Артемов
ИНФОРМАЦИОНН
БЕЗОПАСНОС
курс ле
www.m

А. В. Артемов

Информационная безопасность. Курс лекций

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

Лекция 1 5
Вопрос 1. Место информационной безопасности в системе национальной безопасности России: понятие, структура и содержание 6
Вопрос 2. Основные руководящие документы, регламентирующие вопросы информационной безопасности 8
Вопрос 3. Современные угрозы информационной безопасности в России 11
Лекция 2 21
Вопрос 1. Информационные ресурсы и конфиденциальность информации 22
Вопрос 2. Угрозы конфиденциальной информации организации 27
Вопрос 3. Система защиты конфиденциальной информации 32
Лекция 3 37
Вопрос 1. Понятие информационно-аналитической работы 38
Вопрос 2. Направления аналитической работы 40
Вопрос 3. Этапы аналитической работы 45
Вопрос 4. Методы аналитической работы 50
Конец ознакомительного фрагмента. 51

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 независимо 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 информационного 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 «Развитие 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 поддержании 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 потребностью 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 гармоничного 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 существуют 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 потайные 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 потенциально 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.

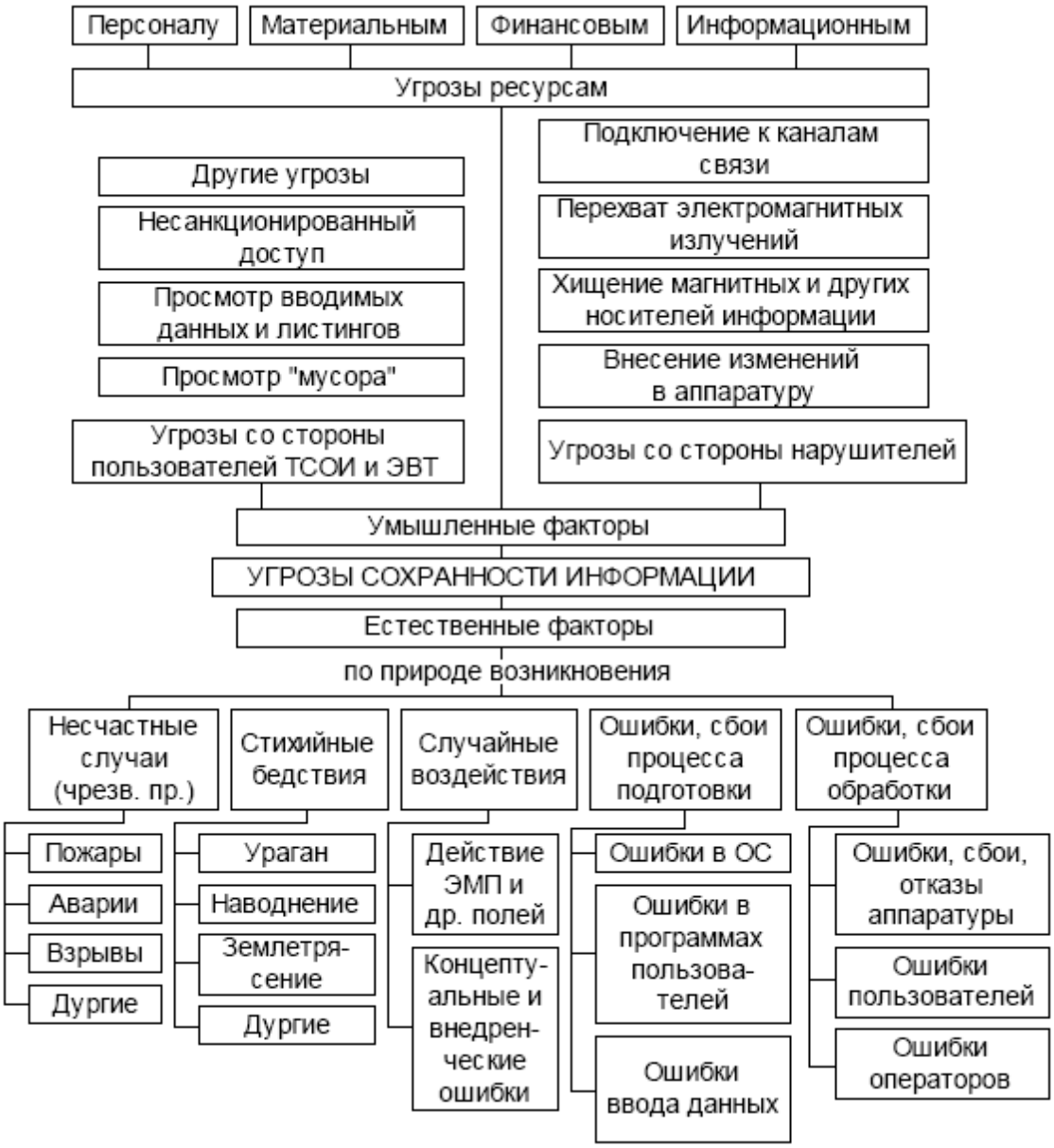

Рис. 1. Классификация угроз безопасности

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 подвержены 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 производственной 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 информационных 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 дезинформации 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 автомати-

зированной 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 использованием 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 сгруппировать 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 установленном 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 информации, 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 анкетную 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 необходимые 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) режиме 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 конкретной ценной информации о проводимых работах, производимой продукции, научных и деловых идеях, технологических новшествах. *В перечень включаются действительно Ценные сведения («изюминки») о каждой работе фирмы.* Следует отметить, что нельзя ограничивать доступ к информации, относящейся к новой продукции, но не имеющей ценности.

Дополнительно может составляться **перечень документов,** в которых защищаемая информация отражается (документируется). В перечень включаются также документы, не содержащие указанную информацию, но представляющие ценность для фирмы и подлежащие охране. Часто обычный открытый правовой акт важно сохранить в целостности и безопасности от похитителя или стихийного бедствия. Перечни формируются индивидуально каждой фирмой в соответствии с рекомендациями специальной комиссии и утверждаются первым руководителем фирмы. Эта комиссия регулярно вносит текущие изменения в перечни в соответствии с динамикой выполнения фирмой конкретных работ.

При заключении любого договора (контракта) стороны должны брать на себя взаимные письменные обязательства по защите конфиденциальной информации другой стороны и документов, полученных при переговорах, исполнении условий договора.

Производственная или коммерческая ценность информации, как правило, недолговечна и определяется временем, необходимым конкуренту для выработки той же идеи или ее хищения и воспроизводства, а также временем до патентования, опубликования и перехода в число общеизвестных.

Документированная информация ограниченного доступа всегда принадлежит к одному из видов тайны – государственной или негосударственной. В соответствии с этим

документы делятся на секретные и несекретные. Обязательным признаком (критерием принадлежности) секретного документа является наличие в нем сведений, составляющих в соответствии с законодательством государственную тайну. Несекретные документы, включающие сведения, относимые к негосударственной тайне (служебной, коммерческой, банковской, профессиональной, производственной и др.), или содержащие персональные данные граждан, именуются конфиденциальными.

Несмотря на то, что *конфиденциальность* является синонимом секретности, термин широко используется исключительно для обозначения информационных ресурсов ограниченного доступа, не отнесенных к государственной тайне. Конфиденциальность отражает ограничение, которое накладывает собственник информации на доступ к ней других лиц, т. е. собственник устанавливает правовой режим этой информации в соответствии с законом. Вместе с тем в соответствии с постановлением Правительства «О перечне сведений, которые не могут составлять коммерческую тайну» от 05.12.91 к конфиденциальным документам нельзя относить учредительные документы, уставы предпринимательских структур, финансовую документацию, сведения о заработной плате персонала и другую документированную информацию, необходимую правоохранительным и налоговым государственным органам.

Под конфиденциальным (закрытым, защищаемым) документом понимается необходимым образом оформленный носитель документированной информации, содержащий сведения ограниченного доступа или использования, которые составляют интеллектуальную собственность юридического или физического лица. Конфиденциальные документы не следует называть служебными или ставить на них гриф секретности, так как конфиденциальные и секретные документы отражают различные виды тайны.

Конфиденциальные документы включают в себя:

• в государственных структурах – служебную информацию ограниченного распространения, именуемую в чиновничьем обиходе информацией для служебного пользования, т. е. информацией, отнесенной к служебной тайне, а также документы, имеющие рабочий характер и не подлежащие публикации в открытой печати (проекты документов, сопутствующие материалы и др.);

• в предпринимательских структурах и направлениях подобной деятельности – сведения, которые их собственник или владелец в соответствии с законодательством имеет право отнести к коммерческой (предпринимательской) тайне, тайне фирмы, тайне мастерства;

• независимо от принадлежности – любые персональные (личные) данные о гражданах, а также сведения, содержащие профессиональную тайну, технические и технологические новшества (до их патентования), тайну предприятий связи, сферы обслуживания и т. п.

Особенностью конфиденциального документа является то, что он представляет собой одновременно:

• массовый носитель ценной, защищаемой информации;

• основной источник накопления и объективного распространения этой информации, а также ее неправомерного разглашения или утечки;

• обязательный объект защиты.

Конфиденциальность документов всегда имеет значительный разброс по срокам ограничения свободного доступа к ним персонала фирмы (от нескольких часов до значительного числа лет). Следует учитывать, что основная масса конфиденциальных документов после окончания их исполнения или работы с ними теряет свою ценность и конфиденциальность. Например, переписка до заключения контракта может иметь гриф конфиденциальности, но после его подписания этот гриф с письменного разрешения первого руководителя фирмы снимается.

Исполненные документы, сохранившие конфиденциальный характер и ценность для деятельности фирмы, формируются в дела в соответствии с номенклатурой дел. Период нахождения конфиденциальных документов в делах может быть кратковременным или долговременным в зависимости от ценности информации, содержащейся в документах дела. Период конфиденциальности документов определяется по указанному выше перечню конфиденциальных сведений и зависит от специфики деятельности фирмы. Например, производственные, научно-исследовательские фирмы обладают более ценными документами, чем торговые, посреднические и др.

Документы долговременного периода конфиденциальности (программы и планы развития бизнеса, технологическая документация ноу-хау, изобретения и др.) имеют усложненный вариант обработки и хранения, обеспечивающий безопасность информации и ее носителя. Документы кратковременного периода конфиденциальности, имеющие оперативное значение для деятельности фирмы, обрабатываются и хранятся по упрощенной схеме и могут не выделяться из технологической системы обработки открытых документов при наличии в этой системе минимальных защитных, контрольных и аналитических элементов.

Вывод: конфиденциальные документы характеризуются специфическими особенностями, которые отражают их сущность как носителей информации ограниченного доступа и определяют построение системы защиты этой информации.

Вопрос 2. Угрозы конфиденциальной информации организации

Все информационные ресурсы фирмы постоянно подвергаются объективным и субъективным угрозам утраты носителя или ценности информации.

Под угрозой или опасностью утраты информации понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление неблагоприятных возможностей внешних или внутренних источников угрозы создавать критические ситуации, события, оказывать дестабилизирующее воздействие на защищаемую информацию, документы и базы данных.

Риск угрозы любым (открытым и ограниченного доступа) информационным ресурсам создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линий связи-Другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица. К угрозам, создаваемым этими лицами, относятся: несанкционированное уничтожение документов, ускорение угасания (старения) текста или изображения, подмена или изъятие документов, фальсификация текста или его части и др.

Для информационных ресурсов ограниченного доступа диапазон угроз, предполагающих утрату информации (разглашение, утечку) или утерю носителя, значительно шире в результате того, что к этим документам проявляется повышенный интерес со стороны различного рода злоумышленников. В отличие от объективного распространения утрата информации влечет за собой незаконный переход конфиденциальных сведений, документов к субъекту, не имеющему права владения ими и использования в своих целях.

Под злоумышленником понимается лицо, действующее в интересах конкурента, противника или в личных корыстных интересах (агентов иностранных спецслужб, промышленного и экономического шпионажа, криминальных структур, отдельных преступных элементов, лиц, сотрудничающих со злоумышленником, психически больных лиц и т. п.).

Основной угрозой безопасности информационных ресурсов ограниченного распространения является несанкционированный (незаконный, неразрешенный) доступ злоумышленника или постороннего лица к документированной информации и как результат – овладение информацией и противоправное ее использование или совершение иных действий. Целью и результатом несанкционированного доступа может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, подмена и т. п. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности фирмы (работники коммунальных служб, экстремальной помощи, прохожие и др.), посетители фирмы, работники других организационных структур, а также сотрудники данной фирмы, не обладающие правом доступа в определенные помещения, к конкретному документу, информации, базе данных. Каждое из указанных лиц может быть злоумышленником или его сообщником, агентом, но может и не быть им.

Обязательным условием успешного осуществления попытки несанкционированного доступа к информационным ресурсам ограниченного доступа является *интерес к ним со стороны конкурентов, определенных лиц, служб и организаций.* При отсутствии такого интереса угроза информации не возникает даже в том случае, если создались предпосылки для ознакомления с ней постороннего лица. Основным виновником несанкционированного доступа к информационным ресурсам является, как правило, персонал, работающий с документами, информацией и базами данных. При этом надо иметь в виду, что утрата информации происходит в большинстве случаев не в результате преднамеренных действий, а из-за невнимательности и безответственности персонала.

Следовательно, утрата информационных ресурсов ограниченного доступа может наступить:

• при наличии интереса конкурента, учреждений, фирм или лиц к конкретной информации;

• при возникновении риска угрозы, организованной злоумышленником или при случайно сложившихся обстоятельствах;

• при наличии условий, позволяющих злоумышленнику осуществить необходимые действия и овладеть информацией. Эти условия могут включать:

• отсутствие системной аналитической и контрольной работы по выявлению и изучению угроз, каналов и степени риска нарушений безопасности информационных ресурсов;

• неэффективную систему защиты информации или отсутствие этой системы;

• непрофессионально организованную технологию обработки и хранения конфиденциальных документов;

• неупорядоченный подбор персонала и текучесть кадров, сложный психологический климат в коллективе;

• отсутствие системы обучения сотрудников правилам защиты информации ограниченного доступа;

• отсутствие контроля со стороны руководства фирмы за соблюдением персоналом требований нормативных документов по работе с информационными ресурсами ограниченного доступа;

• бесконтрольное посещение помещений фирмы посторонними лицами.

Следует всегда помнить, что факт документирования резко увеличивает риск угрозы информации. Великие мастера прошлого никогда не записывали секреты своего искусства, а передавали их устно сыну, ученику. Поэтому тайна изготовления многих уникальных предметов того времени так и не раскрыта до наших дней.

Угрозы сохранности, целостности и конфиденциальности информационных ресурсов ограниченного доступа практически реализуются через *риск образования канала несанкционированного получения (добывания) кем-то ценной информации и документов.* Этот канал представляет собой совокупность незащищенных или слабо защищенных фирмой направлений возможной утраты конфиденциальной информации, которые злоумышленник использует для получения необходимых сведений, преднамеренного незаконного доступа к защищаемой информации.

Каждая конкретная фирма обладает своим набором каналов несанкционированного доступа к информации, что зависит от множества моментов – профиля деятельности, объемов защищаемой информации, профессионального уровня персонала, местоположения здания и т. п.

Функционирование канала несанкционированного доступа к информации обязательно влечет за собой утрату информации, исчезновение носителя информации.

В том случае, когда речь идет об утрате информации по вине персонала, используется термин «разглашение (огласка) информации». Человек может разглашать информацию устно, письменно, с помощью жестов, мимики, условных сигналов, лично, через посредников, по каналам связи и т. д. Термин «утечка информации», хотя и используется наиболее широко, однако в большей степени относится, по нашему мнению, к утрате информации за счет ее перехвата с помощью технических средств разведки, по техническим каналам.

Утрата информации характеризуется двумя условиями, информация переходит а) непосредственно к заинтересованному лицу – конкуренту, злоумышленнику или б) к случайному, третьему лицу. Под третьим лицом в данном случае понимается любое постороннее лицо, получившее информацию во владение в силу обстоятельств или безответственности персонала, не обладающее правом владения ею и, что очень важно, не заинтересованное

в этой информации. Однако от третьего лица информация может легко перейти к злоумышленнику.

Переход информации к третьему лицу представляется достаточно частым явлением, и его можно назвать непреднамеренным, стихийным, хотя при этом факт разглашения информации, нарушения ее безопасности имеет место.

Непреднамеренный переход информации к третьему лицу возникает в результате:

• утери или неправильного уничтожения документа, пакета с документами, дела, конфиденциальных записей;

• игнорирования или умышленного невыполнения сотрудником требований по защите документированной информации;

• излишней разговорчивости сотрудников при отсутствии злоумышленника (с коллегами по работе, родственниками, друзьями, иными лицами в местах общего пользования, транспорте и т. п.);

• работы с документами ограниченного доступа при посторонних лицах, несанкционированной передачи их другому сотруднику;

• использования сведений ограниченного доступа в открытых документации, публикациях, интервью, личных записях, дневниках и т. п.;

• отсутствия маркировки (грифования) информации и документов ограниченного доступа (в том числе документов на технических носителях);

• наличия в документах излишней информации ограниченного доступа;

• самовольного копирования сотрудником документов в служебных или коллекционных целях.

В отличие от третьего лица злоумышленник или его сообщник целенаправленно охотятся за конкретной информацией и преднамеренно, противоправно устанавливают контакт с источником этой информации или преобразуют канал ее объективного распространения в канал ее разглашения или утечки. Такие каналы всегда являются тайной злоумышленника.

Каналы несанкционированного доступа могут быть двух типов: организационные и технические. Обеспечиваются они легальными и нелегальными методами.

Организационные каналы разглашения информации отличаются большим разнообразием видов и основаны на установлении разнообразных, в том числе законных, взаимоотношений злоумышленника с фирмой или ее сотрудником для последующего несанкционированного доступа к интересующей информации.

Основными видами организационных каналов могут быть:

• поступление злоумышленника на работу в фирму, как правило, на техническую или вспомогательную должность (оператором ЭВМ, секретарем, дворником, охранником, шофером и т. п.);

• участие в работе фирмы в качестве партнера, посредника, клиента, использование разнообразных обманных способов;

• поиск злоумышленником сообщника (инициативного помощника), работающего в интересующей его фирме, который становится его соучастником;

• установление злоумышленником доверительных взаимоотношений с сотрудником учреждения, фирмы или посетителем, сотрудником другого учреждения, обладающим интересующими злоумышленника сведениями;

• использование коммуникативных связей фирмы – участие в переговорах, совещаниях, переписке с фирмой и др.;

• использование ошибочных действий персонала или умышленное провоцирование злоумышленником этих действий;

• тайное или по фиктивным документам проникновение в здание фирмы и помещения, криминальный, силовой доступ к информации, т. е. кража документов, дискет, дисков, ком-

пьютеров, шантаж и склонение к сотрудничеству отдельных сотрудников, подкуп сотрудников, создание экстремальных ситуаций и т. п.;

• получение нужной информации от третьего (случайного) лица.

Организационные каналы отбираются или формируются злоумышленником индивидуально в соответствии с его профессиональным умением, конкретной ситуацией, и прогнозировать их крайне сложно. Обнаружение организационных каналов требует проведения серьезной поисковой и аналитической работы.

Широкие возможности несанкционированного получения подобных сведений создает техническое обеспечение офисных технологий. Любая управленческая деятельность всегда связана с обсуждением ценной информации в кабинетах или по линиям связи, проведением расчетов и анализа ситуаций на ЭВМ, изготовлением, размножением документов и т. п.

Технические каналы утечки информации возникают при использовании злоумышленником специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию без непосредственного контакта с персоналом фирмы, документами, делами и базами данных.

Технический канал представляет собой физический путь утечки информации от источника или канала объективного распространения информации к злоумышленнику. Канал возникает при анализе злоумышленником физических полей и излучений, появляющихся в процессе работы вычислительной и другой офисной техники, при перехвате информации, имеющей звуковую, зрительную или иную форму отображения. Основными техническими каналами являются: акустический, визуально-оптический, электромагнитный и др. Это каналы прогнозируемые, носят стандартный характер и перекрываются стандартными средствами противодействия. Обычным и профессионально грамотным является творческое сочетание в действиях злоумышленника каналов обоих типов, например установление доверительных отношений с сотрудником фирмы и перехват информации по техническим каналам с помощью этого сотрудника. Вариантов и сочетаний каналов может быть множество. Изобретательность грамотного злоумышленника не знает предела, поэтому риск утраты информации всегда достаточно велик. При эффективной системе защиты информации фирмы злоумышленник разрушает отдельные элементы защиты и формирует необходимый ему канал получения информации.

В целях практической реализации поставленных задач злоумышленник определяет не только каналы несанкционированного доступа к информации фирмы, но и совокупность методов получения этой информации.

Легальные методы входят в содержание понятий «невинного шпионажа» и «разведки в бизнесе», отличаются правовой безопасностью и, как правило, предопределяют возникновение интереса к конкурирующей фирме. В соответствии с этим может появиться необходимость использования каналов несанкционированного доступа к требуемой информации. В основе «невинного шпионажа» лежит кропотливая аналитическая работа специалистов-экспертов над опубликованными и общедоступными материалами конкурирующей фирмы. Одновременно изучается продукция фирмы, рекламные издания, сведения, полученные в процессе официальных и неофициальных бесед и переговоров с сотрудниками фирмы, материалы пресс-конференций, презентаций фирмы и продукции, научных симпозиумов и семинаров, сведения, получаемые из информационных сетей. Легальные методы дают злоумышленнику основную массу интересующей его информации и позволяют определить состав отсутствующих сведений, которые предстоит добыть нелегальными методами.

Нелегальные методы получения ценной информации всегда носят незаконный характер и используются в целях доступа к защищаемой информации, которую невозможно получить легальными методами. В основе нелегального получения информации лежит поиск злоумышленником существующих в фирме и наиболее эффективных в конкретных условиях

незащищенных организационных и технических каналов несанкционированного доступа к информации, формирование таких каналов при их отсутствии и реализация плана практического комплексного использования этих каналов.

Нелегальные методы предполагают: воровство, продуманный обман, подслушивание разговоров, подделку идентифицирующих документов, взяточничество, инсценирование или организацию экстремальных ситуаций, использование различных криминальных приемов и т. д. В процессе реализации нелегальных методов часто образуется агентурный канал добывания ценной информации. К нелегальным методам относятся также: перехват информации, объективно распространяемой по техническим каналам, визуальное наблюдение за помещениями фирмы и персоналом, анализ продуктов и объектов, содержащих следы защищаемой информации, анализ архитектурных особенностей объектов защиты, анализ отходов производства, мусора, выносимого из офиса.

В результате эффективного использования каналов несанкционированного доступа к информации ограниченного доступа и разнообразных методов ее добывания злоумышленник получает:

• подлинник или официальную копию документа (бумажного, машиночитаемого, электронного), содержащего информацию ограниченного доступа;

• несанкционированно сделанную копию этого документа (рукописную или изготовленную с помощью копировального аппарата, фототехники, компьютера и т. п.);

• диктофонную, магнитофонную, видеокассету с записью текста документа, переговоров, совещания;

• письменное или устное изложение за пределами фирмы содержания документа, ознакомление с которым осуществлялось санкционирование или тайно;

• устное изложение текста документа по телефону, переговорному устройству, специальной радиосвязи и т. п.;

• аналог документа, переданного по факсимильной связи или электронной почте;

• речевую или визуальную запись текста документа, выполненную с помощью технических средств разведки (радиозакладок, встроенных микрофонов и видеокамер, микрофотоаппаратов, фотографирования с большого расстояния). Получение ценных документов или информации ограниченного доступа может быть единичным явлением или регулярным процессом, протекающим на протяжении относительно длительного времени.

Вывод: любые информационные ресурсы фирмы являются весьма уязвимой категорией и при интересе, возникшем к ним со стороны злоумышленника, опасность их утраты становится достаточно реальной.

Вопрос 3. Система защиты конфиденциальной информации

Практической реализацией политики (концепции) информационной безопасности фирмы является технологическая система защиты информации. Защита информации представляет собой жестко регламентированный и динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ценных информационных ресурсов и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности фирмы.

Система защиты информации – рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке. Главными требованиями к организации эффективного функционирования системы являются: персональная ответственность руководителей и сотрудников за сохранность носителя и конфиденциальность информации, регламентация состава конфиденциальных сведений и документов, подлежащих защите, регламентация порядка доступа персонала к конфиденциальным сведениям и документам, наличие специализированной службы безопасности, обеспечивающей практическую реализацию системы защиты и нормативно-методического обеспечения деятельности этой службы.

Собственники информационных ресурсов, в том числе государственные учреждения, организации и предприятия, самостоятельно определяют (за исключением информации, отнесенной к государственной тайне) необходимую степень защищенности ресурсов и тип системы, способы и средства защиты, исходя из ценности информации. Ценность информации и требуемая надежность ее защиты находятся в прямой зависимости. Важно, что структура системы защиты должна охватывать не только электронные информационные системы, а весь управленческий комплекс фирмы в единстве его реальных функциональных и производственных подразделений, традиционных документационных процессов. Отказаться от бумажных документов и часто рутинной, исторически сложившейся управленческой технологии не всегда представляется возможным, особенно если вопрос стоит о безопасности ценной, конфиденциальной информации.

Основной характеристикой системы является ее комплексность, т. е. наличие в ней обязательных элементов, охватывающих все направления защиты информации. Соотношение элементов и их содержания обеспечивают индивидуальность построения системы защиты информации конкретной фирмы и гарантируют неповторимость системы, трудность ее преодоления. Конкретную систему защиты можно представить в виде кирпичной стены, состоящей из множества разнообразных элементов (кирпичиков). Элементами системы являются: правовой, организационный, инженерно-технический, программно-аппаратный и криптографический.

Правовой элемент системы защиты информации основывается на нормах информационного права и предполагает юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные собственником информации ограничительные и технологические меры защитного характера, а также ответственности персонала за нарушение порядка защиты информации. Этот элемент включает:

• наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, контрактах, заключаемых с сотрудниками, в должностных и рабочих инструкциях положений и обязательств по защите конфиденциальной информации;

• формулирование и доведение до сведения всех сотрудников фирмы (в том числе не связанных с конфиденциальной информацией) положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;

• разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

Организационный элемент системы защиты информации содержит меры управленческого, ограничительного (режимного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации фирмы. Эти меры связаны с установлением режима конфиденциальности в фирме. Элемент включает в себя регламентацию:

• формирования и организации деятельности службы безопасности и службы конфиденциальной документации (или менеджера по безопасности, или референта первого руководителя), обеспечения деятельности этих служб (сотрудника) нормативно-методическими документами по организации и технологии защиты информации;

• составления и регулярного обновления состава (перечня, списка, матрицы) защищаемой информации фирмы, составления и ведения перечня (описи) защищаемых бумажных, машиночитаемых и электронных документов фирмы;

• разрешительной системы (иерархической схемы) разграничения доступа персонала к защищаемой информации;

• методов отбора персонала для работы с защищаемой информацией, методики обучения и инструктирования сотрудников;

• направлений и методов воспитательной работы с персоналом, контроля соблюдения сотрудниками порядка защиты информации;

• технологии защиты, обработки и хранения бумажных, машиночитаемых и электронных документов фирмы (делопроизводственной, автоматизированной и смешанной технологий); внемашинной технологии защиты электронных документов;

• порядка защиты ценной информации фирмы от случайных или умышленных несанкционированных действий персонала;

• веления всех видов аналитической работы;

• порядка защиты информации при проведении совещаний, заседаний, переговоров, приеме посетителей, работе с представителями рекламных агентств, средств массовой информации;

• оборудования и аттестации помещений и рабочих зон, выделенных для работы с конфиденциальной информацией, лицензирования технических систем и средств защиты информации и охраны, сертификации информационных систем, предназначенных для обработки защищаемой информации;

• пропускного режима на территории, в здании и помещениях фирмы, идентификации персонала и посетителей;

• системы охраны территории, здания, помещений, оборудования, транспорта и персонала фирмы;

• действий персонала в экстремальных ситуациях;

• организационных вопросов приобретения, установки и эксплуатации технических средств защиты информации и охраны;

• организационных вопросов защиты персональных компьютеров, информационных систем, локальных сетей;

• работы по управлению системой защиты информации;

• критериев и порядка проведения оценочных мероприятий по установлению степени эффективности системы защиты информации.

Элемент организационной защиты является стержнем, основной частью рассматриваемой комплексной системы. По мнению большинства специалистов, меры организационной защиты информации составляют 50–60 % в структуре большинства систем защиты информации. Это связано с рядом факторов и также с тем, что важной составной частью организационной защиты информации является подбор, расстановка и обучение персонала, который будет реализовывать на практике систему защиты информации. Сознательность, обученность и ответственность персонала можно с полным правом назвать краеугольным камнем любой даже самой технически совершенной системы защиты информации. Организационные меры защиты отражаются в нормативно-методических документах службы безопасности, службы конфиденциальной документации учреждения или фирмы. В этой связи часто используется единое название двух рассмотренных выше элементов системы защиты – «элемент организационно-правовой защиты информации».

Инженерно-технический элемент системы защиты информации предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью комплексов технических средств. При защите информационных систем этот элемент имеет весьма важное значение, хотя стоимость средств технической защиты и охраны велика. Элемент включает в себя:

• сооружения физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здание и помещения (заборы, решетки, стальные двери, кодовые замки, идентификаторы, сейфы и др.);

• средства защиты технических каналов утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов и других приборов и офисного оборудования, при проведении совещаний, заседаний, беседах с посетителями и сотрудниками, диктовке документов и т. п.;

• средства защиты помещений от визуальных способов технической разведки;

• средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, сигнализирования, информирования и идентификации);

• средства противопожарной охраны;

• средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств, тайно установленной миниатюрной звукозаписывающей и телевизионной аппаратуры и т. п.);

• технические средства контроля, предотвращающие вынос персоналом из помещения специально маркированных предметов, документов, дискет, книг и т. п. *Программно-аппаратный элемент* системы защиты информации предназначен для защиты ценной информации, обрабатываемой и хранящейся в компьютерах, серверах и рабочих станциях локальных сетей и различных информационных системах. Однако фрагменты этой защиты могут применяться как сопутствующие средства в инженерно-технической и организационной защите. Элемент включает в себя:

• автономные программы, обеспечивающие защиту информации и контроль степени ее защищенности;

• программы защиты информации, работающие в комплексе с программами обработки информации;

• программы защиты информации, работающие в комплексе с техническими (аппаратными) устройствами защиты информации (прерывающими работу ЭВМ при нарушении системы доступа, стирающие данные при несанкционированном входе в базу данных и др.).

Криптографический элемент системы защиты информации предназначен для защиты конфиденциальной информации методами криптографии. Элемент включает:

• регламентацию использования различных криптографических методов в ЭВМ и локальных сетях;

• определение условий и методов криптографирования текста документа при передаче его по незащищенным каналам почтовой, телеграфной, телетайпной, факсимильной и электронной связи;

• регламентацию использования средств криптографирования переговоров по незащищенным каналам телефонной и радиосвязи;

• регламентацию доступа к базам данных, файлам, электронным документам персональными паролями, идентифицирующими командами и другими методами;

• регламентацию доступа персонала в выделенные помещения с помощью идентифицирующих кодов, шифров.

Составные части криптографической защиты, коды, пароли и другие ее атрибуты разрабатываются и меняются специализированной организацией. Применение пользователями собственных систем шифровки не допускается.

В каждом элементе защиты могут быть реализованы на практике только отдельные составные части в зависимости от поставленных задач защиты в крупных и некрупных фирмах различного профиля, малом бизнесе. Структура системы, состав и содержание элементов, их взаимосвязь зависят от объема и ценности защищаемой информации, характера возникающих угроз безопасности информации, требуемой надежности защиты и стоимости системы. Например, в некрупной фирме с небольшим объемом защищаемой информации можно ограничиться регламентацией технологии обработки и хранения документов, доступа персонала к документам и делам. Можно дополнительно выделить в отдельную группу и маркировать ценные бумажные, машиночитаемые и электронные документы, вести их опись, установить порядок подписания сотрудниками обязательства о неразглашении тайны фирмы, организовывать регулярное обучение и инструктирование сотрудников, вести аналитическую и контрольную работу. Применение простейших методов защиты, как правило, дает значительный эффект.

В крупных производственных и исследовательских фирмах с множеством информационных систем и значительными объемами защищаемых сведений формируется многоуровневая система защиты информации, характеризующаяся иерархическим доступом к информации. Однако эти системы, как и простейшие методы защиты, не должны создавать сотрудникам серьезные неудобства в работе, т. е. они должны быть «прозрачными».

Содержание составных частей элементов, методы и средства защиты информации в рамках любой системы защиты должны регулярно изменяться с целью предотвращения их раскрытия заинтересованным лицом. Конкретная система защиты информации фирмы всегда является строго конфиденциальной, секретной. При практическом использовании системы следует помнить, что лица, проектирующие и модернизирующие систему, контролирующие и анализирующие ее работу не могут быть пользователями этой системы.

Вывод: безопасность информации в современных условиях компьютеризации информационных процессов имеет принципиальное значение для предотвращения незаконного и часто преступного использования ценных сведений. Задачи обеспечения безопасности информации реализуются комплексной системой защиты информации, которая по своему назначению способна решить множество проблем, возникающих в процессе работы с конфиденциальной информацией и документами. Основным условием безопасности информационных ресурсов ограниченного доступа от различных видов угроз является прежде всего организация в фирме аналитических исследований, построенных на современном научном уровне и позволяющих иметь постоянные сведения об эффективности системы защиты и

направлениях ее совершенствования в соответствии с возникающими ситуационными проблемами.

Лекция 3
Аналитическая работа в сфере безопасности информационных ресурсов

Учебные вопросы:
1. Понятие информационно-аналитической работы.
2. Направления аналитической работы
3. Этапы аналитической работы.
4. Методы аналитической работы

Вопрос 1. Понятие информационно-аналитической работы

Аналитические методы обработки информации очень важны и успешно используются большинством фирм. Не в последнюю очередь в аналитической обработке нуждаются сведения, получаемые и используемые службой безопасности фирмы. Такие сведения отрывочны, противоречивы, зачастую недостоверны, но именно на их основе принимаются жизненно важные для фирмы решения. Информационно-аналитическая деятельность службы безопасности фирмы представляет собой системное получение, анализ и накопление информации с элементами прогнозирования по вопросам, относящимся к безопасности фирмы, и на этой основе консультирование и подготовка рекомендаций руководству о правомерной защите от противоправных посягательств. Служба безопасности проводит аналитическую работу не только с целью предотвратить утрату собственной информации, но и с целью получения информации о конкурентах. Являясь ядром такого понятия, как «разведка в бизнесе», аналитическая обработка информации позволяет получать по различным оценкам от 80 до 90 % необходимой информации при использовании только открытых источников.

Руководитель каждой фирмы имеет собственный взгляд на построение, направления работы и структуру информационно-аналитической службы (ИАС). На основе многолетнего опыта работы в этой области как отечественных, так и зарубежных специалистов сформировалось мнение, что в силу определенных причин наиболее эффективно такие службы функционируют как ядро службы безопасности. В первую очередь это объясняется тем, что основным потребителем аналитически обработанных данных является сама служба безопасности как подразделение, наиболее нуждающееся в аналитически обработанных данных, работающее на опережение и прогнозирование событий. Кроме того, в ходе аналитической работы очень часто используются (или могут быть получены) конфиденциальные сведения, что также подтверждает рациональность размещения ИАС в службе безопасности. Даже не являющиеся конфиденциальными аналитически обработанные данные представляют собой наиболее ценные информационные ресурсы фирмы.

В настоящее время ИАС фирмы рассматривается как основной поставщик аналитически обработанной информации для нужд всех подразделений фирмы. Основной задачей ИАС становится информационно-аналитическое обеспечение принятия решений по вопросам прежде всего основной деятельности. Таким образом, сотрудники фирмы или его подразделений могут заказать аналитический отчет по интересующему вопросу для принятия более рационального и взвешенного решения. В этой связи очень важной проблемой становится обеспечение информационной безопасности аналитически обработанных данных, представляющих собой ценный информационный ресурс фирмы наряду с другими конфиденциальными сведениями. Процесс заказа аналитического отчета должен быть четко регламентирован, чтобы только сотрудники определенного уровня имели право давать задания ИАС фирмы. Все заказы на аналитические исследования должны фиксироваться, причем темы исследований и авторы заказов на них должны тщательно регламентироваться. Доступ к аналитически обработанным данным должен быть строго ограничен.

Защита информации внутри ИАС представляет собой крайне сложную задачу, так как специфика аналитической работы в ряде случаев вступает в прямое противоречие с нормами защиты информации. Например, обеспечение такого важного принципа, как дробление информации в работе реальных ИАС, в большинстве случаев практически невозможно, так как это тормозит работу всей системы ИАС, где сотрудники должны иметь представление обо всей картине событий. Сокрытие какой-либо информации от сотрудников ИАС может привести их к ложным выводам, а фирму – к принятию неверных решений, а сле-

довательно, и к убыткам. ИАС, являясь ядром службы безопасности фирмы, не имеет и не должна иметь властных функций. Такое положение исключает намеренное искажение обрабатываемой информации и позволяет работать «на стыках» по пограничным вопросам.

Функции ИАС:

• обеспечить своевременное поступление надежной и всесторонней информации по интересующим вопросам;

• описать сценарии действий конкурентов, которые могут затрагивать текущие интересы фирмы;

• осуществлять постоянный мониторинг событий во внешней конкурентной среде и на рынке, которые могут иметь значение для интересов фирмы;

• обеспечить безопасность собственных информационных ресурсов;

• обеспечить эффективность и исключить дублирование при сборе, анализе и распространении информации.

Вывод: ИАС все в большей степени становится важным и функционально емким подразделением любой фирмы и, как правило, входит в состав службы безопасности. В последнее время специалисты все чаще сходятся во мнении, что в ИАС должна быть сосредоточена вся работа по прогнозированию ситуаций, а также формированию соответствующих информационных комплексов, необходимых для эффективного и взвешенного принятия решений.

Вопрос 2. Направления аналитической работы

Направления аналитической работы определяются каждой фирмой самостоятельно и отражают области ее интересов. К основным направлениям аналитической работы, разрабатываемым на многих фирмах, можно отнести: анализ объекта защиты, анализ угроз, анализ каналов несанкционированного доступа к информации, анализ комплексной безопасности фирмы, анализ нарушений режима конфиденциальности, анализ подозрений утраты конфиденциальной информации и т. д.

Можно выделить моменты, общие для всех ИАС. Направления аналитической работы, ведущейся ИАС фирмы, могут быть постоянными, периодическими и разовыми. Постоянные направления аналитической работы являются наиболее важными. Периодические и разовые направления аналитической работы характеризуются своей жесткой зависимостью от постоянных направлений. Промежутки времени, через которые проводятся исследования в области периодических направлений аналитической работы, всецело зависят от результатов анализа по постоянным направлениям. Разовые направления аналитической работы не только жестко зависят от постоянной аналитической работы, но и в подавляющем большинстве случаев являются следствием результатов таких исследований.

В концептуальном отношении ИАС должна представлять собой единую систему анализа, контроля и прогнозирования внешней и внутренней ситуации. Все направления аналитической работы должны быть связаны определенной логикой взаимодействия. Результаты исследований в одном направлении должны влиять на ход других исследований таким образом, чтобы результаты постоянных направлений аналитической работы инициировали проведение периодических и разовых исследований, а результаты последних не выпали из внимания специалистов по постоянным направлениям.

Следовательно, ИАС должна быть единой и взаимосвязанной структурой обеспечения фирм достоверной и аналитически обработанной информацией, направленной на информационную поддержку принятия эффективных решений по всем направлениям безопасности бизнеса.

Каждая фирма ведет индивидуальные направления аналитической работы и самостоятельно решает, следует ли разрабатывать их постоянно, периодически или только по мере надобности. Более того, каждая фирма имеет свои специфические области интересов, в рамках которых проводит аналитические исследования. Направления аналитической работы могут быть различными, но логика взаимодействия и система связей между направлениями исследований должны сохраняться. Принципиально важными представляются ключевые направления, работа по которым ведется постоянно. Как указывалось выше, наиболее сложными для обнаружения являются организационные каналы несанкционированного доступа к защищаемой информации фирмы, связанные с так называемым человеческим фактором. Например, трудно обнаружить инициативное сотрудничество злоумышленника с сотрудником фирмы – секретарем-референтом, экспертом, оператором ЭВМ и др. В основе поиска и обнаружения таких каналов лежит постоянная аналитическая работа, которая должна носить превентивный характер и использовать в качестве инструмента учетный аппарат, предназначенный для фиксирования (протоколирования) необходимых для анализа сведений. В данном случае аналитическая работа представляет собой комплексное исследование различной целевой направленности в целях выявления, структуризации и изучения опасных объективных и субъективных, потенциальных и реальных ситуаций, которые могут создать риск для экономической и информационной безопасности фирмы, ее деятельности или персонала, привести к материальным, финансовым или иным убыткам, падению престижа фирмы или ее продукции.

Результаты аналитической работы показывают степень безопасности интеллектуальной собственности, условий функционирования фирмы и являются основой для построения и совершенствования системы защиты традиционных и электронных информационных ресурсов, формирования рубежей охраны территории, здания, помещений, оборудования, продукции и персонала фирмы. Аналитическое исследование позволяет выработать способы пассивного и активного противодействия злоумышленнику в организационных и технических каналах, разработать и систематически совершенствовать систему защиты информации, определять ее структуру и стоимость в соответствии с реальными опасностями, Угрожающими ценным информационным ресурсам фирмы.

Обнаружение действующего или предполагаемого канала несанкционированного доступа к информации, а также предотвращение его появления возможны только при наличии постоянного контроля и анализа объекта защиты, уровня безопасности информационных ресурсов в источнике и канале распространения информации. Уязвимым является любой элемент информационных ресурсов и информационных систем. Другие пути носят случайный характер ожидания ошибки в тайных действиях злоумышленника.

Обнаружение канала или каналов несанкционированного доступа к ценной информации фирмы входит в число постоянных направлений аналитической работы и в общем виде включает в себя:

• анализ источников конфиденциальной информации;

• анализ каналов объективного распространения информации; • аналитическую работу с источником угрозы информации. Аналитическое исследование источников конфиденциальной информации предусматривает:

• выявление и классификацию существующих и возможных конкурентов и соперников фирмы, криминальных структур и отдельных преступных элементов, интересующихся фирмой;

• выявление и классификацию максимально возможного числа источников конфиденциальной информации фирмы;

• выявление, классификацию и ведение перечня (учетного аппарата) реального состава циркулирующей в фирме конфиденциальной информации (в разрезе источников, обеспечиваемых функций и видов работы, с указанием носителей – документов, дискет, файлов и т. д.);

• изучение данных учета осведомленности сотрудников в тайне фирмы в разрезе каждого руководителя и сотрудника (в том числе технического и вспомогательного), т. е. изучение степени и динамики реального владения (в том числе случайного) сотрудниками конфиденциальной информацией;

• изучение состава конфиденциальной информации в разрезе документов, т. е. изучение правильности расчленения тайны (конфиденциальной информации) между документами и определение избыточности ценной информации в документах;

• учет и изучение выявленных внутренних и внешних, потенциальных и реальных (пассивных и активных) угроз каждому отдельному источнику информации, контроль процесса формирования канала несанкционированного доступа к информации;

• ведение и анализ полноты перечня защитных мер, предпринятых по каждому источнику, и защитных мер, которые могут быть использованы при активных действиях злоумышленника, заблаговременное противодействие злоумышленнику.

Обязательному учету подлежат все санкционированные и несанкционированные обращения сотрудников фирмы к конфиденциальной информации, документам, делам и базам данных.

По отношению к каналам объективного (естественного) распространения защищаемой информации (управленческие и производственные действия, функциональные связи персо-

нала, информационные сети, технические каналы излучения информации и т. п.) применяются следующие аналитические действия и меры превентивного контроля:

• выявление и классификация реального максимального состава каналов объективного распространения конфиденциальной информации в фирме;

• изучение составных элементов каждого канала с целью нахождения опасных участков, способствующих возникновению канала несанкционированного доступа к информации;

• исследование и обобщение способов и сферы распространения информации в каждом канале;

• изучение (учет) состава конфиденциальной информации, циркулирующей в каждом канале;

• изучение (учет) состава конфиденциальной информации, циркулирующей между источниками;

• изучение сферы распространения информации при коммуникативных связях фирмы (по конкурентам, средствам массовой информации, выставкам и ярмаркам, рекламным изданиям и т. п.);

• контроль и перекрытие каналов несанкционированного ознакомления с информацией ограниченного доступа для третьих лиц, случайных, посторонних людей;

• исследование состава и эффективности методов защиты, предпринятых по каждому каналу, и дополнительных мер противодействия злоумышленнику при активных угрозах, экстремальных ситуациях.

Анализ угроз является одним из самых важных разделов аналитической работы и представляет собой ответ на вопрос, от чего или кого следует защищать определенные ранее объекты защиты. Источники угрозы конфиденциальной информации – объективные и субъективные события, явления, факторы, действия и обстоятельства, содержащие опасность для ценной информации.

К объективным источникам можно отнести: экстремальные ситуации, несовершенство технических средств и др. Субъективные источники связаны с человеческим фактором и включают: злоумышленников Различного рода, посторонних лиц, посетителей, неквалифицированный или безответственный персонал, психически неполноценных людей, сотрудников, обиженных руководством фирмы и др. Источники угрозы могут быть внешними и внутренними. Внешние источники находятся вне фирмы и представлены чрезвычайными событиями, а также организационными структурами и физическими лицами, проявляющими определенный интерес к фирме. Внутренние источники угрозы связаны с фатальными событиями в здании фирмы, а также с персоналом. Однако наличие источника угрозы само по себе не является угрозой. Угроза реализуется в действиях.

Аналитическая работа с источником угрозы конфиденциальной информации предусматривает:

• выявление и классификацию максимального состава источников угрозы конфиденциальной информации;

• учет и изучение каждого отдельного субъективного внутреннего и внешнего источника, степени его опасности (анализ риска) при реализации угрозы;

• разработку превентивных мероприятий по локализации и ликвидации объективных угроз.

В области внешних источников угрозы аналитическая работа связана с маркетинговыми исследованиями, которые регулярно ведет любая фирма. Анализ внутренних источников угрозы имеет целью выявление и изучение недобросовестных интересов и злоумышленных устремлений отдельных сотрудников фирмы и партнеров. В процессе анализа источников выявляются факты получения злоумышленником секретов фирмы, факты

сотрудничества персонала фирмы с конкурентами или наличия в составе сотрудников фирмы злоумышленника.

Контрольная и аналитическая работа проводится при потенциальных и пассивных угрозах источникам и каналом распространения информации. При активной угрозе одновременно осуществляется заранее спланированное, продуманное и решительное противодействие злоумышленнику. При несколько упрощенной схеме целью проведения анализа угроз можно считать выявление фигуры противника и его планов по дестабилизирующему воздействию на фирму. В ряде случаев более эффективно проводить анализ не от выявления и рассмотрения всех объектов защиты и каналов распространения информации, а от выявления лица (лиц), которое заинтересовано в реализации каких-либо угроз как конфиденциальной информации,

сотрудникам, так и фирме в целом, т. е. от выявления злоумышленника. Этот метод позволяет не только более четко спрогнозировать дальнейшие действия этого лица, но и оценить границы его действий и материальные возможности. Сначала нужно выяснить, кто является злоумышленником и что ему нужно, затем, исходя из имеющихся у него средств и возможностей, будет гораздо легче спрогнозировать, как именно он попытается достигнуть своей цели. Однако не следует забывать и о том, что достаточно серьезную угрозу могут представлять и субъекты (объекты), не заинтересованные в нанесении ущерба фирме.

Следовательно, наличие, ведение и результаты постоянной аналитической работы определяют необходимость, структуру и содержание системы защиты информации, степень ее требуемой эффективности и направления совершенствования. При отсутствии в фирме серьезной аналитической работы становится практически невозможным выявление и контроль каналов несанкционированного доступа к ценной, конфиденциальной информации фирмы.

Сотрудники ИАС фирмы должны учитывать все каналы несанкционированного доступа к конфиденциальной информации, выявлять, определять наиболее вероятные из них и контролировать их. С этой целью сотрудники ИАС должны принимать непосредственное участие в мероприятиях, в ходе которых имеется вероятность возникновения указанных каналов доступа к конфиденциальной информации фирмы. Так, целесообразным является предварительная оценка аналитиками подготовленных к публикации материалов о фирме, выставочных проспектов, рекламных изданий и т. п., их участие в презентациях, выставках, собраниях акционеров, переговорах, а также собеседованиях и тестированиях кандидатов на должности. Последнее является одной из основных и наиболее важных обязанностей ИАС, так как именно на этом этапе можно с определенной долей вероятности перекрыть один из основных организационных каналов – поступление злоумышленника на работу в фирму. В состав ИАС должны входить профессиональные психологи – специалисты по проведению опросов и тестов среди персонала.

Аналитически обработанные сведения вносятся в электронную базу данных. Аналитические отчеты по каждому направлению представляются с определенной периодичностью. В любой момент времени по требованию руководства ИАС должна быть в состоянии представить сводный обзор по всем направлениям. При выявлении каких-либо подозрений, угроз, пробелов в защите и т. п. сразу же ставятся в известность руководители, а аналитический отчет готовится в кратчайшие сроки.

Не менее важными являются и так называемые периодические направления аналитической работы, которые проводятся через определенные промежутки времени с целью контроля эффективности и возможности внесения улучшений в действующую в фирме систему защиты информации. К такому виду направлений аналитической работы прежде всего относится анализ степени безопасности фирмы. Очевидно, что постоянная и каждодневная аналитическая работа по данному направлению не имеет смысла. Вполне достаточно проводить

анализ через определенные, специально установленные промежутки времени. Это направление аналитической работы находится в прямой зависимости от анализа состава угроз – постоянного направления аналитической работы. Именно результаты аналитической работы по выявлению угроз позволяют установить рациональную периодичность анализа эффективности структуры действующей системы безопасности фирмы. Так, при появлении дополнительных угроз, аналитическую работу (и следовательно, проверки, контрольные мероприятия и т. п.) следует проводить более часто.

Необходимо также периодически проводить анализ нарушении режима конфиденциальности, причем это направление относится также и к разовым направлениям. Рассматриваемые в рамках периодического направления аналитической работы нарушения режима безопасности за определенный период времени анализируются с целью выявления вызвавших их причин и выработки мер для их устранения. Частота проведения исследований такого рода также напрямую зависит от результатов исследований по другим направлениям.

Разовые направления аналитических исследований также являются очень важными в силу того факта, что чаще всего бывают вызваны чрезвычайными обстоятельствами, происшествиями, неожиданно появившимися проблемами и т. п., требуют проведения исследований в кратчайшие сроки. Типичным примером разового направления аналитической работы является проверка подозрения утраты конфиденциальной информации фирмы и злоумышленных действий, а также анализ нарушения режима конфиденциальности в фирме. Последнее направление включается также и в подсистему периодических направлений. Тем не менее факт каждого нарушения режима конфиденциальности должен сразу же расследоваться и анализироваться.

Вывод: все направления аналитической работы независимо от их типа, в том числе имеющие разовый характер, должны быть связаны в единую систему, позволяющую эффективно принимать решения, предотвращать угрозы и прогнозировать развитие событий – работать на опережение.

Вопрос 3. Этапы аналитической работы

Ведение аналитической работы возможно только при наличии необходимой информации, поэтому в первую очередь нужно определить, какая именно информация будет необходима аналитикам для работы, где можно ее получить и какой из источников можно при этом использовать. Как правило, получение информации не относится специалистами непосредственно к аналитической работе, тем не менее, определение круга исходной информации, а также мест и способов ее получения должно решаться непосредственно сотрудниками ИАС.

Интерпретация информации является первым этапом предварительного анализа. Под интерпретацией подразумевается выявление истинного значения той или иной информации. В первую очередь это относится к вербальной информации, так как очень часто то или иное высказывание бывает понято превратно. Это происходит, когда фраза вырвана из контекста либо неправильно понята иностранная речь, интонация, жесты, сленг и т. п. При возникновении такой ситуации в помощь аналитикам целесообразно пригласить знающего специалиста, который сможет правильно интерпретировать то или иное сообщение.

В интерпретации нуждаются не только слова, но и действия. Зачастую факт, внешне подозрительный, на самом деле может иметь абсолютно положительный характер, а многие по сути угрожающие факты могут иногда выглядеть как неопасные.

Язык, используемый для описания информации, может допускать неоднозначность ее понимания. Это создает определенные трудности при интерпретации вербальной информации, но в этом случае истинный смысл можно понять из контекста. Информация, которая хранится в персональных компьютерах, как правило, лишена контекста, поэтому ошибочная интерпретация становится гораздо более вероятной. Западные специалисты определяют цену информации через те действия, которые могут быть предприняты в результате знания этой информации.

Вся информация подразделяется на факты, личные мнения и аналитически обработанные данные. Смешивание или неправильное определение этих различных по своей сути видов информации может приводить к ошибкам в интерпретации и, как следствие, к принятию неправильных решений. Следовательно, процесс интерпретации требует максимальной осторожности и тщательности. В каждом конкретном случае необходимо выявить истинный смысл поступившей информации. Здесь аналитики сталкиваются с такой проблемой, как выделение не относящейся к делу информации.

Выделение посторонней информации составляет следующий этап предварительного анализа. Этот процесс является одним из самых Ложных и ответственных моментов во всей процедуре. Избыток ""формации, так же как и ее недостаток, представляет собой серьезную проблему и затрудняет проведение аналитической работы. Тактика выделения нескольких ключевых деталей гораздо более эффективна, чем разбрасывание между многими разрозненными данными. Вместе с тем именно на этом этапе существует опасность отбросить важную информацию. Как правило, это может произойти в случае неправильной интерпретации сведений на предыдущем этапе. Кроме того, аналитики могут стремиться сохранить не относящуюся напрямую к делу информацию в надежде, что она может пригодиться в будущем. Такая информация должна заноситься в банк данных ИАС таким образом, чтобы впоследствии ее можно было легко найти. С созданием такого информационного фонда и его постоянным пополнением задача поиска и сбора исходной информации для анализа будет значительно облегчена. Тем не менее избыток информации представляет собой серьезную проблему, так как значительно замедляет ведение аналитической работы, старение же и обесценивание информации может происходить очень быстро. Кроме того, избыток не

относящейся к делу информации является для руководителя ИАС сигналом того, что поиск и сбор информации организованы неэффективно.

Оценка информации составляет следующий этап. Под оценкой понимается метод ранжирования источников информации, самой информации и способов ее получения. Как правило, пользуются системой оценок информации, при которой аналитик может выразить свою точку зрения относительно надежности и достоверности полученных сведений, хотя очевидным недостатком данной системы будет определенная субъективность оценок. Например:

Оценка источника:

• надежный источник;

• обычно надежный источник;

• довольно надежный источник;

• не всегда надежный источник;

• ненадежный источник;

• источник неустановленной надежности. Оценка информации:

• подтвержденная другими фактами;

• вероятно правдивая (75 %);

• возможно правдивая (50 %);

• сомнительная (25 %);

• неправдоподобная;

• достоверность не поддается определению.

Оценка способа получения информации источником:

• получил информацию сам (сам видел, слышал и т. п.);

• получил информацию через постоянный источник (через информатора, открытые источники и т. п.);

• получил информацию через разовый источник (случайно подслушанный разговор, слухи и т. п.).

На этапе оценки необходимо установить, насколько информация может соответствовать истине. При этом нужно учитывать, что можно получить не соответствующую истине информацию следующих типов:

• дезинформацию, доведенную до сведения источника;

• преднамеренно или непреднамеренно искаженную источником;

• произвольно или непроизвольно измененную в ходе передачи. При намеренной дезинформации применяется заведомая ложь, полуправда, а также правдивые сведения, которые в данном контексте подтолкнут воспринимающих информацию лиц к ложным выводам.

Искажения, возникающие в процессе передачи исходных данных, могут происходить по многим причинам:

• передача только части сообщения;

• пересказ услышанного своими словами;

• факты, искаженные чьим-либо субъективным восприятием.

Для своевременного выявления искаженной информации, а также для успешной борьбы с вероятной дезинформацией необходимо различать факты и мнения, учитывать субъективные характеристики источника и его предполагаемое отношение к выдаваемому сообщению. Следует четко осознавать, способен ли источник по своему положению иметь доступ к сообщаемым фактам. В качестве страховочных мер всегда нужно иметь дублирующие источники, использовать дублирующие каналы связи и стараться исключать все лишние промежуточные звенья передачи информации. Кроме того, необходимо помнить, что особенно легко воспринимается та дезинформация, которая хорошо соответствует принятой ранее версии, т. е. та, которую предполагают или желают получить.

Следующим этапом является построение предварительных версии, объясняющих место основных полученных фактов в цепи событий. Первым шагом является составление списка сведений, приготовленных для анализа. Это необходимо для дальнейшего ранжирования их по степени важности, кроме того, это является некой гарантией того, что сведения не выпадут из поля зрения и о них не забудут. Далее необходимо выделить ключевые моменты, отделить их от менее важных, не играющих главной роли в данной ситуации. Полученные сведения должны быть четко классифицированы по степени достоверности источника, самих сведений и способа их получения. Самые свежие и полные сведения должны рассматриваться в первую очередь. В перечне сведений, приготовленных для анализа, наиболее важные сведения специально помечаются. Материалы с пометками «источник неустановленной надежности» и «достоверность не поддается определению» откладываются и не участвуют в анализе без крайней необходимости.

Затем необходимо выявить все возможные гипотезы, которые могут объяснять ключевые события, и, расположив их по степени вероятности, поочередно проверять на стыкуемость со всеми данными. Если обнаружено значительное расхождение какой-либо предварительной гипотезы с полученными сведениями, причем последние имеют достаточно высокие оценки достоверности, то следует переходить к следующей гипотезе. Таким образом, выбираются наиболее вероятные предположения. На этом этапе возникает одна из самых серьезных проблем аналитической работы – противоречия в сведениях. Для ее преодоления необходимо сравнить оценки информации и источника, даты получения спорных сведений. Решающее же значение имеет интуиция, знания и опыт самого сотрудника, проводящего анализ. Конфликты в информации должны быть устранены в процессе анализа, для их разрешения собирается дополнительная информация, что соответствует следующему этапу аналитической работы. Если решение, которое будет принято на основе аналитически обработанной информации, является очень важным и нет возможности получить дополнительную информацию для устранения противоречий, то окончательный выбор возлагается на лиц, ответственных за принятие решения. Тем не менее общая доля таких ситуаций должна сводиться к минимуму, так как это свидетельствует о неудовлетворительной работе ИАС.

Следующим этапом является определение потребности в дополнительной уточняющей информации, а также выяснение, какая именно информация необходима и почему. На этом этапе выявляются пробелы в информации. Часть пробелов может быть быстро установлена, так как является результатом недостаточного исследования, другая же часть пробелов в информации может и не быть обнаружена аналитиком, потому что упущена на этапе сбора самих сведений. Очевидно, что второй вид пробелов в информации является гораздо более опасным.

Необходимо четко различать понятия «неполная информация» и «пробел в информации». Неполная информация означает отсутствие не имеющих особой важности сведений, что является естественным, так как никогда нельзя получить абсолютно все сведения. Более того, такая информация была бы избыточной и осложнила бы анализ. Пробел же в информации подразумевает отсутствие сведений, являющихся ключевыми в данной ситуации или необходимыми для устранения противоречий. Такие сведения крайне важны для проведения анализа.

Выявив пробелы в информации, нужно определить их важность для дальнейшего анализа. Нельзя до бесконечности откладывать составление аналитического отчета под предлогом того, что в информации выявлены пробелы. На определенном этапе следует признать, что для решения задачи собрано достаточно данных. Кроме того, имеют значение факторы времени и денег, потому что решение проблемы ограничено тем и другим. Сотрудники ИАС

должны стремиться к решению поставленной задачи имеющимися средствами и в разумные сроки.

На основе выполнения предыдущих этапов приступают к подготовке аналитических отчетов по определенному вопросу, выработке конкретных выводов и предложений. Подготовка отчетов является основной обязанностью аналитика, а готовый отчет представляет собой результат функционирования системы аналитической работы. Отчеты могут быть представлены в различных формах. Наиболее часто отчет составляется в письменном виде, но он также может быть устным, иллюстрируемым графиками, таблицами, диаграммами и т. п. Если сроки жестко ограничены, отчет излагается устно, в форме вопросов и ответов.

В зарубежной литературе выделяют три основных вида аналитических отчетов. Первый вид называют тактическим (оперативным) отчетом. К этому типу относятся экстренные отчеты по какому-либо вопросу небольшого объема, которые необходимы для срочного принятия решения. При этом аналитика редко знакомят с причиной или целью данного задания. Такие отчеты составляются по разовым направлениям аналитической работы. Второй вид составляют стратегические отчеты. Они содержат более полную информацию и менее ограничены сроками. В них включается подробная предыстория данной проблемы и прогноз ее дальнейшего развития, причем для построения реалистичной гипотезы анализируется вся предшествующая информация по данной теме. Отчеты такого типа соответствуют постоянным направлениям аналитической работы. Третий вид представлен периодическими отчетами, основной отличительной особенностью которых является то, что они готовятся по графику. Интервалы между сроками предоставления составляют дни, недели или месяцы. Как правило, такой вид отчетов готовится по проблемам, являющимся объектом постоянного пристального внимания со стороны ИАС фирмы. Этот вид может соответствовать как периодическим, так и постоянным направлениям аналитической работы.

Все письменные отчеты должны содержать глубокий анализ и быть представлены в регламентированной (типовой, унифицированной) форме. Потребителями аналитических отчетов являются ответственные за планирование и принятие решений лица, которые вправе предъявлять определенные требования к содержанию и оформлению отчетов. Аналитический отчет должен быть четко, логично и грамотно составлен. Кроме того, отчет должен абсолютно соответствовать месту сотрудника – потребителя информации в разрешительной системе доступа к конфиденциальной информации: по степени конфиденциальности используемых в отчете сведений, профилю профессиональных знаний сотрудника и деловой необходимости информации для конкретной работы. Нужно учитывать также и то, что внешний вид отчета обязательно будет влиять на восприятие содержащейся в нем информации.

За рубежом используется, как правило, следующая форма изложения данных аналитического отчета:

1) Заключение. Здесь должны содержаться ответы на вопросы, какова степень важности полученной информации, ее значение для принятия конкретных решений, идет ли речь о каких-либо угрозах, подозрениях, выявленных негативных факторах и т. п., какое отношение имеет предмет отчета к другим областям аналитической работы. Факты и сведения, на основе которых получены результаты анализа, не должны смешиваться с самими результатами.

2) Рекомендации. Должны быть указаны конкретные направления дальнейших действий службы безопасности и других структурных подразделений предприятия для улучшения системы безопасности, предотвращения утраты информации, принятия наиболее эффективных решений и т. п.

3) Обобщение информации. Изложение самой существенной информации без излишней детализации.

4) Источники и надежность информации. Должны быть указаны предполагаемые оценки надежности данных и источника на момент написания отчета, так как для принятия решений необходимо оценить надежность материалов, являющихся их базой.

5) Основные и альтернативные гипотезы. Обязательно должны указываться рассмотренные в ходе анализа наиболее вероятные гипотезы, что помогает принимать более взвешенные и адекватные решения, а также позволяет еще раз оценить правильность выбранной гипотезы.

6) Недостающая информация. Четко указывается, какая именно дополнительная информация необходима для подтверждения окончательной гипотезы и принятия решения. Описанная структурная схема проведения аналитического исследования позволяет предоставить в распоряжение пользователя, принимающего решение, структурированный массив ценной информации, отражающей с определенной степенью достоверности сложившуюся ситуацию с обеспечением безопасности информационных ресурсов фирмы.

Вопрос 4. Методы аналитической работы

Основным назначением всех аналитических методов является обработка полученных сведений, установление взаимосвязи между фактами, выявление значения этих связей и выработка конкретных предложений на основе достоверной и полной, аналитически обработанной информации. Существует широкий спектр специальных методов анализа: графические, табличные, матричные и т. п., например, диаграммы связи и матрицы участников, схемы потоков данных, временные графики, графики анализа визуальных наблюдений VIA (visual investigative analysis) и графики оценки результатов PERT (program evaluation review technique). Тем не менее следует отметить, что у каждого аналитика есть свой собственный метод анализа, который может быть как комбинацией вышеперечисленных методов, так и сугубо индивидуальным, уникальным методом аналитической работы.

С помощью диаграмм связей выявляется наличие связи между субъектами, вовлеченными в конкретную ситуацию, подвергающуюся анализу, а также области общения, соприкосновения этих субъектов. На диаграмме связей отмечают как наиболее прочные, так и вспомогательные связи между субъектами. Анализируются все связи без исключения, так как в ходе развития событий и получения дополнительной информации вспомогательные связи могут выступить на первый план. Для большей наглядности следует также указывать на диаграмме связи должностей (для физических лиц) или род деятельности (для юридических лиц).

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.