. По прогнозам международных аналитических агентств темпы роста, сохранятся и в течение следующих пяти лет. Своим ростом отрасль обязана двум основным движущим факторам: расширению общего

проникновения ИТ в бизнес-процессы организаций, в механизмы государственного управления и повседневную жизнь людей. Тенденции к передаче сторонним специализированным организациям части внутренних функций, связанных с использован ИТ и ИТ-инфраструктуры (так называемый «аутсорсинг») этому способствует высокая эффективность ИТ-технологий в оптимизации функционирования делового, частого и государственного секторов.

Популярность передачи сторонним организациям части внутренних функций, связанных с использованием ИТ и ИТ-инфраструктуры вызвана дефицитом квалифицированных кадров на рынке, стремлением организаций сократить затраты и сконцентрироваться на основных направлениях деятельности к основным тенденциям развития отрасли относится постепенное уменьшение доли стоимости оборудования в общем объеме рынка ИТ опережающий рост услуг по отношению сегменту программного обеспечения, а также перемещение ИТ бизнеса из локальных рынков стран Евросоюза в офшор (в основном в страны с низкой стоимостью труда.) Уменьшение доли отражает снижение спроса потребителей на технику с улучшенными техническими характеристиками. Увеличение доли услуг происходит и из-за сложности ИТ-систем, что требует больших усилий и затрат на их установку, развитие и обслуживание, а также приобретение технических навыков персонала.

Перемещение операций в офшор происходит во многих отраслях промышленности. Особенности отрасли ИТ позволяют перенести в другие страны не только программное обеспечение, но и поддержку продуктов. Большое количество фирм 90-ходах, открыло свои подразделения в Индии и Китае и перенесло выполнение функций или целые бизнес-процессы в эти подразделения. Бесспорным лидером во всех сегментах офшора пока является индия, с общим объемом ИТ-экспорта около 25 млрд долларов в 2013 году. В последнее время на рынок вышли страны Восточной Европы, ориентированные на рынок ЕС, а также Китай. Развитие телекоммуникаций и многократное снижение стоимости передачи данных стало критическим фактором, обеспечивающим рост рынка экспортируемых услуг. Наличие хорошей телекоммуникационной

инфраструктуры по конкурентным ценам является необходимым фактором для того, чтобы страна могла претендовать на лидерские позиции на этом рынке.

Таким образом, рынок информационных технологий трансформируется в сторону ориентации на ИТ-услуги, при этом значительная часть этих услуг будет оказываться из развивающихся стран. В отличие от производственных отраслей, где международное разделение труда уже сложилось, географическое распределение отрасли ИТ еще не закончено, и у России есть шанс значительно увеличить свою долю на глобальном рынке.

Текущее состояние отрасли в России

Интенсивное внедрение современных информационных технологий в экономику, государственное управление, а также в разнообразные общественные процессы является важнейшей составляющей ускоренного развития России, структурных преобразований в экономике и реформы государственного управления. Это отражается в растущем внутреннем спросе на информационные технологии. Всего за три года, в период с 2010 по 2013 годы, рынок информационных технологий в России вырос почти вчетверо — более чем до 16 млрд долларов США.

Однако, несмотря на впечатляющие темпы роста, абсолютные объемы отрасли ИТ в России остаются скромными. Рынок ИТ составляет всего 1,4 процента от ВВП России. Для сравнения, в США объем рынка ИТ превышает 500 млрд долларов, что составляет более 5 процентов от ВВП. При этом на российском рынке сохраняется сильный крен в сторону импортного аппаратно-технологического обеспечения, в то время как рынок услуг ИТ (в основном отечественных) составляет лишь 30 процентов от общего объема, а рынок программных продуктов — 14 процентов.

Заметны существенные отличия от мировой практики в структуре участников отечественного рынка ИТ. По сравнению с большинством стран с развитым рынком ИТ, показатели даже крупных российских ИТ-компаний малы. Так, средняя выручка лидирующих индийских (570 млн долл. США), а ирландских (380 млн долл. США) компаний, специализирую-

щихся на продаже программного обеспечения и оказании ИТ-услуг, и превосходит средний оборот аналогичных российских предприятий более чем в 10 и 5 раз соответственно.

Активным потребителем информационных технологий в Российской Федерации выступает государство. Как и в развитых зарубежных странах, доля спроса государства в течение последних 5 лет в отрасли ИТ достигала 30 процентов, являясь существенным стимулом роста отрасли. Значительный объем спроса приходится на несколько крупнейших компаний, находящихся под контролем государства (ОАО «Газпром», АО «Российские железные дороги», ОАО «Аэрофлот», ОАО «Связьинвест»). Оставшийся объем спроса преимущественно приходится на предприятия финансовой и нефтегазовой сферы, а также, в меньшей степени, связи и торговли. Металлургия, машиностроение, транспорт и другие отрасли значительно отстают в использовании ИТ.

Уровень распространенности информационных технологий среди населения России ещё очень далек от показателей развитых стран. Хотя в данном направлении в России за последние годы происходил стремительный рост, подобное положение, как и в целом по отрасли, объясняется начавшимся только несколько лет назад стартом рынка с практически нулевых показателей.

Отечественный рынок ИТ мал в абсолютном выражении, отстает по большинству характеристик как от развитых, так и от многих развивающихся стран, и далёк от насыщения по всем показателям. Отчасти такое положение вызвано общеэкономическими причинами (последствия спада производства в 1990-х годах, нежелание предприятий инвестировать в долгосрочные ИТ-проекты, низкий уровень материального благосостояния большей части населения).

4.2.2. О системах международной и региональной безопасности

Мировая политика и международные отношения являются центральными понятиями политической системы современности. Отношения государств, государственных объединений, международных организаций, транснациональных корпораций переплетаются в сложную сеть взаимодействий,

которые необходимо регулировать. Отдельно стоит выделить вопрос международной безопасности, поскольку при взаимодействии всех субъектов мировой политики неизбежно возникают конфликты интересов. И тема международной безопасности, сохранения баланса сил в глобализирующемся мире является наиболее актуальной в настоящее время, когда, например, с одной стороны, угроза применения ядерного оружия является сдерживающим фактором в развязывании военных конфликтов, а с другой стороны, наличие или разработка такого оружия является причиной введения военных санкций.

Поскольку вопрос международной безопасности относится к сфере международных отношений, то основные принципы находят отражение в официальных международных документах, выступлениях и речах первых лиц государств, в законодательстве. Так, основные тезисы выступления В. Путина на Мюнхенской конференции по вопросам безопасности стали не только основой нового внешнеполитического курса России, но и оказали влияние на международные отношения в целом. Вопросы международной безопасности отражены в Концепции внешней политики России, утвержденной в 2000 г., регулярно обсуждаются на заседаниях Совета Безопасности РФ.

Безопасность и международные отношения. Международная безопасность: понятие и виды

Безопасность в широком смысле этого слова можно истолковать как отсутствие опасности, отсутствие угрозы. В зависимости от того, чему необходима защита от угрозы, безопасность может быть индивидуальной, групповой, национальной, региональной, международной и так далее.

Применительно к международной сфере, в которой главными действующими субъектами являются государства, безопасность — это отсутствие угрозы для одного субъекта со стороны другого, взаимная защищенность субъектов. Однако понятие международной безопасности не является лишь синонимом состояния мира между государствами, оно включает в себя множество аспектов, и действия, направленные на поддержание мира.

Несмотря на то, что на протяжении всего существования человечества вопрос безопасности и защиты от соседей был

так же важен, как и сегодня, сам термин международной безопасности стал появляться в документах после Первой мировой войны, когда люди пришли к выводу, что войны — слишком затратное занятие во всех смыслах, и что стоит пытаться достигать своих целей мирным способом. Первая модель международной, или иначе, коллективной безопасности была создана в рамках организации Лиги Наций и закреплена принятием ее Статуса, ставший правовой основой коллективной безопасности в Европе. Так, согласно статье 10 Статуса Лиги наций, члены Лиги обязывались «уважать и сохранять против всякого внешнего нападения территориальную целостность и существующую политическую независимость всех членов Лиги».

Однако, эти первые попытки создания системы коллективной безопасности не сумели предотвратить наступление Второй мировой войны, с еще большими последствиями. Эта война еще раз показала необходимость взаимных действий по обеспечению безопасности. В итоге, была создана Организация Объединенных Наций, в Уставе которой содержится современное понимание международной безопасности, состоящее в том, чтобы «поддерживать международный мир и безопасность и с этой целью принимать эффективные коллективные меры для предотвращения и устранения угрозы миру и подавления актов агрессии или других нарушений мира и проводить мирными средствами, в согласии с принципами справедливости и международного права, улаживание или разрешение международных споров или ситуаций, которые могут привести к нарушению мира».

Для достижения указанных в Уставе ООН целей применяются самые разные методы, требующие знаний из различных отраслей международного права, мировой политики и даже военного дела. А поскольку каждая из этих наук имеет свою специфику, логично будет использовать системный подход в анализе международной безопасности. Заключающейся объединении структурных элементов и функциональных процессов международной безопасности в регионах в единую глобальную систему международной безопасности.

Глобальные системы делят на несколько подвидов, основанных на разных подходах и критериях. Так, в зависимости от

количества субъектов системы выделяются следующие конкурирующие типы:

Однополярная система безопасности: после распада СССР и окончания холодной войны США утратила единственного противника и стала распространять свое влияние на весь мир. Считается, что раз США играют главенствующую роль в этой системе, то и обеспечение глобальной безопасности лежит на НАТО. Несмотря на то, что изначально НАТО создавалась как региональная организация стран Северной Атлантики, сегодня среди ее членов и европейские, и азиатские страны, а членство в этой организации как бы является синонимом принадлежности к западной, «демократической» цивилизации. Остальные же страны относятся к чужим, «враждебным» цивилизациям, и в какой-то мере становятся объектом насаждения своего влияния, зачастую силовыми методами (имеются в виду войны, которые США развязывают с целью установления в той или иной стране «демократии»). Подобная модель подвергается критике не только со стороны России, стран Европы и Азии, так и самих США, поскольку роль мирового лидера требует больших финансовых затрат. К тому же, современные проблемы не решить одним лишь применением силы.

«Концерт держав» — считается идеальной моделью международной безопасности, в которой безопасность обеспечивается союзом нескольких великих держав. Небольшое объединение стран имеет большую эффективность, так как согласовывать позиции и принимать решения гораздо проще небольшим количеством участников, чем союзом из десятков или сотен членов (как, например, ООН). Однако критики указывают, что такая модель будет дискриминационной по отношению к малым и средним государствам. К тому же, система безопасности, созданная на основе диктата нескольких сильных государств, не будет пользоваться поддержкой большинства членов мирового сообщества.

Многополярная модель: система, которая, по мнению ряда ученых, сложилась после окончания «холодной войны», поскольку ЕС, Япония, Китай, Индия, АСЕАН, Россия, признавая мощь США, все же проводят свой курс в международных делах, часто несовпадающий с американскими интересами. Росту влияния этих центров силы способствует тот факт, что меня-

ется сама природа силы в международных отношениях. На передний план выдвигаются не военные, а экономические, научно-технические, информационные и культурные составляющие этого феномена. Противники многополярной системы подчеркивают, что такая модель не принесет стабильности в международных отношениях, поскольку основана на видении системы международных отношений как поля постоянной конкуренции между «центрами силы», что приводит к конфликтам и переделам сфер влияния.

Глобальная (универсальная) модель. Сторонники этой концепции справедливо считают, что международная безопасность реально может быть обеспечена только на глобальном уровне, в условиях, когда все члены мирового сообщества участвуют в ее создании. Считается, что такая глобальная модель может возникнуть в результате постепенного развития существующего режима международной безопасности, при ведущей роли ООН.

Из приведенных выше четырех концепций в российской внешней политике доминирует многополярная модель, о чем официально было заявлено в знаменитой Мюнхенской речи В. Путина в 2007 году.

Второй тип систем международной безопасности определяется в зависимости от характера отношений между участниками этих систем.

Коллективная безопасность. Данное понятие вошло в обиход в 1920–30-е годы, когда предпринимались попытки создать механизм предотвращения новой мировой войны (в основном на базе Лиги Наций). Главными элементами коллективной безопасности является наличие группы государств, объединенных общей целью (защита своей безопасности), и система военно-политических мер, направленных против потенциального противника или агрессора. Коллективная безопасность фокусирует внимание на военно-стратегических проблемах и не нацелена на решение других аспектов международной безопасности (экономического, общественного, экологического и других измерений). Это ограничивает возможности использования данной модели в современных условиях.

Всеобщая безопасность. Понятие, впервые появившееся в докладе Комиссии Пальме 1982 г. и ставшее популярным в

нашей стране еще в советский период. Эта концепция призвана подчеркнуть многомерный характер международной безопасности, а также необходимость учета законных интересов не только узкой группы государств, но и всех членов мирового сообщества. Институциональную основу всеобщей безопасности должны составлять не только и не столько военно-политические альянсы (как в случае с коллективной безопасностью), сколько глобальные организации типа ООН. К недостаткам такой модели стоит отнести слабое институциональное подкрепление и связанная с этим трудность воплощения в ходе практического строительства региональных или глобальных систем международной безопасности.

Кооперационная безопасность. Модель, ставшая популярной с середины 1990-х гг. С одной стороны, она признает многомерный характер международной безопасности, а с другой — устанавливает определенную иерархию приоритетов и нацеливает субъекты международной деятельности на решение первоочередных задач. Модель кооперационной безопасности отдает предпочтение мирным, политическим средствам решения спорных вопросов, но в то же время не исключает применения военной силы (не только как последнее средство, но и как инструмент превентивной дипломатии и миротворчества). Однако, еще не до конца ясны многие конкретные параметры такой системы: какие институты должны стать ядром новой системы международной безопасности, каковы природа силы и границы ее использования в современных международных отношениях, каковы перспективы национального суверенитета, как сложится судьба существующих военно-политических альянсов, как предотвратить возрождение блоковой политики и т. д.

Факторы, влияющие на международную безопасность

Поскольку мы рассматриваем международную безопасность как систему, то логично предположить, что на работу, функционирование системы влияют внешние и внутренние факторы. Под внешними факторами мы понимаем такие процессы, которые не зависят напрямую от действий самих субъектов мировой политики, такие, как глобализация, международный терроризм, научно-технический прогресс, эколо-

гические проблемы; к внутренним же факторам отнесем такие, которые напрямую зависят от действий той или иной страны, коалиции стран, организации: угроза применения ядерного оружия, насильственная смена режима, региональные конфликты, внутренние конфликты.

Мы выделили процесс глобализации как фактор, влияющий на международную безопасность, поскольку глобализация влечет за собой возрастание степени взаимозависимости субъектов и функциональных областей в сфере международной безопасности. Глобализация ведет к объединению рынков, к информационной и технической взаимозависимости, к усилению экономического и политического влияния транснациональных корпораций (ТНК) на внутреннюю и внешнюю политику государств. Это приводит к появлению политических и информационных транснациональных систем и означает приоритет финансового капитала и экономической и информационной свободы стран, имеющих ТНК, над национальными границами и интересами стран, отставших в «транснационализации».

Стремление экономически-развитых стран влиять на международную политику порой переходит все границы. Порой страны, желающие войти на внутренний рынок той или иной страны с «недемократическим» режимом, применяют силовые методы в обход требований международных организаций. Это, прежде всего, военные конфликты на востоке с участием США. Их стремление установить демократию выливается в жестокие войны с множеством жертв среди мирного населения. Не существует единого мнения на данный момент по поводу допустимости принудительного экспорта демократии путем смены правящих режимов в авторитарных странах, США пользуются этим без раздумий, однако остальная часть демократического сообщества и транзитных режимов видят в этом нарушение одного из основополагающих принципов международного права — свободы выбора того или иного политического режима.

К тому же, насаждение демократии без соответствующих внутренних предпосылок является попросту непродуктивным. Поэтому такой насильственный экспорт демократии со стороны выглядит просто как благородное прикрытие для корыстных

целей в завоевании сфер влияния. Именно глобализация, подталкиваемая Западом и проводимая в его интересах, становится теперь основным источником конфликтов и войн современности.

Научно-технологический прогресс предоставляет новые возможности для развития экономической, социальной, политической, идеологической областей жизнедеятельности человечества. Информационная революция открывает дорогу для научно-технической революции и в военном деле. Внедрение высоких технологий в области военных вооружений существенно меняет характер и возможности обычного оружия, системы разведки и управления войсками, привлекает все новую технику для создания высокоточных вооружений, расширяет возможности ведения войны на расстоянии, обеспечения «малой заметности» военной техники и т. д. Сюда же следует отнести новый вид войны — так называемые «непрямые» войны, которые подразумевают комплексное использование методов экономического и информационного воздействия на противника в сочетании с операциями спецслужб, военными угрозами и демонстрациями военной мощи, но без приготовления к активным военным действиям.

Другим немаловажным фактором, влияющим на международную безопасность является борьба с транснациональным терроризмом. Проблема, связанная с терроризмом, заключается в том, что, во-первых, необходимо принимать превентивные меры для предотвращения совершения терактов, а во-вторых, при применении вооруженной силы для борьбы с негосударственными действующими лицами, коими являются террористы, возникает вопрос применения вооруженной силы для сокращения жертв среди мирного населения. Настоящие мировые инструменты регуляции уже не отражают реалий новой политической картины мира, и отсюда вытекает потребность развития международного права и реформирования ООН, в частности, тех рычагов, которые регулируют нормы международной безопасности.

Еще одним серьезным фактором, который необходимо учитывать в системе современной международной безопасности, является рост невоенных проблем, которые, в то же время, являются глобальными. Это и экономическая проблема (ее мы рассматриваем отдельно от проблемы глобализации, посколь-

ку глобализация отражает другой аспект, относящийся скорее к политическому влиянию), и экологическая, и гуманитарная. Так, проблема глобального потепления и изменения климатических условий на планете серьезно угрожает человечеству, и если не принимать совместные меры, согласованные на международном уровне, то мы рискуем вовсе стать вымирающим видом. Неравномерность распределения экономических ресурсов, или, так называемая проблема отношений стран Севера и Юга, также влияет на состояние международной безопасности — нехватка продовольствия и общее экономическое неблагополучие в странах Юга влечет за собой социальную и политическую нестабильность внутри государств, что выливается в достаточно серьезные последствия для стран Севера, начиная с неконтролируемой миграции беженцев и заканчивая угрозой региональных военных конфликтов.

Заболевания, возникшие в неблагополучных странах и перенесшиеся в страны Севера, рост числа заболевших ВИЧ, невозможность найти средство борьбы с раковыми заболеваниями и СПИДом, появление новых штаммов вирусов (Эбола), устойчивых к известным лекарствам, мировые эпидемии — все это также является весьма важным фактором, и весьма реальной угрозой безопасности человечества.

Также к экологическим факторам можно отнести и истощение запасов природных ресурсов. Однако, вызываемая этим фактором борьба за ресурсы зачастую ведется военными методами. Так, войну США в Ираке, причиной которой официально называлась возможность наличия химического и ядерного оружия у страны, можно с уверенностью назвать войной за нефтяные ресурсы, коими обладает Ирак. То же происходило и в Ливии.

Хотелось бы еще отметить, что мы также выделили группу внутренних факторов влияния, поскольку равновесие системы международной безопасности зависит от функционирования всех своих элементов, коими являются государства, международные организации. Так, неспокойная ситуация в одном регионе — например, в Северной Корее, — влияет на безопасность всего мира, поскольку Северная Корея обладает ядерным оружием и показывает свою готовность его применить в случае малейшей опасности своим интересам.

Современные проблемы военной безопасности. Развитие технологии ведения войны, как угроза международной безопасности

«Холодная война» ознаменовала новый этап эволюции войн, когда война ведется не «горячими» способами, а иными методами, такими, как политическое, дипломатическое и экономическое давление. Сюда относят информационные войны и сетевые войны.

Сетевые войны являются одним из результатов глобализации. Концепция сетевой войны разработана Управлением трансформации военных сил США (Office of Force Transformation), и активно внедрялась в практику ведения боевых действий США в Ираке и Афганистане, проверяется на учениях и отрабатывается на симуляторах.

Разработчики этой теории считают, что в ближайшем будущем эта концепция если не заменит собой традиционную концепцию ведения войны, то существенно и необратимо изменит ее. Главным элементом новой модели войны является «обмен информацией» — максимальное расширение форм производства этой информации, доступа к ней, ее распределения, обратной связи. Сеть представляет собой новое информационное «пространство», в котором разворачиваются основные стратегические операции — как разведывательного, так и военного характера, а также их медийное, дипломатическое, экономическое и техническое обеспечение.

Центральной задачей ведения всех сетевых войн является согласованная организация действий, направленных на формирование должной модели поведения соратников, нейтральных сил и врагов в ситуации мира, кризиса и войны, что означает установление контроля над всеми участниками актуальных или возможных боевых действий и тотальное манипулирование ими во всех ситуациях — и тогда, когда война ведется, и тогда, когда она назревает, и тогда, когда вроде бы пока царит мир. Основные результаты сетевого ведения войны достигаются влиянием на широкую совокупность социальных факторов — экономических, научно-технических, политико-правовых, информационных, социальных, духовных, культурных и т. д. Военные средства применяются лишь как крайняя мера.

Эта новая холодная сетевая война в настоящее время фактически ведется против России и направлена, как и всякая война, на ее покорение, подчинение и порабощение, в каких бы терминах это ни преподносилось. Трудность противостояния сетевым технологиям состоит, во-первых, в том, что сложно распознать сам факт их применения, а во-вторых, в том, что сегменты глобалистской сети созданы и в самой России: прозападное, проамериканское лобби экспертов, политологов, аналитиков, политтехнологов, многочисленные американские фонды, действующие на территории России, представители крупного российского капитала и чиновничества, которые интегрированы в западный мир, где рожают и учат детей, хранят свои сбережения. Сюда же можно отнести большинство СМИ, которые массированно зомбируют читателей и телезрителей потоками визуальной и смысловой информации, выстроенной по американским лекалам.

Что касается информационных войн, то свое начало они также получили в США в начале XXI века.

В феврале 2006 г. в США утвердили документ «Информационные операции», в котором были изложены взгляды американского военного руководства на подготовку и проведение информационных операций и уточнены цели, задачи и основные принципы информационного противоборства. Такие операции включали в себя пять основных составляющих: радиоэлектронную борьбу (electronic warfare), психологические операции (psychological operations), операции в информационно-коммуникационных сетях (computer network operations), военную дезинформацию (military deception), оперативную безопасность (operations security). Были определены и вспомогательные элементы информационных операций, необходимые для достижения успеха операции в мирное и в военное время, в том числе: информационная устойчивость (information assurance), физическое воздействие (physical attack), контрразведка (counterintelligence), физическая безопасность (physical security), сбор и использование данных видовой разведки (combat camera), связь с общественностью (public affairs), гражданско-военные операции (civil-military operations), поддержка структурами Минобороны публичной дипломатии (defense support to public diplomacy)».

В утвержденной в мае 2011 г. президентом США Б. Обамой «Международной стратегии для киберпространства» подтверждается, что информация и национальная информационная инфраструктура в целом — это стратегический ресурс, и подчеркивается, что в XXI веке государство имеет весьма ограниченные возможности управления и контроля в киберпространстве. Между тем, в формирующейся полицентричной системе международных отношений всё более активную роль начинают играть различные негосударственные структуры (в том числе террористические, враждебно настроенные по отношению к США). Поэтому особый акцент американские специалисты делают на международном сотрудничестве в области обеспечения информационной безопасности. Возрастающая роль информационного оружия, как важнейшего элемента в планах ведения войн нового поколения, показывает рост зависимости эффективности боевых действий от новейших цифровых технологий, что, в свою очередь, неизбежно ведет к росту уязвимости всей национальной информационной инфраструктуры, делая ее составляющие приоритетными военными целями для противника.

Таким образом, важнейшим этапом современной войны становится ее первый, информационный этап, когда решаются задачи достижения информационного превосходства над жертвой предстоящего вооруженного нападения. Этому благоприятствует формирование глобального медиа-пространства, открывающее качественно новые возможности для применения информационного оружия и подрыва морального духа противника еще до формального объявления войны. Быстрое развитие технических и информационных технологий позволяет фактически поставить ту или иную страну на колени еще до перехода к активной фазе военной кампании.

В последние годы информационные, сетевые и гибридные войны можно считать жестокой реальностью. К типичным примерам реализации сетевых технологий можно отнести интернет-революции в Тунисе, Египте, Ливии и государственный переворот в 2014 году в Украине.

К другой особенности ведения войн относятся региональные конфликты, вызываемые «государствами-провокаторами», которые стремятся стравить между собой бо-

лее сильные страны и нажиться на их противоречиях. Сейчас эти страны доставляют очень много неприятностей, что явилось результатом дипломатической стратегии создания области управляемой нестабильности в Евразии — Эстония, Грузия, Литва, Польша и Украина.

Другой особенностью ведения войны в современных условиях является неравномерность сил противников — страны третьего мира, которые часто являются объектом нападения сегодня, не имеют такого военного потенциала, как развитые страны. Это стимулирует поиск слабыми странами таких ответных способов, которые нельзя парировать чисто военными средствами. В условиях глобализации перед большинством стран стоит вопрос, как одержать победу, или хотя бы отразить военное нападение, при неблагоприятном соотношении сил. Неспособность противостоять качественно более сильному в военном отношении противнику побуждает слабых игроков на международной арене к действиям партизанского и террористического характера. В современной войне развитого государства против страны, находящейся на более низком уровне экономического и технологического развития, вполне вероятно переплетение боевых действий и партизанских действий, а также террористических акций, что сегодня наблюдается в Ираке, Афганистане, Ливии, Йемене, Сирии.

Проблема новых технологий вооружения

Другой немаловажной проблемой является то, что существенно меняются и сами вооружения, используемые в войне. Во-первых, вооруженная борьба все больше автоматизируется, роботизируется. В США регулярно проходят испытания беспилотных воздушно-космических самолетов, Россия и США используют беспилотников как в военных, так и в разведывательных операциях, разрабатываются роботы с искусственным разумом. Возросшие транспортные возможности вооруженных сил и ускорение транспортных перевозок обеспечивают переброску крупных контингентов войск (бригад и дивизий) в любой регион в течение нескольких дней. Финансовые и технологические возможности большинства развивающихся государств не позволяют обеспечить военно-технологическое равенство с армиями ведущих стран НАТО. На фоне огромных

финансовых вложений развитых западных государств в модернизацию своих армий и использование в военном деле новейших научно-технических разработок, возможности остального мира выглядят в этой сфере более чем скромно.

Помимо перехода от обычных межгосударственных войн в информационную сферу, специалисты отмечают преобладание внутригосударственных и асимметричных конфликтов, порой провоцируемых в рамках информационных операций противников. Это отражается на структуре людских потерь в ходе военных действий. С другой стороны, рост возможностей высокоточного оружия (ВТО) позволяет минимизировать людские потери, которые крайне болезненно воспринимаются общественным мнением в странах с развитой демократией и могут приводить к внутриполитическим кризисам. Крылатые ракеты и другие виды ВТО с обычными боезарядами способны достигать за счет точности попадания той же боевой эффективности, что и носители ядерных боезарядов.

Нельзя обойти стороной и вопросы оружия массового уничтожения (ОМУ) — в первую очередь, ядерного. Конечно, основная гонка ядерных вооружений закончилась еще во времена «холодной войны», ядерное оружие стало скорее сдерживающим фактором, обеспечивающим безопасность от нападения. Однако существуют условия, при которых ядерные страны готовы применить ядерное оружие. В частности, Военная доктрина РФ предусматривает применение ядерного оружия «в ответ на применение против нее и (или) ее союзников ядерного и других видов оружия массового поражения, а также в случае агрессии против Российской Федерации с применением обычного оружия, когда под угрозу поставлено само существование государства». Тем не менее, мы с готовностью идем на взаимное ядерное разоружение с США. Проблему также создают страны, пытающиеся войти в ядерный клуб. Так, ядерные разработки Ирана и Северной Кореи способствуют эскалации напряженности в этих регионах. Эту проблему не решить просто военным вмешательством. Поэтому в приоритетах нашей страны — взаимное уважение национальных границ и интересов и действие на основе международных принципов, заложенных в Уставе ООН.

Другим особым, новым типом оружия является переход военных действий в киберпространство. Американские специалисты считают, что эта совокупность специально организованного и структурированного информационного трафика, который, наряду с новейшими информационными и телекоммуникационными технологиями, позволит целенаправленно видоизменять (уничтожать, искажать, блокировать, копировать) информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование носителей информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-коммуникационных сетей. Появление такого типа оружия основательно меняет сам механизм развития вооруженных конфликтов, так как даже его выборочное применение по объектам военной и гражданской информационной инфраструктуры противника может завершить конфликт на его ранней стадии, еще до начала активных боевых действий. Таким образом, обладание информационным оружием в киберпространстве обеспечивает политическое и военно-стратегическое преимущество над государствами, у которых его нет.

Как и ядерное, информационное оружие может служить как для политического давления, так и для сдерживания. По оценке некоторых влиятельных экспертов, эффект целевого информационного воздействия на противника сравним с применением ОМУ, и угроза подвергнуться такому воздействию может стать важным фактором сдерживания потенциального агрессора. Особую важность приобретает закрепление международных правил обеспечения информационной безопасности на фоне разработки в США концепции проведения возможных военных операций в киберпространстве и создания в составе ВВС США «Киберкомандования» (Air Force Cyber Command — AFCYBER), специального отдела министерства обороны, отвечающего за обеспечение военных действий в виртуальном пространстве и безопасности военных информационных систем.

Таким образом, информационные сети становятся наиболее эффективным и наиболее распространенным видом современного оружия. Доступность новых информационно-коммуникационных технологий и социальных сетей позволяет

использовать их в военных целях. Например, первый крупный митинг на площади Тахрир в Египте был организован активистами молодежного «Движение 6 апреля» путем призыва, распространенного через социальную сеть Facebook. Массовые восстания студентов в Великобритании также связаны с технологией быстрого обмена сообщениями при помощи телефонов Blackberry и в сетях Twitter.

4.2.3. От прав человека и его обязанностей к правам человека в сфере информационно-телекоммуникационных технологий

Стоит начать с того, что все человечество в начале XXI века живет в развивающемся информационном обществе. У многих проектов, идей появилось возможность быть воплощенными, благодаря бурному развитию и совершенствованию в последние десятилетия технологий и различных коммуникаций. Информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти, следовательно, по мере развития и проникновения информационных и коммуникационных технологий во все сферы общественной жизни, приобретаются и определенные обязанности, связанные с использованием информации.

В современном демократическом обществе сложные связи, возникающие между государством и индивидом, и взаимоотношения людей друг с другом фиксируются государством в юридической форме — в форме прав, свобод и обязанностей. С неуклонным их соблюдением обычно связывается представление о справедливости, демократии, правопорядке, законности.

Наиболее важные и социально значимые для отдельного человека, общества и государства права, свободы и обязанности закрепляет Конституция, которая является основным законом государства.

Права и обязанности граждан Российской Федерации

Права и свободы граждан, которые закреплены Конституцией Российской Федерации, гарантируют неприкосновен-

ность конституционных прав и свобод человека и гражданина, строго оговаривая порядок и причины их ограничения со стороны государства.

Целостная система прав и свобод человека и гражданина закрепляется в гл. 2 Конституции РФ, которые гражданин России может самостоятельно осуществлять в полном объеме с 18 лет (ст.60).

Итак, основные права и свободы граждан — это неотъемлемые права и свободы, принадлежащие им от рождения или в силу гражданства, которые закреплены в Конституции.

Конституционные права и свободы человека и гражданина принято подразделять на личные (гражданские), политические, социально-экономические, и культурные. Место каждой группы определено Конституцией, которая последовательно закрепляет вначале личные, потом политические, далее социально-экономические и культурные права и свободы и, наконец, устанавливает ряд обязанностей.

Личные, или естественные, права и свободы неотчуждаемы, принадлежат каждому от рождения и не связаны напрямую с принадлежностью к российскому гражданству. Личные права и свободы человека закреплены в ст. 20–29 Конституции Российской Федерации.

Например, каждый имеет право на неприкосновенность личности, жилища, частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 22, 23, 25). Каждому должна быть обеспечена возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст. 24).

Гарантируются также свобода мысли и слова, свобода массовой информации. В РФ запрещается цензура. Каждый имеет право законным способом свободно распространять информацию. Запрещается пропаганда социального, расового, национального или языкового превосходства (ст. 29).

В отличие от личных естественных прав и свобод, политические права и свободы (ст. 30–33) связаны с принадлежностью к гражданству Российского государства. Именно через

эти права и свободы практически реализуется конституционное положение о том, что носителем суверенитета и единственным источником власти в РФ является ее многонациональный народ. Конкретизируя эту норму основ конституционного строя, ст. 32 закрепляет право граждан РФ участвовать в управлении делами государства как непосредственно, так и через своих представителей. Право на участие в управлении государственными делами реализуется через различные каналы и формы.

Социально-экономические права и свободы касаются важнейших сфер жизни человека. Это труд и собственность, образование и здоровье, отдых и творчество, семья и жилище, социальное обеспечение и окружающая среда. Они направлены на обеспечение физических, материальных, духовных и других социально значимых потребностей личности. В Конституции РФ во многом по-новому определяются социально-экономические права, что связано с отходом от тотального огосударствления экономической и социальной жизни общества.

Обязанности — есть закрепленное конституционными нормами обязательное поведение человека и гражданина, когда на стороне конституционном уровне.

Граждане Российской Федерации обязаны: соблюдать Конституцию и законы РФ; защищать Отечество; уплачивать законно установленные налоги и сборы; заботиться о детях и нетрудоспособных родителях; заботиться о памятниках истории и культуры; бережно относиться к природе и окружающей среде и ряд других обязанностей.

Тесная связь прав и обязанностей граждан подтверждается и самой Конституцией, которая связывает предоставление права и свободы с возложением определенной обязанности. Должное выполнение обязанностей, надлежащее поведение всех физических лиц, без какого-либо отступления от требований.

Конституции — залог жизнедеятельности общества, становления демократического, правового государства.

К гарантиям прав и свобод человека и гражданина относятся государственная защита прав и свобод человека и гражданина и право на их самозащиту, конституционные гарантии правосудия, недопустимость произвольного ограничения прав и свобод человека и гражданина.

Права и обязанности граждан Российской Федерации в сфере информационно-телекоммуникационных технологий

Национальные интересы Российской Федерации в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Обеспечение национальных интересов Российской Федерации в информационной сфере предполагает достижение следующих трех целей.

Первая цель — соблюдение конституционных прав и свобод граждан в области духовной жизни и информационной деятельности, обеспечение духовного возрождения России.

Вторая цель — развитие отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Третья цель — обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в условиях информатизации.

В ст. 22 и 23 Конституции РФ содержатся нормы, провозглашающие основные права личности, касающиеся частной жизни. На органы государственной власти возлагается обязанность обеспечить каждому возможность ознакомления с документами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Стремительно происходящий в настоящее время в нашей стране процесс информатизации предоставляет реальную возможность создавать условия информационной самореали-зации каждой личности для раскрытия творческих возможностей и

способностей в обстановке свободного доступа к любой информации, включенной в память общества, социальные коммуникации и информационные банки на базе новейших информационных технологий.

Законодательную основу этой возможности составляют не только нормы Конституции РФ о праве граждан на информацию, соответствующие международным нормам в этой области, но и другие законы. Так, Федеральным законом «Об информации, информационных технологиях и о защите информации», направленным на регулирование взаимоотношений в информационной сфере, определено, что информационные ресурсы, т.е. отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектом отношений физических, юридических лиц и государства, подлежат обязательному учету и защите, как и всякое материальное имущество собственника. При этом собственнику предоставляется право самостоятельно, в пределах своей компетенции, устанавливать режим защиты информационных ресурсов и доступа к ним. Закон определяет, что «конфиденциальной информацией считается такая документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации».

Также в Законе определены основные цели защиты информации и прав субъектов в области информационных процессов и информатизации:

— предотвращение утечки, хищения, утраты, искажения, подделки информации;

— предотвращение угроз безопасности личности, общества, государства;

— предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

— защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

— сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

— обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Вопросы охраны информации, обеспечения ее безопасности находят свое отражение в Законе «О правовой охране программ для электронных вычислительных машин и баз данных» и в Законе «О правовой охране топологий интегральных микросхем».

Вопросы правового регулирования работы с персональными данными затронуты в основах законодательства Российской Федерации «Об архивном фонде Российской Федерации и архивах»; Федеральном законе «Об оперативно-розыскной деятельности»; законах Российской Федерации «О государственной тайне», «О средствах массовой информации», «Об участии в международном информационном обмене», и в ряде других законов. Развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы и информационные технологии для таких ресурсов с ограниченным доступом, руководствуются в своей деятельности законодательством Российской Федерации.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти в порядке, определяемом Правительством Российской Федерации.

В Законе «Об информации, информационных технологиях и о защите информации» устанавливаются права и обязанности субъектов в области защиты информации. Так, собственник документов, массива документов, информационных систем или уполномоченные им лица устанавливают порядок предоставления пользователю информации с указанием

места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации. Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

4.2.4. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности

Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности — неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Особенность международного сотрудничества Российской Федерации в области обеспечения информационной безопасности состоит в том, что оно осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток

создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики, противодействия укреплению роли России как одного из влиятельных центров формирующегося многополярного мира, усиления технологического отрыва ведущих держав мира и наращивания их возможностей для создания «информационного оружия». Все это может привести к новому этапу развертывания гонки вооружений в информационной сфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной информационной инфраструктуры.

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

— запрещение разработки, распространения и применения «информационного оружия»;

— обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

— координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

— предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При осуществлении международного сотрудничества Российской Федерации в области обеспечения информационной безопасности особое внимание должно уделяться проблемам взаимодействия с государствами — участниками Содружества Независимых Государств.

Для осуществления этого сотрудничества необходимо обеспечить активное участие России во всех международных

организациях, осуществляющих деятельность в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

Все шире применяющиеся информационные технологии кардинальным образом меняют повседневную жизнь миллионов людей. Они привносят изменения не только во внутреннюю политику самых разных по уровню развития стран мира, но и в отношения между этими странами, в роль, которую играют в мировой системе международные организации, общественные движения, финансовые группы, преступные организации и отдельные лица.

Растущую опасность в информационной сфере на международном уровне представляет новый тип социально опасных преступлений, основанных на использовании современно информационной техники и технологии. Основные виды этих преступлений включают махинации с электронными деньгами, компьютерное хулиганство, хищения разнообразной информации, хранящейся или передаваемой в «безбумажном» виде, незаконное ее копирование и т.п.

Современные специальные технические средства способны воздействовать на психику, сознание людей и на информационно-техническую инфраструктуру общества и армии. Их характеризуют как новый вид оружия — электронное или информационное оружие, которое включает различные средства нападения на компьютерные сети: от электронного шпионажа до вирусов, способных разрушать ключевые системы.

В последние десятилетия достижения науки и технологий как никогда прежде начали определять динамику экономического роста, уровень благосостояния населения, конкурентоспособность государств в мировом сообществе, степень обеспечения их национальной безопасности и равноправной интеграции в мировую экономику.

Стремительное развитие и широкое использование информационно-коммуникационных технологий (ИКТ) ознаменовали собой переход человечества на абсолютно новую ступень развития, явившись результатом революции в сфере информатизации. ИКТ трансформировали не только принципы и формы сбора, обработки и передачи информации, они начали

оказывать мощнейшее воздействие на культурный, экономический, политический и военно-стратегический аспекты жизни общества, становясь одним из основных факторов обеспечения и поддержания устойчивого развития.

Наступает новый этап в развитии процессов обмена информацией. Интенсивное внедрение и переплетение современных компьютерных, теле- и радиовещательных, телефонных технологий и коммуникационных служб, быстрое распространение локальных и глобальных коммуникационных сетей создает принципиально новое качество трансграничного информационного обмена и инструментария воздействия на массовое сознание, усиливая значение социально-психологических и культурно-информационных аспектов глобализации.

Контрольные вопросы

1. Информационное общество. Стадии становления.
2. Государственная политика в области формирования информационного общества.
3. Конвенция о защите прав человека и основных свобод.
4. Система информационного права.
5. Информационные правоотношения, возникающие при осуществлении поиска, получения и потребления информации.
6. Конституционная основа поиска, получения и передачи информации.
7. Правовая основа защиты объектов информационных правоотношений от угроз в информационной сфере.
8. Защита прав и свобод в информационной сфере в условиях информатизации.
9. Основные задачи и органы технической разведки.
10. Принципы технической разведки.
11. Основные этапы и процессы добывания информации технической разведки.
12. Классификация технической разведки.
13. Основные направления развития технической разведки.
14. Основные задачи, структура и характеристика государственной системы противодействия технической разведки.

15. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведки.

16. Каким образом осуществляется правовая охрана программных продуктов на международном уровне.

Литература

1. Конституция Российской Федерации. — М.: «Экзамен», 2004 г.
2. Федеральный закон от 02.12.1990 г. № 395-1 «О банках и банковской деятельности».
3. Закон РФ от 27.12.1991 г. № 2124-1 «О средствах массовой информации» (в ред. от 05.08.2000 г.).
4. Закон РФ от 09.07.1993 г. № 5351-1 «Об авторском праве и смежных правах».
5. Закон РФ от 21.07.1993 г. № 5485-1 «О государственной тайне» (с изменениями, внесенными Федеральным законом от 06.10.2007 г. № 131-ФЗ).
6. Закон РФ от 11.02.1993 г. № 4462-1 «Основы законодательства Российской Федерации о нотариатах».
7. Закон РФ от 22.07.1993 г. № 5487-1 «Основы законодательства Российской Федерации об охране здоровья граждан».
8. Федеральный закон РФ от 17.12.1994 г. №67-ФЗ (ред. от 02.07.2013 г.) «О Федеральной фельдъегерской связи».
9. Федеральный закон РФ от 29.12.1994 г. № 77-ФЗ «Об обязательном экземпляре документов».
10. Федеральный закон РФ от 29.12.1994 г. №78-ФЗ «О библиотечном деле».
11. Федеральный закон РФ от 12.02.1995 г. №144-ФЗ (ред. 02.11.21013 г.) «Об оперативно-разыскной деятельности».
12. Федеральный закон РФ от 03.04.1995 г. №40-ФЗ (ред. 25.07.2002 г.) «Об органах Федеральной Службы Безопасности Российской Федерации».
13. Федеральный закон РФ от 27.07.2004 г. №79-ФЗ «О государственной гражданской службе Российской Федерации».
14. Федеральный закон РФ от 05.06.1996 г. № 85-ФЗ «Об участии в международном информационном обмене».
15. Федеральный закон РФ от10.01.1996 г. № 5-ФЗ (ред. от23.06.2014 г.) «О внешней разведке».
16. Федеральный закон РФ от 25.07.1998 г. № 128-ФЗ (ред. от 24.11.2014 г.) «О государственной дактилоскопической регистрации в Российской Федерации».

17. Федеральный закон РФ от 08.08.2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».

18. Федеральный закон РФ от 31.05.2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации».

19. Федеральный закон РФ от 12.06.2002 г. № 67-ФЗ «Об основных гарантиях избирательных прав и прав на участие в референдуме граждан Российской Федерации».

20. Федеральный закон РФ от 27.12.2002 г. № 184-ФЗ «О техническом регулировании».

21. Федеральный закон РФ от 11.02.2002 г. № 19-ФЗ «О внесении изменений и дополнений в Федеральный закон Российской Федерации «Об обязательном экземпляре документов».

22. Федеральный закон РФ от 25.07.2002 г. № 114-ФЗ «О противодействии экстремистской деятельности».

23. Федеральный закон РФ от 24.12.2002 г. № 177-ФЗ «О внесении изменений и дополнений в Федеральный закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных».

24. Федеральный закон РФ от 07.07.2003 г. № 126-ФЗ «О связи».

25. Федеральный закон РФ от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне».

26. Федеральный закон РФ от 22.10.2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации».

27. Федеральный закон РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

28. Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных».

29. Федеральный закон РФ от 13.03.2006 г. № 38-ФЗ «О рекламе».

30. Федеральный закон РФ от 30.12.2008 г. № 307-ФЗ «Об аудиторской деятельности».

31. Федеральный закон РФ от 28.12.2010 г. №403-ФЗ «О следственном комитете».

32. Федеральный закон РФ от27.07.2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

33. Федеральный закон РФ от 28.12.2010 г. № 390-ФЗ «О безопасности».

34. Федеральный закон РФ от 07.02.2011 г. №3-ФЗ «О полиции».

35. Федеральный закон РФ от 07.01.1992 г. №2202-1 (ред. от 13.07.2015 г.) «О прокуратуре».

36. Федеральный закон РФ от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

37. Федеральный закон РФ от28.07.2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты».

38. Федеральный закон РФ от 05.05.2014 г. № 97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей».

39. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Перечень сведений конфиденциального характера».

40. Указ Президента Российской Федерации от 11.03.2003 г. № 308 «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации».

41. Указ Президента Российской Федерации от 11.08.2003 г. № 960 «Положение о Федеральной Службе Безопасности Российской Федерации и ее структуры».

42. Указ Президента Российской Федерации от 12.05.2004 г. № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» (с изменениями, внесенными Указом Президента Российской Федерации от 03.03.2006 г. № 175).

43. Указ Президента Российской Федерации от 07.08.2004 г. № 1013 «Положение о Федеральной службе охраны Российской Федерации».

44. Указ Президента Российской Федерации от 06.10.2004 г. № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны».

45. Указ Президента Российской Федерации от 11.02.2006 г. № 90 «О перечне сведений, отнесенных к государственной тайне».

46. Указ Президента Российской Федерации от 31.12.2015 г. № 683 «О стратегии национальной безопасности Российской Федерации до 2020 года».

47. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Доктрина информационной безопасности Российской Федерации».

48. Постановление Правительства Российской Федерации от 15.09.1993 г. № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от утечки по техническим каналам».

49. Постановление Правительства Российской Федерации от 03.11.1994 г. № 1223 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

50. Постановление Правительства Российской Федерации от 04.09.1995 г. №870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

51. Постановление Правительства Российской Федерации от 26.06.1995 г. № 608 «О сертификации средств защиты информации».

52. Постановление Правительства Российской Федерации от 23.01.2006 г. №32 «Об утверждении Правил оказания услуг связи по передаче данных».

53. Постановление Правительства Российской Федерации от 10.09.2007 г. №575 «Об утверждении правил оказания телеметрических услуг связи».

54. Постановление Правительства Российской Федерации от 20.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

55. Постановление Правительства Российской Федерации от 26.10.2012 г. № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено».

56. Основные направления нормативного правового обеспечения информационной безопасности Российской Федерации, одобренные на заседании Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности (Решение № 5.4 от 27 ноября 2001 г.).

57. Уголовный кодекс Российской Федерации. — М.: «Ось-89», 2007 г.

58. Гражданский кодекс Российской Федерации. — М.: «Ось-89», 2011 г.

59. Кодекс об административных правонарушениях Российской Федерации. — М.: «Ось-89», 2007 г.

60. Военная Доктрина Российской Федерации. Утверждена Президентов Российской Федерации В. В. Путиным 26.12.2014 г.

61. «Хартия Глобального информационного общества», Окинава, 2000 г.

62. ГОСТ 1.1-2002. Межгосударственная система стандартизации. Термины и определения.

63. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования цифровой подписи.

64. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

65. ГОСТ Р ИСО/МЭК 9126-93. Информационная технология, Оценка программной продукции. Характеристики качества и руководства по их применению.

66. ГОСТ Р ИСО/МЭК 12207-99. Информационная технология. Процессы жизненного цикла программных средств.

67. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

68. ГОСТ 15971-90. Системы обработки информации. Термины и определения.

69. ГОСТ 17657-79. Передача данных. Термины и определения.

70. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения информации. Менеджмент инцидентов информационной безопасности.

71. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

72. ГОСТ Р 50170-92. Противодействие иностранной технической разведке. Термины и определения.

73. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

74. ГОСТ Р 50922-2006. Защита информации, Основные термины и определения.

75. ГОСТ Р 51141-98. Делопроизводство и архивное дело. Термины и определения.

76. ГОСТ Р 51188-98. Испытания программных средств на наличие компьютерных вирусов.

77. ГОСТ Р 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

78. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

79. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении.

80. ГОСТ Р 51897-2002. Менеджмент риска. Термины и определения.

81. ГОСТ Р 52069.0-2003. Защита информации. Система стандартов. Основные положения.

82. ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией. Термины и определения.

83. ГОСТ Р 52633-2006. Защита информации, Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

84. ГОСТ Р 52653-2006. Информационно-телекоммуникационные технологии в образовании. Термины и определения.

85. ГОСТ Р 53110-2008. Система обеспечения информационной безопасности сети связи общего пользования. Общие положения.

86. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

87. Защита от НСД. ТО. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения».

88. СТР-К. Решение Коллегии Гостехкомиссии России «Специальные требования и рекомендации по технической защите конфиденциальной информации».

89. Базовая модель УБИ в КСИИ. Руководящий документ ФСТЭК России «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры».

90. ОТ в КСИИ. Руководящий документ ФСТЭК России «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры». Базовая модель УБ ПДн в ИСПДн. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

91. Хоффман Л. Дж. Современные методы защиты информации. — М.: Советское радио, 1980. — 264 с.

92. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. — М.: Энергоатомиздат, 1994. — 176 с.

93. Смирнов С. Н. Безопасность систем баз данных. — М.: Гелеос АРВ, 2007. — 164 с.

94. Хаббард Р. Дианетика: современная наука о разуме. — М.: Нью Эра, 2001. — 876 с.

95. Информационная война и защита информации: словарь основных терминов и определений. — М.: Центр стратегических оценок и прогнозов, 2011. — 68 с.

96. Владимиров А. И. Основы общей теории войны. Монография в 2-х ч. Часть I: Основы теории войны/ Владимиров А. — М.: Синергия, 2013. — 812 с.

97. Некрасов С. И. Конституционное право Российской Федерации: конспект лекций. — М.: Юрайт-Издат, 2007. — 206 с.

98. Вепринцев В. Б., Манойло А. В., Петренко А. И. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник. — 2-е изд. — М.: Горячая Линия, 2011. — 495 с.

99. Ерофеев Е. А., Уфимцев Ю. С. Информационная безопасность России / Е. А. Ерофеев, Ю. С. Уфимцев. — М.: 4-й филиал Воениздата, 2001. — 624 с.

100. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. I / 1. Технические каналы утечки информации. — М.: НПЦ «Аналитика», 2008. — 436 с.: ил.

101. Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право. — М.: ЮНИТИ-ДАНА, Закон и право, 2004. — 336 с.

102. Международная стратегия для киберпространства. Утверждена Президентом США в 2011 году.

103. Емельянов Г. В., Стрельцов А. А. Информационная безопасность России. Часть I. Основные понятия и определения: учеб пос. / под общей ред. А.А.Прохожева. — М.: РАГС при Президенте РФ, 1999. — 52 с.

104. Информационные вызовы национальной и международной безопасности / Под общ. ред. А. В. Федорова, В. Н. Цыгичко. — М.: ПИР-Центр, 2001. — 328 с.

105. Поздняков А. А. Информационная безопасность страны и вооруженных сил/ Актуальные проблемы национальной безопасности. — М.: ВАГШ, 2000. — 241 с.

106. Краковский Ю. М. Информационная безопасность и защита информации. — Ростов на Дону.: МарТ, 2008. — 288 с.

107. Ясенев В. Н. Информационная безопасность в экономических системах. Учебно-методическое пособие. — Нижний Новгород: «Нижегородский гос. унив. им. Н. И. Лобочевского», 2006. — 253 с.

108. Малюк А. А. Информационная безопасность. Концептуальные и методологические основы защиты информации. Учебное пособие. — М.: Горячая линия — Телеком, 2004. — 280с.

109. Ищейнов В. Я. Информационная безопасность и защита информации. Словарь терминов и понятий. — Москва.: РУСАЙНС, 2018. — 228 с.

Интернет ресурсы

1. Манойло А. В. Государственная информационная политика в особых условиях: монография [Электронный ресурс]. — Электрон. дан. — М.: МИФИ, 2003. — Режим доступа: http://www.evartist.narod.ru/text24/0022.htm.

2. Галатенко В. А. Основы информационной безопасности. Интернет-университет информационных технологий – ИНТУИТ.ру, 2008.

3. https://ru. wikipedia.org./wiki/ Категория: Информация.

4. Петров В. П., Петров С. П. Информационная безопасность человека и общества. Электронная библиотека Royal-lib.ru.

Ищейнов Вячеслав Яковлевич

Информационная безопасность и защита информации: теория и практика

Учебное пособие

Ответственный редактор *С. Краснова*
Верстальщик *С. Мартынович*

Подписано к печати 27.11.2019
Формат бумаги 60x90/16
Печать оперативная. Гарнитура Cambria.
Усл. печ. л. 14,1. Тираж экз. 500

Издательство «Директ-Медиа»
117342, Москва, ул. Обручева, 34/63, стр. 1
Тел/факс + 7 (495) 334–72–11
E-mail: manager@directmedia.ru
www.biblioclub.ru