ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Курс лекций

Уфа 2020

УДК 351.74:004.056(470)(075.8)(042.4)
ББК 67.401.133с51(2Рос)я73-2
А72

Рекомендован к опубликованию
редакционно-издательским советом Уфимского ЮИ МВД России

Рецензенты: кандидат юридических наук Е. Ю. Семенов (Орловский юридический институт МВД России имени В. В. Лукьянова);
Р. А. Султанов (Центр информационных технологий, связи и защиты информации МВД по Республике Башкортостан)

Антонов, В. В.
А72 Основы информационной безопасности : курс лекций / В. В. Антонов, В. А. Колесников, З. И. Харисова. – Уфа : Уфимский ЮИ МВД России, 2020. – 96 с. Текст : непосредственный.

ISBN 978-5-7247-1050-3

В работе рассмотрена юридическая природа информационной безопасности, представлена классификация, разновидность методов и способов осуществления информационной безопасности.

Курс лекций предназначен для обучающихся образовательных организаций МВД России, сотрудников органов, организаций, подразделений МВД России.

УДК 351.74:004.056(470)(075.8)(042.4)
ББК 67.401.133с51(2Рос)я73-2

ISBN 978-5-7247-1050-3

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Широкое внедрение персональных компьютеров вывело уровень «информатизации» деятельности органов внутренних дел на качественно новую ступень. В органах внутренних дел на различных носителях данных хранятся значительные объемы информации, в том числе и ограниченного пользования.

Однако внедрение новых информационных технологий и телекоммуникаций в деятельность органов внутренних дел порождает ряд проблем, одной из которых является надежное обеспечение сохранности и установленного статуса использования информации, циркулирующей и обрабатываемой в информационно-вычислительных центрах, системах и сетях. Данная проблема, прежде всего, связана с обеспечением защиты информации.

Проблема обеспечения необходимого уровня защиты информации является весьма сложной и актуальной на сегодняшний день задачей, требующей для своего решения осуществления совокупности научных, научно-технических и организационных мероприятий и применения специальных средств и методов защиты.

Знание основных способов совершения и предупреждения компьютерных преступлений, методов борьбы с угрозами информационной безопасности, а также современных методов защиты информации необходимо в целях повышения эффективности деятельности органов внутренних дел, в частности для разработки комплекса мероприятий по обеспечению необходимого уровня информационной безопасности в повсеместно распространенных автоматизированных информационных системах.

Лекция 1. ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПРОБЛЕМЫ ЕЕ ОБЕСПЕЧЕНИЯ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

План

1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Информационная безопасность в органах внутренних дел.

1.1. Понятие информационной безопасности

В настоящее время промышленно развитые страны переживают новый исторический этап научно-технической революции, связанный с переходом в исторически новое «постиндустриальное общество», основанное на информации (информационное общество).

Информационное общество (далее – ИО) – историческая фаза развития цивилизации, в которой главными продуктами производства становятся информация и знания.

Таким образом, информационное общество – объективно возникшая в ходе исторического процесса стадия общественного процесса. Она предполагает качественно новый, более высокий уровень производственных сил.

Основными чертами информационного общества выступают:

– увеличение роли информации, знаний и информационных технологий в жизни общества;

– рост числа людей, занятых информационными технологиями, коммуникациями и производством информационных продуктов и услуг;

– нарастающая информатизация общества с использованием телефонии, радио, телевидения, сети Интернет, а также традиционных и электронных СМИ;

– создание глобального информационного пространства, обеспечивающего эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам, а также удовлетворение их потребностей в информационных продуктах и услугах.

Понятие «информация» является одним из фундаментальных в современной науке. Об информации много говорят, пишут, спорят и до сих пор не приходят к единой точке зрения, приемлемой для всех. Известны следующие определения информации:

Информация – это всеобщее свойство материи.

Информация – это любое взаимодействие в природе и обществе, основанное на информации.

Информация – это всякий процесс совершения работы есть процесс информационного взаимодействия.

Информация – это продукт отражения действительности.

Информация (лат. Information – разъяснение, изложение, осведомленность) – одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Форма предоставления информации может быть цифровой, текстовой, звуковой, видеографической и пр. В настоящее время вопросы оценки и обеспечения качества информации привлекают внимание все большего числа инженеров, психологов, экономистов и других специалистов.

Понятие «качество информации» является сложным. Его основу может составить базовая система характеристик, включающая показатели трех классов: выдачи (своевременность, актуальность, полнота); обработки (глубина, достоверность) и защищенности (целостность физическая, целостность логическая, безопасность).

Одним из наиболее существенных показателей качества информации является ее безопасность, т. е. степень защищенности от случайного или преднамеренного получения лицами или процессами, не имеющими на это полномочий.

В жизнедеятельности всех социальных систем в основе лежит принцип обеспечения безопасности. Он связан с прогрессивным развитием потребностей ее элементов в выживании этой системы. При этом безопасность устанавливают как неотъемлемый признак системы, состоящий в способности на основе осмысленной деятельности, направленной на обеспечение порядка взаимосвязей, при котором дезорганизующее влияние внешней среды и внутренних противоречий на очень важные интересы ограничивается рамками устойчивого развития. В России определение «безопасность» традиционно связано с отсутствием угрозы или опасности: «Безопасность – состояние, в котором не угрожает опасность, есть защита от опасности». Или безопасность (security) – это отсутствие опасности; состояние деятельности, при которой с определенной вероятностью исключено причинение ущерба здоровью человека, зданиям, помещениям и материально-техническим средствам в них.

В государственной сфере главными объектами безопасности являются человек, общество и государство, а основным субъектом обеспечения безопасности – государство, выполняющее функции в этой области через органы законодательной, исполнительной и судебной властей. Под безопасностью в социальной сфере понимается защищенное состояние общественных отношений, обеспечивающее прогрессивное развитие общества в конкретных исторических и природных условиях от опасностей, источником возникновения которых служат внутренние и внешние противоречия. В советское время термин «безопасность» соотносился с определением «государственная безопасность» наравне с понятиями «военная безопасность», «правоохранительные органы» и т. д. Гражданская составляющая

безопасности в российском государстве стала развиваться лишь в конце двадцатого века.

В настоящее время безопасность понимается как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз[1]. Это определение служит методологическим основанием для выделения видов безопасности. Информационная безопасность – один из видов безопасности.

Выполняя важные функции по обеспечению социума сведениями и знаниями, информация в то же время может причинить ему определенный ущерб. Опасные информационные воздействия могут быть двух видов. Первый – утрата ценной информации, которая либо снижает эффективность собственной деятельности, либо повышает эффективность деятельности противника, конкурента. Второй – внедрение негативной информации, что может привести не только к опасным ошибочным решениям, но и заставить действовать во вред, например, подвести личность к самоубийству, а общество – к катастрофе. Отсюда возникает проблема информационной безопасности, которая включает два аспекта: блокирование негативной информации и защита (поддержание параметров качества) самой информации.

Под информационной безопасностью Российской Федерации понимается 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[2].В Федеральном законе «Об информации, информационных технологиях и о защите информации» приведена более широкая трактовка понятия «информационная безопасность» (information security) – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам и пользователям информации и поддерживающей ее структуре. Часто бывает так, что понятия «информационная безопасность» и «защита информации» выставляют синонимами и очень сильно в этом заблуждаются. Понятие «информационная безопасность» – это состояние защищенности информационной среды (имеет чаще всего научный, теоре-

1 О безопасности : федеральный закон от 28 декабря 2010 г. № 390-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

2 Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 5 декабря 2016 г. № 646 [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

тический окрас), а защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение защитного состояния.

1.2. Основные составляющие информационной безопасности

Обеспечение безопасности информации, в том числе и в компьютерных системах, требует сохранения следующих ее свойств: целостности (integrity); доступности (availability); конфиденциальности (confidentiality). Они же и выступают моделью безопасности (CIA).

Основными категориями модели безопасности являются:

Целостность – гарантия существования информации в исходном виде.

Доступность – возможность получения информации автоматизированным пользователем в нужное для него время.

Конфиденциальность – доступность информации только определенному кругу лиц.

Аутентичность – возможность установления автора информации.

Апеллируемость – возможность доказать, что автором является именно заявленный человек, и никто другой.

Система защиты информации (далее – СЗИ) – это организованная совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

Для полноценной работы системы защиты информации выдвигаются следующие требования:

– непрерывность;

– плановость (разработка детальных планов по защите информации (далее – ЗИ)) с учетом общей цели организации);

– целенаправленность (выборочность защиты);

– конкретность (ранжирование угроз и защиты);

– активность (достаточная степень настойчивости и активности);

– надежность (с необходимой степенью защиты);

– универсальность (независимо от характера, формы и вида информации);

– комплексность (все виды и формы защиты в полном объеме).

Федеральный закон № 149-ФЗ[1] классифицирует информацию в зависимости от категории доступа к ней и от порядка ее предоставления или

[1] Об информации, информационных технологиях и о защите информации : федеральный закон от 27 июля 2006 г. № 149-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

распространения. В соответствии со ст. 5 указанного закона, по категориям доступа информация подразделяется на общедоступную информацию и информацию ограниченного доступа, т. е. такую информацию, доступ к которой ограничен федеральными законами.

По порядку предоставления или распространения информация подразделяется:

– на свободно распространяемую;

– предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

– подлежащую предоставлению или распространению в соответствии с федеральными законами (например, сведения об имущественном положении кандидатов в депутаты);

– ограничиваемую или запрещаемую к распространению в Российской Федерации (например, разжигающую национальную, расовую или религиозную ненависть и вражду).

Право разрешать или ограничивать доступ к информации и определять условия такого доступа принадлежит обладателю информации. Обладатель информации обязан принимать меры по защите информации и ограничивать доступ к информации, если такая обязанность установлена федеральными законами (ст. 6). Ограничение доступа к информации возможно только в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства и устанавливается федеральными законами. Статья 9 устанавливает обязательность соблюдения конфиденциальности информации ограниченного доступа, т. е. «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя».

Информация ограниченного доступа подразделяется на сведения, представляющие собой: государственную тайну; коммерческую тайну; служебную тайну; профессиональную тайну (сведения, полученные гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности); персональные данные граждан (физических лиц).

Система национальных интересов Российской Федерации при этом определяется совокупностью следующих основных интересов[1]:

[1] О Стратегии национальной безопасности Российской Федерации : указ Президента Российской Федерации от 31 декабря 2015 г. № 683 [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

– 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 направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях полицентричного мира.

Информационным ядром выполнения данной Стратегии является федеральная информационная система стратегического планирования, которая содержит в себе информационные ресурсы органов местного самоуправления и органов государственной власти, системы распределенных ситуационных центров и государственных научных организаций. Причем главное и значительное внимание направлено на обеспечение информационной безопасности с учетом стратегических национальных приоритетов.

Информационная безопасность (ИБ) имеет множество самых различных направлений и аспектов (политические, профессиональные, экономические, правовые, и т. д.). Основные составляющие информационной безопасности:

– защита информации – деятельность по охране документированной информации, неправомерное обращение с которой может нанести ущерб пользователям, владельцам, собственникам или иным лицам (государственная, служебная и коммерческая тайна, персональные данные);

– защита информационной инфраструктуры – деятельность по предотвращению случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба информации и поддерживающей инфраструктуре;

– компьютерная безопасность[1] (или безопасность данных) – совокупность специальных методов, аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях, а также мер по защите информации от неавторизо-

[1] Термин «компьютерная безопасность» также зачастую ошибочно отождествляют с термином «информационная безопасность», забывая, что не вся информация компьютерная.

ванного доступа к критическим данным[1], их разрушения, модификации, раскрытия и задержек в доступе с целью обезопасить систему, защитить и гарантировать точность, конфиденциальность и целостность информации и связанных с ней процессов, минимизировать разрушения, которые могут возникнуть в случае модифицирования или разрушения информации;

– защищенность информационных потребностей – обеспечение граждан, отдельных групп и социальных слоев, массовых объединений людей и населения в целом качественной (ценной) информацией, необходимой для их жизнедеятельности (функционирования), образования и развития, иначе – поддержание информационно-психологической удовлетворенности потребностей и защищенности от негативных информационно-психологических и информационно-технических воздействий (информационного оружия).

В практической деятельности в отличие от теории информационная безопасность традиционно понимается лишь как необходимость противодействия утечке закрытой (секретной) информации, а также распространению ложных и враждебных сведений. В разных науках понятие «безопасность» толкуется по-разному либо отсутствует вообще, что является большой проблемой обеспечения безопасности и правоприменения. В основном информационная безопасность трактуется как структурно-организационная, инженерно-техническая или технологическая дисциплина. Причем сфера информационной безопасности близко связана с правовыми и юридическими дисциплинами. Вот почему для регламентации прав, ответственности, формализации управленческих решений нужно четко применять термины, закрепленные в нормативных правовых актах.

Совокупность составляющих формирует национальную безопасность Российской Федерации, которая должна защищать интересы личности, общества и государства. Информационная безопасность является неотъемлемой составной частью национальной безопасности Российской Федерации. Она играет важнейшую роль в системе обеспечения национальной безопасности, т. к. влияние многообразных угроз в информационном поле все более затрагивает интересы личности, общества и государства.

Информация и информационная деятельность – важнейшая структурная составляющая многих объектов безопасности. Например, информация, представляемая средствами массовой информации, позволяет создавать психическое и психологическое воздействие на принятие экономических решений под действием развивающихся ожиданий рынка.

---

[1] Под «критическими данными» понимают данные, требующие зашиты из-за вероятности нанесения или нанесения больших масштабов ущерба в том случае, если произойдет раскрытие (случайное или умышленное), изменение или разрушение данных.

Особенно эффективным это оказывается в обстоятельствах, когда в сферу биржевой деятельности многие миллионы людей оказались втянуты. Многие из них получили доступ к биржам через глобальные компьютерные сети.

Типичным явлением в сфере рыночных отношений, а также и во внешней торговле стали компьютерная борьба и электронный шпионаж. Объектами опасного информационного воздействия (информационной безопасности) оказываются: психика и сознание людей, информационно-технические системы различного предназначения и объема.

К социальным объектам информационной безопасности можно отнести государство, общество, личность. Объектом информационной безопасности может выступать и сама информация, т. к. воздействие угроз приводит к видоизменению качества и снижению ее ценности. В этих случаях содержание информационной безопасности заключается в защите информации от угроз. Как для социальных, так и для технических систем возможная постановка вопроса будет являться характерной.

С возрастанием роли информационных ресурсов и информационных технологий в развитии граждан, общества и государства в двадцатом веке задачи информационной безопасности выходят на первый план в системе обеспечения национальной безопасности.

Среди предопределяющих причин возникают:

– национальные интересы, угрозы им и обеспечение защиты от этих угроз выражаются, реализуются и осуществляются через информацию и информационную сферу;

– проблема национальной безопасности имеет ярко выраженный информационный характер;

– задачи национальной безопасности решаются с помощью использования информационного подхода, являющегося основным научно-практическим методом;

– человек и его права, информация и информационные системы и права на них – это основные объекты не только информационной безопасности, но и основные элементы всех объектов безопасности во всех ее областях.

Состояние информационной безопасности определяется способностью нейтрализовать опасные, дестабилизирующие, ущемляющие интересы государства информационные влияния на основные сферы жизнедеятельности (политика, экономика, наука, образование и т. д.). В условиях возрастающей научно-технической революции в области электронной вычислительной техники и телекоммуникаций, глобализации процессов экономического, политического и социального развития человеческого общества проблемы безопасности развития личности, функционирования общественных структур и органов государства в информационной сфере стано-

вятся все более острыми, затрагивая обширный круг субъектов информационных отношений.

Вместе с появлением новых возможностей в сфере информационной деятельности устанавливаются совершенно новые, часто не имеющие правовых аналогов отношения в виде новых рисков. Виртуальные технологии вскрыли новейшие возможности для системы властных отношений. Новейшие информационные технологии разрешили значительно поднять эффективность воздействия на умственное развитие людей и психологическое общественное сознание.

При этом образованы новейшие виды невидимого манипулирования индивидуальным, групповым и массовым сознанием людей. Информационные влияния могут быть вредны и непредсказуемы, т.к. способны запустить и контролировать мощные материально-энергетические процессы и их последствия.

Наряду с обычными технологиями и формами управления обществом или индивидом все шире получает распространение метод централизованного влияния на огромные массы граждан – метод информационного управления. Вот почему в настоящее время информационная безопасность общества и человека приобретает новый статус, превращаясь из технологической проблемы в социальную, от решения которой зависит устойчивое развитие человечества.

1.3. Информационная безопасность в органах внутренних дел

В деятельности органов внутренних дел нашего государства уделяется важное значение эффективному развитию и внедрению информационных и телекоммуникационных технологий.

Для решения стоящих перед органами внутренних дел (далее – ОВД) задач обеспечения безопасности осуществляется комплекс мер, направленных на совершенствование их информационного обеспечения на основе обеспечения подразделений путем оснащения современными техническими комплексами, внедрения в практическую деятельность новейших передовых и перспективных информационных технологий. В МВД России была спроектирована и реализована ведомственная Программа «Создание единой информационно-телекоммуникационной системы органов внутренних дел» с целью кардинальной модификации положения в данном направлении.

Указом Президента Российской Федерации от 1 марта 2011 г. № 248 в структуре МВД Российской Федерации был создан Департамент информационных технологий, связи и защиты информации МВД России, который реализовывает внедрение современных ИТ-технологий в практическую деятельность органов внутренних дел Российской Федерации.

Активное развитие информационных и телекоммуникационных технологий в деятельности ОВД неразрывно связано с ее защитой и обеспечением информационной безопасности. Требования по обеспечению информационной безопасности регулируются федеральными нормативными актами и внутренними документами МВД России.

Одной из важных задач является стандартизация требований и постоянный контроль выполнения мер по защите информации всеми подразделениями. В настоящее время в ОВД проводится интенсивная работа по модернизации ведомственной системы информационной безопасности, основывающейся на качественно новых подходах.

На текущий момент в развитии ведомственной системы защиты информации достигнуты следующие результаты:

– создана система ведомственных органов по аттестации объектов информатизации, аккредитованных ФСТЭК (Федеральной службой по техническому и экспортному контролю) России;

– переведена на качественно новый технологический уровень ведомственная система криптографической защиты информации, что позволило значительно повысить эффективность защищенного информационного обмена в системе Министерства, в том числе в интересах обеспечения скрытого управления силами и средствами органов внутренних дел.

Однако, как показал анализ, существенного повышения уровня обеспечения информационной безопасности в системе министерства по итогам реализации выработанных ранее решений не произошло. Принимаемые меры по обеспечению информационной безопасности не носили комплексный характер, а применительно к масштабам МВД России реализованная система защиты информации является фрагментарной и сохраняет принципиальные уязвимости по отношению к современным угрозам ее безопасности. К сожалению, приходится констатировать, что актуальные аспекты обеспечения информационной безопасности – целостность и доступность информационных ресурсов – так и остались на стадии проектных решений без практической реализации.

Учитывая предельную значимость реализации в МВД России комплекса неотложных мер по модернизации существующей системы защиты информации, позволяющей на современном уровне обеспечить эффективную защиту ведомственных информационных ресурсов и ассоциированной с ними информационно-телекоммуникационной инфраструктуры, в структуре Департамента информационных технологий, связи и защиты информации МВД России (далее − Департамент ИТСЗИ) создано Управление защиты информации.

В настоящее время основными направлениями совершенствования ведомственной системы защиты информации являются:

– реализация мероприятий по систематизации информации, содержащейся в автоматизированных информационных системах, базах и бан-

ках данных органов, организаций и подразделений МВД России, способствующая унификации процессов перевода информации в электронный вид и эффективному ее использованию, в том числе созданию и ведению Единой модели данных и Единой системы классификации и кодирования, а также унификации подходов к созданию и внедрению информационных средств и технологий;

– организация шифровальной службы в органах, организациях и подразделениях системы МВД России, руководства деятельностью шифровальных органов и органов криптографической защиты информации по специальным вопросам и контроль за ней;

– участие в реализации мероприятий по созданию и развитию системы удостоверяющих центров МВД России;

– организация в установленном порядке разработки и обеспечения ведения единых каталогов аппаратных и программных средств, в том числе систем управления базами данных, алгоритмов и программ автоматизированных информационных систем, баз и банков данных общего пользования, используемых для решения задач по информатизации органов, организаций и подразделений системы МВД России;

– организация и контроль в установленном порядке работ по созданию, развитию и эксплуатации ведомственных сегментов МВД России государственных информационных систем;

– проведение мониторинга состояния оснащенности органов, организаций и подразделений МВД России (за исключением оперативно-технических и оперативно-поисковых подразделений) средствами связи, автоматизации, вычислительной, организационной техникой, в том числе в защищенном исполнении, навигационно-мониторинговыми системами, техническими (криптографическими) средствами защиты информации, специальной и контрольно-измерительной аппаратурой, системным, прикладным и специальным программным обеспечением к ним;

– координация работ по унификации аппаратно-программных средств, в том числе локальных вычислительных сетей и автоматизированных рабочих мест, соответствующих средств обеспечения информационной безопасности и информационных технологий, применяемых в органах, организациях и подразделениях МВД России;

– осуществление в пределах своей компетенции мероприятий по защите государственной тайны и конфиденциальной информации.

Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации определила комплекс мер, направленных на обеспечение защиты информации, информационных ресурсов и информационных систем органов внутренних дел Российской Федерации от специальных программно-технических воздействий, средств технических разведок, несанкционированного доступа, а также утечки информации по техническим каналам. При этом под информационной безопасно-

стью, как правило, понимается состояние защищенности информации, информационных ресурсов и информационных систем ОВД, при котором обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования. В целях создания эффективной системы обеспечения информационной безопасности в МВД России целесообразно осуществлять комплекс мероприятий по защите информации, содержащей сведения, составляющие государственную тайну, и сведения конфиденциального характера, по противодействию техническим разведкам противника, предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней.

Основными задачами обеспечения информационной безопасности ОВД являются:

– совершенствование правовых, научно-практических, нормативно-технических, организационно-методических и иных основ информационной безопасности ОВД;

– реализация комплекса организационных (режимных) и технических мероприятий, направленных на обеспечение защиты информации, информационных ресурсов и информационных систем ОВД от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования;

– создание и развитие системы информационной безопасности ОВД с учетом реализации «облачной архитектуры»;

– формирование и совершенствование системы мониторинга состояния информационной безопасности ОВД;

– организация и совершенствование профессиональной подготовки и переподготовки сотрудников органов внутренних дел в области обеспечения информационной безопасности.

Информационная безопасность ОВД должна реализовываться на основе принципов законности, достаточности, оперативности, системности, комплексности, целенаправленности, приоритетного использования отечественных средств и систем защиты информации.

Обеспечение безопасности информационных систем и ресурсов МВД России осуществляется с соблюдением положений Федерального закона «О персональных данных». Для этого Министерством внутренних дел Российской Федерации были разработаны:

– Методические рекомендации по обеспечению безопасности персональных данных при их обработке в автоматизированных информационных системах МВД России;

– Приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении инструкции по защите персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации» [1];

– Типовое положение о подразделении информационных технологий, связи и защиты информации территориального органа МВД Российской Федерации, утвержденное приказом МВД России от 02 июля 2012 года № 660[2].

Особую значимость для МВД России имеет реализация первоочередных задач государственной политики в области межведомственного взаимодействия, направленных на модернизацию государственного управления и повышение уровня оказываемых госуслуг в условиях развитого информационного общества.

Комплекс ресурсных мероприятий включает в себя внедрение в деятельность органов внутренних дел современных технических средств защиты информации, средств криптографической защиты информации (шифровальной техники), включая работающее совместно с ними оборудование. Внедряется также специальная и контрольно-измерительная аппаратура, средства вычислительной и организационной техники в защищенном исполнении, системное, прикладное и специальное программное обеспечения к ним, а также мобильные устройства удаленного доступа к информационным базам данных.

Инфраструктура обеспечения информационной безопасности в МВД России продолжает развиваться. Так, в настоящее время созданы и функционируют 55 ведомственных органов по аттестации объектов информатизации, аккредитованных ФСТЭК России, оснащенных современным контрольно-измерительным и поисковым оборудованием. По результатам проведенных мероприятий по расширению функциональных возможностей единой ведомственной сети шифровальной связи МВД России, порядка 100 объектов на федеральном, межрегиональном (окружном) и региональном уровнях территориальных органов МВД России и более 350 ОВД на районном уровне обеспечены возможностью использования современной IP-шифровальной связи. Приняты на вооружение и используются образцы специальной техники.

Защита персональных данных. Необходимость обеспечения безопасности персональных данных в наше время объективная реальность. Защита персональных данных является одной из важнейших задач системы обес-

---

[1] О персональных данных : федеральный закон от 27 июля 2006 г. № 152-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

2 Об утверждении Типового положения о подразделении информационных технологий, связи и защиты информации территориального органа Министерства внутренних дел Российской Федерации : приказ МВД России от 2 июля 2012 г. № 660. [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

печения информационной безопасности в организации любого масштаба и любой организационно-правовой формы. Нарушение режима конфиденциальности имеющихся в организации данных клиентов, сотрудников, обслуживаемых граждан является само по себе серьезнейшим инцидентом информационной безопасности, создающим многочисленные риски.

Министерство внутренних дел Российской Федерации в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от 24.04.2020) «О персональных данных» является оператором, организующим и (или) осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональных данных.

Организация работ по созданию и эксплуатации информационных систем обработки персональных данных (далее − ИСПД), а также системы защиты персональных данных (далее − СЗПД) осуществляется в соответствии с законодательством Российской Федерации в области обеспечения безопасности информации и соответствующими государственными стандартами.

Мероприятия по защите персональных данных на объектах информатизации, содержащих ИСПД, осуществляются на основе нормативных правовых актов и методических документов, утверждаемых в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

При обработке персональных данных в ИСПД должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСД к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

Для обеспечения сохранности информационных ресурсов ИСПД производится их резервное копирование на материальный носитель, обеспечивающее возможность восстановления содержащихся в информационной системе сведений.

В целях обеспечения безопасности персональных данных создается СЗПД, которая должна обеспечивать конфиденциальность, целостность и доступность персональных данных при их обработке в ИСПД во всех структурных элементах, на технологических участках обработки и во всех режимах функционирования информационной системы.

СЗПД включает в себя организационные и технические меры, средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных, а также используемые в ИСПД информационные технологии.

Ответственными за соблюдение требований по защите персональных данных при их автоматизированной обработке являются руководители подразделений МВД России, эксплуатирующие, а также использующие ИСПД, администраторы ИСПД, пользователи ИСПД, непосредственно обрабатывающие персональные данные в ИСПД, и инженерно-технический персонал, имеющий доступ к ИСПД с целью обеспечения устойчивого функционирования информационной системы при ее использовании, что отражается в должностных регламентах (должностных инструкциях) указанных лиц.

Лекция 2. ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

План

1. Законодательный уровень информационной безопасности.
2. Полномочия законодательных, исполнительных и судебных органов в области защиты информации.
3. Полномочия специальных субъектов системы защиты информации в России.

2.1. Законодательный уровень информационной безопасности

Вопросы правового обеспечения информационной безопасности имеют первостепенное значение. В настоящее время интенсивно создается нормативно-правовая база данной сферы.

Главной чертой настоящего этапа развития законодательства в области обеспечения информационной безопасности является переход к более глубокому уровню осмысления предмета правового регулирования и, соответственно, построению более развитой нормативной правовой базы.

В систему правового регулирования в сфере информационной безопасности входят три элемента: нормативно-правовая база, субъекты обеспечения безопасности, контролирующие и надзирающие органы.

В данной лекции ограничимся рассмотрением отдельных аспектов деятельности органов внутренних дел, связанных с выявлением, пресечением и раскрытием преступлений и решением других задач оперативно-разыскной деятельности. Массив законодательных актов, регулирующих правовые основы деятельности правоохранительных органов в этой части, достаточно велик, противоречив, а потому относительно сложен для использования на практике, если не знать основных закономерностей, позволяющих его использовать. К числу действующих в данной сфере законодательных актов относятся:

– Конституция Российской Федерации[1] (принята всенародным голосованием 12.12.1993 г.)

[1] Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года : (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

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. Ограничение этого права допускается только на основании судебного решения.

Статья 24

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

Статья 45

1. Государственная защита прав и свобод человека и гражданина в Российской Федерации гарантируется.

– Доктрина информационной безопасности Российской Федерации[1].

Доктрина информационной безопасности РФ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения ИБ РФ.

1. Национальные интересы РФ в информационной сфере и их обеспечение.

Национальные интересы Российской Федерации в информационной сфере – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы.

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.

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

Национальными интересами в информационной сфере являются:

– 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;

[1] Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 5 декабря 2016 г. № 646 [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

– 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.

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.

2. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

– 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;

– 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;

– 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;

– 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;

– повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

– повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

– обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

– совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;

– повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

– нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

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.

Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

– законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

– конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

– соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

– достаточность сил и средств обеспечения информационной безопасности, определяемая, в том числе посредством постоянного осуществления мониторинга информационных угроз;

– 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:

– обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

– оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

– планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

– 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;

– 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.

Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

– Федеральный закон РФ «О полиции» от 07.02.2011 г. № 3-ФЗ[1].

Статья 11.

Полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.

В целях повышения уровня обеспечения автоматизации процессов управления эксплуатацией, поддержки внедрения и администрирования компонентов единой системы информационно-аналитического обеспечения деятельности Министерства внутренних дел Российской Федерации разработан приказ МВД России от 23.11.2016 № 755 «Вопросы эксплуатации центра разработки, поддержки, внедрения и администрирования сервисов единой системы информационно-аналитического обеспечения деятельности МВД России. Данный приказ реализует защиту информационных ресурсов ЕЦЭ ИСОД с учетом концепции и архитектуры подсистемы информационной безопасности контура обработки информации, не содержащей сведений, составляющих государственную тайну, и осуществляется в соответствии с требованиями нормативных правовых актов Российской Федерации в области защиты информации, предъявляемыми к информационным системам 3 уровня защищенности персональных данных и класса защищенности К 3.

На сегодняшний день, с учетом проведенного анализа практики применения автоматизированных информационных систем в деятельности подразделений органов внутренних дел, составлены региональные планы развития автоматизированных информационных систем, баз и банков данных.

Одной из задач внедрения информационных технологий в деятельность органов внутренних дел является организация эффективного внутриведомственного информационного взаимодействия на основе создания единого информационного пространства и внедрения электронного документооборота.

– Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ[2].

---

[1] О полиции : федеральный закон от 7 февраля 2011 № 131 [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

[2] Об оперативно-розыскной деятельности : федеральный закон от 12 августа 1995 г. № 144-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

Глава I. Общие положения.

Статья. 1. Оперативно-разыскная деятельность.

Оперативно-разыскная деятельность (ОРД) – вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим ФЗ (далее – органы, осуществляющие оперативно-разыскную деятельность), в пределах их полномочий посредством проведения оперативно-разыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств.

Статья. 3. Принципы оперативно-разыскной деятельности.

Оперативно-разыскная деятельность основывается на конституционных принципах законности, уважения и соблюдения прав и свобод человека и гражданина, а также на принципах конспирации, сочетания гласных и негласных методов и средств.

Статья. 5. Соблюдение прав и свобод человека и гражданина при осуществлении ОРД.

Органы (должностные лица), осуществляющие ОРД, при проведении оперативно-разыскных мероприятий должны обеспечивать соблюдение прав человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну, неприкосновенность жилища и тайну корреспонденции.

Не допускается осуществление ОРД для достижения целей и решения задач, не предусмотренных настоящим Федеральным законом.

Лицо, полагающее, что действия органов, осуществляющих ОРД, привели к нарушению его прав и свобод, вправе обжаловать эти действия в вышестоящий орган, осуществляющий ОРД, прокурору или в суд.

Органам (должностным лицам), осуществляющим ОРД, запрещается:

разглашать сведения, которые затрагивают неприкосновенность частной жизни, личную и семейную тайну, честь и доброе имя граждан и которые стали известными в процессе проведения оперативно-разыскных мероприятий, без согласия граждан, за исключением случаев, предусмотренных федеральными законами;

при нарушении органом (должностным лицом), осуществляющим ОРД, прав и законных интересов физических и юридических лиц вышестоящий орган, прокурор либо судья в соответствии с законодательством РФ обязаны принять меры по восстановлению этих прав и законных интересов, возмещению причиненного вреда.

Нарушения настоящего Федерального закона при осуществлении ОРД влекут ответственность, предусмотренную законодательством РФ.

Глава II. Проведение оперативно-разыскных мероприятий

Статья. 9. Основания и порядок судебного рассмотрения материалов об ограничении конституционных прав граждан при проведении оперативно-разыскных мероприятий.

Рассмотрение материалов об ограничении конституционных прав граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, на неприкосновенность жилища при проведении оперативно-разыскных мероприятий осуществляется судом, как правило, по месту проведения таких мероприятий или по месту нахождения органа, ходатайствующего об их проведении. Указанные материалы рассматриваются уполномоченным на то судьей единолично и незамедлительно.

Статья. 10. Информационное обеспечение и документирование оперативно-розыскной деятельности.

Органы, осуществляющие ОРД, для решения задач, возложенных на них настоящим ФЗ, могут создавать и использовать ИС, а также заводить дела оперативного учета.

Факт заведения дела оперативного учета не является основанием для ограничения конституционных прав и свобод, а также законных интересов человека и гражданина.

Статья. 12. Защита сведений об органах, осуществляющих оперативно-розыскную деятельность.

Сведения об используемых или использованных при проведении негласных оперативно-разыскных мероприятий силах, средствах, источниках, методах, планах и результатах ОРД, о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих ОРД, и о лицах, оказывающих им содействие на конфиденциальной основе, а также об организации и о тактике проведения оперативно-разыскных мероприятий составляют ГТ и подлежат рассекречиванию только на основании постановления руководителя органа, осуществляющего ОРД.

Предание гласности сведений о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих ОРД, а также о лицах, оказывающих или оказывавших им содействие на конфиденциальной основе, допускается лишь с их согласия в письменной форме и в случаях, предусмотренных Федеральными законами.

Глава VI. Контроль и надзор за ОРД.

Статья. 21. Прокурорский надзор за ОРД.

Прокурорский надзор за исполнением настоящего ФЗ осуществляют Генеральный прокурор РФ и уполномоченные им прокуроры.

По требованию указанных прокуроров руководители органов, осуществляющих ОРД, представляют им оперативно-служебные документы,

включающие в себя дела оперативного учета, материалы о проведении оперативно-разыскных мероприятий с использованием оперативно-технических средств, а также учетно-регистрационную документацию и ведомственные нормативные правовые акты, регламентирующие порядок проведения оперативно-разыскных мероприятий.

Сведения о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих ОРД, а также о лицах, оказывающих содействие этим органам на конфиденциальной основе, предоставляются соответствующим прокурорам только с письменного согласия перечисленных лиц, за исключением случаев, требующих их привлечения к уголовной ответственности.

Прокуроры, указанные в части первой настоящей статьи, обеспечивают защиту сведений, содержащихся в представленных документах и материалах.

– Федеральный закон от 27.05.1996 № 57-ФЗ «О государственной охране». Принят 27 мая 1996 г[1].

Данный ФЗ обязывает органы Федеральной службы охраны (ФСО) РФ осуществлять следующие виды деятельности:

– организовывать и проводить в пределах своих полномочий мероприятия по развитию и совершенствованию системы президентской связи, обеспечению ее надежности, информационной безопасности и оперативности при предоставлении объектам государственной охраны;

– производить шифровальные работы;

– организовывать и проводить на охраняемых объектах, а также в местах постоянного и временного пребывания объектов государственной охраны оперативно-технический контроль;

– осуществлять во взаимодействии с ФСБ, ФСТЭК и др. структурами меры по противодействию утечке информации по техническим каналам.

– Федеральный закон «Об органах федеральной службы безопасности Российской Федерации» № 40-ФЗ от 10 апреля 1995 г.[2]

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 этих лиц.

---

[1] О государственной охране : федеральный закон от 27 мая 1996 г. № 57-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

[2] О федеральной службе безопасности : федеральный закон от 3 апреля 1995 № 40-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

В соответствии со ст. 6 полученные в процессе деятельности органов ФСБ РФ сведения о частной жизни, затрагивающие честь и достоинство гражданина или способные повредить его законным интересам, не могут сообщаться органами ФСБ кому бы то ни было без добровольного согласия данного гражданина, за исключением случаев, предусмотренных федеральными законами.

– Федеральный закон «О внешней разведке» от 10 января 1996 г. № 5-ФЗ [1].

Закон «О внешней разведке» запрещает применение органами внешней разведки методов и средств разведывательной деятельности в отношении граждан России на территории РФ.

Наряду с деятельностью Службы внешней разведки (далее – СВР), этот закон также регламентирует деятельность подразделений и частей радиоразведки ФСБ, которые ведут разведывательную деятельность в сфере шифрованной, засекреченной и иных видов специальной связи.

– Уголовный кодекс РФ от 24 мая 1996 г. № 63-ФЗ[2].

Глава 28 «Преступления в сфере компьютерной информации» определяет какие общественно опасные деяния в сфере использования компьютерной информации являются преступными.

Статья 272 УК РФ устанавливает уголовную ответственность за «неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), в системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети».

Статья 273 УК РФ впервые в отечественном законодательстве устанавливает уголовную ответственность за создание, использование и распространение вредоносных программ для ЭВМ или «внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети».

Статья 274 УК РФ к числу уголовных преступлений теперь относит и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим к ним доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации.

---

[1] О внешней разведке : федеральный закон от 10 января 1996 № 5-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

[2] Уголовный кодекс Российской Федерации : федеральный закон от 13 июня 1996 г. № 63-ФЗ. [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http:// www.pravo.gov.ru (дата обращения: 12.08.2020).

– Гражданский кодекс РФ (часть первая). Принят 30 ноября 1994 г. № 51-ФЗ.

Гражданский кодекс РФ (далее – ГК РФ) рассматривает информацию в качестве объекта гражданского права наряду с интеллектуальной собственностью и имуществом (ст. 128 ГК РФ). В нем также дается определение информации, составляющей служебную и коммерческую тайну.

В статье 139 ГК РФ изложена суть особых формальностей, которые позволяют применять какие-либо санкции к нарушителям конфиденциальности информации:

– во-первых, эта конфиденциальная информация должна иметь действительную или потенциальную коммерческую ценность, и она не может быть известна третьим лицам;

– во-вторых, учреждение, владеющее конфиденциальной информацией, на законных основаниях принимало определенные меры для исключения свободного доступа к этой информации и охране ее конфиденциальности;

– в-третьих, все сотрудники, знакомые с этими сведениями, были официально предупреждены об их конфиденциальности.

– Закон Российской Федерации от 27.12.1991 № 2124-1«О средствах массовой информации».

В соответствии со ст. 40 вышеуказанного закона может быть отказано в получении запрашиваемой информации в случае, если она содержит сведения, составляющие государственную, коммерческую или иную специально охраняемую тайну, а статья 41 ограничивает права на распространение конфиденциальной информации.

Редакция обязана сохранять в тайне источник информации и не в праве называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом».

В статье 4 говорится о недопустимости использования СМИ в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для призыва к захвату власти, насильственному изменению конституционного строя и целостности государства, разжигания национальной, классовой, социальной, религиозной нетерпимости или розни, для пропаганды войны.

Указ Президента РФ № 188 от 6 марта 1997 г.[1].

Перечень сведений конфиденциального характера:

[1] Об утверждении перечня сведений конфиденциального характера : указ Президента РФ от 3 апреля 1995 г. № 334 [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в СМИ в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения, доступ к которым ограничен ОГВ в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

– Указ Президента РФ от 3 апреля 1995 г № 334[1].

В целях усиления борьбы с организованной преступностью и повышения защищенности информационно-телекоммуникационных систем постановляет:

– запретить использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (ЭЦП), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата, а также размещение государственных заказов на предприятиях, использующих несертифицированные технические и шифровальные средства;

– запретить деятельность юридических и физических лиц, связанную с разработкой, производством и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением услуг в области шифрования информации, не имеющих лицензий.

И другие нормативные правовые акты.

[1] О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации : указ Президента РФ от 3 апреля 1995 г . № 334 [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

Объем подзаконного уровня регламентации оперативно-разыскной работы также достаточно велик. В нем в зависимости от различных критериев можно выделить отдельные массивы нормативных правовых актов, которые систематизируются на ведомственном и межведомственном уровнях. Некоторые из них будут рассмотрены по ходу дальнейшего изложения материалов лекции.

В данной лекции остановимся не только на отдельных вопросах защиты информации, но одновременно рассмотрим и более широкое понятие – понятие информационной безопасности, затрагивающей правоотношения, которые возникают при решении задач ОРД.

2.2. Полномочия законодательных, исполнительных и судебных органов в области защиты информации

Для увеличения степени безопасности всех типов тайн, вращающихся в Российском государстве и обществе, в 90-е гг. XX-в. была реализована основная реорганизация системы органов защиты информации. В настоящее время защита строится на следующих первостепенных принципах.

1. Принцип комплексности:

– обеспечение безопасности пользователей, работающих с закрытой информацией, и связанных с материальными и финансовыми ресурсами от всех вероятных угроз всеми возможными и доступными законными методами и средствами;

– способность системы защиты информации к улучшению и совершенствованию в соответствии с преображающимися внешними и внутренними ситуациями;

– предоставление безопасности информационных ресурсов в процессе всего их жизненного цикла, во всех технологических процессах и операциях по формированию, обработке, потреблению и уничтожению информации.

2. Принцип непрерывности, подразумевающий устойчивое обслуживание работоспособности и формирование системы защиты информации.

3. Принцип законности, предполагающий организацию системы защиты информации строго на базе действующих нормативных правовых актов, регламентирующих безопасность информации.

4. Принцип активности, предполагающий проявление напористости и настойчивости в достижении целей и задач защиты информации. Он предусматривает устойчивый маневр силами и средствами защиты информации, а также принятие необычных мер защиты.

5. Принцип своевременности (превентивный характер мер защиты информации). Он предполагает установку задач по комплексной защите

информации на этапе создания системы ее защиты на базе анализа известных и прогнозирования потенциальных угроз безопасности информации, которые могут возникнуть в будущем после активации системы защиты в работу.

6. Принцип обоснованности заключается в научно обоснованных и современных методах и средствах защиты информации и должен отвечать новейшим достижениям науки и техники.

7. Принцип специализации, обеспечивающий привлечение к разработке и внедрению методов и средств защиты информации специализированных субъектов, имеющих государственные лицензии на предопределенные типы деятельности в сфере предоставления услуг по защите информации.

8. Принцип совершенствования, предполагающий стабильную оптимизацию и принятие новых организационных, законодательных, технических мер защиты информации под влиянием объективных и субъективных причин.

9. Принцип взаимодействия и координации деятельности, предусматривающий способ организации точного взаимодействия между всеми субъектами защиты информации, а также координацию всех производимых работ в этой сфере для достижения общих целей.

10. Принцип экономической целесообразности, предполагающий возникновение ущерба, который может наступить вследствие нарушения безопасности оберегаемой информации, не должен превосходить расходы на разработку и реализацию систем защиты информации.

11. Принцип централизации управления, предусматривающий наличие единого координационного центра, который регулирует единые требования по обеспечению безопасности информации и занимающийся задачами управления системой защиты информации.

К первостепенным целям современной российской системы защиты информации относятся:

– предоставление правового режима документированной информации как объекта собственности;

– защита государственной тайны, охрана конфиденциальности документированной информации в соответствии с настоящим законодательством;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;

– предотвращение угроз безопасности государства, общества и личности;

– предотвращение хищения, утраты, утечки, искажения и подделки информации;

– предупреждение несанкционированных действий по искажению, модификации, уничтожению, копированию, блокированию информации, а также предотвращение иных форм противозаконного вторжения в информационные системы и информационные ресурсы;

– обеспечение прав субъектов при создании, изготовлении и использовании информационных систем, технологий и средств их обеспечения.

К числу первостепенных задач государственной системы защиты информации относятся:

– проведение единой политики, организация и координация работ по защите информации в таких сферах деятельности, как политической, экономической, научно-технической, оборонной и др.;

– предотвращение несанкционированного доступа к информации и утечки ее по техническим каналам;

– принятие нормативных правовых актов, регулирующих общественные отношения в области защиты информации;

– исключение или значительное противодействие добычи информации методами и средствами разведки;

– создание средств защиты информации и контроля за ее эффективностью, организация и разработка научно обоснованных сил и методов;

– организация информационного обмена сведениями об осведомленности заграничных разведок о средствах, силах, мероприятиях и методах, обеспечивающих защиту информации внутри и за пределами страны;

– предупреждение вредоносных влияний на информацию, ее носителей, а также технические средства ее создания, использования, обработки, передачи и защиты;

– прогнозирование потенциалов технических средств разведки, анализ их состояния и способов применения;

– контроль за положением мер охраны и защиты информации в органах государственной власти, учреждениях, организациях и др., применяющих охраняемую законом информацию в своей деятельности.

Субъектами системы защиты информации в Российской Федерации являются:

1. Президент Российской Федерации:

– по представлению Правительства Российской Федерации утверждает структуру и состав Межведомственной комиссии по защите государственной тайны, а также Положение о ней;

– в области защиты информации утверждает государственные программы;

– по представлению Правительства Российской Федерации утверждает Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;

– о совместном применении и защите сведений, составляющих государственную тайну заключает международные договоры России;

– по оснащению защиты информации в Администрации Президента определяет полномочия должностных лиц;

– решает другие вопросы в пределах своих полномочий, которые возникают в связи с отнесением информационных данных к тому или иному виду тайны (засекречивание, рассекречивание, их защита).

2. Палаты Федерального Собрания.

– проводят законодательное регулирование отношений в сфере защиты информации;

– рассматривают статьи федерального бюджета на реализацию государственных программ, направленных в части средств по защите информации;

– определяют полномочия должностных лиц в палатах Федерального Собрания по обеспечению защиты государственной тайны.

3. Правительство Российской Федерации:

– организует реализацию законов и международных соглашений в области защиты информации;

– организует разработку и реализацию государственных программ в области защиты информации;

– представляет на утверждение Президенту состав, структуру и Положение о Межведомственной комиссии по защите государственной тайны;

– выносит на утверждение Президенту Перечень должностных лиц органов государственной власти, которые наделяются полномочиями по отнесению сведений к различным видам тайны;

– заключает межправительственные соглашения, а также принимает меры по исполнению международных договоров России по совместному применению и защите сведений, составляющих государственную тайну;

– устанавливает полномочия должностных лиц по предоставлению защиты информации в аппарате Правительства;

– устанавливает размеры и порядок предоставления льгот гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;

– учреждает порядок по определению размеров ущерба в результате несанкционированного распространения сведений, составляющих государственную тайну;

– решает иные вопросы в пределах своих полномочий, возникающие в связи с отнесением сведений к любым видам тайны (засекречивание, рассекречивание, защита).

4. Органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы мест-

ного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:

– обеспечивают защиту охраняемой законом информации, а также засекречиваемых сведений, передаваемых им другими органами государственной власти, учреждениями, организациями и предприятиями и т. д.;

– обеспечивают защиту государственной тайны на подведомственных им организациях, в учреждениях и предприятиях в соответствии с требованиями законодательства Российской Федерации;

– обеспечивают проведение контрольных операций в отношении граждан, допускаемых к государственной тайне в пределах своей компетенции;

– осуществляют установленные законодательством меры по ограничению конституционных прав граждан и обеспечению льгот лицам, владеющим либо имевшим доступ к сведениям, составляющим государственную тайну;

– разрабатывают и вносят в полномочные органы государственной власти предложения по улучшению системы защиты информации.

5. Органы судебной власти:

– обеспечивают судебную защиту органов государственной власти, организаций учреждений, граждан и т. д. в связи с их деятельностью по защите охраняемой законом информации;

– рассматривают гражданские и уголовные дела о нарушениях законодательства в области защиты информации;

– обеспечивают защиту различных видов тайны в течение рассмотрения указанных дел;

– определяют полномочия должностных лиц в органах судебной власти по обеспечению защиты охраняемой законом информации.

6. Органы, являющиеся специальными субъектами в области защиты информации:

– Совет Безопасности Российской Федерации.

– Межведомственная комиссия по защите государственной тайны.

– Федеральная служба по техническому и экспертному контролю (ФСТЭК);

– Федеральная служба безопасности (ФСБ);

– Служба внешней разведки (СВР);

– Федеральная служба охраны (ФСО);

– Министерство обороны (МО);

– Министерство внутренних дел (МВД);

– и другие Министерства и ведомства, организации, учреждения, предприятия и их структурные подразделения по защите охраняемой законом информации.

2.3. Полномочия специальных субъектов системы защиты информации в России

Полномочия Совета Безопасности и Межведомственной комиссии по защите государственной тайны. Полномочия в области защиты информации Федеральной службы по техническому и экспертному контролю. Полномочия органов Федеральной службы безопасности Службы внешней разведки и Министерства обороны.

Целью деятельности Совета Безопасности Российской Федерации в рассматриваемой области является подготовка решений Президента Российской Федерации по вопросам обеспечения защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внешних и внутренних угроз, проведения единой государственной политики в области обеспечения информационной безопасности.

К его ведению относятся вопросы определения жизненно важных интересов личности, общества и государства в информационной сфере, выявление и оценка опасности угроз информационной безопасности Российской Федерации, подготовка проектов решений Президента Российской Федерации по противодействию угрозам, разработка предложений в области обеспечения информационной безопасности России, а также предложений по уточнению отдельных положений концептуальных документов по проблемам обеспечения информационной безопасности.

Властные полномочия Совета Безопасности обусловливаются властными полномочиями Президента Российской Федерации, который утверждает решения Совета Безопасности. В силу этого решения Совета Безопасности становятся обязательными для исполнения, прежде всего, всеми органами обеспечения информационной безопасности, входящими в состав исполнительной власти. Органы законодательной и судебной власти сохраняют гарантированную Конституцией Российской Федерации самостоятельность, но учитывают решения Совета Безопасности в своей деятельности. С этой точки зрения Совет Безопасности является одним из средств реализации возложенной на Президента Российской Федерации конституционной обязанности обеспечивать согласованное функционирование и взаимодействие органов государственной власти, закрепленной в п. 2 ст. 80 Конституции России.

Первый Указ Президента РФ «О Межведомственной комиссии по защите государственной тайны» № 1108, учреждавший эту Комиссию, был подписан 8 ноября 1995 г. Следующим президентским Указом – № 71 от 20 января 1996 г. – были утверждены Положение о Межведомственной комиссии по защите государственной тайны, ее структура и состав по должностям.

В настоящее время действует Положение о Межведомственной комиссии по защите государственной тайны, утвержденное Указом Президента РФ от 6 октября 2004 года № 1286.

В соответствии с п. 4 последнего Положения, Межведомственная комиссия осуществляет следующие полномочия:

– координирует деятельность органов государственной власти, органов местного самоуправления и организаций по вопросам реализации федерального законодательства в области государственной тайны;

– рассматривает и представляет в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации предложения по правовому регулированию вопросов защиты государственной тайны и совершенствованию системы защиты государственной тайны в Российской Федерации, а также предложения по организации разработки и выполнения государственных программ, нормативных правовых актов и методических документов, обеспечивающих реализацию федерального законодательства о государственной тайне;

– формирует перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне;

– формирует перечень сведений, отнесенных к государственной тайне;

– формирует в установленном порядке перечень особорежимных объектов Российской Федерации и представляет его в Правительство Российской Федерации;

– определяет порядок рассекречивания носителей сведений, составляющих государственную тайну, в случае ликвидации организации-фондообразователя и отсутствия ее правопреемника;

– осуществляет рассекречивание и продление сроков засекречивания документов КПСС (Коммунистической партии Советского Союза), Правительства СССР (Правительства Союза Советских Социалистических Республик) и других архивных документов в случае отсутствия организации-фондообразователя и ее правопреемника;

– рассматривает в случаях, предусмотренных Законом Российской Федерации «О государственной тайне», запросы органов государственной власти, органов местного самоуправления, организаций и граждан о рассекречивании сведений, отнесенных к государственной тайне;

– рассматривает вопросы о возможности передачи сведений, составляющих государственную тайну, другим государствам и международным организациям и представляет в установленном порядке в Правительство Российской Федерации соответствующие экспертные заключения;

– принимает решения о передаче органом государственной власти, органом местного самоуправления, организацией сведений, составляющих

государственную тайну, в случаях изменения их функций, форм собственности, ликвидации или прекращения работ с использованием сведений, составляющих государственную тайну, другому органу государственной власти, органу местного самоуправления, организации;

– организует разработку и представляет в установленном порядке в Правительство Российской Федерации предложения о порядке определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого организациям и гражданам в связи с засекречиванием информации, находящейся в их собственности;

– организует разработку и представляет в установленном порядке в Правительство Российской Федерации предложения по правилам отнесения сведений, составляющих государственную тайну, к различным степеням секретности;

– рассматривает по поручениям Президента Российской Федерации и Правительства Российской Федерации экспертные заключения в целях определения размеров возможного ущерба, который может быть нанесен безопасности Российской Федерации вследствие несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, нанесенного организациям и гражданам в связи с засекречиванием информации, находящейся в их собственности;

– рассматривает по поручениям Президента Российской Федерации и Правительства Российской Федерации проекты международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, организует разработку соответствующих предложений и экспертных заключений, участвует в международном сотрудничестве по этим вопросам;

– дает заключения на решения руководителей органов государственной власти, связанные с изменением действующих в органах государственной власти, органах местного самоуправления и организациях перечней сведений, подлежащих засекречиванию, которые могут привести к изменению перечня сведений, отнесенных к государственной тайне, приостанавливает или опротестовывает их решения;

– координирует в установленном порядке работы по техническому регулированию в отношении продукции (работ, услуг), сведения о которых составляют государственную тайну, а также работы по организации сертификации средств защиты информации;

– координирует в установленном порядке проведение работ по лицензированию деятельности организаций, связанной с использованием сведений, составляющих государственную тайну, созданием средств защи-

ты информации, а также осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны;

– решает вопрос о продлении 30-летнего срока засекречивания сведений, составляющих государственную тайну;

– дает по запросу межведомственной комиссии, образуемой для рассмотрения обращений граждан Российской Федерации в связи с ограничениями их права на выезд из Российской Федерации, заключение о том, что сведения особой важности или совершенно секретные сведения, о которых гражданин был осведомлен на день подачи заявления о выезде из Российской Федерации, сохраняют либо утратили соответствующую степень секретности;

– координирует деятельность в области подготовки, переподготовки и (или) повышения квалификации специалистов по вопросам защиты государственной тайны;

– осуществляет разработку методических рекомендаций по организации и проведению государственной аттестации руководителей организаций, ответственных за защиту сведений, составляющих государственную тайну, определяет перечень учебных заведений, свидетельство об окончании которых дает право на освобождение указанных руководителей от государственной аттестации;

– осуществляет иные полномочия в соответствии с федеральным законодательством о государственной тайне.

Подавляющее большинство функций по лицензированию в сфере защиты информации, осуществляет Федеральная служба безопасности России. Однако следует назвать еще один подзаконный нормативный правовой акт – Постановление Правительства РФ от 26 января 2006 г. № 45 «Об организации лицензирования отдельных видов деятельности», которым утверждены Перечень федеральных органов исполнительной власти, осуществляющих лицензирование, и Перечень видов деятельности, лицензирование которых осуществляется органами исполнительной власти субъектов Российской Федерации, и федеральных органов исполнительной власти, разрабатывающих проекты положений о лицензировании этих видов деятельности.

В соответствии с этими документами в качестве федеральных органов, осуществляющих лицензирование в области информационной безопасности, фигурируют:

1. Федеральная служба безопасности России (далее – ФСБ), которая осуществляет:

– разработку, производство, реализацию и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и

юридическими лицами, осуществляющими предпринимательскую деятельность;

– деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– деятельность по распространению шифровальных (криптографических) средств;

– деятельность по техническому обслуживанию шифровальных (криптографических) средств;

– предоставление услуг в области шифрования информации;

– разработку, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

2. ФСТЭК (Федеральная служба по техническому и экспортному контролю) России (прежнее название – Гостехкомиссия при Президенте России) осуществляет деятельность по технической защите конфиденциальной информации;

Теперь перейдем к анализу иных функций в области защиты информации различных органов государственной власти, ключевая роль среди которых, безусловно, принадлежит ФСБ России.

Положение о Федеральной службе безопасности Российской Федерации и современная структура органов федеральной службы безопасности были утверждены Указом Президента РФ от 11 августа 2003 г. № 960[1].

К числу основных задач ФСБ России по защите информации отнесены:

– обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям, осуществляющим техническую разведку;

– 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.

[1] Вопросы Федеральной службы безопасности РФ : указ Президента РФ от 11 августа 2003 г. № 960 // Собрание законодательства РФ. 18.08.2003. № 33. Ст. 3254.

В соответствии с поставленными задачами ФСБ России осуществляет следующие основные функций в области защиты информации:

– в пределах своих полномочий разрабатывает меры по защите сведений, составляющих государственную тайну, осуществляет контроль за обеспечением сохранности сведений, составляющих государственную тайну, в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, воинских формированиях и организациях, осуществляет меры, связанные с допуском граждан к сведениям, составляющим государственную тайну, а также с допуском предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации и с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны;

– координирует деятельность: федеральных органов исполнительной власти по осуществлению контрразведывательных мероприятий и мер по обеспечению собственной безопасности этих органов; федеральных органов исполнительной власти и организаций по обеспечению 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; федеральных органов исполнительной власти в области разработки, производства, закупки, ввоза в Российскую Федерацию и вывоза из Российской Федерации специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, а также их оперативных подразделений по выявлению нарушений установленного порядка разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза из Российской Федерации специальных технических средств, предназначенных для негласного получения информации;

– определяет порядок осуществления контроля за обеспечением защиты сведений, составляющих государственную тайну, в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, воинских формированиях и организациях, а также порядок проведения мероприятий, связанных с допуском граждан к сведениям, составляющим государственную тайну, и с приемом на военную службу (работу) в органы и войска;

– определяет порядок осуществления в пределах своих полномочий контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи, за соблюдением режима секретности при

обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории Российской Федерации и в ее учреждениях, находящихся за пределами Российской Федерации, а также за обеспечением защиты особо важных объектов (помещений) и находящихся в них технических средств от утечки информации по техническим каналам;

– определяет порядок допуска к участию в оперативно-розыскной деятельности и (или) доступа к материалам, полученным в результате ее осуществления органами и войсками;

– участвует в обеспечении закрытой телефонной, шифрованной и иных видов специальной связи с учреждениями Российской Федерации, находящимися за ее пределами (представительская связь), а также в проведении работ по обеспечению ввода в эксплуатацию шифровальных комплексов (в том числе в учреждениях Российской Федерации, находящихся за ее пределами) и развитию системы представительской связи;

– участвует в разработке и реализации мер по обеспечению информационной безопасности страны и защите сведений, составляющих государственную тайну;

– осуществляет и организует в соответствии с федеральным законодательством сертификацию средств защиты информации, систем и комплексов телекоммуникаций, технических средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах, специальных технических средств, предназначенных для негласного получения информации, технических средств обеспечения безопасности и (или) защиты информации; определяет основные направления деятельности органов федеральной службы безопасности в этих областях;

– осуществляет и организует в соответствии с федеральным законодательством лицензирование отдельных видов деятельности;

– организует и осуществляет шифровальную работу в органах и войсках;

– организует и обеспечивает эксплуатацию, безопасность, развитие и совершенствование открытой и засекреченной связи, систем оповещения и звукоусиления на объектах органов и войск;

– осуществляет регулирование в области разработки, производства, реализации, эксплуатации, ввоза в Российскую Федерацию и вывоза из Российской Федерации шифровальных (криптографических) средств и защищенных с использованием шифровальных средств систем и комплексов телекоммуникаций, а также в области предоставления на территории Российской Федерации услуг по шифрованию информации и выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах;

– осуществляет разработку и производство ключевых документов к шифровальным средствам и ручных шифров, снабжение ими федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, нормативно-техническую документацию на производство и использование шифровальных средств, за исключением шифровальных средств, предназначенных для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации;

– обеспечивает выявление на территории Российской Федерации радиоизлучения передающих радиоэлектронных средств, работа которых представляет угрозу безопасности Российской Федерации, а также передающих радиоизлучения радиоэлектронных средств, используемых в противоправных целях; перехватывает передачи и пресекает работу на территории Российской Федерации средств радиосвязи и других передающих радиоэлектронных средств, представляющих угрозу безопасности Российской Федерации; осуществляет регистрацию и централизованный учет радиоданных и радиоизлучений передающих радиоэлектронных средств;

– организует и осуществляет в пределах своих полномочий проведение научных исследований по проблемам обеспечения безопасности личности, общества и государства; проводит научные и опытно-конструкторские работы, разрабатывает и изготавливает специальные и иные технические средства как на собственной научно-производственной базе, так и на базе других предприятий, учреждений и организаций;

– организует и проводит исследования в области защиты информации, экспертные криптографические, инженерно-криптографические и специальные исследования шифровальных средств, специальных и закрытых информационно-телекоммуникационных систем;

– осуществляет подготовку экспертных заключений на предложения о проведении работ по созданию специальных и защищенных с использованием шифровальных (криптографических) средств информационно-телекоммуникационных систем и сетей связи;

– осуществляет сбор, хранение, обработку и использование документированной информации ограниченного доступа для обеспечения контрразведывательной, разведывательной, оперативно-розыскной и иной деятельности, отнесенной федеральным законодательством к компетенции органов и войск;

– разрабатывает, в установленном порядке создает и использует информационные системы, системы связи и передачи данных, а также средства защиты информации, в том числе средства криптографической защиты;

– осуществляет меры по зашифровке сотрудников органов и войск, ведомственной принадлежности подразделений, предприятий, учрежде-

ний, организаций, помещений и транспортных средств, а также личности граждан, оказывающих содействие органам и войскам на конфиденциальной основе, в том числе изготавливает и использует в этих целях документы федеральных органов исполнительной власти, предприятий, учреждений и организаций (документы оперативного прикрытия);

– направляет в федеральные органы исполнительной власти, на предприятия, в учреждения и организации обязательные для исполнения запросы о предоставлении органам федеральной службы безопасности на безвозмездной основе бланков документов и служебных удостоверений, их реквизитов и образцов их заполнения;

– изготавливает документы оперативного прикрытия в интересах федеральных органов исполнительной власти, входящих в систему сил обеспечения безопасности Российской Федерации, на основе заключаемых с этими органами соглашений;

– присваивает в установленном порядке органам и войскам, а также кораблям и судам органов и войск действительные и условные наименования и определяет порядок применения таких наименований;

– осуществляет в установленном порядке финансирование Академии криптографии Российской Федерации, материально-техническое и иное обеспечение ее деятельности.

Положение о ФСТЭК России утверждено Указом Президента Российской Федерации от 16 августа 2004 г. № 1085[1].

В настоящее время в связи с новым Положением указанная Служба 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 системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере (далее – безопасность информации в ключевых системах информационной инфраструктуры);

– противодействия иностранным техническим разведкам на территории Российской Федерации (далее – противодействие техническим разведкам);

– обеспечения защиты (не криптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по тех-

[1] Вопросы Федеральной службы по техническому и экспортному контролю : указ Президента РФ от 16.08.2004 № 1085 [Электронный ресурс] // Официальный интернет-портал правовой информации : [сайт]. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

ническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации (далее – техническая защита информации);

– защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

– осуществления экспортного контроля.

ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.

Она является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну.

ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации, вместе с тем, она подведомственна Минобороны России.

Согласно п. 7 Положения о Министерстве обороны, утвержденного Указом Президента России от 16 августа 2004 г. № 1082 «Вопросы Министерства обороны Российской Федерации», оно выполняет следующие функции в области защиты информации:

– организует деятельность по обеспечению информационной безопасности, защите государственной тайны в Вооруженных Силах;

– организует в установленном порядке в пределах своей компетенции работы по оценке соответствия вооружения и военной техники, а также по сертификации средств защиты информации, стандартизации оборонной продукции и каталогизации предметов снабжения, метрологическому обеспечению войск (сил);

– организует в установленном порядке патентно-лицензионную, изобретательскую, рационализаторскую работу и учет результатов интеллектуальной деятельности, осуществляет распоряжение от имени Российской Федерации результатами интеллектуальной деятельности, полученными при выполнении государственного оборонного заказа, в том числе исключительными правами на них, а также организует рассмотрение заявок и выдачу патентов на секретные изобретения, относящиеся к средствам вооружения и военной техники;

– утверждает тактико-технические требования к образцам вооружения и военной техники, разрешенным для экспорта, экспортную ком-

плектацию продукции военного назначения, а также основные положения научно-исследовательских и опытно-конструкторских работ военного назначения, разрешенных для экспорта;

– осуществляет военно-техническое сопровождение поставок продукции военного назначения, предназначенной для экспорта, в том числе контроль качества и приемку указанной продукции.

В соответствии с этими полномочиями Минобороны выдает соответствующие лицензии на осуществление различных видов деятельности, связанных с информационной безопасностью. Условием их получения является соблюдение лицензиатами требований нормативной и методической документации Министерства обороны РФ в области создания средств защиты информации.

К числу специальных субъектов системы по защите информации относятся также Министерство внутренних дел и Министерство иностранных дел России.

В соответствии с Положением о Министерстве внутренних дел Российской Федерации, утвержденным Указом Президента РФ 19 июля 2004 г. № 927 «Вопросы Министерства внутренних дел Российской Федерации», в этой части на него возложены обязанности по защите государственной тайны в различных сферах осуществления его полномочий, фигурирующих в п. 8 указанного документа.

Различные категории секретной информации, образующейся в ходе оперативно-служебной деятельности органов внутренних дел и требующей соответствующей защиты, систематизированы в развернутых перечнях сведений, подлежащих засекречиванию Министерством внутренних дел Российской Федерации».

На МВД России возложен ряд организационно-практических функций в сфере зашиты информации. Как известно, нарастание, усложнение и видоизменение преступной деятельности, связанной с использованием глобальных компьютерных сетей, приводит к вытеснению примитивного уголовного типа интеллектуальным и предприимчивым преступником с более изощренными способами преступной деятельности. Ученые отмечают «резкий рост организованной преступности, связанной с использованием электронных и телекоммуникационных средств, особенно компьютерных сетей». Для противоправных деяний такого рода характерны конспирация, многообразие способов совершения и сокрытия следов, постоянный поиск новых форм реализации преступных замыслов. Интенсивное развитие российского сегмента Интернета, увеличение объемов финансовых операций, осуществляемых с его использованием, расширение системы электронной торговли позволяют предположить, что в ближайшие годы рост преступности в отечественных глобальных компьютерных сетях будет продолжаться.

В конце 1990-х гг. в системе органов внутренних дел для борьбы с преступлениями в сфере высоких технологий были созданы самостоятельные подразделения «Р», основной функцией которого была борьба с незаконным оборотом радиоэлектронных и специальных технических средств – отсюда и буква «Р» («радио»).

Кардинально изменившиеся условия привели к тому, что отдел «Р» был реорганизован и позже переименован в сложную аббревиатуру УБПСВТ (Управление по борьбе с преступлениями в сфере высоких технологий).

На сегодняшний день Управление по борьбе с преступлениями в сфере высоких технологий преобразовано в отдел «К». Основным направлением его работы является борьба с компьютерными преступлениями и незаконным оборотом радиоэлектронных и специальных технических средств.

Управление «К» – подразделение Министерства внутренних дел России, борющееся с преступлениями в сфере информационных технологий, а также с незаконным оборотом радиоэлектронных средств и специальных технических средств. В субъектах Российской Федерации функционируют соответствующие структурные подразделения службы криминальной полиции – Отделы «К». Управление является одним из самых засекреченных подразделений МВД России.

Управление «К» МВД России в пределах своей компетенции осуществляет выявление, предупреждение, пресечение и раскрытие:

1) преступлений в сфере компьютерной информации:

– неправомерный доступ к охраняемой законом компьютерной информации;

– создание, использование и распространение вредоносных компьютерных программ;

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей;

– мошенничество в сфере компьютерной информации;

2) преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) и направленных против здоровья несовершеннолетних и общественной нравственности:

– изготовление и распространение материалов или предметов с порнографическими изображениями несовершеннолетних;

– использование несовершеннолетнего в целях изготовления порнографических материалов или предметов;

3) преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации;

4) преступлений, связанных с незаконным использованием объектов авторского права или смежных прав.

Указанным Распоряжением осуществление целого ряда важных мероприятий по борьбе с киберпреступностью было возложено и на Министерство иностранных дел России.

Ему, как головному ведомству, совместно с МВД России, ФСБ России, ФСНП России, ФТС России, Миннауки России, Гостелекомом России, Минфином России и Генеральной прокуратурой Российской Федерации предписывалось:

– принять участие в подготовке проектов международных соглашений и иных документов о сотрудничестве в противодействии преступлениям в сфере высоких технологий, разрабатываемых в рамках Организации Объединенных Наций, Совета Европы и других международных организаций;

– обеспечить при достижении соответствующих договоренностей включение в международные соглашения о сотрудничестве в борьбе с преступностью вопросов, связанных с взаимодействием в борьбе с преступлениями в сфере высоких технологий;

– принимать участие в мероприятиях Организации Объединенных Наций, «Группы восьми», Совета Европы и других международных организаций, посвященных проблемам борьбы с преступлениями в сфере высоких технологий, обмену опытом, подготовке и повышению квалификации кадров в этой области.

Существенным фактором для обеспечения развития связи стало принятие Государственной думой в январе 1995 г. Федерального закона «О связи» и утверждение Государственной комиссии по электросвязи (далее – ГКЭС).

За последние годы отлажена четкая система по координации и контролю со стороны ГКЭС за работами по развитию федеральной электросвязи в целях обеспечения планомерного, экономически целесообразного, взаимно сбалансированного и скоординированного развития сетей электросвязи на территории Российской Федерации и создания на этой основе единого телекоммуникационного пространства.

В ходе принятия решения о применении тех или иных средств защиты информации (средств информатизации в специальном защищенном исполнении) необходимо руководствоваться данными из государственного реестра сертифицированных средств защиты информации. Информация о сертифицированных средствах имеется в Управлении информационно-телекоммуникационных технологий и связи Департамента тыла МВД России. Таким образом, с формальной точки зрения, организационно-правовое обеспечение безопасности ведомственной информации, информационных

ресурсов, средств и систем информатизации в области ОРД обеспечивается на достаточно высоком уровне.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

– разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;

– обеспечение баланса созидательных и ограничительных (в первую очередь преследующих цель наказать виновных) законов;

– интеграция в мировое правовое пространство;

– учет современного состояния информационных технологий.

Лекция 3. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

План

1. Каналы утечки информации.
2. Современные угрозы утечки информации.
3. Технические средства обнаружения угроз.
4. Методы и средства блокирования каналов утечки информации.

3.1. Каналы утечки информации

Интегральная защита – это целостная плотная защита, которая напоминает прочную преграду (ограждение) по периметру зоны безопасности. Система безопасности настоящего времени больше напоминает ограждение на отдельных участках со сквозящими в нем дырами.

Речь идет о реальной системе безопасности с организацией мощной системы контроля доступа, системы видеонаблюдения, криптозащиты и т. п., но без блокирования каналов утечки. Например, за счет побочных излучений мониторов компьютеров. В этом случае недоброжелатель, находящийся в радиусе до 1−1,5 км, имеет реальную возможность, использовать определенные технические средства, считывать информацию с экрана дисплеев, не покидая своего рабочего места. При интегральном подходе к созданию системы безопасности подобные казусы исключены.

Одним из важных требований интегральной защиты выступает системный подход. При обнаружении технических каналов утечки информации необходимо применять все приемы элементов защиты, включающие основное оборудование технических средств обработки информации (ТСОИ), системы электропитания, соединительные линии, распределительные и коммуникационные устройства, системы заземления и т. п.

Немаловажное значение, по мимо основных технических средств, непосредственно связанных с обработкой и передачей конфиденциальной информации, стоит обратить внимание и на вспомогательные технические средства и системы (далее − ВТСС). В качестве ВТСС могут выступать технические средства открытой телефонной, громкоговорящей связи, системы охранной и пожарной сигнализации, электробытовые приборы и т. д.

Вспомогательные средства, которые находятся за пределами контролируемой зоны, могут выступать также в качестве каналов утечки информации. К ним можно отнести посторонние провода и кабели, к ним не относящиеся, но проходящие через помещение, где расположены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

В зависимости от метода перехвата, от физических характеристик возникновения сигналов, а также среды их распространения технические каналы утечки информации можно разделить на: электрические, электромагнитные и параметрические.

Электрические каналы

Типовыми факторами образования электрических каналов утечки могут стать:

– при излучении элемента технических средств обработки информационных сигналов образуются наводки электромагнитных технических средств обработки информации. Также наводки могут возникнуть, где расположены соединительные линии технических средств обработки информации и посторонних проводников или линии вспомогательных средств обработки информации;

– при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания может возникнуть просачивание электромагнитных сигналов в цепи электропитания или за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала;

– за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны, происходит просачивание информационных сигналов в цепи заземления;

– съем информации с использованием закладных устройств. Представляют собой минипередатчики, устанавливаемые в технических средствах обработки информации, излучение которых модулируется информационным сигналом и принимается за пределами контролируемой зоны.

Электромагнитные каналы

Для электромагнитных каналов типичными являются побочные излучения:

– электромагнитные излучения на частотах производства высокочастотных генераторов технических средств обработки информации, вспомогательных средств обработки информации. Вследствие внешних влияний информационного сигнала на элементы генераторов наводятся электрические сигналы, они активизируют непроизвольную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство;

– электромагнитные излучения технических средств обработки информации. Носителем информации является электрический ток. Сила тока, напряжение, частота или фаза которого модифицируется по закону информационного сигнала;

– электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты ТСПИ. Самовозбуждение может быть за счет случайных преобразований отрицательных обратных связей в паразитные положительные. Это приводит к переходу усилителя из режима усиления в

режим автогенерации сигналов, причем сигнал на частотах самовозбуждения оказывается промодулированным информационным сигналом.

Воздушные технические каналы

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные и направленные микрофоны, которые соединяются с диктофонами или специальными минипередатчиками. Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют закладными устройствами или акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т. п.

Особого внимания заслуживают закладные устройства, прием информации с которых можно осуществлять с обычного телефонного аппарата. Для этого их устанавливают либо непосредственно в корпусе телефонного аппарата, либо подключают к телефонной линии в телефонной розетке. Подобные устройства, конструктивно объединяющие микрофон и специальный блок коммутации, часто называют «телефонным ухом». При подаче в линию кодированного сигнала или при дозвоне к контролируемому телефону по специальной схеме блок коммутации подключает микрофон к телефонной линии и осуществляет передачу акустической (обычно речевой) информации по линии практически на неограниченное расстояние.

Вибрационные каналы

В отличие от рассмотренных выше каналов в вибрационных, или структурных, каналах утечки информации средой распространения акустических сигналов является воздух, конструкции зданий (стены, потолки, полы), трубы водо- и теплоснабжения, канализации и другие твердые тела. В этом случае для перехвата акустических сигналов используются контактные, электронные (с усилителем) и радиостетоскопы (при передаче по радиоканалу).

Электроакустические каналы

Электроакустические каналы утечки информации обычно образуются за счет электроакустических преобразований акустических сигналов в электрические по двум основным направлениям: путем «высокочастотного навязывания» и путем перехвата через дополнительные технические средства и системы. Технический канал утечки информации путем высокочастотного навязывания образуется путем несанкционированного контактного введения токов высокой частоты от ВЧ-генераторов в линии, имеющие функциональные связи с элементами вспомогательных технических средств и систем, на которых происходит модуляция ВЧ-сигнала информации. Наиболее часто подобный канал утечки информации используют для перехвата разговоров, ведущихся в помещении, через телефонный ап-

парат, имеющий выход за пределы контролируемой зоны. С другой стороны, вспомогательные технические средства и системы могут сами содержать электроакустические преобразования. К таким вспомогательным техническим средствам и системам относятся некоторые датчики пожарной сигнализации, громкоговорители ретрансляции сети и т. д. Используемый в них эффект обычно называют микрофонным эффектом.

Перехват акустических колебаний в этом случае осуществляется исключительно просто. Например, подключая рассмотренные средства к соединительным линиям телефонных аппаратов с электромеханическими звонками, можно при положенной трубке прослушивать разговоры, ведущиеся в помещениях, где установлены эти телефоны.

Оптико-электронные каналы

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких, как стекла окон, зеркала, картины и т. п., создается оптико-электронный, или лазерный, канал утечки акустической информации. Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие, как правило, в ближнем инфракрасном диапазоне волн и известные как «лазерные микрофоны». Дальность перехвата составляет несколько сотен метров.

Параметрические каналы

Параметрический канал утечки информации создастся в следствие влияния акустического поля на элементы высокочастотных генераторов и видоизменения взаимного расположения элементов схем, дросселей, проводов и т. п., что приводит к изменениям параметров сигнала. Промодулированные высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы соответствующими средствами. Параметрический канал утечки информации может быть создан и путем «высокочастотного облучения» комнаты, где поставлены полуактивные заложенные устройства, которые имеют элементы, параметры которых видоизменяются по закону изменения акустического сигнала.

Надо заметить, что акустический канал бывает источником утечки не только речевой информации. В периодической печати встречаются случаи, когда с помощью статистической обработки акустической информации с принтера или клавиатуры получалось перехватывать электронную текстовую информацию.

Большой интерес доставляет перехват информации во время трансляции по каналам связи. В этом случае обеспечивается свободный несанкционированный доступ к передаваемым сигналам. Метод криптографической защиты в этом случае является единственной гарантией защиты информации. Технические каналы перехвата информации в зависимости от

типа каналов связи можно обозначить как электрические, электромагнитные и индукционные.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, полагает контактное подсоединение к этим линиям. Этот канал чаще всего применяется при перехвате телефонных разговоров. Во время чего прослушиваемая информация может быть зафиксирована на диктофон или передана по радиоканалу. Аналогичные приборы, подсоединяемые к телефонным линиям связи и содержащие радиопередатчики для ретрансляции перехваченной информации, как правило, именуются телефонными закладками.

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств. Такой электромагнитный канал перехвата информации обширно применяется для прослушивания телефонных разговоров (радиотелефонам, сотовым телефонам и спутниковым линиям связи).

Однако непосредственное электрическое подключение аппаратуры перехвата является компрометирующем симптомом, поэтому чаще используется индукционный канал перехвата, не требующий контактного подключения к каналам связи. Современные индукционные датчики могут снимать информацию с кабелей, которые защищены помимо изоляции двойной броней из стальной ленты и стальной проволоки, плотно оплетающих кабель.

Утечке видовой информации, которая получается техническими средствами в виде представлений объектов или копий документов путем слежения за объектом, съемки объекта и копирования документов в настоящее время уделяется огромное внимание. Подобные технические средства в виде оптики используются в зависимости от условий наблюдения.

Для документирования последствий наблюдения осуществляется съемка объектов. Для этого применяются фотографические и телевизионные средства, соответствующие условиям съемки. Для снятия копий документов применяются электронные и специальные портативные фотоаппараты всевозможных модификаций. Для дистанционного съема видовой информации используют видеозакладки.

Очень стабильно развиваются в настоящее время методы съема компьютерной информации. Несанкционированный доступ, включающий в себя такие составляющие, как «троянские кони», компьютерные вирусы, программные закладки, «логические бомбы» снабжаются специальным математическим обеспечением.

И так методы приобретения информации сформированы на применении внешних каналов утечки. Но также необходимо остановиться и на внутренних каналах утечки информации.

Внутренние каналы утечки связаны:

– с администрацией;

– обслуживающим персоналом;
– с качеством организации режима работы.

Из них в первую очередь можно отметить такие каналы утечки, как:
– хищение носителей информации;
– использование производственных и технологических отходов;
– визуальный съем информации с дисплея и принтера;
– съем информации с ленты принтера и плохо стертых дискет;
– несанкционированное копирование и т. п.

3.2. Современные угрозы утечки информации

Для защиты от различных атак целесообразно использовать две стратегии. Первая состоит в приобретении самых разрекламированных систем защиты от всех возможных видов атак. Вторая стратегия – в предварительном анализе вероятно возможных угроз и последующем отборе средств и методов защиты от них.

Анализ угроз, или анализ риска, также может осуществляться двумя путями. При первом прежде, чем выбрать наиболее вероятные угрозы, необходимо провести анализ информационной системы, обрабатываемой в ней информации, используемого программно-аппаратного обеспечения и т. д. Сложный, но более эффективный способ. Это позволяет значительно сузить спектр вероятных атак и тем самым увеличить эффективность затраченных денежных вложений в приобретаемые средства защиты. Отрицательным моментом при осуществлении такого анализа является большая затрата времени и средств, высокой квалификации специалистов, производящих исследование анализируемой сети.

При втором можно выбрать средства защиты на основе обычных распространенных стандартных угроз.

Наиболее распространенными преступлениями являются:

– неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

– создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

Процессы глобальной компьютеризации и цифровизации, происходящие в современном мировом сообществе, имеют как положительные, так и отрицательные последствия, порой приводят к модификации преступности, которая стремительно видоизменяется, приобретая новые характеристики.

Согласно статистическим данным за 2018 год правоохранительными органами Российской Федерации было зарегистрировано более ста тысяч преступлений, совершенных с использованием информационно-

телекоммуникационных технологий[1]. По сравнению с 2017 годом количество такого рода преступлений возросло более чем на 33 %. За последние шесть лет киберпреступность, согласно статистике, демонстрирует десятикратный рост. Так, в 2013 году подобных преступлений было порядка 11 тысяч, в 2014 году 44 тысячи, в 2016 году более 66 тысяч. За 2019 год насчитывается порядка 150 тысяч киберпреступлений, что на 149 процентов больше, чем в 2018 году. При этом почти половина всех зафиксированных киберпреступлений (48,5 %) относится к категориям тяжких и особо тяжких.

По опубликованным данным следует, что только с 2015 по 2016 год число мошенничеств в области информационных технологий выросло в шесть раз (с 2,2 тыс. до 13,4 тыс.), число краж возросло более чем в три раза (с 2,3 тыс. до 8,5 тыс.), количество преступлений с использованием глобальной сети Интернет и иных инфокоммуникационных технологий возросло в 5,5 раз (с 995 до 5,5 тыс.). Наносимый материальный ущерб только по сравнению с предыдущим годом возрос на 33,4 %, кроме того отмечается тенденция снижения уровня раскрываемости преступлений правоохранительными органами (в среднем на 2 %), что является следствием вновь организующихся форм правонарушений в этой области и недостатком применения мер по противодействию им. Удельный вес преступлений с использованием инфокоммуникационных технологий от общего числа зарегистрированных за 2018 год преступлений составляет 8,1 %.

Данная статистика наглядно показывает необходимость решения проблем противодействия преступности в глобальной сети Интернет, своевременного принятия мер по предупреждению киберпреступлений.

Так, в апреле 2019 года, согласно, сведениям информационного портала «ItSec – Информационная безопасность»[2], неправомерно был обнародован реестр лиц, сформированный банковскими структурами в соответствии с требованиями Федерального закона № 115-ФЗ от 7 августа 2001 года «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[3]. Сложившаяся ситуация негативно может сказаться не только на статусе лиц, входящих в обна-

---

[1] Ежемесячный сборник о состоянии преступности в России [Электронный ресурс] // Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации, Российская Федерация, 2020 URL: http://crimestat.ru/analytics (дата обращения: 12.08.2020).

[2] ItSec – Информационная безопасность [Электронный ресурс] // Информационный портал. Российская Федерация, 2019. URL: http://www.itsec.ru/news/v-set-utiok-chiorniy-spisok-klientov-bankov-podozreva emih-v-otmivanii-dohodov (дата обращения: 12.08.2020).

3 О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : федеральный закон от 7 августа 2001 года № 115-ФЗ – [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

родованный список, но также подорвать экономическую ситуацию страны в целом.

Решение проблемы кроется не только в шифровании информации и использовании сертифицированных средств криптографической защиты информации, но и в грамотном подходе при проектировании систем защиты информации, повышении ответственности за несоблюдение условий конфиденциальности. Преступления такого рода подпадают под статью о незаконном получении и разглашении сведений, составляющих банковскую тайну, и влекут за собой ответственность в виде лишения свободы сроком до семи лет.

Основными проблемами противодействия преступности в сети Интернет на сегодняшний день являются:

1. Низкое количество сообщений от потерпевших в правоохранительные органы о совершении преступлений с использованием инфокоммуникационных технологий.

2. Недостаточный уровень квалификации сотрудников, привлекаемых к раскрытию преступлений в области информационных технологий.

3. Недостаточное финансирование сферы противодействия киберпреступлениям (проблема оснащения подразделений, занимающихся раскрытием киберпреступлений, современными техническими средствами).

4. Нарушение прав на неприкосновенность частной жизни при расследовании киберпреступлений.

5. Наличие лишь общезаконодательных мер и отсутствие положений, наиболее полно рассматривающих порядок расследования преступлений в сети Интернет.

6. Идентификация преступников, в случаях, когда преступление совершено с использованием незащищенной сети передачи данных (открытые Wi-Fi-сети, локальные сети предприятий, облачные хранилища и пр.).

7. Недостаточный уровень стратегически спланированных мер по предотвращению преступлений в сети Интернет.

Согласно опубликованному Всестороннему исследованию проблем киберпреступности Управления Организации Объединенных Наций по наркотикам и преступлениям (далее – УНП ООН)[1], в среднем, по всему миру, в правоохранительные органы обращается лишь 1 % жертв преступных посягательств в области информационных технологий, в ряде международных исследований частного сектора приводится статистика об обращении лишь 20 % лиц, ставших жертвами киберпреступлений.

[1] Comprehensive study on cybercrime (february 2013) – Всестороннее исследование проблемы киберпреступности (февраль 2013 года) / United Nations Office on Drugs and Crime [Электронный ресурс] // Официальный интернет-портал Управления Организации Объединенных Наций по наркотикам и преступлениям, УНП ООН, 2018. URL: www. unodc.org/documents/organized-crime/cybercrime/cybercrime_ study_210213.pdf (дата обращения: 12.08.2020).

Часто бездействие потерпевших обуславливается безосновательным предположением о крайне низкой вероятности раскрытия преступления. Кроме того, в случае обращения в правоохранительные органы потерпевшие зачастую не могут предоставить минимально необходимые данные и электронные доказательства для создания картины расследования (точки доступа к данным, параметры входа в сеть, учетные данные и пр.), что является следствием пока еще низкого уровня просвещенности населения в области информационно-коммуникационных технологий, в частности в странах с низким показателем индекса человеческого развития. Также, как отмечается в некоторых источниках[1], крупные компании и корпорации не желают сообщать в правоохранительные органы о совершенных преступлениях в сети Интернет в связи с действующей репутационной политикой.

В связи с этим предлагается повышать уровень информированности населения, активизировать просветительскую деятельность, отдельные виды преступлений, в частности, расследования в отношении крупных корпораций и компаний следует брать под особый контроль с учетом сохранения репутационной политики.

Недостаточный уровень квалификации сотрудников, привлекаемых к раскрытию преступлений в области информационных технологий, обусловлен цифровой революцией, часто обучение специалистов осуществляется с большим временным отрывом, что особенно заметно в данной области в условиях глобализации. Для определения уровня развития ведомств по раскрытию преступлений в глобальной сети Интернет введен показатель – количество специалистов на 100 тысяч пользователей[2]. Так, в развитых странах, согласно данным, приводимым УНП ООН, данный показатель варьируется в пределах от 0,4 до 1, в менее развитых странах показатель достигает 0,2. Отдельной проблемой является отставание стран в сфере высоких технологий (например, по индексу развития человеческого потенциала), как следствие уровень национальной информационной безопасности таких стран обеспечивается недостаточно. Решение данной проблемы кроется в разработке образовательных программ с учетом необходимости изучения не только основ информационной безопасности на правовом и организационном уровнях, но и с учетом специфики киберпреступлений на техническом уровне – физическом, аппаратном, программном и криптографическом. При подготовке специалистов отдельно следует рассматривать компьютерную криминалистику (форензику), уделять внимание мето-

[1] Вопросник Управления Организации Объединенных Наций по наркотикам и преступлениям к государствам-членам УНП ООН, УНП ООН. Вопрос 82. 2012. CU 2012/19.

[2] Comprehensive study on cybercrime (february2013) – Всестороннее исследование проблемы киберпреступности (февраль 2013 года) / United Nations Office on Drugs and Crime [Электронный ресурс]. Официальный интернет-портал Управления Организации Объединенных Наций по наркотикам и преступлениям, УНП ООН, 2018. URL: www. unodc.org/documents/organized-crime/cybercrime/cybercrime_ study_210213.pdf (дата обращения: 12.08.2020).

дам сбора цифровых доказательств, изучению фреймворков для криминалистического анализа и проведения оперативных исследований на удаленных конечных точках, анализа сетевого взаимодействия, средств извлечения информации с исследуемых образов операционных систем, жестких дисков и энергозависимой памяти, средств изучения машинных носителей информации, цифровых устройств и тому подобных элементов.

Отдельной проблемой является недостаточный уровень оснащения подразделений, занимающихся раскрытием киберпреступлений, современными техническими средствами, такими как средства выемки аппаратного обеспечения и электронных доказательств, средств создания электронных образов и хэш-кодов, восстановления данных по «отпечаткам» в памяти жестких дисков, обработки и расшифровки данных, средств удаленной экспертизы оборудования и уничтожения информации. Увеличение финансирования этой области является, пожалуй, неотъемлемым условием повышения качества раскрытия киберпреступлений.

Кроме того, получение правоохранительными органами электронных доказательств от поставщиков услуг Интернет часто требует дополнительных вмешательств, связанных с оформлением документов, разрешающих сбор, обработку и перехват интересующей информации. В Российской Федерации признание электронных доказательств введено лишь с 1 января 2017 года, так, в качестве доказательств допустимо использовать письменные и вещественные доказательства, сведения в виде аудиозаписей и видеоматериалов, в том числе электронную переписку. Согласно ч. 3 ст. 75 Арбитражного процессуального кодекса Российской Федерации № 95-ФЗ от 24 июля 2002 года в качестве письменных доказательств допускаются также документы, полученные посредством факсимильной, электронной или иной связи, в том числе с использованием глобальной сети Интернет, также в качестве доказательств отныне допустимо использовать документы, подписанные электронной цифровой подписью[1].

Использование клавиатурных шпионов, программного обеспечения удаленного администрирования и программ сбора данных является вмешательством в частную личную жизнь, лишь ряд международных документов предусматривает порядок проведения удаленной судебной экспертизы сотрудниками правоохранительных органов и экспертами. Для исключения трудностей передачи данных от оператора-обработчика конфиденциальных данных целесообразно пересмотреть механизм предоставления данных.

Отдельной проблемой является невозможность или сложность получения экстерриториальных данных, информации, хранящейся на серверах иностранных государств и находящейся вне юрисдикции следственных ор-

[1] Арбитражный процессуальный кодекс Российской Федерации : федеральный закон от 24 июля 2002 г. № 95-ФЗ. – [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http:// www.pravo.gov.ru (дата обращения: 12.08.2020).

ганов[1]. В этих целях целесообразно налаживать связь с поставщиками услуг и разработчиками информационных систем, обладающими правами использования, хранения и обработки данных о пользователях, в том числе о совершаемых ими действиях.

Часто при получении запросов от правоохранительных органов интернет-провайдеры и поставщики услуг ссылаются на нормы права, ограничивающие передачу конфиденциальных данных. Под передаваемыми данными понимаются IP-адреса, истории соединений, точки доступа и истории сеансов, идентификационные данные, переписки, cookie-файлы, информация об используемом пользователем устройстве и его параметрах, данные о местоположении – так называемые артефакты. Как правило, передача данных производится на основании официальных запросов, что требует значительных усилий специалистов по оформлению всех необходимых для этого документов и продолжительного времени.

Встречаются случаи, когда невозможность причисления отдельных форм преступлений в цифровом пространстве к существующим правовым нормам весьма затрудняет и затягивает ход расследуемого дела. Так, несмотря на наличие общезаконодательных мер, отсутствуют положения, рассматривающие подкатегории киберпреступлений в отдельности, степени нанесения вреда и пр., в связи с этим намечается необходимость проведения мониторинга совершаемых киберпреступлений с целью выработки объективных законодательных мер.

Отдельной проблемой является идентификация преступников, в случаях, когда преступление совершено с использованием незащищенной сети передачи данных (открытые Wi-Fi сети, локальные сети предприятий, облачные хранилища и пр.).

Несмотря на то, что на сегодняшний день практически все общественные сети используют идентификацию абонента, вероятность подмены учетных данных все равно остается. Ежедневно совершаются сотни преступлений с использованием подменных учетных данных, как правило, ситуации такого рода возникают по халатности самих пользователей-потерпевших. В качестве примера можно привести сохраненные связки учетных данных в общественной точке доступа, использование несертифицированного программного обеспечения персональных компьютеров, а также мобильных устройств.

Определенную опасность несут неаттестованные информационные системы предприятий, нешифрованные локальные и облачные хранилища без использования специализированного криптографического программного обеспечения. Как показывает статистика, раскрытие преступлений, свя-

[1] Харисова З. И. Международно-правовые основы информационной безопасности в целях устойчивого развития // Правовое обеспечение развития социального государства в свете целей устойчивого развития: сборник материалов Международной научно-практической конференции. Уфа: РИЦ БашГУ, 2018. С. 103−106.

занных с внедрением злоумышленников в локальные сети и облачные хранилища при отсутствии защищенного с помощью сертифицированных технических и программных средств сегмента сети и несоблюдении требований информационной безопасности практически сводится к нулю.

Поскольку сеть Интернет посредством глобального адресного пространства связывает между собой множество информационных систем и сетей электросвязи всех стран и предоставляет возможность коммуникации лиц с помощью протокола передачи данных важно обеспечивать надлежащее функционирование данной сети в целях предотвращения использования сети Интернет в целях противоречащих концепциям информационной безопасности.

Кроме того, важна своевременность введения поправок в стратегии национальной безопасности[1] и план реализации мероприятий по ее укреплению. В этих целях разработана концепция безопасного функционирования и развития сети Интернет (проект концепции конвенции ООН)[2], где приводятся принципы поведения государств в управлении сетью Интернет международного сотрудничества по управлению глобальной сетью и оказания содействия.

В последние годы виды преступлений в сфере информационных технологий качественно меняются и продолжают непрерывно эволюционировать, становясь высокоорганизованными. Возрастает также техническая оснащенность преступников, в связи со стремительным развитием информационных технологий появляются все новые способы совершения противоправных деяний, а это диктует необходимость принятия незамедлительных и адекватных мер противодействия преступлениям в сфере обращения цифровой информации, необходимости развития компьютерной криминалистики (форензики) и своевременности внесения изменений в программы обучения специалистов в области раскрытия преступлений в области инфокоммуникационных технологий, в частности, и в глобальной сети Интернет.

Обобщив рассмотренные выше результаты, можно провести классификацию возможных угроз безопасности автоматизированных сетей обработки информации (далее − АСОИ), которая представлена ниже.

Показанная классификация угроз безопасности является довольно объемной, ясной и не требует дополнительных разъяснений.

---

[1] Харисова З. И. О некоторых проблемах обеспечения информационной безопасности государства и общества от современных киберугроз / Актуальные проблемы права и государства в XXI веке [Электронное издание]: сборник материалов XI Международной научно-практической конференции, г. Уфа, 18 апреля 2019 года. Уфа: Уфимский ЮИ МВД России, 2019.

[2] Проект концепция конвенции ООН − концепции безопасного функционирования и развития сети «Интернет» [Электронный ресурс] // Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, 2019. URL: https://digital.gov.ru/ru/events/36739/ (дата обращения: 12.08.2020).

Одной из важнейших составляющих политики безопасности является поиск возможно опасных мест в структуре защиты. Выявление угрозы уже до 70 % предопределяет ее ликвидацию.

Известно, что самые большие угрозы в сети происходят от особых специальных программ несанкционированного доступа, компьютерных вирусов и программных закладок, которые определяют угрозу для всех ключевых объектов сети электронных вычислительных машин, в том числе абонентских мест, коммутационных машин и каналов связи, серверов.

Полная открытость сети Интернет делает ее не только уникальной по масштабам, но и создает значительные затруднения в обеспечении безопасности. Интернет стабильно ощущает влияние с использованием несанкционированного доступа. В глубине сети стабильно происходят невидимые вселенной войны в полном соответствии с требованиями современной войны. Есть эффективные информационные средства нападения и защиты, трофеи в виде крупных сумм денег, переведенные на соответствующие счета банков и т. п. Только нет конкретного физического врага, а есть виртуальный противник невидимый, неслышимый неощущаемый. Он только определяется лишь по косвенным признакам, по следствиям его деятельности, которые также тщательно маскируются и скрываются. Но итоговые последствия их влияния являются самыми ощутимыми и реальными, а часто и фатальными.

Подобные операции воздействия недоброжелателей в обычном случае состоят из вытекающих этапов:

- подготовительный;
- несанкционированный доступ;
- основной (разведывательный или диверсионный);
- скрытая передача информации (вспомогательный);
- скрытие следов воздействия.

3.3. Технические средства обнаружения угроз

Угрозы как личной, так и информационной безопасности поджидают нас на каждом шагу. Специалисты уверяют нас, что надежное выявление угрозы – это уже решение алгоритма устранения угрозы на семьдесят процентов. Поэтому в настоящее время интерес к техническим средствам поиска и выявления угроз безопасности существенно усилился. Детекторы и обнаружители являются на сегодня главными и основными элементами многих систем безопасности.

Какие бывают современные обнаружители угроз безопасности?

На сегодняшний день не существует универсальных обнаружителей, причем каждый вид обнаружителей рассчитан на использование при решении определенного класса задач.

Наиболее крупную группу образуют технические средства, используемые для обеспечения информационной безопасности в обнаружения радио-, видео- и телефонных закладок. В большей степени по сбыту на рынке представлены устройства поиска по электромагнитному излучению: приемники, сканеры, частотомеры, шумометры, анализаторы, спектра, детекторы инфракрасного излучения, селективные микровольтметры, панорамные приемники и т. д. Основная задача для всех таких устройств – обнаружение сигнала.

Специализированные приемники для розыска активированных передатчиков в широком диапазоне частот на российском рынке представлены рядом фирм США, Японии и Германии. В основном, современные сканеры обладают возможностью подсоединения к компьютеру. В связи, с чем специально разработанные программы дозволяют автоматически управлять всеми режимами, воспроизводить итоги работы на мониторе, делать запись и сохранять информацию на жестком диске компьютера, помимо всего прочего представлять информацию спектра на мониторе в текущем времени и дает возможность сравнивать его с предыдущим. Результаты анализа в электронном виде выводятся на печать и т. д.

Процесс выявления закладок способом радиомониторинга упрощается больше при применении сканеров, реализующих дополнительную функцию измерения частоты.

Приборы на основе приемников-сканеров, реализующие одновременно несколько функций по поиску закладок, создают отдельную группу. Одним из ярких представителей этой группы можно назвать комплекс OSCOR-5000 и его модификации. Такой комплекс автоматически 24 часа в сутки осуществляет мониторинг источников угрозы. Имеется возможность перехода от обзора широкого спектра к детальному анализу индивидуального сигнала с его демодуляцией и построением графика. Радиоприемник создан по схеме супергетеродина с четырьмя преобразованиями частоты и тремя синтезаторами фазовой подстройки частоты. Предусмотрена демодуляция сигналов в режимах: FM, AM, FMSC, FMW, SSB CW. Имеется жидкокристаллический дисплей и термопринтер. Конструктивно прибор выполнен в корпусе кейса, общий вес комплекса составляет 12,7 кг.

Анализаторы спектра позволяют значительно облегчить просмотр радиоапазона (отечественные разработки анализаторов СМ-4-2 и СМ-4-21).

Для обнаружения скрытных вблизи находящихся радиопередатчиков на малоразмерных объектах благополучно используются детекторы электромагнитного поля. Действие выявления заключается в обнаружении радиопередатчика по увеличению напряженности электромагнитного поля в ближней зоне антенны передатчика. При этом детекторы поля разрабатываются и используются в переносном варианте с установкой их в часах (Ej-6), в кейсе (VL-22H), в книге (VL-34), в пачке сигарет (PK 865), в авторуч-

ке (PK 860) или на теле оператора (DM-19). А также могут использоваться и в стационарном варианте с установкой их в цифровых часах (V-4330), в коробке сигар (PK 865-3) и т. п. Широкая полоса тракта приема и отсутствие настройки на частоты сигналов является свойственной чертой детекторов поля. Недостаточная чувствительность детекторов поля и наличие ложных срабатываний приводят к снижению надежности выявления и увеличения времени поиска. Помимо всего, аналогичные устройства не могут найти передатчики с программным и дистанционным управлением.

Свободными от указанных недостатков являются обнаружители, принципы работы которых основаны на эффекте «нелинейной радиолокации». При облучении радиоэлектронных устройств, содержащих нелинейные элементы (транзисторы, диоды и т. д.), происходит отражение сигнала на высших кратных гармониках. Отраженные сигналы регистрируются локатором независимо включено радиоэлектронное устройство или выключено.

В последнее время в России нелинейные локаторы энергично совершенствуются и находят использование в следующих сферах:

– выявление несанкционированного выноса маркированных предметов из служебных зданий, объектов;

– выявление радиоаппаратуры и электронных элементов при попытке тайно обойти их сквозь контрольно-пропускные пункты таможен режимных объектов, складов и т. д.;

– выявление и определение месторасположения скрытых электронных средств промышленного шпионажа (приемопередающие устройства подслушивания и передачи данных и т. д.);

– дистанционный контроль радиоэлектронных систем, входящих в состав взрывных устройств, размещенных в багаже пассажиров;

– поиск маркированных нелинейных пассивными маркерами людей в разрушенных зданиях, снежных завалах и др.

Главное место среди обнаружителей угроз безопасности занимают детекторы паразитных излучений аппаратуры. Они предназначены для обнаружения активных средств приема и регистрации аудио-, видео- и иной информации. На практике среди них в первую очередь применяются детекторы магнитофонов и обнаружители телекамер. Детекторы магнитофонов используются для скрытного обнаружения носимых магнитофонов и конструктивно применяются в носимом или в стационарном варианте. Операция обнаружения заключается в выявлении паразитного излучения моторчиков магнитофонов, генераторов стирания, электронных схем и т. п.

3.4. Методы и средства блокирования каналов утечки информации

В настоящее время номенклатура технических средств коммерческой разведки весьма обширна, что делает задачу надежного блокирования каналов утечки и несанкционированного доступа к информации исключительно сложной.

Решение подобной задачи возможно только с использованием профессиональных технических средств и с привлечением квалифицированных специалистов. В таблице 1 рассмотрены каналы утечки информации и возможные методы их блокирования.

Основным направлением противодействия утечке информации является обеспечение физической (технические средства, линии связи, персонал) и логической (операционная система, прикладные программы и данные) защиты информационных ресурсов. При этом безопасность достигается комплексным применением аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий.

Таблица 1

Основные методы и средства несанкционированного получения информации и возможная защита от них

№	Действие человека (типовая ситуация)	Каналы утечки информации	Методы и средства получения информации	Методы и средства защиты информации
1	Разговор в помещении или на улице	Акустика, виброакустика, гидроакустика	Подслушивание, стетоскоп, вибродатчик, гидроакустический датчик	Шумовые генераторы, поиск закладок, ограничение доступа
2	Разговор по проводному телефону	Акустика, электросигнал в линии, наводки	Параллельный телефон, прямое подключение, диктофон, телефонная закладка	Маскировка, шифрование, спецтехника
3	Документ на бумажном носителе	Наличие	Кража, копирование, фотографирование	Ограничение доступа, спецтехника
4	Изготовление документа на небумажном носителе	Изображение на дисплее	Копирование, фотографирование, специальные радиотехнические устройства	Контроль доступа, криптозащита
5	Передача документа по каналу связи	Электрические и оптические сигналы	Несанкционированное подключение, имитация пользователя	Криптозащита

Лекция 4. ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

План

1. Идентификация, аутентификация, авторизация.
2. Разграничение доступа.
3. Протоколирование и аудит.
4. Экранирование.

4.1. Идентификация, аутентификация, авторизация

Идентификацию и аутентификацию можно полагать ядром программно-технических средств безопасности, потому что другие сервисы предназначены на поддержание именованных субъектов. Идентификация и аутентификация – это первая линия обороны, информационного пространства учреждения. Идентификация дает пользователю или процессу, действующему от имени определенного пользователя, или аппаратно-программному компоненту обозначить себя. За счет аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. Аутентификация (проверка подлинности) может быть:

– односторонней, когда пользователь доказывает свою подлинность серверу (например, процедура входа пользователя в систему);

– двусторонней, т. е. взаимной.

В сетевой среде, когда стороны идентификации/аутентификации территориально находятся в разных местах, у рассматриваемого сервиса существует два ключевых аспекта:

– как защищен обмен данными идентификации/аутентификации;

– что используется для доказательства подлинности субъекта.

Субъект может подтвердить свою подлинность, предъявив одну из следующих сущностей:

– пользователь владеет личной карточкой или иным устройством подобного назначения;

– пользователь знает пароль, криптографический ключ, личный идентификационный номер и т. п.;

– пользователь является владельцем своих биометрических данных: голоса, отпечатков пальцев и т. п.

В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута. В общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, модификации и/или воспроизведения данных. Передача паролей в открытом виде сказывается отрицательно; не улучшает ситуацию и

шифрование паролей, потому что оно не защищает от воспроизведения. Необходимы наиболее сложные протоколы аутентификации. Надежная идентификация сложна не только лишь из-за сетевых угроз, но и по целому ряду причин:

– почти все аутентификационные сущности возможно познать, похитить или дублировать;

– между надежностью аутентификации, с одной стороны, и сервисными возможностями пользователя и системного администратора с другой стороны существует противоречие. Оно заключается в том, что для безопасности с определенной частотой нужно просить пользователя вторично вводить аутентификационную информацию, а это может повысить вероятность подсматривания за вводом данных.

– чем практичнее и надежнее средство защиты, тем оно дороже.

Современные средства идентификации/аутентификации обязаны поддерживать систему единого входа в сеть. Это, в первую очередь, требование комфорта для пользователей. Когда в коллективной сети большое количество информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация делается слишком затруднительной. Пока невозможно осуществить единый вход в сеть, преобладающие решения пока не выработались. Поэтому нужно искать компромисс между доступностью по цене, надежностью по качеству, комфортом применения и администрирования средств идентификации и аутентификации. Надо сказать, что сервис идентификации/аутентификации способен стать объектом атак на доступность. В том случае если система разработана так, что после некоторого числа неудачных попыток устройство ввода идентификационной информации блокируется, то недоброжелатель способен заблокировать работу легального пользователя в буквальном смысле слова несколькими нажатиями клавиш.

Парольная аутентификация.

Основное преимущество парольной аутентификации – простота и постоянство. Пароли издавна внедрены в операционные системы и иные сервисы. При точном использовании пароли могут обеспечить приемлемый для многих учреждений степень безопасности. И все таки, по своим характеристикам они являются самым слабым средством контроля подлинности. Для того чтобы пароль запоминался, его нередко придумывают примитивным и ли совсем несложным. При этом элементарный пароль несложно угадать, особенно если знать приверженности или слабости определенного пользователя. Зачастую пароли содержат стандартные значения (например, указанные в документации) и с самого начала не хранятся в тайне, а после установки новой системы не производится их смена.

Ввод пароля возможно подглядеть. Часто для этого даже применяются оптические приборы. Пароли нередко сообщают сослуживцам, для подмены на некоторое время владельца пароля. Теоретически в аналогич-

ных случаях правильнее использовать средства управления доступом, но практически никто не поступает таким образом. И давно известно, что тайна, о которой знают двое и более, уже не является тайной. Пароль возможно распознать. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, если использовать известный алгоритм шифрования.

Какие же меры помогут существенно увеличить надежность и эффективность парольной защиты:

– пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т. п.;
– ограничение числа неудачных попыток входа в систему;
– контроль за сроком действия паролей (периодическая смена);
– инструктаж пользователей;
– ограничение доступа к файлу паролей;
– применение программных генераторов паролей.

Перечисленные меры рационально использовать постоянно, даже если наряду с паролями применяются иные методы аутентификации.

Одноразовые пароли.

Рассмотренные нами пароли можно назвать многоразовыми; их расшифровка дает возможность злоумышленнику орудовать от имени легального пользователя. Гораздо более мощным средством, устойчивым к пассивному прослушиванию сети, оказываются одноразовые пароли.

В компании Bellcore разработана система S/KEY, которая является наиболее известным программным генератором одноразовых паролей.

Идентификация/аутентификация с помощью биометрических данных.

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации пользователей на основе их поведенческих и физиологических характеристик. К поведенческим характеристикам можно отнести стиль работы с клавиатурой или подпись авторучкой. К физиологическим характеристикам относятся узоры отпечатков пальцев, роговицы и сетчатки глаз, геометрия руки, пальцев, лица и т. п. Очень близко находится анализ специфики голоса и распознавания речи.

В настоящее время спрос на биометрические продукты из-за развития электронной коммерции устойчиво и крайне интенсивно увеличивается. Пользователю гораздо спокойнее и комфортнее предъявить самого себя, чем что-то запоминать. Спрос рождает предложение, поэтому на рынке появились сравнительно недорогие аппаратно-программные технические средства, ориентированные первостепенно на распознавание отпечатков пальцев.

Каким образом организована работа с биометрическими данными? Вначале формируется и хранится база данных характеристик потенциаль-

но возможных пользователей. Для чего снимаются и обрабатываются биометрические характеристики пользователя. Результат обработки (биометрический шаблон) вносится в базу данных. Такие исходные данные как результат сканирования роговицы глаз или пальца, как правило, не хранятся. Далее для идентификации/аутентификации пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. Если поиск личности пользователя успешно осуществлен, то подлинность считается установленной.

Для аутентификации достаточно совершить сопоставление с одним биометрическим шаблоном, выбранным на основании предварительно внесенных данных. Как правило биометрию используют совместно с другими аутентификаторами. Активность в области биометрии очень велика. Организован соответствующий консорциум, активно ведутся работы по стандартизации разных аспектов технологии (формата обмена данными, прикладного программного интерфейса и т. п.), публикуется множество рекламных статей, в которых биометрия преподносится как средство предоставления сверхбезопасности, ставшее доступным обширным массам.

Нужно учитывать, что биометрия подвержена тем же угрозам, что и другие методы аутентификации, поэтому к ней необходимо относиться крайне осмотрительно:

– биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения (много чего в пути может произойти);

– биометрические методы не более надежны, чем база данных шаблонов;

– биометрические данные пользователя меняются, что образует некоторые сложности как пользователя, так и для администратора;

– надлежит учитывать отличие между использованием биометрии на контролируемой территории, под охраной, или когда к устройству сканирования могут поднести муляж и т. п.

Но самая большая опасность заключается в том, что любая «пробоина» для биометрии оказывается роковой. При такой ситуации пароли можно сменить, утерянную аутентификационную карту можно аннулировать и обзавестись новой, а палец, глаз или голос подменить невозможно. Если биометрические данные окажутся скомпрометированы, придется, как минимум в лучшем случае, осуществить значительную модернизацию всей системы.

4.2. Разграничение доступа

Разграничение доступа, вероятно, является самой исследованной областью информационной безопасности. «Дискрец» и «мандатное» управление вошли во все теоретические курсы и критерии оценки. Доминируют они и на практике.

В настоящее время следует признать не полностью соответствующим действительности утверждение о том, что разграничение доступа обращено на защиту от злоумышленников. Нынешние информационные системы характеризуются чрезмерной сложностью и их внутренние ошибки представляют не меньшую угрозу.

Динамичность современной информационной программной сферы в комбинации со сложностью отдельных элементов значительно сужает область использования самой потребительской дискреционной модели управления доступом. При установлении допустимости доступа главное не только кто обратился к объекту, но и то, какова семантика деяния. Без привлечения семантики невозможно определить троянские программы, противостоять которым любое управление доступом не в состоянии.

В настоящее время возникают новые модели управления доступом, например, модель «песочницы» в Java-технологии. Но и она не в состоянии учитывать семантику программ, что, является главным фактором обнаруживаемых слабостей в системе безопасности.

Энергично развиваемое ролевое управление доступом решает не столько проблемы безопасности, сколько увеличивает эффективность управляемости систем. Между пользователями и их предпочтениями размещены промежуточные сущности – роли. Для конкретного пользователя в одно и то же время могут быть активными множество ролей. Каждая дает ему определенные права.

Сложность информационной системы характеризуется, в первую очередь, количеством существующих в ней связей. Пользователей и привилегий гораздо больше, чем ролей, поэтому их (ролей) применение способствует уменьшению сложности, а, следовательно, эффективности управляемости. Также на основании ролевой модели можно выполнить такие значительные принципы, как разделение обязанностей. Между ролями могут быть установлены динамические или статические отношения несовместимости (невозможности одному субъекту по очереди или одновременно активизировать обе роли), что и обуславливает необходимую защиту.

Для некоторых употребительных сервисов, таких как Web, ролевое управление доступом может быть реализовано относительно просто (в Web-случае – на основе cgi-процедур). Правда, следует позаботиться о средствах администрирования, но, разумеется, существуют и они. Так что в данном случае слово за системными администраторами.

4.3. Протоколирование и аудит

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой комплект возможных событий. Их можно разделить на:

– внешние (вызванные действиями других сервисов);

– внутренние (вызванные действиями самого сервиса);

– и клиентские (вызванные действиями пользователей и администраторов).

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически с целью приобретения объективной оценки о протекающем состоянии системы, мероприятиях и фактах совершающихся в ней. Проведение аудита дает возможность оценить проходящую безопасность функционирования информационной системы, оценить и управлять рисками, корректно и обоснованно решать вопросы обеспечения безопасности информационных ресурсов.

Датой рождения аудита принято считать 1844 г., когда в Англии приняли закон об акционерных компаниях, согласно которому их правления должны были ежегодно отчитываться перед аукционерами, причем отчет должен был быть проверен и подтвержден специальным человеком – независимым аудитором.

Оперативный аудит с автоматическим реагированием на обнаруженные нештатные ситуации именуется активным. Задача активного аудита – оперативно обнаруживать сомнительную активность и обеспечивать средствами для автоматического реагирования на нее. Под сомнительной активностью понимается поведение пользователя информационной системы, оказывающееся не соответствующим с ранее определенной политикой безопасности.

Средства активного аудита могут размещаться на всех линиях охраны информационной системы. На границе контролируемой зоны они могут обнаруживать подозрительную активность в точках подключения к внешним сетям. В корпоративной сети, в рамках информационных сервисов и сервисов безопасности активный аудит в состоянии обнаружить и пресечь подозрительную активность внешних и внутренних пользователей, выявить проблемы в работе сервисов, вызванные как нарушениями безопасности, так и аппаратно-программными ошибками.

В составе средств активного аудита можно выделить следующие функциональные компоненты:

– компоненты генерации регистрационной информации. Они находятся на стыке между средствами активного аудита и контролируемыми объектами;

– компоненты хранения сгенерированной регистрационной информации;

– компоненты извлечения регистрационной информации (сенсоры). Обычно различают сетевые и хостовые сенсоры, имея в виду под первыми выделенные компьютеры, сетевые карты которых установлены в режим прослушивания, а под вторыми – программы, читающие регистрационные журналы операционной системы;

– компоненты просмотра регистрационной информации могут помочь при принятии решения о реагировании на подозрительную активность;

– компоненты анализа информации, поступившей от сенсоров. В соответствии с данным выше определением средств активного аудита выделяют пороговый анализатор, анализатор нарушений политики безопасности, экспертную систему, выявляющую сигнатуры атак, а также статистический анализатор, обнаруживающий нетипичное поведение;

– компоненты хранения информации, участвующей в анализе. Такое хранение необходимо, например, для выявления атак, протяженных во времени;

– компоненты принятия решений и реагирования. Можно получать информацию не только от локальных, но и от внешних анализаторов, проводя так называемый корреляционный анализ распределенных событий;

– компоненты хранения информации о контролируемых объектах. Здесь могут храниться как пассивные данные, так и методы, необходимые, например, для извлечения из объекта регистрационной информации или для реагирования;

– компоненты, играющие роль организующей оболочки для менеджеров активного аудита, называемые мониторами;

– компоненты интерфейса с администратором безопасности.

Средства активного аудита строятся в архитектуре менеджер/агент. Основными агентскими компонентами являются сенсоры. Анализ, принятие решений – функции менеджеров. Очевидно, что между менеджерами и агентами должны быть сформированы доверенные каналы.

4.4. Экранирование

Формальная установка задачи экранирования состоит в следующем. Пусть имеется два множества информационных систем. Экран – это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран выполняет свои функции, контролируя все информационные потоки между двумя множествами систем. Контроль потоков заключается в их фильтрации, может быть с выполнением некоторых преобразований.

На следующем уровне детализации экран (полупроницаемую мембрану) удобно представлять как последовательность фильтров. Каждый из фильтров, проанализировав данные, может задержать (не пропустить) их, а может и сразу «перебросить» за экран. Кроме того, допускается преобразование данных, передача порции данных на следующий фильтр для продолжения анализа или обработки данных от имени адресата и возврат результата отправителю.

Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией.

Обычно экран не является симметричным, для него определены понятия «внутри» и «снаружи». При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны (МЭ) (предложенный автором перевод английского термина firewall) чаще всего устанавливают для защиты корпоративной сети организации, имеющей выход в сеть Интернет (см. следующую тему).

Экранирование помогает поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности в ИС организации.

Подчеркнем, что экранирование может использоваться как сервис безопасности не только в сетевой, но и в любой другой среде, где происходит обмен сообщениями. Важнейший пример подобной среды – объектно-ориентированные программные системы, когда для активизации методов объектов выполняется (по крайней мере, в концептуальном плане) передача сообщений. Весьма вероятно, что в будущих объектно-ориентированных средах экранирование станет одним из важнейших инструментов разграничения доступа к объектам.

Экранирование может быть частичным, защищающим определенные информационные сервисы. Экранирование электронной почты описано в статье «Контроль над корпоративной электронной почтой: система «Дозор-Джет»» (Jet Info, 2002, 5).

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда

гипертекстовые документы формируются динамически. Каждый пользователь видит лишь то, что ему положено видеть. Можно провести аналогию между динамически формируемыми гипертекстовыми документами и представлениями в реляционных базах данных, с той существенной оговоркой, что в случае Web возможности существенно шире.

Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, например, таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация данных.

Архитектурные аспекты.

Бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем (далее – ОС) не представляется возможным. Универсальная ОС – это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для нелегального получения привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений. Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т. п.). Единственный перспективный путь связан с разработкой специализированных сервисов безопасности, которые в силу своей простоты допускают формальную или неформальную верификацию. Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

Межсетевой экран (далее – МЭ) располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети). В первом случае говорят о внешнем МЭ, во втором – о внутреннем. В зависимости от точки зрения, внешний МЭ можно считать первой или последней (но никак не единственной) линией обороны. Первой – если смотреть на мир глазами внешнего злоумышленника. Последней – если стремиться к защищенности всех компонентов корпоративной сети и пресечению неправомерных действий внутренних пользователей.

МЭ – идеальное место для встраивания средств активного аудита. С одной стороны, и на первом, и на последнем защитном рубеже выявление подозрительной активности по-своему важно. С другой стороны, МЭ способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой. Правда, нужно отда-

вать себе отчет в том, что соединение двух сервисов безопасности в принципе может создать брешь, способствующую атакам на доступность.

На МЭ целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

В силу принципов эшелонированности обороны для защиты внешних подключений обычно используется двухкомпонентное экранирование. Первичная фильтрация (например, блокирование пакетов управляющего протокола SNMP, опасного атаками на доступность, или пакетов с определенными IP-адресами, включенными в «черный список») осуществляется граничным маршрутизатором (см. также следующий раздел), за которым располагается так называемая демилитаризованная зона (сеть с умеренным доверием безопасности, куда выносятся внешние информационные сервисы организации – Web, электронная почта и т. п.) и основной МЭ, защищающий внутреннюю часть корпоративной сети.

Теоретически МЭ (особенно внутренний) должен быть многопротокольным, однако на практике доминирование семейства протоколов TCP/IP столь велико, что поддержка других протоколов представляется излишеством, вредным для безопасности (чем сложнее сервис, тем он более уязвим).

Вообще говоря, и внешний, и внутренний МЭ может стать узким местом, поскольку объем сетевого трафика имеет тенденцию быстрого роста. Один из подходов к решению этой проблемы предполагает разбиение МЭ на несколько аппаратных частей и организацию специализированных серверов-посредников. Основной МЭ может проводить грубую классификацию входящего трафика по видам и передоверять фильтрацию соответствующим посредникам (например, посреднику, анализирующему HTTP-трафик). Исходящий трафик сначала обрабатывается сервером-посредником, который может выполнять и функционально полезные действия, такие как кэширование страниц внешних Web-серверов, что снижает нагрузку на сеть, вообще, и основной МЭ, в частности.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, являются скорее исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети Интернет. В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний МЭ является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

Противоположностью составным корпоративным МЭ (или их компонентами) являются персональные МЭ и персональные экранирующие устройства. Первые являются программными продуктами, которые устанавливаются на персональные компьютеры и защищают только их. Вторые

реализуются на отдельных устройствах и защищают небольшую локальную сеть, такую как сеть домашнего офиса.

При развертывании межсетевых экранов следует соблюдать рассмотренные нами ранее принципы архитектурной безопасности, в первую очередь, позаботившись о простоте и управляемости, об эшелонированности обороны, а также о невозможности перехода в небезопасное состояние. Кроме того, следует принимать во внимание не только внешние, но и внутренние угрозы.

Классификация МЭ.

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. МЭ также целесообразно классифицировать по уровню фильтрации – канальному, сетевому, транспортному или прикладному. Соответственно, можно говорить об экранирующих концентраторах (мостах, коммутаторах) (уровень 2), маршрутизаторах (уровень 3), о транспортном экранировании (уровень 4) и о прикладных экранах (уровень 7). Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

Фильтрация информационных потоков осуществляется МЭ на основе набора правил, являющихся выражением сетевых аспектов политики безопасности организации. В этих правилах, помимо информации, содержащейся в фильтруемых потоках, могут фигурировать данные, полученные из окружения, например, текущее время, количество активных соединений, порт, через который поступил сетевой запрос и т. д. Таким образом, в МЭ используется очень мощный логический подход к разграничению доступа.

Возможности МЭ непосредственно определяются тем, какая информация может использоваться в правилах фильтрации и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует МЭ, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее он может быть сконфигурирован.

Экранирующие маршрутизаторы (и концентраторы) имеют дело с отдельными пакетами данных, поэтому иногда их называют пакетными фильтрами. Решения о том, пропустить или задержать данные, принимаются для каждого пакета независимо, на основании анализа адресов и других полей заголовков сетевого (канального) и, быть может, транспортного уровней. Еще один важный компонент анализируемой информации – порт, через который поступил пакет.

Экранирующие концентраторы являются средством не столько разграничения доступа, сколько оптимизации работы локальной сети за счет организации так называемых виртуальных локальных сетей. Последние можно считать важным результатом применения внутреннего МЭ.

Современные маршрутизаторы позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты, как на входе, так и на выходе. В принципе, в качестве пакетного фильтра может использоваться и универсальный компьютер, снабженный несколькими сетевыми картами.

Основные достоинства экранирующих маршрутизаторов – доступная цена (на границе сетей маршрутизатор нужен практически всегда, вопрос лишь в том, как задействовать его экранирующие возможности) и прозрачность для более высоких уровней модели OSI. Основной недостаток – ограниченность анализируемой информации и, как следствие, относительная слабость обеспечиваемой защиты.

Транспортное экранирование позволяет контролировать процесс установления виртуальных соединений и передачу информации по ним. С точки зрения реализации экранирующий транспорт представляет собой довольно простую, а значит, надежную программу.

По сравнению с пакетными фильтрами, транспортное экранирование обладает большей информацией, поэтому соответствующий МЭ может осуществлять более тонкий контроль за виртуальными соединениями (например, он способен отслеживать количество передаваемой информации и разрывать соединения после превышения определенного порога, препятствуя тем самым несанкционированному экспорту информации). Аналогично, возможно накопление более содержательной регистрационной информации. Главный недостаток – сужение области применения, поскольку вне контроля остаются датаграммные протоколы. Обычно транспортное экранирование применяют в сочетании с другими подходами, как важный дополнительный элемент.

МЭ, функционирующий на прикладном уровне, способен обеспечить наиболее надежную защиту. Как правило, подобный МЭ представляет собой универсальный компьютер, на котором функционируют экранирующие агенты, интерпретирующие протоколы прикладного уровня (HTTP, FTP, SMTP, telnet и т. д.) в той степени, которая необходима для обеспечения безопасности.

При использовании прикладных МЭ, помимо фильтрации, реализуется еще один важнейший аспект экранирования. Субъекты из внешней сети видят только шлюзовой компьютер; соответственно, им доступна только та информация о внутренней сети, которую он считает нужным экспортировать. Прикладной МЭ на самом деле экранирует, то есть заслоняет, внутреннюю сеть от внешнего мира. В то же время, субъектам внутренней сети кажется, что они напрямую общаются с объектами внешнего мира. Недостаток прикладных МЭ – отсутствие полной прозрачности, требующее специальных действий для поддержки каждого прикладного протокола.

Отметим также следующие дополнительные возможности межсетевых экранов:

- контроль информационного наполнения (антивирусный контроль «на лету», верификация Java-апплетов, выявление ключевых слов в электронных сообщениях и т. п.);
- выполнение функций ПО промежуточного слоя.

Особенно важным представляется последний из перечисленных аспектов. ПО промежуточного слоя, как и традиционные межсетевые экраны прикладного уровня, скрывает информацию о предоставляемых услугах. За счет этого оно может выполнять такие функции, как маршрутизация запросов и балансировка нагрузки. Представляется вполне естественным, чтобы эти возможности были реализованы в рамках МЭ. Это существенно упрощает действия по обеспечению высокой доступности экспортируемых сервисов и позволяет осуществлять переключение на резервные мощности прозрачным для внешних пользователей образом. В результате к услугам, традиционно предоставляемым межсетевыми экранами, добавляется поддержка высокой доступности сетевых сервисов.

Лекция 5. ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

План

1. Особенности защиты информации в сетях ЭВМ.
2. Архитектура вычислительной сети и безопасность.
3. Механизмы защиты в вычислительных сетях.

5.1. Особенности защиты информации в сетях ЭВМ

В настоящее время используются автоматизированные системы (далее − АС) разнообразных характеристик и архитектур, большинство вновь вводимых в эксплуатацию автоматизированных объектов является сетями ЭВМ. Очевидные преимущества обработки информации в сетях ЭВМ порой принимают проблемный характер при организации их защиты в следующих случаях.

Расширение зоны контроля

Администратор или оператор отдельной системы или подсети должен контролировать деятельность пользователей, находящихся вне пределов его досягаемости, возможно, в другой стране. При этом он должен поддерживать рабочий контакт со своими коллегами в других организациях/подразделениях.

Комбинация различных программно-аппаратных средств

Соединение нескольких систем в сеть усиливает уязвимость всей системы в целом. Система настроена на исполнение своих специфических требований безопасности, которые могут оказаться несовместимыми с требованиями в других системах. В случае соединения разнородных систем риск увеличивается.

Неизвестный периметр

Небольшое увеличение сетей приводит к тому, что установить границы сети иногда бывает проблемно, поскольку один и тот же узел может быть доступен для пользователей различных сетей. Более того, не всегда удается верно установить количество пользователей, обладающих доступом к определенному узлу, и, кем они являются.

Множество точек атаки

В сетях один и тот же набор данных или сообщений может передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Это не способствует увеличению защищенности сети. Ко многим современным сетям можно получить доступ с помощью коммутируемых линий связи и модема, что во много раз увеличивает количество возможных точек атаки. Такой способ прост, легко осуществим и трудно контролируем, по этой причине он считается одним из наиболее уязвимых. В списке проблемных локаций сети также фи-

гурируют линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы, модемы и т. п.

Сложность управления и контроля доступа к системе

Многие атаки на сеть могут производиться без приобретения физического доступа к определенному узлу с помощью сети из удаленных точек. В этом случае идентификация злоумышленника может оказаться не выполнимой, а времени атаки может оказаться недостаточным для принятия адекватных мер. По своей сути проблемы защиты сетей обусловлены их двойственным характером. С одной стороны, сеть есть единая система с едиными правилами обработки информации, с другой, – совокупность обособленных систем, каждая из которых имеет свои собственные правила обработки информации. В частности, эта двойственность относится и к проблемам защиты.

Защита сетей, как и защита отдельных систем, преследует цели: поддержание конфиденциальности передаваемой и обрабатываемой в сети информации, целостности и доступности ресурсов (компонентов) сети.

Как и для любой системы, защита сети должна планироваться как единый комплекс мер, охватывающий все особенности обработки информации. В этом смысле организация защиты сети, разработка политики безопасности, ее реализация и управление защитой подчиняются общим правилам, которые были рассмотрены ранее. Однако необходимо учитывать, что каждый узел сети должен иметь индивидуальную защиту в зависимости от выполняемых функций и от возможностей сети. При этом защита отдельного узла должна являться частью общей защиты.

Таким образом, защита сети как единой системы складывается из мер защиты каждого отдельного узла и защиты потоков данных сети. Далее приводится классификация угроз, специфических именно для сетей.

Пассивные угрозы – угрозы, нарушающие конфиденциальность информационных данных, транслируемых в сети; просмотр и/или запись данных, передаваемых по линиям связи:

– при просмотре сообщений (злоумышленник имеет возможность просматривать текст сообщения, передаваемого по сети);

– при анализе трафика (злоумышленник может просматривать заголовки пакетов, циркулирующих в сети, и на основе содержащейся в них информации делать заключения об отправителях и получателях пакета и условиях их передачи (время отправления, класс сообщения, категория безопасности и т. д.); кроме того, он может выяснить объем трафика.

Активные угрозы – несанкционированное использование устройств, имеющих доступ к сети для модификации отдельных сообщений или потока сообщений:

– внедрение сетевых вирусов – передача по сети программы вируса с его последующей активизацией злоумышленником удаленного или локального узла;

– отказ служб передачи сообщений. Злоумышленник может уничтожать или задерживать отдельные сообщения или весь поток сообщений;

– «маскарад». Злоумышленник может присвоить своему узлу чужой идентификатор и получать или отправлять сообщения от чужого имени;

– модификация потока сообщений. Злоумышленник может выборочно уничтожать, изменять, задерживать, переупорядочивать и дублировать сообщения, а также вставлять поддельные сообщения.

Все перечисленные действия с отдельными сообщениями и потоком в целом могут привести к нарушениям работы сети или утечке конфиденциальной информации. Особенно это касается служебных сообщений, несущих информацию о состоянии сети или отдельных узлов, о происходящих на отдельных узлах событиях. Активные атаки на такие сообщения могут привести к потере контроля за сетью. Поэтому протоколы, формирующие сообщения и ставящие их в поток, должны предпринимать меры для их защиты и неискаженной доставки получателю.

5.2. Архитектура вычислительной сети и безопасность

Первостепенными чертами архитектуры вычислительной сети, напрямую связанными с экономическими аспектами деятельности любого учреждения, являются:

– эффективное управление и налаженные коммуникации в учреждении;

– простота и возможность интеграции технологий.

С предоставленной точки зрения наиболее предпочтительной является архитектура «Интранет», т. е. использование технологии Internet в рамках корпоративных систем, частной организации. Реализованный на базовом протоколе HTTP и созданный по принципу клиент-сервер, интранет-сайт доступен с любого компьютера через веб-браузер. Поэтому, «Интранет» – это «частный» Интернет, ограниченный виртуальным пространством отдельно взятого учреждения.

Многие проблемы в обычных системах «клиент-сервер» пропадают в системах архитектуры Интранет, которые сосредоточил и соединил в себе оптимальные качества централизованных систем и традиционных систем «клиент-сервер».

Отличительными для системы «Интранет» являются следующие особенности:

– на сервере сконцентрирована прикладная система;

– информация пользователям передается в виде, годном для восприятия человеком;

– между клиентом и сервером применяется протокол открытого стандарта для обмена информацией;

– на сервере получается конечный продукт – информация специализированная для предъявления пользователю.

Рабочее место пользователя – элементарное универсальное устройство, фактически, это терминал для обработки информации (сетевой компьютер, снабженный программным обеспечением). На сервере образуется вся потребляемая информация. Доступ к ней осуществляется через программу, которая не требует локальных сведений. Важное качество систем Интранет – облегченное централизованное управление, причем не только серверной частью, но и рабочими местами.

Вопрос информационной безопасности в таких системах решается гораздо легче, поскольку большее число ресурсов централизовано. Централизованными ресурсами легче управлять и проще защищать. Внешние интерфейсы оказываются стандартными и унифицированными. Технологий взаимодействия центрального сервера с удаленным рабочим местом оказывается крайне мало. Нет необходимости беспокоиться о сотнях приложений на компьютерах-клиентах и для каждого из них решать задачу защиты взаимодействия клиента с сервером. Для одного рабочего места достаточно обеспечить стандартное решение, которое будет унифицированным для всех. После централизации данных появляется возможность «тиражировать» конфигурации в разнообразные точки учреждения, чтобы решать дополнительные задачи, возникающие в глобальной информационной системе с целью увеличения производительности и надежности. Кардинально решить задачу по обеспечению надежности информационной системы за счет дублирования и раздельного хранения важной информации позволяет технология тиражирования информации.

Глобальная связанность применительно к системам Интранет означает защиту сетей, пользующихся внешними сервисами, организованными на протоколах TCP/IP. Внешние сервисы могут располагаться географически распределенно. Из факта глобальной связанности вытекает также меньшая эффективность мер физической защиты данных, трудности решения проблем, связанных с защитой от несанкционированного доступа, необходимость привлечения для их решения новых программно-технических средств, таких как, например, межсетевые экраны.

Разнородность аппаратных и программных платформ требует от изготовителей средств защиты информации соблюдения определенной технологической цепочки. Важны не только чисто защитные характеристики, но и возможность встраивания этих систем в современные корпоративные информационные структуры.

Корпоративные информационные системы оказываются разнородными, когда в разных частях этих систем хранятся и обрабатываются данные разной степени важности и секретности. Целесообразно в таком случае ввести информационные «границы», разделяющие сегменты разного характера.

В целом, следствие применения технологии «клиент-сервер» для информационной безопасности заключается в следующем:

– любой сервис имеет специфические угрозы;
– любой сервис имеет свое определение понятий субъекта и объекта;
– любой сервис владеет своим определением первостепенных аспектов информационной безопасности;
– в любой сервис необходимо встраивать средства безопасности.

Важно, чтобы наличие многочисленных сервисов не противоречило простоте и удобству использования информационной системы. В противном случае, даже без попыток взлома извне или изнутри, будет трудно добиться устойчивой работы системы.

В Интранет-системах ключевым является Web-сервис, поэтому вопрос защищенности Web-серверов принципиально важен. Эти серверы должны поддерживать традиционные защитные средства, такие как аутентификация, разграничение доступа и подотчетность, кроме того, необходимо обеспечение безопасности программной среды и на серверной, и на клиентской сторонах.

Сведем воедино список упомянутых выше защитных сервисов, необходимых для обеспечения информационной безопасности Интранет-систем:

– защита подключений к внешним сетям;
– разграничение доступа между сегментами корпоративной сети;
– защита корпоративных потоков данных в открытых сетях;
– защита потоков данных между клиентами и серверами;
– обеспечение безопасности распределенной программной среды;
– защита важнейших сервисов (в первую очередь – Web-сервиса);
– аутентификация в открытых сетях;
– протоколирование и аудит в рамках сетевых конфигураций;
– обеспечение простоты архитектуры информационной системы.

Таковы задачи в области информационной безопасности, возникающие в связи с переходом на технологию «Интранет». Как правило, данные задачи решаются централизованно в рамках организации, специалистами по обеспечению информационной безопасности, инженерно-техническим составом. Далее будут рассмотрены аппаратные и программные продукты, необходимые для решения задач по защите информации.

5.3. Механизмы защиты в вычислительных сетях

Рассмотрим механизмы обеспечения безопасности сетей и систему безопасности в соответствии со стандартом ISO, которая учитывает следующие параметры безопасности:

– аутентификация (проверка подлинности) объекта, происходящая при установлении соединения или во время обмена данными для подтверждения того, что объект является тем, за кого себя выдает;

– аутентификация источника данных, подтверждающая, что источником блока данных является именно тот, кто ожидал, но не предотвращающая дублирование или модификацию блоков данных;

– контроль доступа, который предотвращает несанкционированное использование ресурсов. Контроль доступа может применяться раздельно к некоторым видам доступа (чтение/запись данных, активизация информационных ресурсов, исполнение операций над ресурсами);

– конфиденциальность соединения, обеспечивающая конфиденциальность всех данных пользователя этого соединения;

– конфиденциальность выделенного поля, обеспечивающая конфиденциальность определенного поля в блоке данных (например, пароля) в режиме без установления соединения;

– конфиденциальность трафика, предотвращающего получение информации путем наблюдения трафика;

– целостность соединения с восстановлением, обеспечивающая целостность всех данных пользователя этого соединения и позволяющая обнаружить модификацию, подстановку или изъятие любых данных или целого сервисного блока данных с возможным последующим восстановлением;

– целостность соединения без восстановления, обеспечивающая те же возможности, что и предыдущий параметр, но без попытки восстановления;

– целостность выделенного поля в режиме с установлением соединения, обеспечивающая, целостность выделенного поля данных пользователя во всем потоке сервисных блоков данных, передаваемых через это соединение, и обнаруживающая модификацию, подстановку или изъятие этого поля;

– доказательство источника, заключающееся в предоставлении получателю данных доказательства (в виде данных) с предотвращением любой попытки отправителя отрицать впоследствии факт передачи;

– доказательство доставки, заключающееся в предоставлении отправителю данных доказательства (в виде данных) с предотвращением любой попытки получателя отрицать впоследствии факт получения данных.

Механизмы безопасности предназначены для реализации услуг безопасности. Выделяют следующие механизмы безопасности:

Механизмы шифрования, которые обеспечивают конфиденциальность передаваемых данных и/или информации о потоках данных.

Различают два способа шифрования: канальное, когда шифруются все передаваемые по каналу данные, и оконечное, при этом шифруются только пользовательские данные, служебная информация остается открытой.

В первом случае вся информация оказывается открытой на промежуточных узлах – ретрансляторах, шлюзах и т. д.; пользователь не принимает участия в выполняемых операциях; для каждой пары узлов требуется свой ключ.

Оконечное шифрование позволяет обеспечивать конфиденциальность данных, передаваемых между двумя прикладными объектами. Другими словами, отправитель зашифровывает данные, получатель – расшифровывает, на промежуточных узлах восстановить информацию невозможно, поэтому маршрут передачи несущественен – в любом канале информация останется защищенной.

Выбор того или иного способа шифрования или их комбинации зависит от результатов анализа риска. Вопрос стоит следующим образом: что более уязвимо – непосредственно отдельный канал связи или содержание сообщения, передаваемое по различным каналам. Канальное шифрование быстрее (применяются другие, более быстрые, алгоритмы), прозрачно для пользователя, требует меньше ключей. Оконечное шифрование более гибко, может использоваться выборочно, однако требует участия пользователя. В каждом конкретном случае вопрос должен решаться индивидуально.

Функции защиты протоколов (правил) каждого уровня определяются их назначением:

1. Физический уровень – контроль электромагнитных излучений линий связи и устройств, поддержка коммуникационного оборудования в рабочем состоянии. Защита на данном уровне обеспечивается с помощью экранирующих устройств, генераторов помех, средств физической защиты передающей среды.

2. Канальный уровень – увеличение надежности защиты (при необходимости) с помощью шифрования передаваемых по каналу данных. В этом случае шифруются все передаваемые данные, включая служебную информацию.

3. Сетевой уровень – наиболее уязвимый уровень с точки зрения защиты. На нем формируется вся маршрутизирующая информация, отправитель и получатель фигурируют явно, осуществляется управление потоком. Кроме того, протоколами сетевого уровня пакеты обрабатываются на всех маршрутизаторах, шлюзах и других промежуточных узлах. Почти все спе-

цифические сетевые нарушения осуществляются с использованием протоколов данного уровня (чтение, модификация, уничтожение, дублирование, переориентация отдельных сообщений или потока в целом, маскировка под другой узел и др.). Защита от всех подобных угроз осуществляется протоколами сетевого и транспортного уровней (см. ниже) и с помощью средств криптозащиты. На данном уровне может быть реализована, например, выборочная маршрутизация.

4. Транспортный уровень осуществляет контроль за функциями сетевого уровня на приемном и передающем узлах (на промежуточных узлах протокол транспортного уровня не функционирует). Механизмы транспортного уровня проверяют целостность отдельных пакетов данных, последовательность пакетов, пройденный маршрут, время отправления и доставки, идентификацию и аутентификацию отправителя и получателя и другие функции. Все активные угрозы становятся видимыми на данном уровне. Гарантом целостности передаваемых данных является криптозащита данных и служебной информации. Никто, кроме имеющего секретный ключ получателя и / или отправителя, не может прочитать или изменить информацию таким образом, чтобы изменение осталось незамеченным. Анализ трафика предотвращается передачей сообщений, не содержащих информацию, которые, однако, выглядят как настоящие. Регулируя интенсивность этих сообщений в зависимости от объема передаваемой информации, можно постоянно добиваться равномерного трафика. Однако все эти меры не могут предотвратить угрозу уничтожения, переориентации или задержки сообщения. Единственной защитой от таких нарушений может быть параллельная доставка дубликатов сообщения по другим путям.

5. Протоколы верхних уровней обеспечивают контроль взаимодействия принятой или переданной информации с локальной системой. В функции защиты протокола прикладного уровня входит управление доступом к определенным наборам данных, идентификация и аутентификация определенных пользователей, а также другие функции, определяемые конкретным протоколом. Более сложными эти функции являются в случае реализации полномочной политики безопасности в сети.

Рассмотренные механизмы защиты распределены по уровням защиты корпоративной сети: рабочего места; системы (сервера); приложения (например, системы управления базой данных); корпоративной сети; телекоммуникаций.

Возрастание уровня защиты (и, следовательно, активация новых механизмов) возникает в процессе развития сети или ее модернизации.

В настоящее время значительную угрозу Целям устойчивого развития всего мира в целом (далее − ЦУР), наряду с такими преступлениями как терроризм, незаконный оборот наркотиков и коррупция, создают преступления, направленные на подрыв международной информационной безопасности. Новое тысячелетие характеризуется стремительным разви-

тием информационных технологий, все большие объемы информации подлежат обработке и аналитике с применением средств на основе искусственного интеллекта, кроме того, обработка больших массивов данных осуществляется преимущественно в удаленном режиме, т.е. посредством глобальной сети Интернет. В связи с мировой тенденцией передачи данных через всемирную паутину с каждым годом растет число пользователей глобальной сети, пропорционально которому увеличивается количество киберпреступлений. Так, по всему миру, от деятельности криминальных группировок организациям и незащищенным слоям населения наносится уязвимость в размере 1,5 триллионов долларов в год[1]. По этой причине поддержание международной информационной безопасности вносит значительный вклад в развитие как экономических, так и социальных приоритетов, стратегической безопасности государств, так, в качестве одного из ориентиров ЦУР, обозначенных членами Организации Объединенных Наций 25 сентября 2015 года[2] было выделено международное сотрудничество в области информационных технологий, науки и инноваций, которое позволяет достичь согласования и координации механизма передачи информации, использования высокоэффективных информационно-телекоммуникационных технологий, мер укрепления доверия в информационном взаимодействии (задачи ЦУР 17.6, 17.8).

Поскольку от уровня безопасности мирового информационного пространства зависит устойчивость развития мировой цивилизации, было важно провести всестороннее исследование проблемы киберпреступности, в результате которого Управлением Организации Объединенных Наций по наркотикам и преступлениям в феврале 2013 года был подготовлен масштабный проект[3] с целью укрепления существующих мер противодействия информационным угрозам, а также выработки новых международно-правовых мер в области противодействия киберпреступности.

Однако в связи со стремительным развитием сквозных технологий, электронно-вычислительной техники и средств связи, совершенствованием

---

[1] Доклад 27-ой сессии Комиссии по предупреждению преступности и уголовному правосудию [Электронный ресурс] // Официальный интернет-портал Управления Организации Объединенных Наций по наркотикам и преступности, УНП ООН, 2020. URL: http://www.unodc.org/ (дата обращения: 12.08.2020).

[2] Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года. Резолюция, принятая Генеральной Ассамблеей 25 сентября 2015 года [Электронный ресурс] // Официальный интернет-портал Генеральной Ассамблеи Организации Объединенных Наций, 2020. Режим доступа: https://unctad.org/ meetings /en/SessionalDocuments/ares70d1_ru.pdf (дата обращения: 12.08.2020).

[3] Comprehensive study on cybercrime (february2013) – Всестороннее исследование проблемы киберпреступности (февраль 2013 года) / United Nations Office on Drugs and Crime [Электронный ресурс] // Официальный интернет-портал Управления Организации Объединенных Наций по наркотикам и преступлениям, УНП ООН, 2020. URL: www.unodc.org/documents/ organized-crime/cybercrime/cyber crime_study_210213. pdf (дата обращения: 12.08.2020).

программного обеспечения, внедрением нейротехнологий, элементов искусственного интеллекта, промышленного Интернета, технологий беспроводной связи, а также виртуальной и дополненной реальности можно сформировать несколько отдельных направлений обеспечения информационной безопасности, с целью своевременного принятия предупреждающих мер.

Помимо столь же остро стоящих по сей день проблем снижения риска использования информационных технологий для осуществления враждебных действий, представляющих угрозу международной безопасности и стабильности государств, например, в экстремистских, террористических аспектах, в области трансграничной передачи данных, совершенствования методик расследований киберпреступлений правоохранительными органами, следует отметить необходимость деанонимизации пользователей глобальной сети, обеспечения повышенной защищенности персональных данных граждан во многих странах мира в рамках развития программ обработки данных исключительно в цифровом виде (в том числе биометрических данных), а также своевременного выявления и прогнозирования новых киберугроз.

Часть из предложенных для рассмотрения проблем, а также вопросы формирования системы обеспечения международной информационной безопасности в целом представлены в Выписке основных направлений исследований в области обеспечения информационной безопасности Российской Федерации, которая была утверждена 31 августа 2017 года Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым[1].

В частности, необходимость деанонимизации пользователей сети Интернет объясняется отсутствием на сегодняшний день действенных альтернативных методов борьбы с посещениями запрещенных Интернет-ресурсов, контент которых, например, направлен на информационное взаимодействие террористических и экстремистских организаций, распространение наркотиков, пропаганду запрещенных идеологий или разжигание межнациональной розни. Деанонимизация предполагает запрет анонимных и прокси сетей (анонимайзеров) на уровне провайдеров и корпоративных сетей, а также недопустимость использования виртуальных частных сетей.

Повышенная защищенность персональных данных граждан в рамках глобальных программ цифровизации и виртуализации данных, особенно на ранних этапах их развития, обусловлена сложностью обработки больших массивов данных и обеспечения их достоверности. Кроме того, глобальная

[1] Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации: утверждена Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым 31 августа 2017 г. [Электронный ресурс] // Официальный интернет-портал Совета Безопасности Российской Федерации, 2020. URL: http://www.scrf.gov.ru/security/ information/ document155/ (дата обращения: 12.08.2020).

цифровизация характеризуется сложным и длительным периодом внедрения, а также проблемами ограниченности доступа к сети Интернет и низкого уровня знаний у населения в области информационных технологий. При условии обработки биометрических данных накладываются еще более жесткие меры на обеспечение их конфиденциальности. Значительно повысить уровень защищенности персональных данных можно применением специальных мер по отношению к серверам обработки данных (использование криптографических ключей, фаерволов и прочих технологий, контроль обнаружения атак и вторжений).

С целью снижения затрат по ликвидации последствий от преступлений в области информационной безопасности важно заблаговременно исключать потенциально возможные угрозы, принимать меры по прогнозированию киберугроз, проводить своевременные мониторинг и анализ технологий передачи и обработки данных на предмет уязвимостей.

В этих целях актуальными являются вопросы подготовки квалифицированных кадров, постоянного повышения уровня квалификации действующих специалистов, проведения просветительской работы, что особенно актуально для развивающихся стран. В связи с глобальной цифровизацией необходимым условием является повсеместное расширение штата сотрудников, деятельность которых направлена на предупреждение преступлений в сфере информационно-коммуникационных технологий, проведения полноценных исследований, касающихся выявления причин и последствий киберпреступлений, разработки новых методик сбора и выявления доказательств в электронной форме[1].

Подходя к проблеме киберпреступности комплексно следует отметить, что каждым государством должны быть также приняты законодательные и иные меры для обеспечения информационной безопасности по перечисленным направлениям, разработаны стратегии и политики противодействия преступлениям в информационном пространстве, применяться специальные методы расследований.

Таким образом, перечисленные меры будут способствовать созданию безопасного международного информационного пространства с использованием информационно-коммуникационных технологий, что предполагает ускорение достижения всех целей устойчивого развития.

---

[1] Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности. Приложение к письму Постоянного представителя Российской Федерации при Организации Объединенных Наций от 11 октября 2017 года на имя Генерального секретаря [Электронный ресурс] // Официальный интернет-портал Министерства иностранных дел Российской Федерации, 2020. URL: http:// www.mid.ru/diverse/-/asset_publisher/zwI2FuDbhJx9/ content/proekt-konvencii-organizacii-ob-edinennyh-nacij-o-sotrudnicestve-v-sfere-protivo-dejstvia-informacionnoj-prestupnosti (дата обращения: 12.08.2020).

ЗАКЛЮЧЕНИЕ

Таким образом, в курсе лекций были рассмотрены основные вопросы, связанные с понятием и обеспечением информационной безопасности. Знание и соблюдение основ информационной безопасности и защиты информации позволит существенно снизить влияние такого субъективного фактора, как низкий уровень информированности в этой области, что, в свою очередь, повысит уровень защищенности информации ограниченного доступа.

Знание основных способов совершения и предупреждения компьютерных преступлений, методов борьбы с угрозами информационной безопасности, а также современных методов защиты информации необходимо для разработки комплекса мероприятий по обеспечению защиты автоматизированных информационных систем органов внутренних дел в том числе. Все это будет способствовать повышению эффективности деятельности органов внутренних дел в целом.

В арсенале специалистов по информационной безопасности имеется широкий спектр защитных мер: законодательных, морально-этических, административных (организационных), физических и технических (аппаратурных и программных) средств. Все они обладают своими достоинствами и недостатками, которые необходимо знать и правильно учитывать при создании систем защиты. Все возможные каналы проникновения и утечки информации должны быть перекрыты с учетом анализа риска, вероятностей реализации угроз безопасности в конкретной прикладной системе и обоснованного рационального уровня затрат на защиту. Наилучшие результаты при этом достигаются при системном подходе к вопросам безопасности компьютерных систем и комплексном использовании определенных совокупностей различных мер защиты на всех этапах жизненного цикла системы, начиная с самых ранних стадий ее проектирования.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Официальные документы и нормативно-правовые акты

1. **Российская Федерация. Законы.** Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года : (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ). – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

2. **Российская Федерация. Законы.** Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ. – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

3. **Российская Федерация. Законы.** О безопасности : Федеральный закон от 28 декабря 2010 г. № 390-ФЗ. – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

4. **Российская Федерация. Законы.** О полиции : Федеральный закон от 07.02.2011 № 3-ФЗ. – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

5. **Российская Федерация. Законы.** Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 № 144-ФЗ. – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

6. **Российская Федерация. Законы.** О государственной охране : Федеральный закон от 27.05.1996 № 57-ФЗ. Собрание законодательства РФ. – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

7. **Российская Федерация. Законы.** О федеральной службе безопасности : Федеральный закон от 3 апреля 1995 года № 40-ФЗ. – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

8. **Российская Федерация. Законы.** Вопросы Федеральной службы безопасности РФ : Указ Президента РФ от 11 августа 2003 г. № 960. – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

9. **Российская Федерация. Законы.** Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 5 декабря 2016 г. № 646. – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

10. **Российская Федерация. Законы.** О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 31.12.2015 № 683. – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

11. **Российская Федерация. Законы.** Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. Собрание законодательства РФ. 1996. № 25. Ст. 2954. – Текст : электронный // Официальный интернет-портал правовой информации : [сайт]. – URL: http://www.pravo.gov.ru (дата обращения: 12.08.2020).

II. Статьи из журналов

1. **Антонов, В. В., Куликов, Г. Г., Харисова, З. И., Родионова Л. Е.** Теоретико-множественный подход к построению дуальной системной модели пак для исследуемой области деятельности со смешанными реальными и виртуальными объектами Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2019. Т. 20. № 1. С. 5–15.

2. **Харисова, З. И.** О некоторых проблемах обеспечения информационной безопасности государства и общества от современных киберугроз / Актуальные проблемы права и государства в XXI веке [Электронное издание]: сборник материалов XI Международной научно-практической конференции, г. Уфа, 18 апреля 2019 года. – Уфа, Уфимский ЮИ МВД России, 2019. – Текст : непосредственный.

3. **Харисова, З. И.** Международно-правовые основы информационной безопасности в целях устойчивого развития / Правовое обеспечение развития социального государства в свете целей устойчивого развития: сборник материалов Международной научно-практической конференции. – Уфа: РИЦ БашГУ. – 2018. – Текст : непосредственный.

4. **Харисова, З. И.** Актуальные проблемы деятельности правоохранительных органов по противодействию преступности в глобальной сети «Интернет» // Вестник Уфимского юридического института МВД России. 2019. №3(85). С. 92–98.

5. **Лонщакова, А. Р., Харисова, З. И., Антонов, В. В.** Обеспечение достоверности и информационной безопасности проведения психофизиологических исследований в рамках уголовного судопроизводства в Российской Федерации и за рубежом» // Евразийский юридический журнал. 2019. № 9 (136), Москва, 2019. С. 240–242.

III. Учебники, учебные пособия

1. **Щеглов, А. Ю.** Защита информации: основы теории : учебник / А. Ю. Щеглов, К. А. Щеглов. – Москва : Юрайт, 2019. – 309 с. – ISBN 978-5-534-04732-5. – Текст : электронный // ЭБС Юрайт : [сайт]. – URL: https://urait.ru/bcode/433715 (дата обращения: 12.08.2020).

2. **Нестеров, С. А.** Информационная безопасность : учебник и практикум / С. А. Нестеров. — Москва : Юрайт, 2019. – 321 с. – ISBN 978-5-534-07979-1. – Текст : электронный // ЭБС Юрайт : [сайт]. – URL: https:// urait.ru/bcode/442312 (дата обращения: 12.08.2020).

3. **Внуков, А. А.** Защита информации : учебное пособие / А. А. Внуков. – 2-е изд., испр. и доп. – Москва : Юрайт, 2019. – 161 с. – ISBN 978-5-534-07248-8. – Текст : электронный // ЭБС Юрайт : [сайт]. – URL: https://urait.ru/book/zaschita-informacii-422772 (дата обращения: 12.08.2020).

4. **Запечников, С. В.** Криптографические методы защиты информации : учебник / С. В. Запечников, О. В. Казарин, А. А. Тарасов. – Москва, 2019. – 309 с. – ISBN 978-5-534-02574-3. – Текст : электронный // ЭБС Юрайт : [сайт]. – URL: https:// urait.ru/bcode/433133 (дата обращения: 12.08.2020).

5. **Казарин, О. В.** Надежность и безопасность программного обеспечения : учебное пособие / О. В. Казарин, И. Б. Шубинский. – Москва: Юрайт, 2019. – 342 с. – ISBN 978-5-534-05142-1. – Текст : электронный // ЭБС Юрайт : [сайт]. – URL: https://urait.ru/bcode/441287 (дата обращения: 12.08.2020).

IV. Электронные ресурсы

1. Доклад 27-ой сессии Комиссии по предупреждению преступности и уголовному правосудию. – Официальный интернет-портал Управления Организации Объединенных Наций по наркотикам и преступности, УНП ООН, 2020. – Режим доступа: http://www.unodc.org/unodc/en /commissions/CCPCJ/session/27_Session_2018/session-27-of-the-ccpcj.html (дата обращения: 12.08.2020). – Текст : электронный.

2. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года. Резолюция, принятая Генеральной Ассамблеей 25 сентября 2015 года – Официальный интернет-портал Генеральной Ассамблеи Организации Объединенных Наций, 2018. – Режим доступа: https://unctad.org/ meetings /en/SessionalDocuments/ares70d1_ru.pdf (дата обращения: 12.08.2020). – Текст : электронный.

3. Comprehensive study on cybercrime (february2013) – Всестороннее исследование проблемы киберпреступности (февраль 2013 года) / United Nations Office on Drugs and Crime – Официальный интернет-портал Управления Организации Объединенных Наций по наркотикам и преступлениям,

УНП ООН, 2020. – Режим доступа: www.unodc.org/documents/ organized-crime/cybercrime/cyber crime_study_210213.pdf (дата обращения: 12.08.2020). – Текст :электронный.

4. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации / Утверждена Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым 31 августа 2017 г. – Официальный интернет-портал Совета Безопасности Российской Федерации, 2020. – Режим доступа: http://www.scrf.gov.ru/security/information/document155/ (дата обращения: 12.08.2020). – Текст : электронный.

Учебное издание

Антонов Вячеслав Викторович
Колесников Валерий Александрович
Х**арисова** Зарина Ирековна

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Курс лекций

Редактор Е. А. Ермолаева

Подписано в печать	15.09.2020	
Гарнитура Times		Формат 60x84 1/16
Уч.-изд. л. 5,8	Заказ № 76	Усл. печ. л. 6
Тираж 100 экз.		

Редакционно-издательский отдел
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2

Отпечатано в группе полиграфической и оперативной печати
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2