
Артемов А. В.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
курс лекций
Академия МАБИВ
www.mabiv.ru

А. В. Артемов
Информационная безопасность

Текст предоставлен правообладателем
http://www.litres.ru/pages/biblio_book/?art=9066361
Информационная безопасность: курс лекций [Электронный ресурс] /
А.В. Артемов: МАБИВ; Орел; 2014

Аннотация

Информатизация социально-политической, экономической и военной деятельности страны и, как следствие, бурное развитие информационных систем сопровождаются существенным ростом посягательств на информацию как со стороны иностранных государств, так и со стороны преступных элементов и граждан, не имеющих доступа к ней. Несомненно, в создавшейся обстановке одной из первоочередных задач, стоящих перед правовым государством, является разрешение глубокого противоречия между реально существующим и необходимым уровнем защищенности информационных потребностей личности, общества и самого государства, обеспечение их ИБ. Предназначено для преподавателей и студентов вузов по специальности «Информационная безопасность», специалистов по безопасности, менеджеров и руководителей компаний.

Содержание

А. В. Артемов
Информационная безопасность: курс лекций

Рецензент:

кандидат экономических наук, доцент кафедры «Предпринимательство и маркетинг» ФГБОУ ВПО «Госуниверситет – УНПК» Н.А. Лебедева

А. В. Артемов, кандидат технических наук, доцент кафедры «Электроника, вычислительная техника и информационная безопасность» ФГБОУ ВПО «Госуниверситет – УНПК»

Лекция 1
Информационная безопасность как определяющий компонент национальной безопасности россии

Учебные вопросы:

1. Место информационной безопасности в системе национальной безопасности России: понятие, структура и содержание.

2. Основные руководящие документы, регламентирующие вопросы информационной безопасности.

3. Современные угрозы информационной безопасности в России

Вопрос 1. Место информационной безопасности в системе национальной безопасности России: понятие, структура и содержание

Информатизация социально-политической, экономической и военной деятельности страны и, как следствие, бурное развитие информационных систем сопровождаются существенным ростом посягательств на информацию как со стороны иностранных государств, так и со стороны преступных элементов и граждан, не имеющих доступа к ней. Несомненно, в создавшейся обстановке одной из первоочередных задач, стоящих перед правовым государством, является разрешение глубокого противоречия между реально существующим и необходимым уровнем защищенности информационных потребностей личности, общества и самого государства, обеспечение их ИБ. При этом ***под информационной безопасностью (ИБ) личности, общества, государства и современных автоматизированных и телекоммуникационных систем*** понимается *состояние защищенности информационной среды, соответствующей интересам (потребностям) личности, общества и государства в информационной сфере, при котором обеспечиваются их формирование, использование и возможности развития незави-*

симо от наличия внутренних и внешних угроз.

Информационная безопасность определяется *способностью государства (общества, личности):*

– обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;

– противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;

– вырабатывать личностные и групповые навыки и умения безопасного поведения;

– поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Национальный информационный ресурс является сегодня одним из главных источников экономической и военной мощи государства. Проникая во все сферы деятельности государства, информация приобретает конкретное политическое, материальное и стоимостное выражение. На этом фоне все более актуальный характер приобретают ***вопросы обеспечения ИБ*** Российской Федерации как неотъемлемого

элемента национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач.

В любой стране ИБ придается особое значение. В своем развитии эта задача проходит множество этапов в зависимости от потребностей государства, возможностей, методов и средств добывания сведений (в частности, разведки), правового режима государства и реальных его усилий по обеспечению защиты информации.

Важным этапом становления и совершенствования такой системы в нашей стране явился период 70–80-х гг. С началом 70-х гг. в разведывательной деятельности ведущих стран мира началось широкомасштабное применение технических средств разведки. 80-е гг., ознаменовавшись бурным научно-техническим прогрессом, особенно в военной области, дали новые импульсы в дальнейшем наращивании возможностей технических средств иностранных разведок: до 70 % разведывательной информации добывалось в то время с помощью технических средств.

Сложившаяся обстановка потребовала совершенствования системы мер противоборства иностранным разведкам. Задачей государственной важности и одной из составных частей в общей системе мер по сохранению государственной и служебной тайны стало противодействие техническим разведкам.

К началу 90-х гг. произошли качественные изменения

в военно-политической и научно-технической сфере, заставившие во многом пересмотреть государственную политику в области защиты информации в целом.

Во-первых, информационные технологии принципиально изменили объем и важность информации, обращающейся в технических средствах ее передачи и обработки. Во-вторых, в России отошла в прошлое фактическая государственная монополия на информационные ресурсы, в частности получило конституционное закрепление право гражданина искать, получать и распространять информацию. В-третьих, прежний административный механизм управления защитой информации стал неэффективен, в то же время необходимость межведомственной координации в этой сфере объективно возросла. В-четвертых, в связи с усиливающимся включением России в международное разделение труда, укреплением экономических, культурных, гуманитарных контактов с другими государствами многие режимно-ограничительные меры, облегчающие защиту информации, например система регионов, закрытых для посещения иностранными гражданами, стали неприемлемы.

В сложившихся условиях с учетом рассмотренных угроз ИБ личности, общества и государства важным является рассмотрение проблем и задач обеспечения ИБ являющейся неотъемлемой составной частью обеспечения национальной безопасности любого государства мирового сообщества на новом этапе своего развития – этапе формирования инфор-

мационного общества. Известными характерными признаками такого общества является явная обусловленность экономического, социального, научного и всего развития страны широким внедрением новых информационных технологий, обеспечивающих эффективную информатизацию общества, которая, в свою очередь, обеспечивает информационную безопасность общества, в том числе обеспечивает его качественной информацией, информационными продуктами, услугами и знаниями, являющимися сегодня важнейшим стратегическим ресурсом страны. Информатизация личности, общества – это важнейшее, стратегическое направление деятельности государства, определяющее стабильное и безопасное социально-экономическое и политическое развитие и приоритеты во всех сферах, в том числе в информационной и видах деятельности в мировом сообществе. Подтверждением этому являются практические шаги ведущих стран мира и России, что подтверждается принятием ими ряда нормативных правовых актов и иных документов:

– 2000 г. – «Окинавская хартия глобального информационного общества» (от имени России подписана Президентом);

– 2000 г. Концепцией национальной безопасности Российской Федерации (утверждена Указом Президента, в ред. от 10.01.2000);

– 2000 г. – Федеральные целевые программы «Разви-

тие единой образовательной информационной среды (2001–2005 годы)», «Электронная Россия»;

– 25 июля 2007 г. – программа «Стратегия развития информационного общества в России» (принята Советом Безопасности Российской Федерации);

– 2002 г. – Федеральная целевая программа «Электронная Россия на 2002–2010 годы» (утверждена Постановлением Правительства России от 28 января 2002 года № 65);

– 2007 г. «Стратегия развития информационного общества в России» (утверждена 25 июля 2007 года Советом Безопасности Российской Федерации) и другие.

Вопрос 2. Основные руководящие документы, регламентирующие вопросы информационной безопасности

Рассматривая Концепцию национальной безопасности России, утвержденную Указом Президента РФ от 17.12.97 № 1300 (в ред. от 10.01.2000), которая отражает названную «Окинавскую хартию глобального информационного общества», можно утверждать, что в ней система национальных интересов России определяется совокупностью следующих основных интересов:

личности – состоят в реальном обеспечении конституционных прав и свобод, личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии;

– *общества* – включают в себя упрочение демократии, достижение и поддержание общественного согласия, повышение созидательной активности населения и духовное возрождение России;

– *государства* – состоят в защите конституционного строя, суверенитета и территориальной целостности России, в установлении политической, экономической и социальной стабильности, в безусловном исполнении законов и поддер-

жании правопорядка, в развитии международного сотрудничества на основе партнерства.

Концепция определяет национальные интересы России в информационной сфере.

Национальные интересы России обусловливают необходимость сосредоточения усилий общества и государства на решении определенных задач. Такими являются:

– соблюдение конституционных прав и свобод граждан в области получения информации и обмена ею;

– защита национальных духовных ценностей; – пропаганда национального, культурного наследия, норм морали и общественной нравственности;

– обеспечение права граждан на получение достоверной информации;

– развитие современных телекоммуникационных технологий. Планомерная деятельность государства по реализации этих задач позволит Российской Федерации стать одним из центров мирового развития в XXI в. В то же время недопустимо использование информации для манипулирования массовым сознанием. Необходима защита государственного информационного ресурса от утечки важной политической, экономической, научно-технической и военной информации.

В соответствии с данной Концепцией важнейшими ***задачами обеспечения ИБ*** являются:

– установление необходимого баланса между потребно-

стью в свободном обмене информацией и допустимыми ограничениями ее распространения;

– совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;

– разработка соответствующей нормативной правовой базы и координация, при ведущей роли Федерального агентства правительственной связи и информации при Президенте РФ, деятельности федеральных органов государственной власти и других органов, решающих задачи обеспечения ИБ;

– развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;

– защита государственного информационного ресурса, прежде всего в федеральных органах государственной власти и на предприятиях оборонного комплекса.

Доктрина информационной безопасности Российской Федерации от 09.09.2001 № Пр-1895 представляет собой *совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения ИБ Российской Федерации*. Она служит основой:

– для формирования государственной политики в области

обеспечения ИБ Российской Федерации;

– подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения ИБ;

– разработки целевых программ обеспечения ИБ Российской Федерации.

По структуре Доктрина состоит из 4 разделов и 11 глав. В первом разделе ***«Информационная безопасность Российской Федерации»*** дается *понятие ИБ, выделяются национальные интересы личности, общества и государства в информационной сфере*. В Доктрине они уточнены более подробно, чем в Концепции национальной безопасности.

Стратегические и текущие задачи внутренней и внешней политики государства по обеспечению ИБ формируются на основе нижеперечисленных интересов в информационной:

– *личности* – заключаются в реализации конституционных прав человека и гражданина на доступ к информации, использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность;

– *общества* – заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России;

– *государства* – заключаются в создании условий для гар-

моничного развития российской информационной инфраструктуры, реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Определяются виды угроз ИБ и их источники. Они также, в отличие от Концепции национальной безопасности, подробно уточнены.

Во втором разделе ***«Методы обеспечения информационной безопасности»***:

– определяются общие методы обеспечения ИБ Российской Федерации;

– раскрываются особенности обеспечения ИБ Российской Федерации в различных сферах общественной жизни;

– определяется международное сотрудничество в сфере обеспечения ИБ.

В третьем разделе ***«Основные положения государственной политики обеспечения информационной безопасности Российской Федерации»*** содержатся:

– принципы обеспечения государственной политики;

– первоочередные мероприятия по реализации государственной политики обеспечения ИБ Российской Федерации.

Четвертый раздел ***«Организационная основа системы обеспечения информационной безопасности Российской Федерации»*** закрепляет основные функции системы обеспечения ИБ и ее организационную основу.

В Доктрине определены особенности обеспечения информационной безопасности в сфере:

– экономики;

– внутренней и внешней политики;

– науки и техники;

– духовной жизни;

– общегосударственных информационных и телекоммуникационных систем;

– обороны;

– правоохранительной и судебной, а также в условиях чрезвычайных ситуаций.

Это первая попытка законодательного закрепления направлений деятельности государства по обеспечению ИБ. Нет необходимости говорить о значении такого закрепления, потому что оно касается всех сфер деятельности государства и занимает практически приоритетное место в системе национальной безопасности.

Вопрос 3. Современные угрозы информационной безопасности в России

Согласно Закону о безопасности под **угрозой безопасности** понимается *совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства*. Концепция национальной безопасности РФ не дает определения угрозы, но называет некоторые из них в информационной сфере. Так, опасность представляют:

– стремление ряда стран к доминированию в мировом информационном пространстве;

– вытеснение государства с внутреннего и внешнего информационного рынка;

– разработка рядом государств концепции информационных войн;

– нарушение нормального функционирования информационных систем;

– нарушение сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Это так называемые ***внешние угрозы***, которые обусловлены *конкурентным характером развития межгосударственных и международных отношений*. Соответственно суще-

ствуют и ***внутренние угрозы***, связанные во многом с *недостаточным проведением экономических, социально-политических и иных преобразований в сфере* ИБ. Концепция национальной безопасности называет их в качестве предпосылок возникновения угроз. С учетом этих предпосылок, по нашему мнению, к источникам внутренних угроз можно отнести:

– отставание России в сфере информатизации органов государственной власти;

– несовершенство системы организации государственной власти по формированию и реализации единой государственной политики обеспечения ИБ;

– криминализацию общественных отношений, рост организованной преступности;

– увеличение масштабов терроризма;

– обострение межнациональных и осложнение внешних отношений.

Для нейтрализации информационных угроз существует исторически сложившаяся система сохранения государственной тайны, включающая подсистемы:

– криптографической сети конфиденциальной связи;

– противодействия иностранным техническим разведкам;

– обеспечения режима секретности на закрытых государственных объектах.

Наряду с традиционными приоритетами иностранных технических разведок в сферу их интересов все в большей мере вовлекаются вопросы технологий, финансов, торговли,

ресурсов, доступ к которым открывается в связи с конверсией, развитием международных интеграционных процессов, широким внедрением компьютерных технологий. Из существующих информационных угроз наиболее актуальными являются угрозы экономической безопасности предприятий и фирм, определяемые недобросовестной конкуренцией, экономическим и промышленным шпионажем. Промышленный шпионаж существовал всегда.

Промышленный шпионаж представляет собой *несанкционированную передачу конфиденциальной технологии, материалов, продукции, информации о них.*

Методы и способы ведения шпионажа остаются неизменными на протяжении многих столетий развития общества и государства. При этом меняются только средства и формы его ведения. К таким методам относятся: подкуп, шантаж, деятельность послов-шпионов, перехват сообщений, представленных на различных носителях (магнитные носители, письма и др.).

Что касается ***анализа полученной информации***, то все осталось без изменений. Им занимается человек или группа людей, осуществляющих аналитико-синтетическую переработку информации, в том числе с использованием новых информационных технологий.

Развитие техники вплоть до начала XX в. не влияло на средства несанкционированного получения информации: сверлили дырки в стенах и потолках, использовали потай-

ные ходы и полупрозрачные зеркала, устраивались у замочных скважин и под окнами. Появление телеграфа и телефона позволило использовать технические средства получения информации. Гигантское количество сообщений стало перехватываться, влияя на ведение войн и положение на бирже. В 30–40 гг. появились диктофоны, миниатюрные фотоаппараты, различные радиомикрофоны.

Развитие новых информационных технологий позволило осуществлять перехват гигантского количества сообщений, оказывая влияние на все сферы социально-экономического развития общества, в том числе на развитие промышленности.

Анализ результатов исследований угроз информации позволяет утверждать, что одной из основных угроз государственной безопасности Российской Федерации являются попытки западных спецслужб добывать ***конфиденциальные сведения***, составляющие государственную, промышленную, банковскую и другие виды тайн. Ведущие западные страны продолжают модернизировать и развивать свои разведывательные службы, совершенствовать техническую разведку, наращивать ее возможности.

С учетом рассмотренного содержания понятия угрозы государству, обществу и личности в широком смысле рассмотрим угрозы, непосредственно воздействующие на обрабатываемую конфиденциальную информацию. Система угроз безопасности представляет собой реальные или потенциаль-

но возможные действия или условия, приводящие к хищению, искажению, несанкционированному доступу, копированию, модификации, изменению, уничтожению конфиденциальной информации и сведений о самой системе и, соответственно, к прямым материальным убыткам.

При этом угрозы сохранности информации определяются случайными и преднамеренными разрушающими и искажающими воздействиями внешней среды, надежностью функционирования средств обработки информации, а также преднамеренного корыстного воздействия несанкционированных пользователей, целью которых является хищение, уничтожение, разрушение, модификации и использование обрабатываемой информации. Анализ содержания свойств угроз позволяет предложить следующие варианты их классификации (рис. 1).

Проявление угроз характеризуется рядом закономерностей. Во-первых, незаконным овладением конфиденциальной информацией, ее копированием, модификацией, уничтожением в интересах злоумышленников, с целью нанесения ущерба. Кроме этого, непреднамеренные действия обслуживающего персонала и пользователей также приводят к нанесению определенного ущерба. Во-вторых, основными путями реализации угроз информации и безопасности информации выступают:

– агентурные источники в органах управления и защиты информации;

– вербовка должностных лиц органов управления, организаций, предприятий и т. д.;

– перехват и несанкционированный доступ к информации с использованием технических средств разведки;

– использование преднамеренного программно-математического воздействия;

– подслушивание конфиденциальных переговоров в служебных помещениях, транспорте и других местах их ведения.

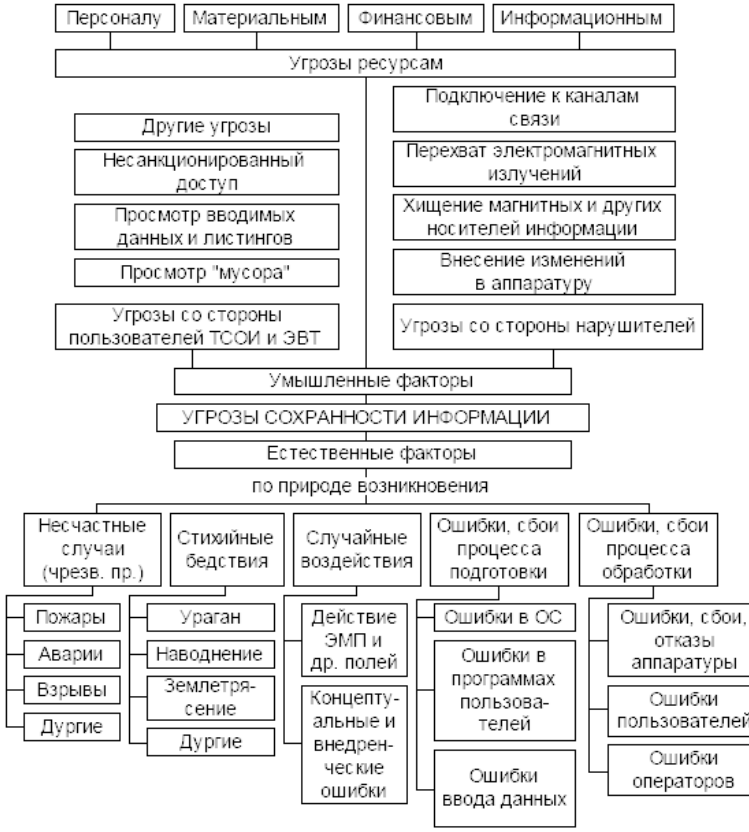

Рис. 1. Классификация угроз безопасности

Основными факторами воздействия угроз, обусловливающими информационные потери и приводящими к различным видам ущерба, возрастание убытков от неправомерных

действий, являются:

– несчастные случаи, вызывающие выход из строя оборудования и информационных ресурсов (пожары, взрывы, аварии, удары, столкновения, падения, воздействия химических или физических сред);

– поломки элементов средств обработки информации;

– последствия природных явлений (наводнения, бури, молнии, землетрясения и др.);

– кражи, преднамеренная порча материальных средств;

– аварии и выход из строя аппаратуры, программного обеспечения, баз данных;

– ошибки накопления, хранения, передачи, использования информации;

– ошибки восприятия, чтения, интерпретации содержания информации, соблюдения правил, ошибки как результат неумения, оплошности, наличие помех, сбоев и искажений отдельных элементов и знаков или сообщения;

– ошибки эксплуатации: нарушение защиты, переполнение файлов, ошибки языка управления данными, ошибки при подготовке и вводе информации, ошибки операционной системы, программирования, аппаратные ошибки, ошибки толкования инструкций, пропуск операций и др.;

– концептуальные ошибки внедрения;

– злонамеренные действия в материальной сфере;

– болтливость, разглашение; – убытки социального характера (уход, увольнение, забастовка и др.).

Информационный ущерб в ряде случаев может быть оценен в зависимости от вида потерь. Это могут быть:

– *потери, связанные с компенсацией или возмещением утраченных, похищенных материальных средств*, которые включают:

• стоимость компенсации возмещения другого косвенно утраченного имущества;

• стоимость ремонтно-восстановительных работ;

• расходы на анализ и исследование причин и величины ущерба;

• другие расходы;

– *дополнительные расходы* на персонал, обслуживающий технические средства обработки конфиденциальной информации, восстановление информации, возобновление работы информационных систем по сбору, хранению, обработке, контролю данных, в том числе расходы:

• на поддержку информационных ресурсов ТСОИ;

• обслуживающий персонал, не связанный с обработкой информации;

• специальные премии, расходы на перевозку и др.;

– *эксплуатационные потери*, связанные с ущербом банковских интересов или финансовыми издержками, потерей клиентов, заказчиков, требующие дополнительных расходов на восстановление: банковского доверия; размеров прибыли; утерянной клиентуры; доходов организации и др.;

• утрата фондов или порча имущества, не подлежащего

восстановлению, которые снижают финансовые возможности (деньги, ценные бумаги, денежные переводы и др.);

• расходы и потери, связанные с возмещением морального ущерба, обучением, экспертизой и др.

Анализируя количественные данные потерь, можно сделать вывод о том, что убытки от злонамеренных действий, и особенно от экономического шпионажа, непрерывно возрастают и являются наиболее значимыми. Выводы западных экспертов показывают, что утечка 20 % коммерческой информации в 60 случаях из 100 приводит к банкротству фирмы.

Подводя итоги краткому анализу существующих угроз конфиденциальной информации, можно выделить два направления воздействия угроз, снижающих безопасность информации.

Первое, традиционно сложившееся в рамках защиты конфиденциальных сведений, представляет собой *воздействия*, способствующие несанкционированному доступу к этим сведениям. Второе, сложившееся в рамках широкого понимания проблем ИБ, связано с *использованием* современных технических и организационных систем, а также с участием людей, коллективов людей и общества в целом и их подверженностью внешним, негативным информационным воздействиям.

Так, теоретически доказано, а практикой многократно подтверждено то, что психика и мышление человека под-

вержены внешним информационным воздействиям и при их надлежащей организации возникает возможность программирования поведения человека. Более того, в последнее время ведутся разработки методов и средств компьютерного проникновения в подсознание, для того чтобы оказывать на него глубокое воздействие. Поэтому актуальной является проблема не только защиты информации, но и защиты от разрушающего воздействия информации, приобретающей международный масштаб и стратегический характер. В силу изменения концепции развития стратегических вооружений, определяющей, что вооруженное решение мировых проблем становится невозможным, все более прочно входит в обиход понятие ***информационной войны***. Сейчас эффективность наступательных средств информационной войны, информационного оружия превосходит эффективность систем защиты информации.

Представляют интерес угрозы утраты охраняемых сведений в ходе информационных процессов, участники которых представляют противоположные интересы. Анализ этих угроз позволил выявить ряд их характерных признаков. В большинстве случаев активные действия сторон вполне осознанны и целенаправленны. К таким действиям относятся:

– разглашение конфиденциальной информации ее обладателем;

– утечка информации по различным, главным образом техническим, каналам;

– несанкционированный доступ к конфиденциальной информации различными способами.

Разглашение информации – это *умышленные или неосторожные действия должностных лиц и граждан, которым в установленном порядке были доверены соответствующие сведения по работе, приведшие к оглашению охраняемых сведений, а также передача таких сведений по открытым техническим каналам*. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, при обсуждении, утере и оглашении любыми иными способами конфиденциальной информации лицам и организациям, не имеющим права доступа к охраняемым секретам. Разглашение информации может происходить по многим каналам, в том числе через почтовые отправления, радио, телевидение, печать и т. п. Разглашение возможно в ходе деловых встреч, бесед, при обсуждении совместных работ, в договорах, в письмах и документах, деловых встречах и др. В ходе таких мероприятий партнеры ведут интенсивный обмен информацией. Именно при общении между ними устанавливаются "доверительные" отношения, приводящие к оглашению коммерческих секретов.

Как правило, факторами, способствующими разглашению конфиденциальной информации, являются:

– слабое знание (или незнание) требований по защите конфиденциальной информации;

– ошибочность действий персонала из-за низкой произ-

водственной квалификации;

– отсутствие системы контроля за оформлением документов, подготовкой выступлений, рекламы и публикаций;

– злостное, преднамеренное невыполнение требований по защите коммерческой тайны.

Разглашение конфиденциальной информации неизбежно приводит к материальному и моральному ущербу.

Утечку информации в общем виде можно рассматривать как *бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена*. При этом природа утечки охраняемой информации характеризуется как обстоятельствами происхождения, так и причинами, условиями возникновения утечки.

Неправомерному овладению конфиденциальной информацией вследствие ***неудовлетворительного управления персоналом*** со стороны должностных лиц, организаций и ведомств способствует наличие следующих обстоятельств:

– склонность сотрудников организации к излишней разговорчивости – 32 %;

– стремление сотрудников зарабатывать деньги любыми способами и любой ценой – 24 %;

– отсутствие в фирме службы безопасности – 14 %; – привычка сотрудников делится друг с другом информацией о своей служебной деятельности – 12 %;

– бесконтрольное использование в фирме информацион-

ных систем – 10 %;

– предпосылки возникновения конфликтных ситуаций в коллективе вследствие отсутствия психологической совместимости сотрудников, случайного подбора кадров, отсутствия работы руководителя по сплочению коллектива и др. – 8 %.

Также утечка охраняемой информации обусловлена наличием соответствующих условий, связанных:

– с ***появлением конкурента*** (злоумышленника), который такой информацией интересуется и затрачивает определенные силы и средства для ее приобретения;

– ***несовершенством норм по сохранению коммерческих секретов, а также нарушением этих норм***, отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и другими материалами, содержащими конфиденциальную информацию;

– разными факторами и обстоятельствами, которые складываются в процессе научной, производственной, рекламной, издательской, информационной и иной деятельности организации и создают предпосылки для ***утечки сведений, составляющих различные виды тайн***.

К таким факторам и обстоятельствам могут, например, относиться:

– недостаточное знание работниками правил защиты соответствующего вида тайны и непонимание необходимости

их тщательного соблюдения;

– утрата удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей – 12 %;

– пронос без разрешения работников службы безопасности (СБ) на территорию организации кино-, звуко-, фото– и видеозаписывающей, радиопередающей, принимающей и множительно-копировальной аппаратуры личного пользования; недонесение о фактах возможной утечки секретных сведений руководству подразделения и СБ; вынос с предприятия секретных документов и изделий без разрешения руководителя организации или начальника СБ – 4 %;

– неправильное определение грифа секретности документа (изделия) – 3 %;

– несвоевременное направление документов для приобщения к делу с отметками об исполнении и с резолюцией начальника подразделения; оставление открытыми и неопечатанными после окончания работы помещений (спецхранилищ) – 3 %;

– оставление секретных документов на рабочих столах при выходе из помещения, нарушение установленного порядка ознакомления прикомандированных лиц с секретными документами и изделиями, перевозка секретных документов и изделий личным и общественным транспортом и перемещение с ними в места, не связанные с выполнением заданий, – 2 %;

– неправильное оформление секретных документов в печать; несоблюдение порядка отчетности перед СБ за числящиеся за исполнителем документы и изделия при увольнении, перед уходом в отпуск, выездом в командировки; несвоевременное сообщение в кадровую службу об изменениях анкетных и автобиографических данных; ведение переговоров по секретным вопросам по незащищенным линиям связи; выполнение секретных работ на дому; снятие копий с секретных документов или производство выписок из них без письменного разрешения начальника СБ; передача и взятие без расписки секретных документов и изделий – 1 % по каждому случаю.

Причинами неправомерного овладения конфиденциальной информацией могу быть следующие обстоятельства:

– ***использование не аттестованных технических средств*** обработки конфиденциальной информации

– ***слабый контроль за соблюдением правил защиты информации*** правовыми организационными и инженерно-техническими мерами

– ***текучесть кадров***, в том числе владеющих сведениями, составляющими коммерческую тайну;

– ***нарушения, не попадающие в поле зрения администрации и СБ***, – это могут быть:

• ознакомление лиц с конфиденциальными документами, изделиями, работами, не входящими в круг их служебных обязанностей;

• направление адресатам конфиденциальных документов, к которым они не имеют отношения;

• подготовка конфиденциальных документов на неучтенных носителях;

• нарушение порядка работы с конфиденциальными документами, изделиями, который не допускает обзор их посторонними лицами;

• несвоевременное сообщение в СБ данных о внеслужебных связях с родственниками, проживающими за границей, с родственниками, выезжающими за границу на постоянное место жительства;

• посещение без разрешения руководства организации посольств, консульств, иностранных частных компаний и фирм;

• установление радиосвязи с радиолюбителями иностранных государств;

• использование конфиденциальных сведений в несекретной служебной переписке, технических заданиях, статьях, докладах и выступлениях;

• преждевременная публикация научных и других работ, которые могут расцениваться на уровне изобретений или открытий или опубликование которых запрещено в установленном порядке;

• сообщение устно или письменно кому бы то ни было, в том числе родственникам, конфиденциальных сведений, если это не вызвано служебной необходимостью;

• сообщение каких-либо сведений о проводимых конфиденциальных работах при обращении по личным вопросам с жалобами, просьбами и предложениями в федеральные государственные органы власти, органы власти субъектов РФ и органы местного самоуправления.

Кроме того, утечке информации способствуют стихийные бедствия, катастрофы, неисправности, отказы, аварии технических средств и оборудования.

Способы **несанкционированного доступа** (НСД) как проблему утечки конфиденциальной информации предлагается рассматривать со следующих позиций. Вопрос обеспечения защиты от НСД связан с проблемой сохранности не только информации как вида интеллектуальной собственности, но физических и юридических лиц, их имущественной собственности и личной безопасности. Известно, что такая деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Как только информация представляет определенную цену, факт ее получения злоумышленником приносит ему определенный доход, ослабляя тем самым возможности конкурента. Отсюда главная цель противоправных действий – получение информации о составе, состоянии и деятельности объекта конфиденциальной информации для удовлетворения своих информационных потребностей в корыстных целях и внесение изменений в состав информации. Такое действие может привести к дезинфор-

мации в определенных сферах деятельности и отражаться, в частности, на учетных данных, результатах решения управленческих задач.

Более опасной угрозой является уничтожение накопленных информационных массивов в документальной или магнитной форме и программных продуктов в среде автоматизированной системы обработки данных. ***Уничтожение*** – это *противоправное действие, направленное на нанесение материального и информационного ущерба конкуренту со стороны злоумышленника*.

Таким образом, рассмотренные угрозы в отношении информации, за исключением последней, как правило, нацелены и ведут к получению злоумышленником конфиденциальной информации. Анализ традиционных приемов и методов получения конфиденциальной информации позволил выделить наиболее характерные источники и методы ее получения, которые в общем виде описывают действия субъектов правовых отношений в сфере обеспечения ИБ:

– сбор информации, содержащейся в средствах массовой информации, включая официальные документы;

– использование сведений, распространяемых служащими конкурирующих организаций;

– документы, отчеты консультантов, финансовые отчеты и документы, выставочные экспонаты и проспекты и др.;

– изучение продукции конкурирующих и других организаций, представляющих интерес для соответствующих видов

разведки, использование данных, полученных во время бесед с обслуживающим персоналом;

– замаскированные опросы и "выуживание" информации у служащих организации на научно-технических конгрессах;

– непосредственное наблюдение, осуществляемое скрытно;

– беседы о найме на работу (без намерений приема их на работу);

– наем на работу служащего конкурирующей фирмы или организации для получения требуемой информации;

– подкуп служащего; – подслушивание переговоров, ведущихся в служебных и иных помещениях, перехват телеграфных сообщений, подслушивание телефонных разговоров;

– кража чертежей, документов и т. д.

– шантаж и вымогательство и др.

Рассмотренные источники и методы не является исчерпывающими, однако они позволяют сгруппировать все ***вероятные источники утечки информации*** следующим образом:

– *персонал, имеющий доступ* к конфиденциальной информации;

– *документы*, содержащие эту информацию; – *технические средства и системы обработки информации*, в том числе линии связи, по которым она передается.

Анализ зарубежных публикаций по источникам утечки информации в коммерческих фирмах позволил выявить, что, несмотря на высокий процент каналов, связанных с ис-

пользованием для добывания сведений технических средств разведки и различных технологических приемов, персонал остается одним из главных причин и одним из источников утечки конфиденциальной информации, что подтверждается примерными следующих процентных соотношений по каналам утечки информации:

– подкуп, шантаж, переманивание служащих, внедрение агентов – 43;

– подслушивание телефонных переговоров – 5;

– кража документов – 10;

– проникновение в ПЭВМ – 18;

– съем информации с каналов "в темную» – 24.

Для раскрытия характеристик правонарушений, совершаемых в информационной сфере, существенное значение имеют характеристики вероятных каналов утечки информации, которые определяются наличием соответствующих источников конфиденциальной информации. Такую классификацию целесообразно рассматривать с учетом того, что обработка конфиденциальной информации осуществляется в организациях, представляющих собой сложные ***системы организационно-технического типа***, функционирующие в условиях внешних воздействий и внутренних изменений состояния. При этом независимо от рассматриваемых воздействий на конфиденциальную информации и систему ее обработки возникающие каналы утечки информации проявляются через такие правонарушения. Эти каналы можно сгруп-

пировать в рамках рассмотренных трех основных групп вероятных источников утечки информации. Так, первая группа – **персонал, имеющий доступ к конфиденциальной информации**, – представляет собой *людские потоки* и является важнейшей группой возможных каналов утечки информации. По распространенности возможные каналы утечки информации этой группы характеризуются следующими примерными показателями:

– приема и увольнения работников предприятия – 32 %;

– посещения предприятия командированными лицами – 28 %;

– проведения совещаний по секретным вопросам – 15 %;

– ведения секретных работ в рабочих помещениях – 15 %;

– допуска, доступа и обращения с секретной (конфиденциальной) информацией – 14 %;

– выезда специалистов за границу – 10 %;

– организации пропускного и внутриобъектового режима – 8 %;

– прохождения практики студентами – 7 %;

– посещения международных выставок – 7 %;

– обучения на курсах повышения квалификации – 5 %;

– подготовки постановлений и решений, приказов и других документов – 4 %.

Типовые нарушения при приеме и увольнении персонала:

– прием на работу лиц без оформления допуска в уста-

новленном порядке;

– доступ персонала к конфиденциальной информации в нарушение установленных требований;

– несвоевременное и неполное ознакомление персонала с требованиями нормативных правовых актов по обеспечению ИБ;

– неудовлетворительные знания нормативных правовых актов;

– увольнение персонала, являющегося носителем конфиденциальной информации.

Характерные нарушения при посещении предприятий командированными лицами:

– допуск командированных лиц с ведома руководителей подразделений к конфиденциальным работам и документам без соответствующего оформления разрешения;

– невыполнение требований инструкций для внутренних объектов по сопровождению прибывших в подразделения командированных лиц;

– отсутствие в предписаниях отметок о действительно выданной информации представителям других предприятий;

– прием командированных лиц с предписаниями, в которых отсутствуют основания командирования (номер и дата хозяйственного договора, ТЗ совместного плана НИОКР и др.);

– не определена степень конфиденциальности материалов, к которым допускается командированное лицо.

Нарушения, связанные с проведением служебных совещаний:

– проведение совещаний без соответствующего разрешения руководителя предприятия или его заместителей;

– допуск на совещание лиц, не имеющих отношения к обсуждаемым вопросам и участие которых не вызывается служебной необходимостью;

– несоблюдение очередности рассмотрения вопросов конфиденциального характера;

– несоблюдение требований режима внутреннего объекта при проведении совещаний;

– фотографирование, демонстрация конфиденциальных изделий, фильмов без согласования с СБ;

– звукозапись выступлений участников совещания на носителе, не учтенном в СБ;

– направление тетрадей (записей) секретного характера в учреждения, которых эти сведения непосредственно не касаются;

– недостаточное знание работниками, участвующими в приеме командированных лиц, требований инструкции о порядке приема командированных лиц (об этом заявили около 45 % опрошенных лиц).

Нарушения при ведении конфиденциальных работ в рабочих помещениях заключаются в отсутствии обеспечения:

– специальных средств защиты конфиденциальной ин-

формации, связи, звукозаписи, звукоусиления, переговорных и телевизионных устройств;

– средств изготовления и размножения документов;

– средств пожарной и охранной сигнализации;

– систем электронной часофикации, электрооборудования и других дополнительных технических средств защиты, исключающих утечку информации за счет побочных электромагнитных излучений и наводок.

Такие каналы утечки, как ***доступ и обращение с конфиденциальной информацией***, образуются за счет расширения круга лиц, имеющих допуск к документам, изделиям, техническим заданиям.

Нарушения в организации пропускного и внутриобъектового режима включают:

– утрату удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (шкафов), личных печатей – 12 %;

– пронос без разрешения СБ на территорию предприятия кино– и фотоаппаратуры, радиопередающей и принимающей, а также множительно-копировальной аппаратуры личного пользования;

– вынос из предприятия секретных документов и изделий без разрешения;

– оставление незакрытыми и не опечатанными после работы помещений (хранилищ).

Каналы утечки конфиденциальных сведений за счет

неправильной организации прохождения технологической и преддипломной практики студентов проявляются в следующем: студенты и учащиеся вузов и средних специальных учебных заведений после прохождения практики не зачисляются на постоянную работу, где они проходили практику и познакомились со сведениями, составляющими государственную или коммерческую тайну, и другие причины.

Характерные нарушения при решении задач отраслевого и межотраслевого характера:

– включение конфиденциальных сведений в открытые документы с целью упрощения порядка доставки и согласования документов;

– ведение секретных записей в личных блокнотах, записных книжках;

– ознакомление с конфиденциальными работами и сведениями лиц, в круг служебных обязанностей которых они не входят;

– направление адресатам конфиденциальных документов, к которым они не имеют отношения.

Таким образом, проведенный анализ угроз информации позволяет уточнить ее свойства, подлежащие правовой защите. При этом содержание этих свойств будет рассматриваться с учетом положений действующих нормативных актов.

Лекция 2
Основные направления обеспечения безопасности информационных ресурсов

Учебные вопросы:

1. Информационные ресурсы и конфиденциальность информации.
2. Угрозы конфиденциальной информации организации.
3. Система защиты конфиденциальной информации.

Вопрос 1. Информационные ресурсы и конфиденциальность информации

В соответствии с действующим Федеральным законом «Об информации, информатизации и защите информации» информационные ресурсы предприятия, организации, учреждения, банка, компании и других государственных и негосударственных предпринимательских структур (далее по тексту – фирмы) включают в себя отдельные документы и отдельные массивы документов (дела), документы и комплексы документов в информационных системах (библиотеках, архивах, фондах, банках данных компьютеров и других информационных системах) на любых носителях, в том числе обеспечивающих работу вычислительной и организационной техники.

Информационные ресурсы (информация) являются объектами отношений физических и юридических лиц между собой и с государством. В совокупности они составляют информационные ресурсы России и защищаются законом наряду с другими видами ресурсов. Документирование информации (создание официального документа) является обязательным условием включения информации в информационные ресурсы. Следует учитывать, что документ может быть не только и даже не столько управленческим (деловым), имеющим в большинстве случаев текстовую, табличную или ан-

кетную форму. Значительно большие объемы наиболее ценных документов представлены в изобразительной форме:

1) конструкторские документы,

2) картографические документы,

3) научно-технические документы,

4) документы на фотографических, магнитных и иных носителях.

По принадлежности к тому или иному виду собственности информационные ресурсы могут быть государственными или негосударственными и как элемент состава имущества находиться в собственности граждан, органов государственной власти, исполнительных органов, органов местного самоуправления, государственных учреждений, организаций и предприятий, общественных объединений, предпринимательских структур.

В соответствии с интересами обеспечения национальной безопасности и степенью ценности для государства, а также правовыми, экономическими и другими интересами предпринимательских структур информационные ресурсы могут быть: а) *открытыми,* т. е. общедоступными, используемыми в работе без специального разрешения, публикуемыми в средствах массовой информации, оглашаемыми на конференциях, в выступлениях и интервью; б) *ограниченного доступа* и использования, т. е. содержащими сведения, составляющие тот или иной вид тайны и подлежащие защите, охране, наблюдению и контролю.

Запрещается относить к информации ограниченного доступа:

• законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, исполнительных органов, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

• документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

• документы, содержащие информацию о деятельности органов государственной власти, исполнительных органов и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, относящихся к государственной тайне;

• документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, исполнительных органов, органов местного самоуправления, организаций, общественных объединений, представляющие общественный интерес или необходи-

мые для реализации прав, свобод и обязанностей граждан.

Накопители информационных ресурсов называются источниками (обладателями) информации. Они представляют собой пассивные концентраторы этой информации и включают в себя:

- публикации о фирме и ее разработках;
- рекламные издания, выставочные материалы, документацию;
- персонал фирмы и окружающих фирму людей;
- физические поля, волны, излучения, сопровождающие работу вычислительной и другой офисной техники, различных приборов и средств связи.

Источники содержат информацию как открытого, так и ограниченного доступа. Причем информация того и другого рода находится в едином информационном пространстве и разделить ее без тщательного содержательного анализа часто не представляется возможным. Например, систематизированная совокупность открытой информации может в комплексе содержать сведения ограниченного доступа.

Документация как источник информации ограниченного доступа включает:

- документацию, содержащую ценные сведения, ноу-хау;
- комплексы обычной деловой и научно-технической документации, содержащей общеизвестные сведения, организационно-правовые и распорядительные документы;
- рабочие записи сотрудников, их служебные дневники,

личные рабочие планы, переписку по производственным вопросам;

• личные архивы сотрудников фирмы. В каждой из указанных групп могут быть:

• документы на традиционных бумажных носителях (листах бумаги, ватмане, фотобумаге и т. п.);

• документы на технических носителях (магнитных, фотопленочных и т. п.);

• электронные документы, банки электронных документов, изображения документов на экране дисплея (видеограммы).

При выполнении управленческих и производственных действий любая информация источника всегда распространяется во внешней среде. Тем самым увеличивается число опасных источников разглашения или утечки информации ограниченного доступа, источников, подлежащих учету и контролю.

Каналы распространения информации носят объективный характер, отличаются активностью и включают в себя:

• деловые, управленческие, торговые, научные и другие коммуникативные регламентированные связи;

• информационные сети;

• естественные технические каналы излучения, создания фона. Канал распространения информации представляет собой путь перемещения сведений из одного источника в другой в санкционированном (разрешенном, законном) режи-

ме или в силу объективных закономерностей. Например: обсуждение важного вопроса на закрытом совещании, запись на бумаге содержания изобретения, переговоры с потенциальным партнером, работа на ЭВМ и т. д.

Следовательно, *информационные ресурсы фирмы представляют собой динамичную категорию, что проявляется прежде всего в процессе документирования информации, объективном возникновении и расширении состава источников и каналов ее распространения.*

Документированные информационные ресурсы, которые используются предпринимателем в бизнесе и управлении фирмой, являются его собственной или частной информацией, представляющей для него значительную ценность. Эта информация составляет интеллектуальную собственность предпринимателя.

Ценность информации может быть стоимостной категорией и характеризовать конкретный размер прибыли при ее использовании или размер убытков при ее утрате. Информация часто становится ценной ввиду ее правового значения для фирмы или развития бизнеса, например: учредительные документы, программы и планы, договоры с партнерами и посредниками и т. д. Ценность может проявляться в ее перспективном научном, техническом или технологическом значении.

Обычно выделяется два вида информации, интеллектуально ценной для предпринимателя:

техническая, технологическая: методы изготовления продукции, программное обеспечение, производственные показатели, химические формулы, рецептуры, результаты испытаний опытных образцов, данные контроля качества и т. п.;

деловая: стоимостные показатели, результаты исследования рынка, списки клиентов, экономические прогнозы, стратегия действий на рынке и т. п.

Ценная информация охраняется нормами права (патентного, авторского, смежных прав и др.), товарным знаком или защищается включением ее в категорию информации, составляющей тайну фирмы.

Процесс выявления и регламентации реального состава ценной информации, составляющей тайну фирмы, является основополагающей частью системы защиты информации. Состав этих сведений фиксируется в специальном **перечне,** закрепляющем факт отнесения их к защищаемой информации и определяющем период (срок) конфиденциальности (т. е. недоступности для всех) этих сведений, уровень (гриф) их конфиденциальности, список сотрудников фирмы, которым дано право использовать эти сведения в работе. В основе перечня лежит типовой состав защищаемых сведений фирм данного профиля. Перечень является постоянным /рабочим материалом руководства фирмы, служб безопасности и конфиденциальной документации. Он представляет собой классифицированный список типовой и конкрет-

ной ценной информации о проводимых работах, производимой продукции, научных и деловых идеях, технологических новшествах. *В перечень включаются действительно Ценные сведения («изюминки») о каждой работе фирмы.*

Конец ознакомительного фрагмента.