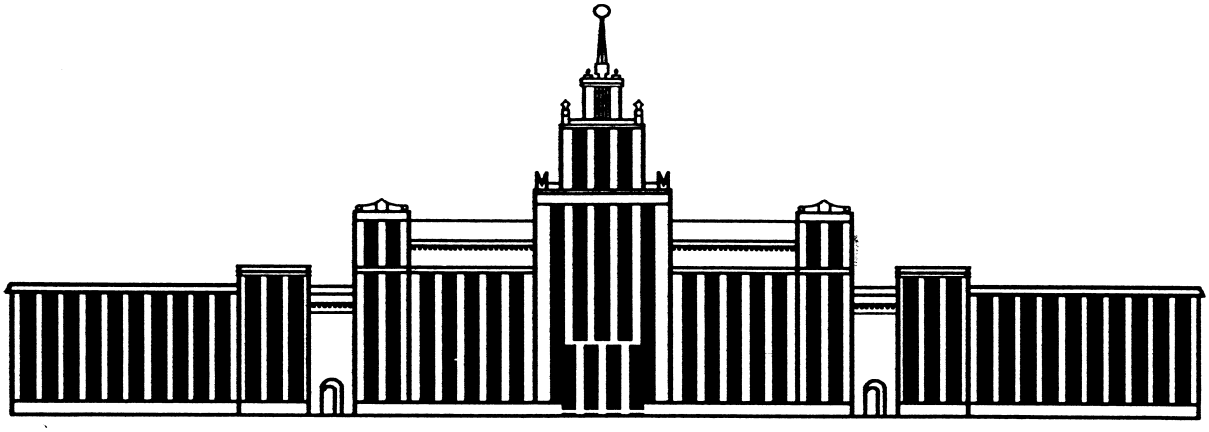
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ



ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

004(07)
А91

Л.В. Астахова

ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Челябинск
2014

Министерство образования и науки Российской Федерации
Южно-Уральский государственный университет
Кафедра «Безопасность информационных систем»

004(07)
А91

Л.В. Астахова

ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Челябинск
Издательский центр ЮУрГУ
2014

УДК 004.056(075.8)
А91

Одобрено
Советом Приборостроительного (КТУР)
факультета

Рецензенты:
В.М. Чернов, В.Н. Худяков

Астахова, Л.В.

А91 Теория информационной безопасности и методология защиты информации: учебное пособие / Л.В. Астахова. – Челябинск: Издательский центр ЮУрГУ, 2014. – 137 с.

В учебном пособии рассмотрены основные теоретико-методологические вопросы информационной безопасности и защиты информации: понятия информационной безопасности и защиты информации, структура и содержание угроз защищаемой информации, виды, методы и средства защиты информации, ресурсное обеспечение защиты информации. Учебное пособие рассчитано на студентов, изучающих дисциплину «Теория информационной безопасности и методология защиты информации», включенную в базовую часть профессионального цикла дисциплин ФГОС-3 по специальности 090915 «Безопасность информационных технологий в правоохранительной сфере». Также оно может быть полезно студентам, изучающим дисциплину «Основы информационной безопасности» в рамках других направлений, связанных с защитой информации: 090900 «Информационная безопасность», 090303 «Информационная безопасность автоматизированных систем» и др.

УДК 004.056(075.8)

ВВЕДЕНИЕ

Дисциплина «Теория информационной безопасности и методология защиты информации» включена в базовую часть профессионального цикла дисциплин ФГОС-3 по специальности 090915 – Безопасность информационных технологий в правоохранительной сфере.

Целью освоения учебной дисциплины «Теория информационной безопасности и методология защиты информации» является приобретение теоретических знаний по основам информационной безопасности (предметов и объектов защиты, анализу и оценке угрозы информационной безопасности), а также знаний методологии и методики защиты информации в организациях.

В результате освоения дисциплины студент должен обладать следующими компетенциями:

- способностью понимать социальную значимость своей профессии, цель и смысл государственной службы, выполнять гражданский и служебный долг, профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета (ОК-4);
- способностью владеть культурой научного мышления, анализировать логику рассуждений и высказываний (ОК-8);
- способностью осуществлять устную и письменную коммуникации на русском языке, логически верно, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии (ОК-9);
- способностью анализировать свои возможности, самосовершенствоваться и повышать свой интеллектуальный и общекультурный уровень, профессиональную квалификацию, развивать социальные и профессиональные компетенции, изменять вид и характер своей профессиональной деятельности, адаптироваться к изменяющимся социокультурным условиям и меняющимся условиям профессиональной деятельности (ОК-13);
- способностью выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОК-14).
- способностью участвовать в исследовании и проверке объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации (ПК-6);
- способностью разрабатывать предложения по совершенствованию системы управления безопасностью информации (ПК-23);
- способностью соблюдать в профессиональной деятельности требования нормативных правовых актов и иных нормативных документов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности (ПК-24);

- способностью проводить анализ состояния безопасности информации на объектах и в отдельных системах с использованием отечественных и зарубежных стандартов (ПК-30);
- способностью принимать участие в создании системы защиты информации на объекте информатизации (ПК-38).

Учебное пособие состоит из четырех разделов.

В первом разделе освещены базовые понятия в области информационной безопасности, их соотношения друг с другом, организация системы обеспечения информационной безопасности в России, вопросы государственной политики в области информационной безопасности Российской Федерации**.**

Второй раздел посвящен информации как предмету и объекту защиты: понятию защищаемой информации, критериям отнесения информации ограниченного доступа и общедоступной информации к защищаемой. Особое внимание уделено видам защищаемой информации ограниченного доступа, к которым относятся государственная тайна, служебная тайна, коммерческая тайна, профессиональная тайна, персональные данные, объекты интеллектуальной собственности.

Третий раздел включает в себя вопросы понятия и классификации угроз защищаемой информации. В ней уделено внимание видам и способам дестабилизирующего воздействия на защищаемую информацию со стороны разных источников: людей; технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи; систем обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации; технологических процессов отдельных промышленных объектов; природных явлений. Отдельно освещены каналы и методы несанкционированного доступа к конфиденциальной информации.

Четвертый раздел характеризует методологию защиты информации: виды, методы, средства защиты информации, ее ресурсное обеспечение, ключевые моменты создания комплексной системы защиты информации.

Учебное пособие рассчитано на студентов, изучающих дисциплину «Теория информационной безопасности и методология защиты информации», включенную в базовую часть профессионального цикла дисциплин ФГОС-3 по специальности 090915 – Безопасность информационных технологий в правоохранительной сфере. Также оно может быть полезно студентам, обучающимся по другим направлениям, связанным с защитой информации: 090900 – Информационная безопасность, 090303 – Информационная безопасность автоматизированных систем и др.

Раздел I
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ: БАЗОВЫЕ ПОНЯТИЯ И ОРГАНИЗАЦИЯ

Тема 1. Проблема понятия «информационная безопасность»

1.1. Понятие информационной безопасности в «Доктрине информационной безопасности Российской Федерации».
1.2. Интерпретация понятия информационной безопасности А.И. Алексенцева.
1.3. Деятельностный подход к понятию информационной безопасности.
1.4. Рисковый подход к понятию информационной безопасности.

1.1. Понятие информационной безопасности в «Доктрине информационной безопасности Российской Федерации»

В законе Российской Федерации «О безопасности» (5 марта 1992 года) безопасность определена как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз (ст. 1).

Жизненно важные интересы – это совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства (Ст. 1).

В «Доктрине информационной безопасности Российской Федерации» (2000 год) дано следующее определение:

Информационная безопасность Российской Федерации – это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Это определение основано на теории интересов и требует конкретизации, во-первых, интересов личности, общества и государства и, во-вторых, – угроз этим интересам.

В соответствии с Доктриной:

Интересы личности в информационной сфере заключаются:

- в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития;
- в защите информации, обеспечивающей личную безопасность;
- в защите права интеллектуальной собственности (И.Л. Бачило);

- в обеспечении права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации.

Интересы общества в информационной сфере заключаются:

- в обеспечении интересов личности в этой сфере;
- в упрочении демократии, создании правового социального государства;
- в достижении и поддержании общественного согласия, в духовном обновлении России;
- в сохранение нравственных ценностей, утверждение в обществе идеалов высокой нравственности, патриотизма и гуманизма, развитие многовековых духовных традиций России, пропаганда национального культурного наследия, норм морали и общественной нравственности;
- в предотвращении манипулирования массовым сознанием;
- в приоритетном развитии современных телекоммуникационных технологий, сохранение и развитие отечественного научного и производственного потенциала.

Интересы государства в информационной сфере заключаются:

- в создании условий для гармоничного развития российской информационной инфраструктуры, для 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;
- в развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной инфор-

мации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Очевидно, что информационная безопасность тесно взаимосвязана с информатизацией. Согласно закону «Об информации, информатизации и защите информации» (1995), утратившем силу в 2006 году, информатизация – это «организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов».

Все составляющие национальных интересов РФ в информационной сфере, названные в Доктрине информационной безопасности РФ, – это ключевые процессы информатизации общества.

Угрозы информационной безопасности Российской Федерации соответствуют составляющим национальных интересов России в информационной сфере и подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;

- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

1.2. Интерпретация понятия информационной безопасности А.И. Алексенцева

По мнению А.И. Алексенцева, смысловое содержание понятия информационная безопасность предполагает и в какой-то мере предопределяет включение в него трех составляющих.

Первой составляющей является удовлетворение информационных потребностей субъектов, включенных в информационную среду. Здравый смысл подсказывает, что не может быть обеспечена информационная безопасность субъекта без наличия у него необходимой информации. Информационные потребности различных субъектов не одинаковы, однако в любом случае отсутствие необходимой информации может иметь и, как правило, имеет отрицательные последствия. Эти последствия могут носить

различный характер, их тяжесть зависит от состава отсутствующей информации.

Необходимая для удовлетворения информационных потребностей информация должна отвечать определенным требованиям.

Во-первых, информация должна быть относительно полной. Относительно, потому что абсолютно полной информации ни один субъект иметь не может. Полнота информации характеризуется ее достаточностью для принятия правильных решений.

Во-вторых, информация должна быть достоверной, ибо искаженная информация приводит к принятию неправильных решений.

В-третьих, информация должна быть своевременной, так как необходимые решения эффективны лишь тогда, когда они принимаются вовремя.

Вторая составляющая информационной безопасности – обеспечение безопасности информации. Требования полноты, достоверности и своевременности информации относятся не только к ее первоначальному статусу. Эти требования имеют силу на все время циркулирования информации, потому что их нарушение на стадии последующего использования информации также может привести к неправильным решениям или вообще к невозможности принятия решений, как и нарушение статуса конфиденциальности может обесценить информацию. Поэтому информация должна быть защищена от воздействий, нарушающих ее статус. А это относится к сфере безопасности информации. Стало быть, обеспечение безопасности информации должно являться второй составляющей информационной безопасности.

Третья составляющая информационной безопасности – обеспечение защиты субъектов информационных отношений от негативного информационного воздействия. К принятию неверных решений может привести не только отсутствие необходимой информации, но и наличие вредной, опасной для субъекта информации, которая чаще всего целенаправленно навязывается. Это требует обеспечения защиты субъектов информационных отношений от негативного информационного воздействия.

При таком подходе А.И. Алексенцев формулирует следующее определение:

Информационная безопасность – состояние информационной среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации и защиту субъектов от негативного информационного воздействия.

1.3. Деятельностный подход к понятию информационной безопасности

Структура деятельности по обеспечению информационной безопасности включает в себя:

- цель и результат деятельности по обеспечению информационной безопасности – информационная безопасность как состояние защищен-

ности объекта для удовлетворения его информационных потребностей;

- объект деятельности по обеспечению информационной безопасности (на кого она должна быть направлена). Мы уже говорили о том, что в практическом преломлении и информация, и информационная безопасность не существуют вообще, безотносительно к субъектам информационных отношений, именно субъект (автор или адресат информационного сообщения) определяет смысл информации, интерпретирует факты, а также – диктует показатели такой безопасности. Это относится не только к конкретным субъектам, но и к личности, обществу и государству в целом. Поэтому в основе определения информационной безопасности должен лежать главный объект деятельности – субъект информационных отношений (личность, общество и государство);
- субъект деятельности по обеспечению информационной безопасности – тот, кто осуществляет деятельность по обеспечению информационной безопасности. В роли субъектов могут выступать уполномоченные государственные структуры, отдельные организации, хозяйствующие субъекты, отдельные граждане;
- процессы деятельности по обеспечению информационной безопасности. Для обеспечения состояния защищенности субъектов информационных отношений в целях удовлетворения их информационных потребностей необходимо осуществить два основных процесса:

1) обеспечение качественного уровня их (субъектов) информационного пространства (доступность, достоверность, оперативность функционирующей в обществе информации), обеспечение их защищенности от негативных информационных воздействий (результат – качество информации, а значит – информационно-психологическая безопасность субъектов);

2) обеспечение безопасности защищаемой ими информации (результат – безопасность информации).

- средства деятельности по обеспечению информационной безопасности – то, с помощью чего и как осуществляется эта деятельность (методология, методы, способы, технологии). Каждый из названных выше процессов имеет свои, специфические средства. Так, обеспечение качественной информационной среды связано с методологией информатизации, со способами психологической защиты личности, обеспечение безопасности информации – с правовыми, организационными и техническими методами.

Таким образом, с точки зрения методологии деятельностного подхода информационная безопасность – это результат деятельности, направленной на удовлетворение информационных потребностей субъектов информационных отношений, сущностью которой является достижение состояния их защищенности в информационной среде, которое включает в себя качество окружающей их информационной среды и защищенность собственной информации.

Информационная безопасность – это состояние защищенности субъектов информационных отношений, включающее в себя: 1) качественную информационную среду (качество потребляемой информации, защищенность субъектов от негативных информационных воздействий) (информационно-психологическая безопасность) и 2) защищенность их информации (безопасность информации), обеспечивающее полное удовлетворение информационных потребностей субъектов.

1.4. Рисковый подход к понятию информационной безопасности

В законе «О техническом регулировании» (2002) безопасность продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации (далее – безопасность) определена как состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений.

Если взять за основу это определение, то информационную безопасность можно определить как состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда субъекту со стороны некачественной информационной среды, и защищаемой им информации.

Рекомендуемые источники и литература

1. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.

2. Алексенцев, А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» / А.И. Алексенцев // Безопасность информационных технологий. – 1999. – № 1.

3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2006.

4. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 09 сентября 2000 г. – М., 2000.

5. О безопасности: Закон Рос. Федерации от 5 марта 1992 г. № 2446-I // Рос. газ. – 1992. – 6 мая.

6. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 24-ФЗ // Рос. газ. – 2006. – 29 июля.

7. О техническом регулировании: Федер. закон Рос. Федерации от 27 дек. 2002 г. № 184-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации

15 дек. 2002 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 18 дек. 2002 г. // Рос. газ. – 2002. – 31 дек.

8. Информационная безопасность и защита информации: учеб. пособие / В.П. Мельников и др.; под ред. С.А. Клейменова. – М.: Академия, 2009. – 330 с.

Тема 2. Общие методы обеспечения информационной безопасности Российской Федерации

2.1. Правовые методы.
2.2. Организационно-технические методы.
2.3. Экономические методы.

2.1. Правовые методы

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;
- законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;

- разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;
- уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;
- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;
- определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;
- создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

2.2. Организационно-технические методы

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих

опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;
- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

2.3. Экономические методы

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Рекомендуемые источники и литература

1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 09 сентября 2000 г. – М., 2000.

2. Стратегия развития информационного общества в России до 2015 года» (2008) // http://www.scrf.gov.ru

3. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 24-ФЗ // Рос. газ. – 2006. – 29 июля.

4. О техническом регулировании: Федер. закон Рос. Федерации от 27 дек. 2002 г. № 184-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 15 дек. 2002 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 18 дек. 2002 г. // Рос. газ. – 2002. – 31 дек.

5. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.

6. Информационная безопасность и защита информации: учеб. пособие / В.П. Мельников и др.; под ред. С.А. Клейменова. – М.: Издательский центр «Академия», 2009. – 330 с.

7. Организационно-правовое обеспечение информационной безопасности: учеб. пособие / А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др.; под ред. А.А. Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.

8. Романов, О.А. Организационное обеспечение информационной безопасности: учебник / О.А. Романов, С.А. Бабин, С.Г. Жданов. – М.: Издательский центр «Академия», 2008. – 240 с.

9. Гришина, Н.В. Организация комплексной системы защиты информации / Н.В. Гришина. – М.: Гелиос АРВ, 2007. – 256 с.

10. Тихонов, В.А. Информационная безопасность: организационные, правовые и технические аспекты / В.А. Тихонов, В.В. Райх. – М.: Гелиос АРВ, 2006. – 516 с.

Тема 3. Государственная политика обеспечения информационной безопасности Российской Федерации

3.1. Принципы государственной политики обеспечения информационной безопасности Российской Федерации

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

- соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;
- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Фе-

дерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

3.2. Реализация государственной политики обеспечения информационной безопасности Российской Федерации

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются:

- разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности Российской Федерации;
- разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;
- принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, обеспечение технологической независимости страны в области соз-

дания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;

- развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации;
- гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

3.3. Стратегия развития информационного общества в Российской Федерации

Стратегия развития информационного общества в Российской Федерации (Утверждена Президентом Российской Федерации В. Путиным 7 февраля 2008 г., № Пр-212) является логическим продолжением Доктрины информационной безопасности Российской Федерации, развивая один из национальных интересов в информационной сфере – развитие отечественной информационной индустрии.

Целью формирования и развития информационного общества в Российской Федерации, согласно Стратегии, является повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий.

К числу основных задач, требующих решения для достижения поставленной цели, относятся:

1) формирование современной информационной и телекоммуникационной инфраструктуры, предоставление на ее основе качественных услуг и обеспечение высокого уровня доступности для населения информации и технологий;

2) повышение качества образования, медицинского обслуживания, социальной защиты населения на основе развития и использования информационных и телекоммуникационных технологий;

3) совершенствование системы государственных гарантий конституционных прав человека и гражданина в информационной сфере;

4) развитие экономики Российской Федерации на основе использования информационных и телекоммуникационных технологий;

5) повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и бизнеса с органами государственной власти, качества и оперативности предоставления государственных услуг;

6) развитие науки, технологий и техники, подготовка квалифицированных кадров в сфере информационных и телекоммуникационных технологий;

7) сохранение культуры многонационального народа Российской Федерации, укрепление нравственных и патриотических принципов в общественном сознании, развитие системы культурного и гуманитарного просвещения;

8) противодействие использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам России.

Развитие информационного общества в Российской Федерации базируется на следующих принципах:

- партнерство государства, бизнеса и гражданского общества;
- свобода и равенство доступа к информации и знаниям;
- поддержка отечественных производителей продукции и услуг в сфере информационных и телекоммуникационных технологий;
- содействие развитию международного сотрудничества в сфере информационных и телекоммуникационных технологий;
- обеспечение национальной безопасности в информационной сфере.

В Стратегии определены основные направления ее реализации:

1. В области формирования современной информационной и телекоммуникационной инфраструктуры, предоставления на ее основе качественных услуг в сфере информационных и телекоммуникационных технологий и обеспечения высокого уровня доступности для населения информации и технологий:

- создание инфраструктуры широкополосного доступа на всей территории Российской Федерации, в том числе с использованием механизмов частно-государственного партнерства;
- повышение доступности для населения и организаций современных услуг в сфере информационных и телекоммуникационных технологий;
- формирование единого информационного пространства, в том числе для решения задач обеспечения национальной безопасности;
- модернизация системы телерадиовещания, расширение зоны уверенного приема российских телерадиопрограмм;
- создание системы общественных центров доступа населения к государственным информационным ресурсам, в том числе государственной системы правовой информации.

2. В области повышения качества образования, медицинского обслуживания, социальной защиты населения на основе развития и использования информационных и телекоммуникационных технологий:

- расширение использования информационных и телекоммуникационных технологий для развития новых форм и методов обучения, в том числе дистанционного образования;

- внедрение новых методов оказания медицинской помощи населению, а также дистанционного обслуживания пациентов;
- предоставление гражданам социальных услуг на всей территории Российской Федерации с использованием информационных и телекоммуникационных технологий.

3. В области совершенствования системы государственных гарантий конституционных прав и свобод человека и гражданина в информационной сфере основным направлением является развитие законодательных механизмов.

4. В области развития экономики Российской Федерации на основе использования информационных и телекоммуникационных технологий:

- стимулирование применения организациями и гражданами информационных и телекоммуникационных технологий;
- создание условий для развития конкурентоспособной отечественной индустрии информационных и телекоммуникационных технологий, средств вычислительной техники, радиоэлектроники, телекоммуникационного оборудования и программного обеспечения;
- привлечение инвестиций для развития российской отрасли информационных и телекоммуникационных технологий, а также отечественной электронной промышленности;
- создание условий для развития компаний, работающих в области электронной торговли;
- развитие венчурного финансирования высокотехнологичных инновационных проектов в сфере информационных и телекоммуникационных технологий;
- стимулирование создания новых компаний, занятых производством высокотехнологичного оборудования и продукции в сфере информационных и телекоммуникационных технологий;
- увеличение объемов экспорта продукции и услуг в сфере информационных и телекоммуникационных технологий;
- повышение экономической эффективности использования российскими правообладателями объектов интеллектуальной собственности;
- развитие системы региональной информатизации.

5. В области повышения эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и бизнеса с органами государственной власти, качества и оперативности предоставления государственных услуг:

- обеспечение эффективного межведомственного и межрегионального информационного обмена;
- интеграция государственных информационных систем и ресурсов;
- увеличение объемов и качества государственных услуг, предоставляемых организациям и гражданам в электронном виде;

- совершенствование нормативно-правового обеспечения стандартизации и администрирования государственных услуг;
- совершенствование системы предоставления государственных и муниципальных услуг гражданам и организациям.

6. В области развития науки, технологий, техники и подготовки квалифицированных кадров в сфере информационных и телекоммуникационных технологий:

- развитие приоритетных направлений науки, технологий и техники на основе формируемых долгосрочных прогнозов технологического развития (форсайт);
- создание условий для коммерциализации и внедрения результатов научных исследований и экспериментальных разработок, а также расширение обмена научной информацией;
- создание правовых, организационных и иных условий для укрепления научно-исследовательского сектора высшей школы, государственных академий и отраслевой науки, оснащения вузов, научных организаций и исследовательских центров современным научно-исследовательским, технологическим и учебным оборудованием;
- повышение качества подготовки специалистов и создание системы непрерывного обучения государственных служащих в области информационных и телекоммуникационных технологий.

7. В области сохранения культуры многонационального народа Российской Федерации, укрепления нравственных и патриотических принципов в общественном сознании, развития системы культурного и гуманитарного просвещения:

- развитие системы библиотечных фондов на основе применения информационных и телекоммуникационных технологий;
- поддержка реализации социально значимых проектов в средствах массовой информации;
- формирование государственного заказа на создание и распространение кинематографической и печатной продукции, телерадиопрограмм и интернет-ресурсов в области культуры;
- поддержка деятельности государственных и негосударственных организаций по сохранению культурных и нравственных ценностей, традиций патриотизма и гуманизма в обществе;
- пропаганда культурных и нравственных ценностей российского народа;
- сохранение культурного наследия России, обеспечение его доступности для граждан.

8. В области противодействия использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам России:

- обеспечение безопасности функционирования информационно-телекоммуникационной инфраструктуры;

- обеспечение безопасности функционирования информационных и телекоммуникационных систем ключевых объектов инфраструктуры Российской Федерации, в том числе критических объектов и объектов повышенной опасности;
- повышение уровня защищенности корпоративных и индивидуальных информационных систем;
- создание единой системы информационно-телекоммуникационного обеспечения нужд государственного управления, обороны страны, национальной безопасности и правопорядка;
- совершенствование правоприменительной практики в области противодействия угрозам использования информационных и телекоммуникационных технологий во враждебных целях;
- обеспечение неприкосновенности частной жизни, личной и семейной тайны, соблюдение требований по обеспечению безопасности информации ограниченного доступа;
- противодействие распространению идеологии терроризма и экстремизма, пропаганде насилия.

Особенностью данного документа являются Контрольные значения показателей развития информационного общества в Российской Федерации на период до 2015 года. Так, например, в результате реализации основных направлений и мероприятий Стратегии развития информационного общества в Российской Федерации (далее – Стратегия) к 2015 году должны быть достигнуты следующие контрольные значения показателей:

- место Российской Федерации в международных рейтингах в области развития информационного общества – в числе двадцати ведущих стран мира;
- место Российской Федерации в международных рейтингах по уровню доступности национальной информационной и телекоммуникационной инфраструктуры для субъектов информационной сферы – не ниже десятого;
- доля государственных услуг, которые население может получить с использованием информационных и телекоммуникационных технологий, в общем объеме государственных услуг в Российской Федерации – 100 %;
- доля электронного документооборота между органами государственной власти в общем объеме документооборота – 70 %;
- доля библиотечных фондов, переведенных в электронную форму, в общем объеме фондов общедоступных библиотек – не менее 50 %, в том числе библиотечных каталогов – 100 % и т. п.

Рекомендуемые источники и литература

1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 09 сентября 2000 г. – М., 2000.

2. Стратегия развития информационного общества в России до 2015 года» (2008) // http://www.scrf.gov.ru

3. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 24-ФЗ // Рос. газ. – 2006. – 29 июля.

4. О техническом регулировании: Федер. закон Рос. Федерации от 27 дек. 2002 г. № 184-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 15 дек. 2002 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 18 дек. 2002 г. // Рос. газ. – 2002. – 31 дек.

5. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: Конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.

Тема 4. Организационная основа системы обеспечения информационной безопасности

4.1. Основные функции системы обеспечения информационной безопасности Российской Федерации.

4.2. Организация системы обеспечения информационной безопасности Российской Федерации.

4.3. Силы обеспечения информационной безопасности Российской Федерации.

4.1. Основные функции системы обеспечения информационной безопасности Российской Федерации

Основные функции системы обеспечения информационной безопасности Российской Федерации:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;

- оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;
- координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;
- контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;
- предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
- организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;
- проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;
- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;
- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
- совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;
- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

4.2. Организация системы обеспечения информационной безопасности Российской Федерации

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются:

1) Президент Российской Федерации;

2) Совет Федерации Федерального Собрания Российской Федерации;

3) Государственная Дума Федерального Собрания Российской Федерации;

4) Правительство Российской Федерации;

5) Совет Безопасности Российской Федерации;

6) федеральные органы исполнительной власти;

7) межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации;

8) органы исполнительной власти субъектов Российской Федерации;

9) органы местного самоуправления;

10) органы судебной власти;

11) общественные объединения;

12) граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации.

Президент Российской Федерации:

- руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации;
- санкционирует действия по обеспечению информационной безопасности Российской Федерации;
- в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности Российской Федерации;
- определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации настоящей Доктрины.

Палаты Федерального Собрания Российской Федерации на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формируют законодательную базу в области обеспечения информационной безопасности Российской Федерации.

Правительство Российской Федерации в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Россий-

ской Федерации Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности Российской Федерации:

- проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации;
- оперативно подготавливает проекты решений Президента Российской Федерации по предотвращению таких угроз;
- разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации, а также предложения по уточнению отдельных положений настоящей Доктрины;
- координирует деятельность органов и сил по обеспечению информационной безопасности Российской Федерации;
- контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента Российской Федерации в этой области.

Федеральные органы исполнительной власти:

- обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации;
- в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации.

Главными федеральными органами исполнительной власти в области защиты информации являются Федеральная служба безопасности (ФСБ) и Федеральная служба по техническому и экспортному контролю (ФСТЭК).

Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации.

Органы исполнительной власти субъектов Российской Федерации:

- взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации, а также по вопросам реализации федеральных программ в этой области;

- совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации;
- вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Органы местного самоуправления обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности Российской Федерации.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности Российской Федерации.

4.3. Силы обеспечения информационной безопасности Российской Федерации

Основу сил обеспечения информационной безопасности РФ составляют органы исполнительной власти, в задачи которых, в соответствии с законодательством, входит деятельность по обеспечению информационной безопасности. Для этого эти органы имеют соответствующие части, подразделения и службы. К ним относятся:

- Федеральная служба безопасности Российской Федерации (ФСБ);
- Служба внешней разведки Российской Федерации (СВР);
- Федеральная служба по техническому и экспортному контролю (ФСТЭК – бывшая Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России);
- Министерство внутренних дел Российской Федерации (МВД);
- Органы судебной власти Российской Федерации;
- Федеральная таможенная служба Российской Федерации;
- Федеральная служба по техническому регулированию и метрологии Российской Федерации.

Функции ФСБ по защите информации:

– участвует в разработке и реализации мер по обеспечению информационной безопасности страны, по защите сведений, составляющих государственную тайну, в лицензировании деятельности предприятий, учреждений и организаций, связанной с использованием сведений, составляющих государственную тайну, оказанием услуг по защите государственной тайны; определяет основные направления деятельности органов федеральной службы безопасности в этих областях;

– осуществляет контроль за обеспечением защиты сведений, составляющих государственную тайну, в государственных органах, воинских формированиях, на предприятиях, в учреждениях и организациях; в установленном порядке осуществляет мероприятия, связанные с допуском граждан к сведениям, составляющим государственную тайну, а также с приемом на военную службу (работу) в органы ФСБ;

– организует и осуществляет шифровальные работы в ФСБ, а также контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов, воинских формирований, предприятий, учреждений и организаций (за исключением учреждений РФ, находящихся за ее пределами)и другие функции определённые в Положении о Федеральной службе безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 6 июля 1998 г. N 806).

ФСБ выполняет также функции, выполняемые ранее федеральными органами правительственной связи и информации (ФАПСИ).

– организация и обеспечение эксплуатации, безопасности, развития и совершенствования правительственной связи, иных видов специальной связи и систем специальной информации для государственных органов;

– обеспечение в пределах своей компетенции сохранности государственных секретов; организация и обеспечение криптографической и инженерно-технической безопасности шифрованной связи в Российской Федерации и ее учреждениях за рубежом;

– лицензирование деятельности в области криптографической защиты информации и сертификация криптографических средств защиты.

СВР Российской Федерации выполняет те же функции в этой области за рубежом.

Федеральная Служба по техническому и экспортному контролю Российской Федерации (ФСТЭК РФ) является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению технической защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную или служебную тайну а также единую государственную научно-техническую политику в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

ФСТЭК организует деятельность государственной системы защиты информации в РФ от технических разведок и от ее утечки по техническим каналам. ФСТЭК и региональные центры входят в состав государственных органов обеспечения безопасности Российской Федерации.

В соответствии со своими функциями она осуществляет:

– координацию деятельности органов и организаций в области защиты информации, обрабатываемой техническими средствами;

– организационно-методическое руководство деятельностью по защите информации в КС;

– разработку и финансирование научно-технических программ по защите информации;

– утверждение нормативно-технической документации;

– функции государственного органа по сертификации продукции по требованиям безопасности информации;

– лицензирование деятельности предприятий по оказанию услуг в области защиты информации.

Федеральная Служба по техническому регулированию и метрологии разрабатывает стандарты в области защиты информации.

Органы МВД ведут борьбу с правонарушителями в информационной сфере и компьютерными преступлениями. Для этого в структуре МВД создано специальное управление «К» для предотвращения и раскрытия компьютерных преступлений, преступлений связанных с нарушением авторских прав в сфере высоких технологий.

Федеральная таможенная служба обязана предупреждать незаконный ввоз и вывоз из России «пиратской» продукции, обеспечивая тем самым защиту авторских и патентных прав.

Рекомендуемые источники и литература

1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 09 сентября 2000 г. – М., 2000.

2. Положения об органах – составляющих СОИБ Российской Федерации.

3. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.

4. Шиверский, А.А. Защита информации: проблемы теории и практики / А.А. Шиверский. – М.: Юристъ, 1996. – 112 с.

5. Управление безопасностью: учеб. пособие / Л.П. Гончаренко, Е.С. Куценко; Рос. экон. акад. им. Г.В. Плеханова. – М.: КноРус, 2010. – 272 с.

6. Информационная безопасность и защита информации: учеб. пособие / В.П. Мельников и др.; под ред. С.А. Клейменова. – М.: Академия, 2009. – 330 с.

7. Организационно-правовое обеспечение информационной безопасности: учебное пособие / А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др.; под ред. А.А. Стрельцова. – М.: Издат. центр «Академия», 2008. – 256 с.

8. Организационное обеспечение информационной безопасности: учебник / О.А. Романов, С.А. Бабин, С.Г. Жданов. – М.: Издательский центр «Академия», 2008. – 240 с.

9. Гришина, Н.В. Организация комплексной системы защиты информации / Н.В. Гришина. – М.: Гелиос АРВ, 2007. – 256 с.

10. Тихонов, В.А. Информационная безопасность: организационные, правовые и технические аспекты / В.А. Тихонов, В.В. Райх. – М.: Гелиос АРВ, 2006. – 516 с.

Тема 5. Понятие защиты информации

5.1. Понятие защиты информации и ее целей в российском законодательстве.

5.2. Понятие защиты информации в зависимости от видов ее уязвимостей.

5.1. Понятие защиты информации в российском законодательстве

Ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации» (2006) гласит:

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

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

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации».

Названные три вектора защиты информации – это три цели, три аспекта защиты информации. Целостность, конфиденциальность и доступность информации – цели защиты информации и ее результаты.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Целостность информации – свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению.

Доступ к информации – возможность получения информации и ее использования. Доступность информации – это состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно.

5.2. Понятие защиты информации в зависимости от видов ее уязвимости

Самым опасным для собственника информации является нарушение установленного статуса информации, поэтому содержательной частью защиты должно быть предотвращение такого нарушения.

Нарушение статуса информации обусловлено ее уязвимостью, которая означает неспособность информации самостоятельно противостоять дестабилизирующим воздействиям, сохранять при таких воздействиях свой статус.

Формы уязвимости

К формам проявления уязвимости информации, выражающим результаты дестабилизирующего воздействия на информацию, должны быть отнесены:

1. Хищение носителя информации или отображенной в нем информации (кража). Хищение информации часто ставится в один ряд с ее несанкционированным копированием, размножением, съемом, перехватом. Однако последние являются не формами проявления уязвимости информации, а способами хищения.
2. Потеря носителя информации (утеря).
3. Несанкционированное уничтожение носителя информации или отображенной в нем информации (разрушение).
4. Искажение информации (несанкционированное изменение, несанкционированная модификация, подделка, фальсификация). Термины модификация, подделка, фальсификация не совсем адекватны термину искажение, они имеют нюансы, но суть их одна и та же – несанкционированное частичное или полное изменение первоначальной информации.
5. Блокирование информации.
6. Разглашение информации (несанкционированное распространение, раскрытие).

Та или другая форма уязвимости информации может реализоваться при преднамеренном или случайном, непосредственном или опосредованном дестабилизирующем воздействии различны-ми способами на носитель информации или саму информацию со стороны определенных источников воздействия.

Виды уязвимости – утрата и утечка.

Результатами проявления форм уязвимости информации могут быть либо утрата, либо утечка информации, либо одновременно то и другое.

К утрате как конфиденциальной, так и защищаемой части открытой информации приводят хищение и потеря носителей информации, несанкционированное уничтожение носителей информации или только отображенной в них информации, искажение и блокирование информации. Утрата может быть полной или частичной, безвозвратной или временной (при

блокировании информации), но в любом случае она наносит ущерб собственнику информации.

Термин утечка информации, вероятно, не самый благозвучный, однако он более емко, чем другие термины, отражает суть явления, к тому же он давно уже закрепился в научной литературе и нормативных документах. Правда, единого подхода к определению этого термина нет.

Утечка информации – неправомерный выход конфиденциальной информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, результатом которого является получение информации лицами, не имеющими к ней санкционированного доступа.

Каково соотношение понятий утечка, разглашение, распространение, передача информации?

Термин «утечка информации» нередко, в том числе и в нормативных документах, заменяется или отождествляется с терминами разглашение информации, распространение информации и даже передача информации. Такой подход представляется неправомерным.

Термин разглашение информации означает несанкционированное доведение конфиденциальной информации до потребителей, не имеющих права доступа к ней, таким образом, он предполагает, что разглашение исходит от кого-то, осуществляется кем-то. Результатом разглашения является утечка информации, но утечка не сводится только к разглашению. Утечка – результат разглашения.

Согласно ФЗ «Об информации, информационных технологиях и о защите информации», «распространение информации – это действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц». Поэтому термин распространение применительно к конфиденциальной информации без слов несанкционированное или необоснованное ничего не выражает, поскольку распространение информации может быть и обоснованным, к тому же он опять-таки предполагает, что информация исходит от кого-то.

Помимо разглашения, утечка может произойти и в результате потери и хищения носителя конфиденциальной информации, а также хищения отображенной в носителе информации при сохранности носителя у собственника (владельца). Может произойти – не означает, что произойдет. Выше уже отмечалось, что потеря носителя не всегда приводит к утечке информации. Хищение конфиденциальной информации также не всегда связано с получением ее лицами, не имеющими к ней доступа. Имелось немало случаев, когда хищение носителей конфиденциальной информации осуществлялось у коллег по работе допущенными к этой информации лицами с целью подсидки, причинения вреда коллеге. Такие носители, как правило, уничтожались лицами, похитившими их. Но в любом случае потеря и хищение если и не приводят к утечке информации, то создают угрозу утечки.

Поэтому можно сказать, что к утечке конфиденциальной информации приводит ее разглашение и могут привести хищение и потеря. Сложность состоит в том, что зачастую невозможно определить:

- во-первых, сам факт разглашения или хищения информации при сохранности носителя информации у собственника (владельца);
- во-вторых, попала ли информация вследствие ее хищения или потери посторонним лицам.

При этом не следует отождествлять хищение с разглашением, как это иногда делается. Хищение может привести и часто приводит к разглашению и в последнем случае выступает в роли опосредованного способа разглашения, но, во-первых, результатом хищения не всегда бывает разглашение, во-вторых, разглашение конфиденциальной информации осуществляется не только посредством ее хищения.

Защита информации – деятельность по предотвращению утраты и утечки конфиденциальной информации и утраты защищаемой открытой информации.

Учитывая, что определение должно быть лаконичным, а термин утрата и утечка защищаемой информации поглощает все формы проявления уязвимости конфиденциальной и защищаемой части открытой информации, А.И. Алексенцев определил защиту информации как деятельность по предотвращению утраты и утечки защищаемой информации.

Другие подходы к понятию защиты информации скорее вносят путаницу в трактовку его сущности. Так, определение этого понятия, содержащееся в ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» сформулировано так: Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищае мую информацию.

Рекомендуемые источники и литература

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2006.

2. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 24-ФЗ // Рос. газ. – 2006. – 29 июля.

3. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: Конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.

4. Алексенцев, А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» / А.И. Алексенцев // Безопасность информационных технологий. – 1999. – № 1.

Тема 6. Понятия теории и методологии защиты информации

6.1. Понятие теории защиты информации.
6.2. Методологические принципы защиты информации.
6.3. Методология защиты информации в организации.

6.1. Понятие теории защиты информации

Определение теории защиты информации дают В.А. Герасименко и А.А. Малюк: теория защиты информации – это система основных идей, относящихся к защите информации в современных системах ее обработки, дающая целостное представление о сущности проблемы защиты, закономерностях развития и существенных связях с другими отраслями знания, формирующаяся и развивающаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

Целевое назначение теории защиты информации:

1) предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты;

2) полно и адекватно отображать структуру и содержание взаимосвязей с родственными и смежными областями знаний;

3) аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации;

4) ориентировать в направлении наиболее эффективного решения основных задач защиты и предоставлять для этого научно-методологические и инструментальные средства;

5) формировать научно обоснованные перспективные направления развития теории и практики защиты информации.

Иными словами, цель теории защиты информации – определять и объяснять сущность, цели, задачи, принципы, закономерности, тенденции, методы, средства защиты информации и связи между ними.

А.И. Алексенцев называет следующие основные положения теории защиты информации:

1. Общетеоретические положения:

- объективная необходимость и общественная потребность в защите информации;
- зависимость системы и состояния защиты информации от политико-правовых и социально-экономических реальностей;
- тесная взаимосвязь защиты информации с информатизацией общества;
- баланс между потребностью в свободном обмене информацией и ограничениями на ее распространение;
- соблюдение баланса интересов государства, общества и личности (теория интересов);

- влияние защиты информации на права, свободы и безопасность граждан;
- сходство и различия в межгосударственных, государственных и ведомственном подходах к защите информации и информационной безопасности;
- социальные последствия защиты информации.

2. Методологические принципы защиты информации:

- обеспечение единства, взаимосвязи и сбалансированности в решении задач производственной деятельности и защиты информации;
- сочетание общих норм защиты с нормами, обусловленными спецификой деятельности предприятий различного профиля;
- обеспечение сбалансированного соотношения объективной необходимости с экономической целесообразностью защиты информации;
- сочетание максимального ограничения доступа к защищаемой информации с качественным выполнением служебных обязанностей;
- обеспечение персональной ответственности за защиту информации и др.

Названные общетеоретические и методологические положения являются основами государственной политики в области информационной безопасности и защиты информации.

6.2. Методологические принципы защиты информации

Принципы защиты информации – это основополагающие идеи, важнейшие рекомендации по организации и осуществлению этой деятельности на различных этапах решения задач.

Принципы защиты информации можно разделить на три группы: правовые, организационные и используемые при защите информации от ТСР и в средствах вычислительной техники (СВТ).

Правовые принципы защиты информации

Основными правовыми принципами защиты информации, по мнению А.А. Шиверского, являются следующие:

1. Принцип законности. В рамках долженствующего существования правового государства деятельность предприятий и организаций всех форм собственности, всех должностных лиц и граждан должна осуществляться в рамках действующих законов.

2. Принцип приоритета международного права над внутригосударственным. Россия как преемница взятых бывшим Советским Союзом на себя обязательств признает также принцип приоритета международного права над внутренним. В частности, наша страна взяла на Венской встрече обязательство привести свое внутреннее законодательство в соответствие с положениями международных конвенций и соглашений, участником которых она является.

3. Принцип одинаковой секретности будет способствовать укреплению мер доверия в международных отношениях, помогать устранению асимметрии режимных ограничений, сложившихся в различных странах. Излишнее стремление по сокрытию информации от другой стороны всегда вызывает подозрение, так как такие действия обычно связывают с недобрыми намерениями одной стороны по отношению к другой.

4. Принцип собственности и экономической целесообразности. Радикальные перемены, происходящие в российском обществе, не могли не затронуть лежащие в основе экономической реформы отношений по поводу собственности. Был принят ряд законов, регламентирующих сферу имущественных отношений, отношений собственности, в том числе относящихся к регулированию прав на интеллектуальную собственность, на владение и распоряжение информацией, на защиту информации.

Это дало собственникам информации, объектов интеллектуальной собственности право принимать меры к их защите с помощью различных правовых механизмов, в том числе с помощью патентов, норм авторского права, коммерческой тайны. Лишь собственник (владелец) информации имеет право определять, какую информацию следует засекретить (и до какой степени) и защищать как государственную или коммерческую тайну, или же запатентовать и защищать с помощью патента и оплачивать деятельность по защите любой охраняемой информации.

Организационные принципы защиты информации

1. Научный подход к организации защиты информации.

Функционирующая в нашей стране общегосударственная система защиты информации создана с учетом имеющихся объемов защищаемой информации и используемых для ее обработки средств, традиций и опыта в области защиты государственных секретов, накопленных в предыдущие десятилетия. Создание такой системы потребовало научного осмысления таких проблем, как:

- разграничение компетенции в области защиты государственной тайны по всей иерархической лестнице многочисленных органов и организаций и защиты коммерческой тайны;
- научное и законодательное определение понятий «государственная» и «коммерческая тайна», «служебная тайна», «персональные данные» и т. д.;
- разработка научных критериев определения степени секретности информации и т. д.

В научных исследованиях проблем защиты информации используются научные методы: комплексный и системный подходы к организации защиты информации на предприятии и др.

2. Максимальное ограничение числа лиц, допускаемых к защищаемой информации.

Основной смысл этого принципа сводится к тому, что сохранность засекреченной информации находится в зависимости от количества лиц,

допущенных к обращению с нею. Чем уже этот круг, тем выше вероятность сохранения в тайне данной информации.

3. Персональная ответственность за сохранность доверенных секретов. Этот принцип хорошо «работает», если каждый сотрудник, допущенный к защищаемой информации, понимает и осознает, что сохранение в тайне этой информации и в его собственных интересах.

4. Единство в решении производственных, коммерческих, финансовых и режимных вопросов. В этом принципе заложено одно из проявлений комплексного подхода к организации защиты информации, имеющего, однако, относительно самостоятельное значение. Знание и учет этого принципа заключается в том, что лица, принимающие решения о засекречивании информации, болеющие больше, конечно, за решение производственных, финансовых, маркетинговых и иных подобных задач, не должны забывать и упускать из вида необходимость одновременного решения и режимных вопросов, там, где это необходимо.

5. Непрерывность защиты информации. Данный принцип заключается в том, что защита секретной или конфиденциальной информации должна начинаться с момента ее появления (получения, создания, генерирования) на всех этапах ее обработки, передачи, использования и хранения, вплоть до этапа ее уничтожения или рассекречивания.

Принципы, используемые при защите информации от технических средств разведки

В организации деятельности по защите информации от технических средств разведки (ТСР) и в средствах вычислительной техники (СВТ) руководствуются, прежде всего, теми же организационными и правовыми принципами, о которых говорилось выше. Это объясняется тем, что эти принципы имеют достаточно общий и универсальный характер. Эти принципы «работают» независимо от того, где, когда и кем осуществляется защита информации.

Однако имеются и специфические принципы, обусловленные особенностями предмета защиты, то есть носителей, на которых отображена защищаемая информация, используемых при этом силах, средствах и методах, а также учитываются средства и методы добывания защищаемой информации соперником с помощью ТСР.

1. Принципы защиты информации, используемые при организации противодействия ТСР:

- активность защиты информации – выражается в целенаправленном навязывании технической разведке ложного представления об объекте его разведывательных устремлений, в соответствии с замыслом защиты;
- убедительность защиты информации – состоит в оправданности замысла защиты условиям обстановки в соответствии с характером защищаемого объекта или свойствам окружающей среды, в применении тех-

нических решений защиты, соответствующих климатическим, сезонным и другим условиям;

- непрерывность защиты информации предполагает организацию защиты объекта на всех стадиях его жизненного цикла: предпроектном, проектном, в период разработки, изготовления (строительства), испытания, эксплуатации и утилизации;
- разнообразие защиты информации – предусматривает исключение шаблона, повторяемости в выборе объекта прикрытия и путей реализации смысла защиты, в том числе с применением типовых решений.

2. Принципы защиты информации, используемые в СВТ. Основными принципами защиты информации, имеющими специфический характер и используемыми в организации защиты информации в СВТ, являются, по мнению А.А. Шиверского, следующие:

- введение избыточности элементов системы;
- резервирование элементов системы;
- защитные преобразования данных;
- контроль состояния элементов системы, их работоспособности и правильности функционирования.

6.3. Методология защиты информации в организации

Методологию защиты информации конкретной организации отражает Концепция защиты информации – это система взглядов на сущность, цели, принципы и организацию защиты информации в этой организации.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения информационной безопасности;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
- координации деятельности структурных подразделений при проведении работ по созданию, развитию и эксплуатации информационных систем с соблюдением требований обеспечения безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности защищаемой информации.

Правовой основой Концепции должны являться Конституция Российской Федерации. Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы действующего законода-

тельства Российской Федерации, документы Федеральной службы по техническому и экспортному контролю (ФСТЭК) и других нормативных документов, регламентирующих вопросы защиты информации.

При разработке Концепции должны учитываться основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации, а также текущее состояние и перспективы развития информационных технологий.

Основные положения Концепция должны базироваться на качественном осмыслении вопросов безопасности информации и не концентрировать внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

Концепция защиты информации предполагает:

1) определение понятия, сущности и целей защиты информации субъекта;

2) какую информацию необходимо защищать, каковы критерии отнесения ее к защищаемой;

3) дифференциация защищаемой информации: а) по степеням конфиденциальности, б) по собственникам и владельцам;

4) определение состава и классификация носителей защищаемой информации;

5) определение состава угроз безопасности информации;

6) определение источников, видов и способов дестабилизирующего воздействия на информацию, причин, обстоятельств и условий воздействий, каналов, методов и средств несанкционированного доступа к информации;

7) определение методов и средств защиты информации;

8) кадровое и ресурсное обеспечение защиты информации.

Рекомендуемые источники и литература

1. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.

2. Малюк, А.А. Введение в защиту информации в автоматизированных системах: учебное пособие / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – М.: Горяч.Линия-Телеком, 2005. – 147 с.

3. Алексенцев, А.И. О концепции защиты информации / А.И. Алексенцев // Безопасность информационных технологий. – 1998. – № 4.

4. Герасименко, В.А. Основы защиты информации: учебник / В.А. Герасименко, А.А. Малюк. – М., 1997. – 538 с.

5. Шиверский, А.А. Защита информации: проблемы теории и практики / А.А. Шиверский. – М.: Юристъ, 1996. – 112 с.

6. Шумский, А.А. Системный анализ в защите информации: учеб. пособие для студ. вузов, обучающихся по спец. в обл. информ. безопасности / А.А. Шумский, А.А. Шелупанов. – М.: Гелиос АРВ, 2005. – 224 с.

7. Информационная безопасность и защита информации: учеб. пособие / В.П. Мельников и др.; под ред. С. А. Клейменова. – М.: Академия, 2009. – 330 с.

8. Организационно-правовое обеспечение информационной безопасности: учебное пособие / А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова, и др.; под ред. А.А. Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.

9. Романов, О.А. Организационное обеспечение информационной безопасности: учебник / О.А. Романов, С.А. Бабин, С.Г. Жданов. – М.: Издательский центр «Академия», 2008. – 240 с.

10. Гришина, Н.В. Организация комплексной системы защиты информации / Н.В. Гришина. – М.: Гелиос АРВ, 2007. –256 с.

11. Тихонов, В.А. Информационная безопасность: организационные, правовые и технические аспекты / В.А. Тихонов, В.В. Райх. – М.: Гелиос АРВ, 2006. – 516 с.

Раздел II
ИНФОРМАЦИЯ КАК ПРЕДМЕТ И ОБЪЕКТ ЗАЩИТЫ

Тема 7. Защищаемая информация

7.1. Понятие защищаемой информации.
7.2. Критерии отнесения общедоступной информации к защищаемой.
7.3. Критерии и условия отнесения информации ограниченного доступа к защищаемой.
7.4. Понятие объекта защиты.

7.1. Понятие защищаемой информации

Федеральный закон «Об информации, информационных технологиях и защите информации» вводит новые правила, устанавливающие правовой режим информации и новое правомочие на информацию – право на обладание информацией.

Информация определяется как сведения (сообщения, данные) независимо от формы их представления. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Понятие защищаемой информации неоднозначно. Существует два подхода к понятию «защищаемая информация»:

Первый подход (А.А. Шиверский и др.). Защищаемая информация – сведения, на использование и распространение которых введены ограничения их собственником. Иными словами, это информация ограниченного доступа.

Второй подход (А.И. Алексенцев и др.) – более широкий. Достоинство его в том, что он отражает реалии современной практики. В состав защищаемой информации включается не только информация ограниченного доступа, те или иные виды тайны, но и общедоступная информация. К защищаемой информации относится:

1. Часть открытой (общедоступной) информации, определяемая ее обладателем. Защита открытой информации направлена не на ограничение доступа к информации, а на сохранность информации в рамках установленных правил ее обработки и использования. Она защищается от утраты. Главные цели ее защиты – целостность и доступность.

Защита общедоступной информации существовала всегда и производилась путем: регистрации ее носителей; учета их движения и местонахождения; создания безопасных условий хранения.

2. Информация ограниченного доступа – конфиденциальная информация, в том числе составляющая государственную тайну (защищается от утечки и утраты).

Именно этот подход закреплен в Федеральном законе «Об информации, информационных технологиях и о защите информации». Согласно п. 2 ст. 5закона, «информация в зависимости от категории доступа к ней подразделяется на общедоступную, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)».

Ограничение доступа к информации регулируется ст. 9 закона. Она гласит, что соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами, является обязательным. Далее речь идет о регулировании отношений, связанных с защитой информации, составляющей государственную тайну (ч. 3), «коммерческую, служебную и иную тайну» (ч. 4), профессиональную тайну (ч. 5, 6, 7), личную и семейную тайну (ч. 8), персональные данные (ч. 9).

В п. 1 ст.16 закона указывается, что защита информации направлена на «соблюдение конфиденциальности информации ограниченного доступа». П.3 ст.16 гласит о том, что могут устанавливаться и «требования о защите общедоступной информации».

7.2. Критерии отнесения общедоступной информации к защищаемой

При решении вопроса об отнесении конкретной информации к защищаемой нужно руководствоваться определенными критериями, т.е. признаками, при наличии которых информация может быть отнесена к защищаемой.

Общей основой для отнесения информации к защищаемой является ценность информации, поскольку именно ценность информации диктует необходимость ее защиты. Поэтому критерии отнесения информации к защищаемой являются по существу критериями определения ее ценности.

Критерии отнесения общедоступной информации к защищаемой:

- необходимость информации для правового обеспечения деятельности предприятия (документированная информация, регламентирующая статус предприятия, права, обязанности и ответственность его работников);
- необходимость информации для производственной деятельности (информация, относящаяся к научно-исследовательской, проектной, конструкторской, технологической, торговой и другим сферам производственной деятельности);

- необходимость информации для управленческой деятельности (информация, требующаяся для принятия управленческих решений, для организации производственной деятельности и обеспечения ее функционирования);
- необходимость информации для финансовой деятельности;
- необходимость информации для обеспечения функционирования социальной сферы;
- необходимость информации как доказательного источника на случаи возникновения конфликтных ситуаций;
- важность информации как исторического источника, раскрывающего направления и особенности деятельности предприятия.

Эти критерии обусловливают необходимость защиты открытой информации от утраты.

7.3. Критерии и условия отнесения информации ограниченного доступа к защищаемой

Названные выше критерии отнесения общедоступной информации к защищаемой вызывают потребность в защите от утраты и конфиденциальной информации.

Однако основной, определяющий критерий отнесения информации к конфиденциальной и защиты ее от утечки – возможность получения преимуществ от использования информации за счет неизвестности ее третьим лицам.

Этот критерий имеет две составляющие:

1. Неизвестность информации третьим лицам.

2. Получение преимуществ от использования информации (получение выгоды, предотвращение политического, экономического или морального ущерба).

Эти две составляющие взаимосвязаны и взаимообусловлены с одной стороны, неизвестность информации третьим лицам сама по себе ничего не значит, если не обеспечивает преимуществ тому, кто ее защищает, с другой стороны, преимущества можно получить только за счет такой неизвестности.

При отсутствии названных выше критериев нет оснований для перевода информации в категорию защищаемой. Но наличие этих критериев не означает, что информация во всех случаях без исключения должна быть отнесена к защищаемой. Критерии – лишь объективные показатели возможности отнесения информации к защищаемой. Для реализации этой возможности в действительности необходимы следующие условия:

1. Если информация не является общедоступной на законном основании, т. е. не содержит сведений, которые запрещено относить к конфиден-

циальным. Перечни таких сведений содержатся в нескольких нормативных актах: законах «О государственной тайне», «О коммерческой тайне», «Об информации, информационных технологиях и о защите информации», «О благотворительной деятельности и благотворительных организациях», Постановлении Правительства от 5 декабря 1991 года №35 «О перечне сведений, которые не могут составлять коммерческую тайну», «Положении о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» (утверждено Постановлением Правительства РФ от 3.11.1994 № 1233).

2. Если имеются технические возможности для защиты носителей информации. Речь идет об объектах, которые практически невозможно скрыть от технических средств обнаружения и фиксации, особенно спутниковых.

3. Если затраты на защиту информации не превысят количественных и качественных показателей преимуществ, получаемых при ее защите.

Таким образом, правовой и методологической основой для разработки перечней защищаемой информации являются:

- критерии отнесения информации к защищаемой;
- условия отнесения информации к защищаемой;
- понятие соответствующего вида тайны (их характеристики и показатели);
- специфика предприятия (для коммерческой тайны): например, то, что для одних является коммерческой тайной, для других – рекламная информация.

7.4. Понятие объекта защиты

1. ГОСТ Р 50922-2006 «Защита информации: Основные термины и определения» дает следующее определение объекта защиты:

Объект защиты – это информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Согласно этому определению, к объектам защиты должны относиться:

1) лица, допущенные к работе с охраняемой законом информацией либо имеющие доступ в помещения, где эта информация обрабатывается;

2) объекты информатизации – средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний, заседаний и переговоров;

3) охраняемая законом информация – информация, доступ к которой ограничен в соответствии с законодательством России (конфиденциальная информация);

4) материальные носители охраняемой законом информации;

5) средства защиты информации;

6) технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации.

Согласно нормативно-методическим документам ФСТЭК, защите подлежит речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитооптической и иной основе. При этом объектами защиты являются:

- средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе – информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации;
- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);
- защищаемые помещения (ЗП) – помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т. п.).

Рекомендуемые источники и литература

1. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 24-ФЗ // Рос. газ. – 2006. – 29 июля.

2. Об утверждении перечня сведений конфиденциального характера: Указ Президента Рос. Федерации от 6 марта 1997 г. № 188 // Рос. газ. – 1997. – 14 марта.

3. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.

4. Алексенцев, А.И. О составе защищаемой информации / А.И. Алексенцев // Безопасность информационных технологий. – 1999. – № 2.

5. Шиверский, А.А. Защита информации: проблемы теории и практики / А.А. Шиверский. – М.: Юристъ, 1996. – 112 с.

Тема 8. Виды защищаемой информации ограниченного доступа

8.1. Государственная тайна.
8.2. Служебная тайна.
8.3. Коммерческая тайна.
8.4. Профессиональная тайна.
8.5. Персональные данные.
8.6. Объекты интеллектуальной собственности как составная часть защищаемой информации

8.1. Государственная тайна

Определение государственной тайны сформулировано в Федеральном законе «О государственной тайне»: «Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации».

В этом определении закреплены главные признаки государственной тайны:

- ее собственником является государство (содержится в названии тайны);
- области деятельности, в которых может быть информация, составляющая государственную тайну, – военная, внешнеполитическая, экономическая, разведывательная, контрразведывательная и оперативно-розыскная деятельность;
- охрана государственной тайны возложена на государство;
- критерий отнесения информации к гостайне – распространение этих сведений может нанести ущерб безопасности РФ.

«Концепция защиты государственной тайны в Российской Федерации» представляет собой систему взглядов на проблему защиты государственной тайны, определяет основную идею и пути ее решения в различных сферах деятельности государства.

При защите государственной тайны объектами защиты являются носители сведений, составляющих государственную тайну, независимо от физической природы носителя. Существуют три класса таких носителей:

1) носители, хранящие записи «готовой информации», то есть информации, непосредственно раскрывающей сведения, составляющие государственную тайну (бумажные носители, магнитные носители, оптические носители и т.д.);

2) носители «готовой информации» информации в процессе ее передачи (всевозможные системы связи);

3) носители признаков проявления сведений, составляющих госу-

дарственную тайну, или так называемых демаскирующих признаков объектов защиты. Демаскирующие признаки могут быть непосредственно присущи объекту или проявляться в виде следов деятельности объектов. Носителями демаскирующих признаков могут быть образцы вооружения, технологические процессы, защищаемые природные ресурсы и другие носители.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

8.2. Служебная тайна

В 1987 году термин «служебная и производственная тайна» был заменен термином «служебная тайна». Она по-прежнему объединяла сведения со степенью «секретно», но стала сферой государственных интересов, так как к этим сведениям были отнесены охраняемые государством сведения, разглашение которых могло нанести ущерб интересам государства.

Закон «О государственной тайне» 1992 г. включил в состав гостайны особой важности, совершенно секретные и секретные сведения, поэтому как бы автоматически упразднил служебную тайну. Однако термин «служебная тайна» продолжал употребляться, в том числе и в нормативных документах, и в него вкладывается различное значение:

- в Гражданском кодексе Российской Федерации, Уголовном кодексе Российской Федерации;
- в законах «Об основах государственной службы Российской Федерации», «О науке и государственной научно-технической политике»;
- в Федеральном законе «О федеральных органах налоговой полиции»;
- в Федеральном законе «О космической тайне»;
- в Федеральном законе «О коллективных договорах и соглашениях»;

- в Федеральном законе «О государственном регулировании в области генно-инженерной области»;
- в Положениях об архиве Президента Российской Федерации;
- в Положении о Государственной технической комиссии при Президенте Российской Федерации;
- в Перечне сведений конфиденциального характера.

В Гражданском кодексе изложены условия (основания) отнесения информации к служебной тайне: действительная или потенциальная коммерческая ценность информации в силу ее неизвестности третьим лицам; отсутствие к ней свободного доступа на законном основании; принятие мер к охране ее конфиденциальности. Те же критерии Гражданский кодекс определяет и для коммерческой тайны.

Закон «Об основах государственной службы Российской Федерации» определяет служебную тайну как поступающие в органы государственной налоговой службы сведения об имущественном положении служащих (ст. 12). Кроме того, по смыслу служебную тайну составляют (хотя и не названы служебной тайной) «сведения, затрагивающие частную жизнь, честь и достоинство граждан», которые госслужащие не должны разглашать» (Ст. 10).

В Перечне сведений конфиденциального характера, утвержденном Указом Президента Российской Федерации от 6.03.97 № 188 к служебной тайне отнесены «служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами».

Таким образом, по действующим в России нормативным документам служебная тайна – это информация: 1) составляющая коммерческую тайну; 2) относящаяся к частной жизни граждан, которая стала достоянием государственных и муниципальных органов власти в результате осуществления ими служебной деятельности.

Каково соотношение понятий «служебная тайна» и «служебная информация»? Многие считают, что служебную тайну составляют т.н. несекретные сведения ограниченного распространения с грифом «Для служебного пользования» (ДСП). Они возникли в 1926 году, когда появился термин «переписка, не подлежащая оглашению».

В 1994 году Постановлением Правительства Российской Федерации от 3 ноября 1994 года №1233 было утверждено «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти». Служебная информация ограниченного распространения, согласно Положению, – это несекретная информация, касающаяся деятельности федеральных органов исполнительной власти, а также подведомственных им предприятий, учреждений и организаций, ограничения на распространение которой диктуются служеб-

ной необходимостью. Гриф – «ДСП». Очевидно, что по всем признакам – это служебная тайна. Однако об отнесении этих сведений к служебной тайне в Положении не упоминается.

В Федеральном Законе «Об информации, информационных технологиях и о защите информации» (2006 г.) в п. 4. ст. 9 указывается, что условия отнесения информации к сведениям, составляющим служебную тайну (наряду с другими тайнами), устанавливаются федеральными законами.

8.3. Коммерческая тайна

Определение коммерческой тайны дано в Федеральном законе «О коммерческой тайне» от 29 июля 2004 года: «Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду».

В законе дается также определение информации, составляющей коммерческую тайну. Информация, составляющая коммерческую тайну, – «научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны».

В Федеральном законе «О коммерческой тайне» от 29 июля 2004 года в статье 5 перечислены сведения, которые не могут составлять коммерческую тайну. К ним относятся:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

В Федеральном законе «О коммерческой тайне» не названы сведения, которые могут составлять коммерческую тайну. Практика показала, что в Примерный перечень сведений, составляющих коммерческую тайну организации, входят сведения следующих категорий:

1. Производство: Сведения о структуре и масштабах производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов, комплектующих и готовой продукции.

2. Управление: Сведения о применяемых оригинальных методах управления организацией (фирмой). Сведения о подготовке. Принятии и исполнении отдельных решений руководства фирмы по коммерческим, организационным и др. вопросам.

3. Планы: Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях, сведения о планах инвестиций, закупок и продаж.

4. Совещания: Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления организации.

5. Финансы: Сведения о кругообороте средств организации, финансовых операциях, состоянии банковских счетов организации и проводимых операциях, об уровне доходов организации, о состоянии кредитов организации (пассивы и активы). Главная книга организации.

6. Рынок: Сведения о применяемых фирмой оригинальных методах изучения рынка (маркетинга). Сведения о результатах сегментации рынка, содержащие оценки состояния и перспектив развития рыночной конъюнктуры. Сведения о рыночной стратегии фирмы, о применяемых ею ориги-

нальных методах осуществления продаж, об эффективности служебной или коммерческой деятельности фирмы.

7. Партнеры: Обобщенные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах, состоящих в деловых отношениях с организацией.

8. Конкуренты: Обобщенные сведения о внутренних и зарубежных предприятиях как потенциальных конкурентах, оценка качества деловых отношений с конкурирующими предприятиями.

9. Переговоры: Сведения о подготовке, проведении и результатах переговоров с деловыми партнерами.

10. Контракты: Сведения об условиях конфиденциальности, из которых можно установить порядок соглашения и другие обязательства организации с партнерами, клиентами.

11. Цены: Сведения о методах расчета, структуре, уровне реальных цен на продукцию и размеры скидок.

12. Торги, аукционы: Сведения о подготовке к участию в торгах и аукционах, результатах приобретения или продажи на них товаров.

13. Наука и техника: Сведения о целях, задачах, программах перспективных научных исследований. Ключевые идеи научных разработок, параметры разрабатываемых технологических процессов (размеры, объемы, конфигурации и др.). Данные об условиях экспериментов и оборудовании, на котором они проводились. Сведения о материалах, из которых изготовлены отдельные детали, об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный эффект. Сведения о методах защиты от подделки товарных и фирменных знаков, о состоянии парка ПЭВМ и программного обеспечения.

14. Технология: Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения, об условиях их производства и транспортировке продукции.

15. Безопасность: Сведения о порядке и состоянии организации защиты служебной или коммерческой тайны, о порядке и состоянии организации охраны, системы сигнализации, пропускном режиме. Сведения, составляющие служебную или коммерческую тайну организаций, предприятий-партнеров и передаваемые ими в пользование на доверительной основе.

Степени конфиденциальности сведений, составляющих коммерческую тайну. Если в отношении государственной тайны законом «О государственной тайне» установлено три степени секретности (Особой важности, совершенно секретно и секретно), то закон «О коммерческой тайне» гласит, что на документах, предоставляемых органам государственной власти, иным государственным органам, органам местного самоуправления и со-

держащих информацию, составляющую коммерческую тайну, «должен быть нанесен гриф «Коммерческая тайна» с указанием ее обладателя (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

В процессе функционирования на предприятии коммерческая информация может быть ранжирована по степени ее важности для предприятия с тем, чтобы регулировать ее распространение среди работающих на предприятии, указывать пользователей этой информации, уровень ее защиты и т. д. Для обозначения степени важности коммерческой информации для предприятия предлагаются разные системы обозначения степени ее конфиденциальности (грифы конфиденциальности), например: коммерческая тайна – строго конфиденциально (КТ – СК); коммерческая тайна – конфиденциально (КТ – К); коммерческая тайна (КТ).

Режим коммерческой тайны – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности (ст. 3 ФЗ «О коммерческой тайне»).

Меры по охране конфиденциальности информации, принимаемые ее обладателем, в соответствии со ст. 10 закона должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Режим коммерческой тайны считается установленным только после принятия обладателем информации, составляющей коммерческую тайну, названных мер.

Права обладателя информации, составляющей коммерческую тайну, закреплены ст. 7 Федерального закона «О коммерческой тайне».

1. Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны;

2. Обладатель информации, составляющей коммерческую тайну, имеет право, кроме всего прочего:

- требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;
- требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;
- защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

8.4. Профессиональная тайна

В Российской империи профессиональная тайна трактовалась очень широко и включала тайну профессиональной деятельности предприятия любой организационно-правовой формы, тайну частной жизни клиентов и коммерческую тайну других предприятий, ставших известными в силу профессионального положения.

В советское время термин «профессиональная тайна» вышел из употребления. В постсоветский период отношение к нему почти не изменилось, хотя этот вид тайны предусмотрен Декларацией прав и свобод человека и гражданина. Лишь в Уголовном кодексе Российской Федерации содержится выражение «служебная и профессиональная тайна», однако термин не раскрывается, и состав информации, которая может быть отнесена к профессиональной тайне, не определен. Кроме того, в ст. 155 к профессиональной тайне отнесена тайна усыновления.

В Основах законодательства Российской Федерации о нотариате (ст. 5, 14, 16) упоминается профессиональная тайна нотариуса, в Постановлении Конституционного Суда Российской Федерации от 27.03.1996 № 8 – П – профессиональная тайна адвоката.

В Перечне сведений конфиденциального характера профессиональная тайна хотя и не названа, но, тем не менее, обозначена как «сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, те-

лефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и так далее)».

В ст. 11 Закона «О социальном обслуживании граждан пожилого возраста и инвалидов» сказано, что «сведения личного характера, ставшие известными работникам учреждения социального обслуживания при оказании социальных услуг, составляют профессиональную тайну».

Очевидно, что главный признак отбора информации для отнесения к профессиональной тайне – это профессия, в силу которой лицу доверяется или становится известной конфиденциальная информация.

Другой признак – конфиденциальная информация добровольно доверяется лицу, исполняющему профессиональные обязанности, по выбору владельца этой информации и, как правило, затрагивает частную жизнь последнего. Поэтому профессиональная тайна – это защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Таким образом, можно сделать вывод, что профессиональная тайна является тайной не определенной информации, отнесенной к этому виду тайны, а обобщенным понятием, включающим чужие тайны, если они становятся достоянием уполномоченных на то юридических и физических лиц, если они получены в результате осуществления профессиональной деятельности.

В состав профессиональной тайны входят:

1. Врачебная тайна – информация, содержащая:

- результаты обследования лица, вступившего в брак;
- сведения о факте обращения за медицинской помощью, о состоянии здоровья, диагнозе заболевания и иные сведения, полученные при обследовании и лечении гражданина;
- сведения о проведенных искусственном оплодотворении и имплантации эмбриона, а также о личности донора;
- сведения о доноре и реципиенте при трансплантации органов и (или) тканей человека;
- сведения о наличии психического расстройства, фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья гражданина;
- иные сведения в медицинских документах гражданина (Федеральный закон 21 ноября 2011 года N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»).

2. Тайна связи – тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (Законы «О связи» от 07.07.2003 N 126-ФЗ и «О почтовой связи» от 17.07.1999 N 176-ФЗ (ред. от 06.12.2011)).

3. Нотариальная тайна – сведения, доверенные нотариусу в связи с совершением нотариальных действий («Основы законодательства Российской Федерации о нотариате» от 11 февраля 1993 г. N 4462-I (в ред. 21 июля 2014 г.).

4. Адвокатская тайна – сведения, сообщенные адвокату гражданином в связи с оказанием ему юридической помощи (Федеральный закон от 31 мая 2002 г. N 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»).

5. Тайна усыновления – сведения об усыновлении ребенка, доверенные на законном основании иным лицам, кроме судей, вынесших решение об усыновлении, и должностных лиц, осуществляющих государственную регистрацию этого усыновления (ст. 139 Семейного кодекс РФ (СК РФ) от 29.12.1995 N 223-ФЗ).

6. Тайна страхования – сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц, полученные страховщиком в результате своей профессиональной деятельности (Закон РФ от 27 ноября 1992 г. N 4015-I «Об организации страхового дела в Российской Федерации» (в ред. от 04.11.2014 (с изм. и доп., вступ. в силу с 01.01.2015).

7. Тайна исповеди – сведения, доверенные священнослужителю гражданином на исповеди (Федеральный закон от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях»).

А.И. Алексенцев относит к профессиональной тайне также тайну следствия и судопроизводства, журналистскую и банковскую тайну, тайну голосования, персональные данные. По мнению ученого, разновидностью профессиональной тайны должна быть также определена служебная тайна, поскольку государственные структуры – это тоже профессиональная деятельность.

Согласно ст. 9 Федерального закона №149-ФЗ «Об информации, информационных технологиях и о защите информации» (2006 г.) «информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации». К таким законам относятся законы «О связи», «Основы законодательства РФ о нотариате», «О социальном обслуживании граждан пожилого возраста и инвалидов», «Основы законодательства об охране здоровья граждан», «Профессиональный кодекс нотариусов РФ» и др.

К основным субъектам профессиональной тайны относятся доверители (владельцы), держатели и пользователи профессиональной тайны.

Доверитель – физическое лицо (независимо от гражданства), доверившее сведения другому лицу, а также его правопреемники (в том числе наследники).

Держатель – физическое или юридическое лицо, которому исключительно в силу его профессиональной деятельности (профессиональных обязанностей) были доверены или стали известны сведения, составляющие профессиональную тайну.

Держателями профессиональной тайны в соответствии с действующим законодательством РФ являются:

- лица, участвующие в рассмотрении в суде дела об усыновлении;
- учреждения государственной и муниципальной системы здравоохранения, их должностные лица, врачи, медицинские и фармацевтические работники, в том числе частнопрактикующие;
- организации электрической и почтовой связи, их должностные и иные лица и работники;
- нотариальные палаты, нотариусы и иные лица, работающие в нотариальной конторе;
- коллегии адвокатов и адвокаты;
- страховщики;
- священнослужители;
- частные детективы.

Пользователь – лицо, которому сведения, составляющие профессиональную тайну, стали известны на законных основаниях в связи с выполнением им своих служебных обязанностей в случаях и порядке, установленных законом. К ним относятся:

В отношении врачебной тайны:

- Суд, судья – по делам, находящимся в производстве;
- Прокурор, органы дознания и следствия – в связи с проведением расследований по конкретным делам.

Особое место в системе видов защищаемой информации принадлежит банковской тайне. Сегодня среди юристов нет единства относительно ее понятия и содержания. Одни считают ее специфическим видом коммерческой тайны, другие – служебной тайны. Одни считают, что необходим специальный федеральный закон «О банковской тайне» (И.Л. Бачило), другие – что банковская тайна есть разновидность профессиональной тайны (А.И. Алексенцев). Отношения, связанные с банковской тайной, регулируются Федеральным законом «О банках и банковской деятельности от 02.12.1990 N 395-1 (в ред. от 01.12.2014).

Банковская тайна – это защищаемые банками и иными кредитными организациями сведения о вкладах и счетах своих клиентов, банковских опе-

рациях по счетам и сделкам в интересах клиентов, а также сведения о клиентах, разглашение которых может разрушить право последних на неприкосновенность частной жизни.

Владельцы банковской тайны – клиент или корреспондент (физическое или юридическое лицо), доверивший банку и иной кредитной организации сведения, которые могут составлять банковскую тайну.

Пользователи банковской тайны – лица, которым сведения, составляющие банковскую тайну, были доверены или стали известны в связи с выполнением ими служебных обязанностей. К ним относятся:

- банки и иные кредитные организации;
- Центральный банк РФ, получающий сведения, составляющие банковскую тайну, в ходе выполнения функций по регулированию, контролю и надзору за банковской деятельностью;
- Агентство по реструктуризации кредитных организаций;
- государственные органы, должностным лицам которых банковская тайна может быть предоставлена исключительно в случаях и в порядке, предусмотренных Федеральным законом «О банках и банковской деятельности» (суды, Счетная Палата РФ, органы государственной налоговой службы, таможенные органы, органы предварительного следствия, нотариальные конторы, иностранные консульские учреждения – в отношении счетов иностранных граждан, аудиторские организации).

8.5. Персональные данные

Персональные данные – это особый институт охраны права на неприкосновенность частной жизни. Право на неприкосновенность частной жизни является одним из конституционных прав человека. Конституционными гарантиями являются:

- Конституционный запрет осуществлять сбор, хранение, использование и распространение информации о частной жизни лица без его согласия (ст. 24);
- Конституционная обязанность органов государственной власти и органов местного самоуправления обеспечить каждому возможность ознакомления с документами и материалами, затрагивающими его права и свободы (ст. 24) и др.

Одним из принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации в ст. 5 закона «Об информации, информационных технологиях и о защите информации» (2006 г.) назван принцип неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия. Согласно п. 8. ст. 9 закона «О персональных данных» (2006 г.), запрещается требовать от гражданина

(физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Информация, затрагивающая неприкосновенность частной жизни, лица и ставшая известной на законных основаниях другим лицам, должна охраняться:

- в режиме профессиональной тайны – если она получена ими исключительно в силу исполнения своих профессиональных обязанностей, не связанных с государственной или муниципальной службой;
- в режиме служебной тайны – если она получена представителями государственных органов или органов местного самоуправления в силу исполнения своих служебных обязанностей.

Как следует из Доктрины информационной безопасности РФ, права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, закрепленные в Конституции РФ, практически не имеют достаточного правового, организационного и технического обеспечения. Это проявляется, в частности, в том, что неудовлетворительно организована защита данных о физических лицах (персональных данных), собираемых федеральными органами власти, органами власти субъектов федерации, органами местного самоуправления.

Проблема персональных данных стала особенно актуальной в связи с созданием и использованием баз данных о гражданах в компьютерных сетях государственных и негосударственных структур. Естественным образом встала задача обеспечения неприкосновенности частной жизни.

В Европе для охраны и защиты права на неприкосновенность частной жизни в условиях автоматизированной обработки личных данных о гражданах более 30 лет назад был введен особый институт правовой охраны личности – институт защиты персональных данных. Более чем в 20 европейских государствах приняты национальные законы о персональных данных (в 2006 году такой закон был принят и в России), в ряде стран введены уполномоченные по защите персональных данных, во всех странах Европейского Союза с 1998 г. создана единая унифицированная система защиты персональных данных, в том числе в секторе телекоммуникаций.

Трудовой кодекс Российской Федерации определяет персональные данные работника как информацию, необходимую работодателю в связи с трудовыми отношениями и касающуюся конкретного работника.

Федеральный закон «Об информации, информационных технологиях и о защите информации» относит персональные данные к информации ограниченного доступа и устанавливает, что порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Закон «О персональных данных» (2006 г.) дает следующее определение персональных данных: Персональные данные – данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Ученые считают, что к персональным данным могут быть отнесены сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам:

- биографические и опознавательные данные (в том числе об обстоятельствах рождения, усыновления, развода);
- личные характеристики (в том числе о личных привычках и наклонностях);
- сведения о семейном положении (в том числе о семейных отношениях);
- сведения об имущественном, финансовом положении (кроме случаев, прямо установленных в законе);
- сведения о состоянии здоровья.

Следует отметить, что такие сведения становятся персональными данными, когда они находятся не у лица, к которому относятся, а у уполномоченных на то юридических и физических лиц. Сведения, относящиеся к персональным данным, могут и не являться личной тайной субъекта, однако при этом будут охраняться уполномоченными на то лицами. Учитывая, что персональные данные относятся к информации ограниченного доступа, которая является защищаемой, они являются составной частью защищаемой информации наряду с различными видами тайн.

Субъектами права в области персональных данных выступают:

- субъекты персональных данных – лица, к которым относятся соответствующие данные, и их наследники;
- держатели персональных данных – органы государственной власти и органы местного самоуправления, юридические и физические лица, осуществляющие на законных основаниях сбор, хранение, передачу, уточнение, блокирование, обезличивание, уничтожение персональных данных.

Субъект персональных данных в соответствии с Трудовым кодексом РФ в отношении своих данных имеет право:

- на полную информацию об их персональных данных и обработке этих данных;
- на свободный доступ к своим персональным данным;
- уточнять свои персональные данные;
- требовать об исключении своих персональных данных;

- обжаловать неправомерные действия или бездействия в отношении персональных данных.

Ограничение права на свои персональные данные возможно в случаях:

- если субъект персональных данных допущен к сведениям, составляющим государственную тайну;
- если персональные данные получены в результате оперативно-розыскной деятельности; если субъект задержан по подозрению в совершении преступления либо ему предъявлено обвинение по уголовному делу.

Глава 3 закона «О персональных данных» (2006 г.) полностью посвящена правам субъекта персональных данных: на доступ к своим персональным данным; при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации; при принятии решений на основании исключительно автоматизированной обработки их персональных данных; на обжалование действий или бездействия оператора.

В законе «О персональных данных» (2006 г.) введено понятие «оператор» – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

Глава 4 закона полностью посвящена обязанностям оператора: при сборе персональных данных; по обеспечению безопасности персональных данных при их обработке; при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных; по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных; по уведомлению об обработке персональных данных.

Государство может регулировать действия операторов (держателей) персональных данных в формах:

- лицензирования действий с персональными данными;
- регистрации баз персональных данных;
- регистрации держателей персональных данных;
- сертификации информационных систем, предназначенных для обработки персональных данных.

Этим вопросам посвящена Глава 5 Федерального закона «О персональных данных» (2006 г.).

Защита персональных данных в России осуществляется также согласно документам ФСТЭК: Приказу от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», специальным нормативным доку-

ментам «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (2008 год), «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (2008) и др.

8.6. Объекты интеллектуальной собственности как составная часть защищаемой информации

Защищаемой нормами об интеллектуальной собственности информацией являются секреты производства (ноу-хау), а также базы данных, охраняемые смежным с авторским правом. Данные меры охраны вводятся частью 4 Гражданского кодекса РФ, которая вступила в силу с 1 января 2008 года.

Охрана прав на секреты производства осуществляется главой 75 Гражданского кодекса РФ «Право на секрет производства (ноу-хау)». Секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Обладателю секрета производства принадлежит исключительное право не противоречащим закону способом (исключительное право на секрет производства), в том числе при изготовлении изделий и реализации экономических и организационных решений. Обладатель секрета производства может распоряжаться указанным исключительным правом.

Лицо, ставшее добросовестно и независимо от других обладателей секрета производства обладателем сведений, составляющих содержание охраняемого секрета производства, приобретает самостоятельное исключительное право на этот секрет производства.

Исключительное право на секрет производства действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих его содержание. С момента утраты конфиденциальности соответствующих сведений исключительное право на секрет производства прекращается у всех правообладателей.

Исключительные права на секрет производства передаются по договору об отчуждении исключительного права или по лицензионному договору о предоставлении права использования секрета производства.

По договору об отчуждении исключительного права на секрет производства одна сторона (правообладатель) передает или обязуется передать

принадлежащее ей исключительное право на секрет производства в полном объеме другой стороне – приобретателю исключительного права на этот секрет производства. При отчуждении исключительного права на секрет производства лицо, распорядившееся своим правом, обязано сохранять конфиденциальность секрета производства до прекращения действия исключительного права на секрет производства.

По лицензионному договору одна сторона – обладатель исключительного права на секрет производства (лицензиар) предоставляет или обязуется предоставить другой стороне (лицензиату) право использования соответствующего секрета производства в установленных договором пределах. Лицензионный договор может быть заключен как с указанием, так и без указания срока его действия. В случае, когда срок, на который заключен лицензионный договор, не указан в этом договоре, любая из сторон вправе в любое время отказаться от договора, предупредив об этом другую сторону не позднее, чем за шесть месяцев, если договором не предусмотрен более длительный срок. При предоставлении права использования секрета производства лицо, распорядившееся своим правом, обязано сохранять конфиденциальность секрета производства в течение всего срока действия лицензионного договора. Лица, получившие соответствующие права по лицензионному договору, обязаны сохранять конфиденциальность секрета производства до прекращения действия исключительного права на секрет производства.

Ответственность за нарушение исключительного права на секрет производства. Нарушитель исключительного права на секрет производства, в том числе лицо, которое неправомерно получило сведения, составляющие секрет производства, и разгласило или использовало эти сведения, а также лицо, обязанное сохранять конфиденциальность секрета производства обязано возместить убытки, причиненные нарушением исключительного права на секрет производства, если иная ответственность не предусмотрена законом или договором с этим лицом.

Лицо, которое использовало секрет производства и не знало и не должно было знать о том, что его использование незаконно, в том числе в связи с тем, что оно получило доступ к секрету производства случайно или по ошибке, не несет ответственность.

Право изготовителя базы данных и смежное с авторским право на базу данных. На базы данных распространяется авторское право на подбор и расположение материала в ней. В соответствие с частью 4 Гражданского кодекса РФ также вводится специальное смежное с авторским право изготовителя на базу данных, а точнее на информацию в ней содержащуюся.

Изготовителем базы данных признается лицо, организовавшее создание базы данных и работу по сбору, обработке и расположению составляющих ее материалов. При отсутствии доказательств иного изготовителем базы данных признается гражданин или юридическое лицо, имя или наименова-

ние которых указано обычным образом на экземпляре базы данных и (или) его упаковке.

Изготовителю базы данных принадлежат:

– исключительное право изготовителя базы данных;

– право на указание на экземплярах базы данных и (или) их упаковках своего имени или наименования.

Изготовителю базы данных, создание которой (включая обработку или представление соответствующих материалов) требует существенных финансовых, материальных, организационных или иных затрат, принадлежит исключительное право извлекать из базы данных материалы и осуществлять их последующее использование в любой форме и любым способом (исключительное право изготовителя базы данных). Изготовитель базы данных может распоряжаться указанным исключительным правом. При отсутствии доказательств иного базой данных, создание которой требует существенных затрат, признается база данных, содержащая не менее десяти тысяч самостоятельных информационных элементов (материалов), составляющих содержание базы данных.

Никто не вправе извлекать из базы данных материалы и осуществлять их последующее использование без разрешения правообладателя, кроме случаев, предусмотренных Гражданским Кодексом. При этом под извлечением материалов понимается перенос всего содержания базы данных или существенной части составляющих ее материалов на другой информационный носитель с использованием любых технических средств и в любой форме.

Исключительное право изготовителя базы данных признается и действует независимо от наличия и действия авторских и иных исключительных прав изготовителя базы данных и других лиц на составляющие базу данных материалы, а также на базу данных в целом как составное произведение.

Лицо, правомерно пользующееся базой данных, вправе без разрешения правообладателя извлекать из такой базы данных материалы и осуществлять их последующее использование в личных, научных, образовательных и иных некоммерческих целях в объеме, оправданном указанными целями, и в той мере, в которой такие действия не нарушают авторские права изготовителя базы данных и других лиц. Использование материалов, извлеченных из базы данных, способом, предполагающим получение к ним доступа неограниченного круга лиц, должно сопровождаться указанием на базу данных, из которой эти материалы извлечены.

Исключительное право изготовителя базы данных возникает в момент завершения ее создания и действует в течение пятнадцати лет, считая с 1 января года, следующего за годом ее создания. Исключительное право изготовителя базы данных, обнародованной в указанный период, действует в течение пятнадцати лет, считая с 1 января года, следующего за годом ее обнародования. Вышеуказанные сроки возобновляются при каждом обновлении базы данных.

Рекомендуемые источники и литература

1. Гражданский кодекс Российской Федерации. Часть вторая: Кодекс Рос. Федерации от 26 янв. 1996 г. № 14-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 22 дек. 1995 г.: Ввод. Федер. законом Рос. Федерации от 26 янв. 1996 г. № 15-ФЗ // Рос. газ. – 1996. – 6–8, 10 февр.

2. О государственной тайне: Закон Рос. Федерации от 21 июля 1993 г. № 5485-I // Рос. газ. – 1993. – 21 сент.

3. О внесении изменений и дополнений в Закон Российской Федерации «О государственной тайне»: Федер. закон Рос. Федерации от 6 окт. 1997 г. № 131-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 19 сент. 1997 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 24 сент. 1997 г. // Рос. газ. – 1997. – 9 окт.

4. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 24-ФЗ // Рос. газ. – 2006. – 29 июля.

5. О коммерческой тайне: Федер. закон Рос. Федерации от 29 июля 2004 г. № 98-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 9 июля 2004 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 15 июля 2004 г. // Рос. газ. – 2004. – 5 авг.

6. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: Постановление правительства РФ от 3 ноября 1994 г. № 1233 // Собр. законодательства Рос.Федерации. – 2005. – № 30 (ч. II), ст. 3165.

7. О банках и банковской деятельности в РСФСР: Закон Рос. Совет. Федератив. Социалист. Респ. от 2 дек. 1990 г. № 395-I // Рос. газ. – 1990. – 11 дек.

8. Основы законодательства Российской Федерации об охране здоровья граждан: Основы законодательства Рос. Федерации от 22 июля 1993 г. № 5487-I // Рос. газ. – 1993. – 18 авг.

9. Основы законодательства Российской Федерации о нотариате: Основы законодательства Рос. Федерации от 11 февр. 1993 г. № 4462-I // Рос. газ. – 1993. – 13 марта.

10. Профессиональный кодекс нотариусов Российской Федерации, принятый 18 апреля 2001 года (с изм. от 31.03. 2006) // Собрание представителей нотариальных палат субъектов Российской Федерации. – 2006.

11. Уголовный кодекс Российской Федерации: Кодекс Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г.: Ввод. Федер. законом Рос. Федерации от 13 июня 1996 г. № 64-ФЗ // Рос. газ. – 1996. – 18-20, 25 июня.

12. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных(выписка) (архив RAR) // http://www.fstec.ru/_razd/_isp0o.htm

13. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Документ MS Word) // http://www.fstec.ru/_razd/_isp0o.htm

14. О персональных данных: Федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Рос. газ. – 2006. – 29 июля.

15. Трудовой кодекс Российской Федерации: Кодекс Рос. Федерации от 30 дек. 2001 г. № 197-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 21 дек. 2001 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 26 дек. 2001 г. // Рос. газ. – 2001. – 31 дек.

16. Портал персональных данных // http://pd.rsoc.ru

17. Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»// http://pd.rsoc.ru/law/document45.htm?print=1

18. Постановление Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» // http://pd.rsoc.ru/law/document21.htm?print=1

19. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // http://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii

20. Алексенцев, А.И. О классификации конфиденциальной информации по видам тайны / А. И. Алексенцев // Безопасность информационных технологий. – 1999. – № 3.

21. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006.– 361с.

22. Бачило, И.Л. Информационное право: учебник / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов; под ред. Б.Н. Топорнина. – СПб.: Юридический центр Пресс, 2001. – 787 с.

23. Шиверский, А.А. Защита информации: проблемы теории и практики / А.А. Шиверский. – М.: Юристъ, 1996. – 112 с.

24. Чумарин, И.Г. Тайна предприятия: что и как защищать / И.Г. Чумарин. – СПб.: ООО «Издательство ДНК», 2001. – 160 с.

25. Тихомирова, Л.В. Защита персональных данных работника: учебно-практическое пособие (CD) / Л.В. Тихомирова. – М.: Термика-М, 2004. – 124 с.

Раздел III
УГРОЗЫ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Тема 9. Классификация угроз защищаемой информации

9.1. Признаки классификации угроз защищаемой информации.
9.2. Виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны людей.
9.3. Виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи
9.4. Виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны систем обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации
9.5. Виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны технологических процессов отдельных промышленных объектов
9.6. Виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны природных явлений.
9.7. Другие признаки структурирования угроз защищаемой информации.

9.1. Признаки классификации угроз защищаемой информации

К признакам структурирования угроз относятся: сущностные проявления угроз, факторы, наличие условий реализации угрозы и результат, к которому может привести дестабилизирующее воздействие на информацию.
Первый признак структурирования угроз – сущностные проявления. Любое проявление, обнаружение чего-то принято называть явлением. Следовательно, одним из признаков и вместе с тем одной из составляющих угрозы должны быть явления.

К сущностным проявлениям угрозы относятся:

1) источники дестабилизирующего воздействия на информацию (от кого или от чего исходит дестабилизирующее воздействие): люди; технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи; системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации; технологические процессы отдельных категорий промышленных объектов; природные явления;

2) виды дестабилизирующего воздействия на информацию (каким образом (по каким направлениям) происходит дестабилизирующее воздействие);

3) способы дестабилизирующего воздействия на информацию (какими приемами, действиями осуществляются (реализуются) виды дестабилизирующего воздействия).

Рассмотрим виды и способы дестабилизирующего воздействия на защищаемую информацию по источникам воздействия.

9.2. Виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны людей

Виды и способы дестабилизирующего воздействия на защищаемую информацию дифференцируются по источникам воздействия. Самое большее количество видов и способов дестабилизирующего воздействия на информацию имеет отношение к людям.

Со стороны людей возможны следующие виды воздействия:

1) непосредственное воздействие на носители защищаемой информации.

2) несанкционированное распространение конфиденциальной информации.

3) вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.

4) нарушение режима работы перечисленных средств и технологии обработки информации.

5) вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Способами непосредственного воздействия на носители защищаемой информации могут быть:

– физическое разрушение носителя (поломка, разрыв и др.);

– создание аварийных ситуаций для носителей (поджог, искусственное затопление, взрыв и т. д.);

– удаление информации с носителей (замазывание, стирание, обесцвечивание и др.);

– создание искусственных магнитных полей для размагничивания носителей;

– внесение фальсифицированной информации в носители.

Этот вид дестабилизирующего воздействия приводит к реализации трех форм проявления уязвимости информации: уничтожению, искажению и блокированию.

К непосредственному воздействию на носители защищаемой информации можно с оговоркой отнести и непреднамеренное оставление их в неохраняемой зоне, чаще всего в общественном транспорте, магазине, на рынке, что приводит к потере носителей.

Несанкционированное распространение конфиденциальной информации может осуществляться путем:

- словесной передачи (сообщения) информации;

- передачи копий (снимков) носителей информации;
- показа носителей информации;
- ввода информации в вычислительные сети;
- опубликования информации в открытой печати;
- использования информации в открытых публичных выступлениях, в том числе по радио, телевидению.

К несанкционированному распространению может привести и потеря носителей информации.

Этот вид дестабилизирующего воздействия приводит к разглашению конфиденциальной информации.

К способам вывода из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи можно отнести:

- неправильный монтаж средств;
- поломку (разрушение) средств, в том числе разрыв (повреждение) кабельных линий связей;
- создание аварийных ситуаций для технических средств (поджог, искусственное затопление, взрыв и др.);
- отключение средств от сетей питания;
- вывод из строя или нарушение режима работы систем обеспечения функционирования средств;
- вмонтирование в ЭВМ разрушающих радио- и программных закладок.

Этот вид дестабилизирующего воздействия приводит к реализации трех форм проявления уязвимости информации: уничтожению, искажению и блокированию.

Способами нарушения режима работы технических средств отображения, хранения, обработки, воспроизведения, передача информации, средств связи и технологии обработки информации могут быть:

- повреждение отдельных элементов средств;
- нарушение правил эксплуатации средств;
- внесение изменений в порядок обработки информации;
- заражение программ обработки информации вредоносными программами;
- выдача неправильных программных команд;
- превышение расчетного числа запросов;
- создание помех в радио эфире с помощью дополнительного звукового или шумового фона, изменения (наложения) частот передачи информации;
- передача ложных сигналов;
- подключение подавляющих фильтров в информационные цепи, цепи питания и заземления;
- нарушение (изменение) режима работы систем обеспечения функционирования средств.

Данный вид дестабилизирующего воздействия также приводит к уничтожению, искажению и блокированию информации.

К способам вывода из строя и нарушения режима работы систем обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации следует отнести:

- неправильный монтаж систем;
- поломку (разрушение) систем или их элементов;
- создание аварийных ситуаций для систем (поджог, искусственное затопление, взрыв и т. д.);
- отключение систем от источников питания;
- нарушение правил эксплуатации систем.

Этот вид дестабилизирующего воздействия приводит к тем же результатам, что и два предыдущих вида.

9.3. Виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи

К видам дестабилизирующего воздействия на защищаемую информацию со стороны второго источника воздействия – технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи – относятся:

1) выход средств из строя;
2) сбои в работе средств;
3) создание электромагнитных излучений.

Выход средств из строя, приводящий к невозможности выполнения операций, может происходить путем:

- технической поломки, аварии (без вмешательства людей);
- возгорания, затопления (без вмешательства людей);
- выхода из строя систем обеспечения функционирования средств;
- воздействия природных явлений;
- воздействия измененной структуры окружающего магнитного поля;
- заражения программ обработки информации вредоносными программами (путем размножения последних или с зараженных дискет);
- разрушения или повреждения носителя информации, в том числе размагничивания магнитного слоя диска (ленты) из-за осыпания магнитного порошка.

Этот вид дестабилизирующего воздействия приводит к реализации трех форм проявления уязвимости информации: уничтожению, искажению, блокированию.

Сбои в работе средств, приводящие к неправильному выполнению операций (ошибкам), могут осуществляться посредством:

- возникновения технических неисправностей элементов средств;
- заражения программ обработки информации вредоносными программами (путем размножения последних или с зараженных дискет);
- воздействия природных явлений;
- воздействия окружающего магнитного поля;
- частичного размагничивания магнитного слоя диска (ленты) из-за осыпания магнитного порошка;
- нарушения режима функционирования систем обеспечения функционирования средств.

Данный вид дестабилизирующего воздействия приводит к реализации четырех форм проявления уязвимости информации: уничтожению искажению, блокированию, разглашению (пример последней – соединение с номером телефона не того абонента, который набирается, или слышимость разговора других лиц из-за неисправности в цепях коммутации телефонной станции).

Электромагнитные излучения, в том числе побочные, образующиеся в процессе эксплуатации средств, приводят к хищению информации.

9.4. Виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны систем обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации

Третий источник дестабилизирующего воздействия на информацию – системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации – включает два вида воздействия: выход систем из строя и сбои в работе систем.

Выход систем из строя может происходить путем:

- поломки, аварии (без вмешательства людей);
- возгорания, затопления (без вмешательства людей);
- выхода из строя источников питания;
- воздействия природных явлений.

Этот вид дестабилизирующего воздействия приводит к реализации трех форм проявления уязвимости информации: уничтожению, блокированию, искажению.

Сбои в работе систем могут осуществляться посредством:

- появления технических неисправностей элементов систем;
- воздействия природных явлений;

- нарушения режима работы источников питания.

Результатом дестабилизирующего воздействия также являются уничтожение, блокирование, искажение информации.

9.5. Виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны технологических процессов отдельных промышленных объектов

Видом дестабилизирующего воздействия на информацию со стороны технологических процессов отдельных промышленных объектов является изменение структуры окружающей среды.

Это воздействие осуществляется путем:

- изменения естественного радиационного фона окружающей среды, происходящего при функционировании объектов ядерной энергетики;
- изменения химического состава окружающей среды, происходящего при функционировании объектов химической промышленности;
- изменения локальной структуры магнитного поля, происходящего вследствие деятельности объектов радиоэлектроники и по изготовлению некоторых видов вооружения и военной техники.

Этот вид дестабилизирующего воздействия в конечном итоге приводит к хищению конфиденциальной информации.

9.6. Виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны природных явлений

Пятый источник дестабилизирующего воздействия на информацию – природные явления, как уже отмечалось, включает стихийные бедствия и атмосферные явления (колебания).

К стихийным бедствиям и одновременно видам воздействия следует отнести:

- землетрясение,
- наводнение,
- ураган (смерч),
- шторм,
- оползни,
- лавины,
- извержения вулканов.

К атмосферным явлениям (видам воздействия) относят:

- грозу,
- дождь,
- снег,
- перепады температуры и влажности воздуха,

- магнитные бури.

Способами воздействия со стороны и стихийных бедствий, и атмосферных явлений могут быть:

- разрушение (поломка),
- затопление,
- сожжение носителей информации, средств отображения, хранения, обработки, воспроизведения, передачи информации и кабельных средств связи, систем обеспечения функционирования этих средств,
- нарушение режима работы средств и систем, а также технологии обработки информации.

Эти виды воздействия приводят к пяти формам проявления уязвимости информации: потере, уничтожению, искажению, блокированию и хищению.

9.7. Другие признаки структурирования угроз защищаемой информации

Второй признак структурирования угроз – факторы. В основе любого явления лежат соответствующие причины, которые являются его движущей силой и которые, в свою очередь, обусловлены определенными обстоятельствами или предпосылками. Эти причины и обстоятельства (предпосылки) относятся к факторам, создающим возможность дестабилизирующего воздействия на информацию.

К факторам, создающим возможность дестабилизирующего воздействия на информацию, относятся:

1. Причины, вызывающие дестабилизирующие воздействия на защищаемую информацию.
2. Обстоятельства, способствующие появлению этих причин.
3. Наличие каналов несанкционированного доступа к защищаемой информации для воздействия на информацию со стороны лиц, не имеющих к ней разрешенного доступа.
4. Наличие методов несанкционированного доступа к конфиденциальной информации.

Третий признак структурирования угроз – наличие условий. Факторы могут стать побудительной силой для явлений, а последние могут «сработать» лишь при наличии определенных условий (обстоятельств) для этого.

К условиям, создающим возможность для дестабилизирующего воздействия на информацию, можно отнести:

- недостаточность мер, принимаемых для защиты информации, в том числе из-за нехватки ресурсов;
- недостаточный контроль и внимание со стороны администрации вопросам защиты, информации;
- принятие решений по производственным вопросам без учета требований по защите информации;

- плохие взаимоотношения между сотрудниками и сотрудников с администрацией.

Условиями, обеспечивающими реализацию дестабилизирующего воздействия на информацию со стороны технических средств, могут являться:

- недостаточное внимание к составу и качеству средств со стороны администрации, нередко из-за недопонимания их значения;
- нерегулярный профилактический осмотр средств;
- низкое качество обслуживания средств.

Четвертый признак структурирования угроз – направленность, результат, к которому может привести дестабилизирующее воздействие на информацию. Таким результатом во всех случаях реализации угрозы является нарушение установленного статуса информации.

На основе сказанного А.И. Алексенцев формулирует следующее определение угрозы: Угроза защищаемой информации – совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.

Согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», угроза (безопасности информации) – это совокупность условий и факторов, создающихпотенциальную или реально существ ующую опасность нарушения безопасности информации.

Рекомендуемые источники и литература

1. Алексенцев, А.И. Понятие и структура угроз защищаемой информации / А.И. Алексенцев // Безопасность информационных технологий. – М., 2000. – № 3.
2. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.
3. Герасименко, В.А. Основы защиты информации: учебник / В.А. Герасименко, А.А. Малюк. – М., 1997. – 538 с.
4. Малюк, А.А. Введение в защиту информации в автоматизированных системах: учебное пособие / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – М.: Горяч. Линия-Телеком, 2005. – 147 с.
5. Скиба, В. Руководство по защите от внутренних угроз информационной безопасности / В. Скиба, В. Курбатов. – СПб.: Питер, 2008. – 320 с.
6. Информационная безопасность и защита информации: учеб. пособие / В.П. Мельников и др.; под ред. С. А. Клейменова. – М.: Академия, 2009. – 330 с.
7. Организационно-правовое обеспечение информационной безопасности: учебное пособие / А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др.; под ред. А.А. Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.

8. Романов, О.А. Организационное обеспечение информационной безопасности: учебник / О.А. Романов, С.А. Бабин, С.Г. Жданов. – М.: Издательский центр «Академия», 2008. – 240 с.

9. Гришина, Н.В. Организация комплексной системы защиты информации / Н.В. Гришина. – М.: Гелиос АРВ, 2007. – 256 с.

10. Тихонов, В.А. Информационная безопасность: организационные, правовые и технические аспекты / В.А. Тихонов, В.В. Райх. – М.: Гелиос АРВ, 2006. – 516 с.

Тема 10. Каналы и методы несанкционированного доступа к конфиденциальной информации

10.1. Понятие несанкционированного доступа к информации.

10.2. Понятие несанкционированного доступа к информации и каналов утечки информации.

10.3. Каналы и методы НСД.

10.4. Разведывательная деятельность: формы, направления, виды.

10.1. Понятие несанкционированного доступа к информации

Несанкционированный доступ (несанкционированные действия) (НСД) – это доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Иными словами, это преднамеренный или случайный доступ к информации, не разрешенный в установленном порядке.

Утечка информации – это неправомерный выход конфиденциальной информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, результатом которого является получение информации лицами, не имеющими к ней санкционированного доступа.

Различия понятий «несанкционированный доступ» и «утечка информации» заключаются в следующем.

1. Вектор движения конфиденциальной информации:

- утечка конфиденциальной информации происходит от носителя информации к лицам, не имеющим доступа к информации;
- несанкционированный доступ – от лиц, не имеющих доступа к конфиденциальной информации, – к носителям информации.

2. Формы проявления уязвимости информации:

- к утечке информации приводят или могут привести три формы проявления уязвимости (разглашение информации, потеря и хищение носителя или содержащейся в нем информации);

- несанкционированный доступ может привести к пяти формам проявления уязвимости информации: хищению, уничтожению, искажению, блокированию, потере и разглашению информации.

3. Субъекты:

- к утечке информации могут быть причастны лица, как имеющие, так и не имеющие санкционированный доступ к информации;
- несанкционированный доступ возможен только со стороны лиц, не имеющих отношения к данной информации по характеру выполняемой работы.

Соответственно, отличаются друг от друга и понятия каналов несанкционированного доступа к информации и каналов утечки информации.

10.2. Понятие несанкционированного доступа к информации и каналов утечки информации

Канал утечки информации определяют:

- как технологию (способ) доступа к информации;
- как дестабилизирующие факторы, позволяющие получить информацию;
- как физический путь от источника информации к несанкционированному получателю;
- как совокупность условий и событий, приводящих к неправомерному выходу информации за пределы установленной сферы ее обращения.

Наиболее адекватным с точки зрения русского языка является определение канала (и утечки информации, и несанкционированного доступа) как пути. Канал включает в себя две составляющие: объект использования (воздействия) и использование объекта (воздействие на него). Сам по себе объект (например, кабель) не является каналом, он превращается в составляющую канала только при определенном воздействии на него.

На основе понятия канала можно сформулировать определение каналов утечки информации и каналов несанкционированного доступа к конфиденциальной информации.

Канал утечки информации – путь неправомерного выхода информации за пределы защищаемой зоны ее функционирования или установленного круга лиц.

Канал несанкционированного доступа к конфиденциальной информации – путь, используя который можно получить неразрешенный преднамеренный или случайный доступ к информации.

Технический канал утечки информации – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

10.3. Каналы и методы НСД

К каналам несанкционированного доступа к информации относятся:

1. Установление контакта с лицами, имеющими или имевшими доступ к конфиденциальной информации.

Методы:

- выведывание информации под благовидным предлогом («использование втемную»);
- действительный прием на работу («переманивание»), одной из целей которого является получение от лица, принятого на работу, конфиденциальной информации, относящейся к прежнему месту его работы;
- разовая покупка конфиденциальной информации;
- принуждение к выдаче конфиденциальной информации шантажом, различного рода угрозами, применением физического насилия как к лицу, владеющему информацией, так и к его родственникам и близким;
- склонение к выдаче конфиденциальной информации убеждением, лестью, посулами, обманом, в том числе с использованием национальных, политических, религиозных факторов.

2. Вербовка и (или) внедрение агентов.

Методы:

- методы, применяемые при использовании первого канала, а также:
- ознакомление с документами, находящимися на рабочих местах других сотрудников, в том числе с выведенными на экран дисплея, в отсутствие сотрудников (можно использовать и фотографирование) и при их присутствии;.
- осмотр доступной продукции, наблюдение за технологическим процессом считывание информации в массивах других пользователей, в том числе с использованием паролей и терминалов этих пользователей;
- подслушивание разговоров, в том числе телефонных, напрямую и с использованием радиозакладок;
- прослушивание публичных выступлений, проводимых на предприятии;
- участие в различного рода комиссиях, общественных объединениях, использующих конфиденциальную информацию;
- кража носителей информации, в том числе и с помощью изготовления дубликатов ключей от сейфов (шкафов).

3. Организация физического проникновения к носителям конфиденциальной информации.

Методы:

- использование подложного, украденного или купленного (в том числе и на время) пропуска;
- маскировка под другое лицо, если пропуск не выдается на руки;
- проход под видом внешнего обслуживающего персонала;

- проезд спрятанным в автотранспорте;
- - отвлечение внимания охраны для прохода незамеченным (путем создания чрезвычайных ситуаций, с помощью коллеги и т. д.);
- изоляция или уничтожение охраны (в редких, чрезвычайных обстоятельствах);
- преодоление заграждающих барьеров (заборов) минуя охрану, в том числе и за счет вывода из строя технических средств охраны.

4. Организация физического проникновения к средствам отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средствам связи, а также к системам обеспечения функционирования названных средств.

Методы:

- взлом дверей хранилищ и сейфов (шкафов) или их замков, через окна.

Способы:

- с персонального компьютера с использованием телефонного набора или с несанкционированного терминала со взломом парольно-ключевых систем защиты или без взлома с помощью маскировки под зарегистрированного пользователя;
- с помощью закладных устройств; с помощью прямого присоединения к кабельным линиям связи, в том числе с использованием параллельных телефонных аппаратов;
- за счет электромагнитных наводок на параллельно проложенные провода или методов высокочастотного навязывания.

5. Подключение к средствам отображения, хранения, обработки, воспроизведения и передачи информации, средствам связи.

По применяемым методам практически не отличается от третьего канала.

6. Подключение к системам обеспечения функционирования перечисленных в предыдущем пункте средств.

Методы:

- замеры потребления электроэнергии, воды,
- подключение к сетям питания, заземления.

7. Прослушивание речевой конфиденциальной информации.

Методы:

- подслушивание непосредственных разговоров лиц, допущенных к данной информации;
- прослушивание речевой информации, зафиксированной на носителе, с помощью подключения к средствам ее звуковоспроизведения, передачи, средствам связи.

8. Визуальный съем конфиденциальной информации.

Методы:

- чтение документов на рабочих местах пользователей (в том числе с экранов дисплеев, с печатающих устройств) в присутствии пользователей и при их отсутствии;

- осмотр продукции, наблюдение за технологическим процессом изготовления продукции;
- просмотр информации, воспроизводимой средствами видеовоспроизводящей техники и телевидения;
- чтение текста, печатаемого на машинке и размножаемого множительными аппаратами;
- наблюдение за технологическими процессами изготовления, обработки, размножения информации;
- считывание информации в массивах других пользователей, в том числе чтением остаточной информации.

9. Перехват электромагнитных излучений.

Методы:

- поиск сигналов;
- выделение из них сигналов, несущих конфиденциальную информацию;
- съем с них информации;
- ее обработка и анализ.

10. Замеры и взятие проб окружающей объект среды.

Методы:

- замеры уровня радиационного фона;
- замеры структуры магнитного поля;
- взятие проб воздуха, почвы, воды, снега, донных отложений, растений и исследование их или содержащихся на них осадков на предмет химического или биологического состава.

11. Исследование выпускаемой продукции, производственных отходов и отходов процессов обработки информации.

Методы:

- приобретение и разборка (расчленение, выделение отдельных составных частей, элементов) выпускаемых изделий, их химический и физический анализ (обратный инжиниринг);
- сбор и изучение остатков боевой и испытательной техники на испытательных полигонах, поломанных изделий, макетов изделий, бракованных узлов, блоков, устройств, деталей, созданных на стадии опытно-конструкторских разработок, а также руды и шлаков, позволяющих определить состав материалов, а нередко и технологию изготовления продукции;
- сбор и прочтение черновиков и проектов конфиденциальных документов, копировальной бумаги, красящей ленты печатающих устройств, прокладок, испорченных магнитных дискет.

12. Изучение доступных источников информации.

Методы:

- изучения научных публикаций, содержащихся в специализированных журналах (сборниках);

- просмотра (прослушивания) средств массовой информации (газет, журналов, теле- и радиопередач);
- изучения проспектов и каталогов выставок;
- прослушивания публичных выступлений на семинарах, конференциях и других публичных мероприятиях;
- изучения банков данных о предприятиях, формируемых специализированными коммерческими структурами.

13. Анализ архитектурных особенностей некоторых категорий объектов.

Методы:

- наблюдения,
- фотографирования,
- замеров зданий или их отдельных частей.

10.4. Разведывательная деятельность: формы, направления, виды

Разведка как разведывательная деятельность – это совокупность мероприятий, целенаправленно осуществляемых по добыванию защищаемой информации о вероятном или действительном конкуренте, противнике (в дальнейшем – сопернике).

Разведка подразделяется, чаще всего, на стратегическую и тактическую. Тактическая разведка обычно носит войсковой характер, проводится командирами и штабами объединений и соединений войск, частей и подразделений. Этому виду разведки мы внимания уделять не будем. Стратегическая разведка (в дальнейшем – просто разведка) организуется руководством государств и правительств, военных и других ведомств, высшим военным командованием.

В зависимости от сил и средств, используемых в разведывательной деятельности для добывания секретной информации о других государствах, различают три формы разведки:

1. Нелегальная разведка (т. е. агентурная, шпионаж).

Понятие «агентурная разведка» происходит от термина «агент» (лат.), что означает действующий, т. е. лицо, действующее по поручению кого-либо; представитель учреждения, организации и т.п., выполняющий поручения, уполномоченный. Под агентурной разведкой понимается добывание разведывательной, защищаемой информации с помощью агентов, т.е. лиц, действующих по поручению разведки.

2. Легальная разведка.

Легальными методами сбора сведений, составляющих государственную тайну являются:

- приобретение открытой литературы, периодических изданий и других материалов о РФ;

• выведывание информации у российских граждан на официальных приемах, симпозиумах, конференциях, при частных встречах, а также направление запросов в различные организации и учреждения нашей страны, анкетирование и т. п.;

• визуальное наблюдение при поездках под благовидным предлогом по территории страны.

3. Разведка научно-техническая.

Технические средства разведки (ТСР), по словам многих руководителей спецслужб, не заменяют, а дополняют агентурную разведку. Однако техническая разведка имеет и относительно самостоятельное значение в рамках системы всех разведывательных средств и методов, используемых спецслужбами для добывания защищаемой соперником информации.

Под технической разведкой (ТР) понимается вид разведывательной деятельности спецслужб, где основную роль в непосредственном выявлении и фиксировании данных о интересующих объектах играют технические средства, сведенные, как правило, в самостоятельные организационные системы.

Рассмотрим направления и виды разведывательной деятельности, их соотношение и взаимосвязь.

Направленность деятельности разведок и других специальных служб государств, корпораций и фирм обусловливается различными задачами. Однако основными из них будут те, которые ставит перед собой руководство государства, корпорации или фирмы и, следовательно, их разведывательные службы.

Направления деятельности спецслужб можно разделить на две группы:

1. Первая группа характеризуется целями деятельности спецслужб.

2. Вторая группа обусловлена содержанием информации, которую стремятся добывать спецслужбы.

В первой группе, которая характеризуется целями деятельности спецслужб, можно выделить следующие основные направления.

1. Добывание разведывательной информации. Спецслужбы имеют в своем составе оперативные подразделения, которые занимаются добыванием информации по странам, регионам, отдельным проблемам и т. д.

2. Исследование и аналитическая обработка добытой информации. Собранная оперативными подразделениями информация – это исходный материал разведки, который без соответствующей аналитической обработки иногда может стоить не очень много. Анализ информации, подготовка выходных документов и их реализация – одна из важнейших функций разведки.

3. Создание условий для работы разведки. Основная база ведения государством военно-политической разведки – «легальные» резидентуры разведслужб государств в посольствах своих стран за границей. Резидентуры основных разведслужб в своих посольствах в Москве имеют практи-

чески все крупные государства. Улучшение отношений нашего государства с другими странами, развитие экономических связей создают новые возможности в работе для спецслужб государств и корпораций. Разведчики могут использовать более глубокие прикрытия – создавать коммерческие фирмы и действительно заниматься коммерцией, но сотрудниками такой фирмы могут быть кадровые разведчики как ЦРУ, так и какой-либо корпорации, фирмы.

4. Непосредственные действия, или ведение подрывных акций – чтобы ослабить своего противника. В государственном масштабе это могут быть политические и экономические подрывные акции. Такие же подрывные акции могут проводить и фирмы в отношении своих конкурентов. Подобные факты имеют место и в нашей стране.

Во второй группе направлений разведывательной деятельности, обусловленной содержанием информации, которую стремятся добывать спецслужбы, в свою очередь можно выделить следующие.

1. Военно-политический шпионаж, который стремится добывать политическую, биографическую, военную и военно-техническую информацию.

2. Экономический шпионаж занимается добыванием информации по таким вопросам, как распределение национального дохода по отраслям, разведка запасов и природных ресурсов, состояние экономики страны и регионов, отражаемые в конфиденциальной информации.

3. Промышленный шпионаж добывает информацию по таким вопросам, как издержки, себестоимость, маркетинг, реклама (коммерческий шпионаж), технология (технологический шпионаж), новые образцы и модели продукции (научно-технический шпионаж).

Каждое из этих направлений разведывательной деятельности показывает, какие секреты могут интересовать ту или иную разведку, от кого следует ожидать попыток проникновения к защищаемой информации, ее носителям.

Рекомендуемые источники и литература

1. О внешней разведке: Федер. закон Рос. Федерации от 10 янв. 1996 г. № 5-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 8 дек. 1995 г. // Рос. газ. – 1996. – 17 янв.

2. Об оперативно-розыскной деятельности: Федер. закон Рос. Федерации от 12 авг. 1995 г. № 144-ФЗ // Рос. газ. – 1995. – 18 авг.

3. Алексенцев, А.И. Понятие и структура угроз защищаемой информации / А.И. Алексенцев // Безопасность информационных технологий. – М., 2000. – № 3.

4. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361с.

5. Зайцев, А.П. Технические средства и методы защиты информации: учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов. – 4-е изд., испр и доп. – М.: Горячая Линия-Телеком, 2009. – 343 с.

6. Ленков, С.В. Методы и средства защиты информации: в 2 т. Т. 1. Несанкционированное получение информации / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – М.: Арий, 2008. – 464 с.

7. Галатенко, В.А. О каналах скрытых, потайных, побочных. И не только / В.А. Галатенко. – http://www.citforum.ru/security/articles/channels/ – Загл. с экрана.

8. Торокин, А.А. Инженерно-техническая защита информации / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

9. Шиверский, А.А. Защита информации: проблемы теории и практики / А.А. Шиверский. – М.: Юристъ, 1996. – 112 с.

Раздел IV. МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 11. Виды и методы защиты информации

11.1. Правовая защита информации.
11.2. Организационная защита информации.
11.3. Инженерно-техническая защита информации.
11.4. Программно-математическая защита (программно-аппаратная и криптографическая) информации.

11.1. Правовая защита информации

В основе классификации видов защиты информации лежат используемые для защиты информации силы, средства и методы. Согласно эти критериям классификации к видам защиты информации относятся: правовая защита информации, организационная защита информации, программно-математическая (программно-аппаратная и криптографическая) защита информации, инженерно-техническая защита информации.

Правовая защита информации. Правовые меры, регулирующие вопросы защиты секретной и конфиденциальной информации, можно разделить на две основные группы:

1) нормативные акты, регламентирующие правила и процедуры защиты информации, которые регламентируются законами и подзаконными актами, в частности указами Президента РФ, постановлениями Правительства РФ;

2) нормативные акты, устанавливающие ответственность за покушение на сведения, составляющие государственную или коммерческую тайну, и за преступления против установленного порядка сохранения засекреченной информации, регулируются уголовным, гражданским и административным кодексами РФ.

Уголовно-правовые нормы по своему содержанию являются, с одной стороны, запрещающими, то есть они под страхом применения мер уголовного наказания запрещают гражданам нарушать свои обязанности и совершать преступления, а с другой стороны, они обязывают соответствующие органы государства (ФСБ, МВД, прокуратуру) привлечь лиц, виновных в совершении преступления, к уголовной ответственности.

Кроме того, нарушения режима секретности, правил сохранения государственной и коммерческой тайны, не являющиеся преступлением, могут повлечь ответственность материального, дисциплинарного или административного характера в соответствии с действующими нормативными актами: отстранение от работы, связанной с секретами, или перевод на другую работу, менее оплачиваемую и тоже не связанную с засекреченной информацией.

11.2. Организационная защита информации

Данная группа мер защиты секретной и конфиденциальной информации преследует цель проведения организационной работы по выполнению правил, процедур и требований защиты государственной и коммерческой тайны на основе правил, установленных законами и подзаконными правовыми актами (инструкциями, положениями и т. п.).

Организационные меры по защите информации предусматривают прежде всего подбор и расстановку кадров, которые будут осуществлять мероприятия по защите информации, обучение сотрудников правилам защиты засекреченной информации, осуществление на практике принципов и методов защиты информации.

Нормативно-правовые организационные режимные меры являются основой для решения таких важных вопросов защиты информации, как соблюдение принципа максимального ограничения числа лиц, допускаемых к секретным работам и документам. Организационные меры защиты информации требуют детального соблюдения правил секретного делопроизводства, чтобы исключить или свести к минимуму утрату секретных или конфиденциальных документов, а также сохранение изделий и других носителей защищаемой информации.

Организационные меры решают проблему предотвращения утечки защищаемой информации в печати, при вывозе материалов за границу, при контактах сотрудников предприятия или фирмы с иностранцами и возникновении других условий, создающих объективные предпосылки появления каналов утечки информации.

Основное назначение организационных мер защиты информации – предупредить несанкционированный доступ к информации ограниченного доступа и утечку защищаемой информации.

11.3. Инженерно-техническая защита информации

Это самостоятельное направление защиты секретов, приобретающее в последнее время все большее значение. Развитие технических средств разведки (ТСР), совершенствование радио, радиотехнической и других видов этой разведки потребовало от государства создания системы мер противодействия сбору разведывательной информации с помощью ТСР.

Инженерно-технические меры защиты информации – это комплекс организационных и инженерно-технических мероприятий, направленных на то, чтобы исключить или существенно затруднить добывание с помощью ТСР защищаемой информации. Концепция инженерно-технических мер базируется на той идее, что какое-то действие требует и противодействия. Противостоять ТСР с помощью только организационных режимных мер явно недостаточно, так как ТСР нередко не имеют границ (космическая,

радио, радиолокационная и др.) и на их деятельность не влияют время года и суток, состояние погоды.

Всю совокупность инженерно-технических мер защиты информации можно разделить на три группы:

1) общепредупредительные меры, которые включают правовое регулирование использования технических средств в процессе осуществления международных связей; установление и поддержание режимов, направленных на предотвращение утечки защищаемой информации по каналам, доступным ТСР и др.;

2) организационные меры включают в себя такие мероприятия, как анализ и обобщение информации о ТСР, определение их возможностей и выработка прогнозов их развития, появление новых возможностей получения защищаемой информации с помощью ТСР, определение, какие параметры и каких образцов техники требуют защиты от ТСР и выработка путей защиты этих параметров;

3) технические меры включают комплекс инженерно-технических средств и мероприятий, используемых для скрытия от ТСР защищаемых сведений об объектах защиты и технической дезинформации соперника. Они включают: создание и использование экранированных помещений; специальных транспортных средств, укрытий и аппаратуры засекречивания; снижение и изменение различных излучений путем использования эквивалентных антенн, естественных и индустриальных помех, а также режима молчания и соблюдение установленных правил использования средств связи и СВТ.

11.4. Программно-математическая защита (программно-аппаратная и криптографическая) информации

Программно-математическая защита (программно-аппаратная и криптографическая) информации – предусматривает проведение комплекса мер защиты информации в СВТ. Эта проблема носит комплексный характер и является относительно самостоятельным направлением защиты информации. Защита информации в СВТ включает в себя ряд определенных групп мер:

- меры организационно-режимного характера: режим помещений СВТ; секретное и конфиденциальное делопроизводство, особенность которого заключается в том, что оно осуществляется с документами как на привычных (бумага) носителях информации, так и на машинных и др.;
- меры инженерно-технического характера: место расположения СВТ, экранирование помещений, создание помех и др.;
- меры, решаемые путем программирования, – создание предпосылок для регламентации и ранжирования субъектов по их правам на доступ к

соответствующей категории защищаемой информации; ограждение СВТ от программ – «вирусов»; автоматическое или целенаправленное стирание информации из оперативной памяти по миновании в ней надобности и др.;

- кодирование и шифрование информации, вводимой в СВТ.

Рекомендуемые источники и литература

1. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361с.

2. Баяндин, Н.И. Основы деловой разведки / Н.И. Баяндин; под ред. Л.М. Кунбутаева. – М.: Изд. МЭИ, 2005. – 320 с.

3. Доронин, А.И. Бизнес-разведка / А.И. Доронин. – М.: Изд-во «Ось-89», 2003. – 384 с.

4. Шиверский, А.А. Защита информации: проблемы теории и практики / А.А. Шиверский. – М.: Юристъ, 1996. – 112 с.

5. Герасименко, В.А., Малюк, А.А. Основы защиты информации: учебник / В.А. Герасименко, А.А. Малюк. – М., 1997. – 538 с.

6. Романов, О.А. Организационное обеспечение информационной безопасности: учебник / О.А. Романов, С.А. Бабин, С.Г. Жданов. – М.: Издательский центр «Академия», 2008. – 240 с.

7. Служба защиты информации предприятия. Что она из себя представляет и как ее организовать. – http://www.spektrsec.ru/sluzhba-zaschityi-informatsii-predpriyatiya.-chto-ona-iz-sebya-predstavlyaet-i-kak-ee-organizovat.html – Загл. с экрана.

8. Организационно-правовое обеспечение информационной безопасности: учебное пособие / А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др.; под ред. А.А. Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.

9. Торокин, А.А. Инженерно-техническая защита информации / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

10. Информационная безопасность и защита информации: учеб. пособие / В.П. Мельников и др.; под ред. С.А. Клейменова. – М.: Академия, 2009. – 330 с.

11. Гришина, Н.В. Организация комплексной системы защиты информации / Н.В. Гришина. – М.: Гелиос АРВ, 2007. – 256 с.

12. Тихонов, В.А. Информационная безопасность: организационные, правовые и технические аспекты / В.А. Тихонов, В.В. Райх. – М.: Гелиос АРВ, 2006. – 516 с.

13. Программно-аппаратная защита информации: учебное пособие для студентов специальности 090103 «Орг. и технология защиты информ.» и специальности 090104.65 «Комплекс. защита объектов информ.» / В.А. Семененко, Н.В. Федоров; Моск. гос. индустр. ун-т. – М.: Издательство МГИУ, 2007. – 339 с.

Тема 12. Методы и средства защиты информации

12.1. Методы защиты информации.
12.2. Средства защиты информации.

12.1. Методы защиты информации

Метод – в самом общем значении это способ достижения цели, определенным образом упорядоченная деятельность.

Основными методами, используемыми в защите информации, являются следующие: скрытие, ранжирование, дезинформация, дробление, страхование, морально-нравственные, учет, кодирование, шифрование.

Скрытие – как метод защиты информации является в основе своей реализацией на практике одного из основных организационных принципов защиты информации – максимального ограничения числа лиц, допускаемых к секретам. Реализация этого метода достигается обычно путем: а) засекречивания информации, то есть отнесения ее к секретной или конфиденциальной информации различной степени секретности и ограничение в связи с этим доступа к этой информации в зависимости от ее важности для собственника, что проявляется в проставляемом на носителе этой информации грифе секретности; б) устранения или ослабления технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них.

Скрытие – один из наиболее общих и широко применяемых методов защиты информации.

Ранжирование как метод защиты информации включает, во-первых, деление засекречиваемой информации по степени секретности, и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций. Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности информации и определяется матрицей доступа.

Ранжирование как метод защиты информации является частным случаем метода скрытия: пользователь не допускается к информации, которая ему не нужна для выполнения его служебных функций, и тем самым эта информация скрывается от него и всех остальных (посторонних) лиц.

Дезинформация – один из методов защиты информации, заключающийся в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности, положении дел на предприятии и т. д.

Дробление (расчленение) информации на части с таким условием, что знание какой-то одной части информации (например, знание одной операции технологии производства какого-то продукта) не позволяет восстановить всю картину, всю технологию в целом.

Применяется достаточно широко при производстве средств вооружения и военной техники, а также при производстве товаров народного потребления. Менее известен пример по членению технологии при изготовлении денег; например, на фабрике Гознака.

Страхование как метод защиты информации пока еще только получает признание. Сущность его сводится к тому, чтобы защитить права и интересы собственника информации или средства информации как от традиционных угроз (кражи, стихийные бедствия), так и от угроз безопасности информации, а именно: защита информации от утечки, хищения, модификации (подделки), разрушения и др.

Страховые методы защиты информации применяются, прежде всего, для защиты коммерческих секретов от промышленного шпионажа. Особенно страховые методы эффективны в независимом секторе экономики, где административные методы и формы управления, а особенно контроля, плохо применимы.

При страховании информации должно быть проведено аудиторское обследование и дано заключение о сведениях, которые предприятие будет защищать как коммерческую тайну, надежность средств защиты.

Морально-нравственные методы защиты информации можно отнести к группе тех методов, которые, исходя из известного выражения, что «тайну хранят не замки, а люди», играют очень важную роль в защите информации. Именно человек, сотрудник предприятия или учреждения, допущенный к секретам и накапливающий в своей памяти колоссальные объемы информации, в том числе секретной, нередко становится источником утечки этой информации, или по его вине соперник получает возможность несанкционированного доступа к носителям защищаемой информации.

Морально-нравственные методы защиты информации предполагают проведение специальной работы с сотрудником, направленной на формирование у него системы определенных качеств, взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично), а также обучение сотрудника, осведомленного в сведениях, составляющих охраняемую тайну, правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Учет – также один из важнейших методов защиты информации, обеспечивающий возможность получения в любое время данных о любом носителе защищаемой информации, о количестве и местонахождении всех носителей засекреченной информации, а также данные о всех пользовате-

лях этой информации. Без учета решать проблемы было бы невозможно, особенно когда количество носителей превысит какой-то минимальный объем.

Кодирование – метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации. Он заключается в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи, направлении письменного сообщения, когда есть угроза, что оно может попасть в руки соперника, а также при обработке и хранении информации в СВТ.

Шифрование – метод защиты информации, используемый чаще при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником. Шифрование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если перехвативший не имеет сведений (ключа) для раскрытия шифра.

12.2. Средства защиты информации

Средства защиты информации – это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В качестве основания классификации средств защиты информации перечислим основные группы задач, решаемые с помощью технических средств:

1) создание физических (механических) препятствий на путях проникновения злоумышленника к носителям информации (решетки, сейфы, замки и т. д.);

2) выявление попыток проникновения на объект охраны, к местам сосредоточения носителей защищаемой информации (электронные и электронно-оптические сигнализаторы);

3) предупреждение о возникновении чрезвычайных ситуаций (пожар, наводнение и т. п.) и ликвидация чрезвычайных происшествий (средства пожаротушения и т. д.);

4) поддержание связи с различными подразделениями, помещениями и другими точками объекта охраны;

5) нейтрализация, поглощение или отражение излучения эксплуатируемых или испытываемых изделий (экраны, защитные фильтры, разделительные устройства в сетях электроснабжения и т. п.);

6) введение технических разведок в заблуждение (дезинформация) относительно истинной дислокации объекта защиты и его функционального назначения;

7) комплексная проверка технического средства обработки информации и выделенного помещения на соответствие требованиям безопасности обрабатываемой речевой информации установленным нормам;

8) комплексная защита информации в автоматизированных системах обработки данных с помощью фильтров, электронных замков и ключей в целях предотвращения несанкционированного доступа, копирования или искажения информации.

Рекомендуемые источники и литература

1. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.

2. Герасименко, В.А. Основы защиты информации: учебник / В.А. Герасименко, А.А. Малюк. – М., 1997. – 538 с.

3. Романов, О.А. Организационное обеспечение информационной безопасности: учебник / О.А. Романов, С.А. Бабин, С.Г. Жданов. – М.: Издательский центр «Академия», 2008. – 240 с.

4. Служба защиты информации предприятия. Что она из себя представляет и как ее организовать. – http://www.spektrsec.ru/sluzhba-zaschityi-informatsii-predpriyatiya.-chto-ona-iz-sebya-predstavlyaet-i-kak-ee-organizovat.html – Загл. с экрана.

5. Организационно-правовое обеспечение информационной безопасности: учебное пособие / А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др.; под ред. А.А. Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.

6. Шиверский, А.А. Защита информации: проблемы теории и практики / А.А. Шиверский. – М.: Юристъ, 1996. – 112 с.

7. Торокин, А.А. Инженерно-техническая защита информации / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

8. Информационная безопасность и защита информации: учеб. пособие / В. П. Мельников и др.; под ред. С. А. Клейменова. – М.: Академия, 2009. –330 с.

9. Гришина, Н.В. Организация комплексной системы защиты информации / Н.В. Гришина. – М.: Гелиос АРВ, 2007. –256 с.

10. Тихонов, В.А. Информационная безопасность: организационные, правовые и технические аспекты / В.А. Тихонов, В.В. Райх. – М.: Гелиос АРВ, 2006. – 516 с.

Тема 13. Ресурсное обеспечение защиты информации

13.1. Кадровые ресурсы.

13.2. Материальные и информационные ресурсы.

13.3. Финансовые ресурсы

13.1. Кадровые ресурсы

В систему кадрового обеспечения защиты информации, составляющей государственную тайну, входят:

1) руководители предприятий и структурных подразделений;

2) специальные комиссии по защите информации;

3) специализированные подразделения, входящие в состав единой службы безопасности, или существующие отдельно:

- первый (секретный) отдел;
- отдел режима;
- сектор анализа;
- третий отдел;
- подразделение ВОХР (военизированной охраны);
- подразделение ПД ИТР (противодействия иностранным техническим разведкам).

В систему кадрового обеспечения защиты информации, составляющей другие виды тайн, входят:

1. руководители предприятий и структурных подразделений.
2. специальные комиссии по защите информации.
3. служба безопасности.

Руководители предприятий и структурных подразделений, администрация организаций, ведущих работы по защите государственной (коммерческой, служебной, профессиональной) тайны, персональных данных:

- несут ответственность за обеспечение надлежащего режима секретности (конфиденциальности) проводимых работ, за своевременную разработку и осуществление необходимых мероприятий по сохранению тайн;
- издают приказы, распоряжения, положения, инструкции и другие документы, регламентирующие режим секретности (конфиденциальности) проводимых работ с учетом специфики работы предприятия;
- осуществляют качественный подбор и специальную подготовку кадров, которым поручается выполнение секретных работ;
- создают на производственных участках необходимые условия для строгого выполнения сотрудниками установленных требований режима секретности (конфиденциальности);

- постоянно контролируют соблюдение работниками требований действующего законодательства и руководящих документов предприятия по обеспечению режима секретности (конфиденциальности);
- принимают решения об отстранении от секретных работ лиц, нарушивших требования режима секретности (конфиденциальности), допустивших аморальные поступки;
- имеют право лишать отдельных работников полностью или частично премий за нарушение режима секретности (конфиденциальности), рассматривая такие нарушения как производственные упущения;
- организуют воспитательно-профилактическую работу среди сотрудников по разъяснению им требований режима секретности (конфиденциальности);
- организуют и проводят работы по предупреждению утечки секретных (конфиденциальных) сведений в прессе, научной, производственной и административно-хозяйственной деятельности предприятия на основе аналитических исследований, главной задачей которых является выявление и локализация слабых мест в защите секретов.

Постоянно действующая техническая комиссия (ПДТК) изучает все стороны деятельности организации и вырабатывает рекомендации руководителям по управлению системой защиты в организации; выявлению и закрытию возможных каналов неправомерного распространения защищаемой информации, организации и координации работ по ПД ИТР и технической защите информации, физической защите объекта и др.

В состав ПДТК включаются специалисты по защите гостайны, ПД ИТР и технической защите информации, специалисты профильных структурных подразделений организации. Возглавляет ПДТК один из заместителей руководителя организации.

Для защиты коммерческой и других видов тайны в организации создается подобная комиссия, но она может иметь другое наименование, например – постоянно действующая экспертная комиссия (ПДЭК). ПДЭК создается приказом руководителя предприятия и должна работать на постоянной основе с заменой в необходимых случаях отдельных ее членов.

Задачами такой комиссии должны быть:

- разработка перечней сведений, составляющих коммерческую и служебную тайну;
- разработка перечней издаваемых предприятием конфиденциальных документов;
- снижение или снятие степени конфиденциальности сведений и грифа конфиденциальности документов;
- разработка Положения о системе доступа к конфиденциальным документам;

- экспертиза ценности конфиденциальных документов с целью установления сроков их хранения и отбора документов на основе этих сроков для архивного хранения и уничтожения;
- проведение аналитической работы по предотвращению утечки и утраты конфиденциальной информации.

Учитывая важность задач ПДЭК, в ее состав следует включать высококвалифицированных сотрудников, в первую очередь руководителей подразделений, имеющих доступ к конфиденциальной информации.

Кроме того, в состав комиссии должны входить руководитель службы безопасности предприятия и руководитель подразделения конфиденциального делопроизводства, а также руководитель архива предприятия (при наличии архива).

Председателем комиссии необходимо назначать одного из заместителей руководителя предприятия, допущенного ко всем конфиденциальным документам.

Квалификационные характеристики работников режимно-секретных органов (РСО) Министерств, ведомств, учреждений, предприятий и организаций Российской Федерации были утверждены Постановлением Минтруда №37 от 21.08.1998 г. Они призваны способствовать правильному решению вопросов подбора и расстановки кадров, повышения их деловой квалификации, разделения труда между руководителями и специалистами, а также обеспечения единства в определении должностных обязанностей этих категорий работников. Наименования должностей руководителей, специалистов и других работников режимно-секретных органов установлены в соответствии с классификатором профессий рабочих и должностей служащих (начальник, специалист, инженер, инспектор и др):

- начальник первого отдела;
- инженер первого отдела;
- инспектор первого отдела;
- начальник отдела (бюро) режима;
- начальник отдела комплексной защиты информации;
- главный специалист по комплексной защите информации;
- инженер по комплексной защите информации и т. д.

Квалификационные характеристики работников РСО распространяются на работников подразделений безопасности предприятий (организаций).

Укомплектование штатов названных структурных подразделений по защите информации в настоящее время осуществляется из числа выпускников направления «Информационная безопасность»: 090900 – Информационная безопасность (Бакалавриат); 090303 – Информационная безопасность автоматизированных систем, 090915 – Безопасность информационных технологий в правоохранительной сфере (специалитет) и др.

Выпускники бакалавриата получают квалификацию «бакалавр», специальностей – «специалист по защите информации».

Кроме высшего профессионального образования, в России развивается система повышения квалификации и переподготовки кадров по различным направлениям защиты информации.

13.2. Материальные и информационные ресурсы

Как любая деятельность, деятельность по защите информации, кроме кадрового обеспечения, нуждается в обеспечении другими ресурсами: материальными, финансовыми и информационными.

Материальные ресурсы для защиты информации имеют специфические особенности, по сравнению с другими функциональными направлениями деятельности предприятия. К ним относятся: специальные выделенные помещения, специальное оборудование, компьютерная и оргтехника, аттестованные в соответствии с принятыми нормами, аппаратные средства, программные средства и комплексы, средства защиты информации и др.

Информационные ресурсы – это информация, на основе которой принимаются оптимальные управленческие решения по защите информации на предприятии. К ним относится:

- правовая информация (нормативная база по проблемам безопасности);
- коммерческая информация (информация о предприятиях и производимых ими продуктах и услугах в области информационной безопасности);
- научно-техническая информация (информация о государственной политике безопасности в России и зарубежных странах, теоретических, методологических и технических проблемах информационной безопасности и т. д.);
- информация о производственно-технологических процессах на предприятии;
- аналитическая информация, полученная в результате информационно-аналитической деятельности, о состоянии информационной безопасности предприятия, угроз информационной безопасности и т. д.

Важнейшим информационным ресурсом защиты информации является аналитическая информация.

Аналитическая работа является неотъемлемой составной частью всей работы по предупреждению утечки защищаемой информации. Под аналитическим исследованием понимается процесс детального и всестороннего исследования особенностей, условий и обстоятельств прохождения, обращения, использования и надежности обеспечения сохранности всех видов защищаемой информации с целью выявления и устранения всех возможностей ее утечки.

Виды аналитических исследований (АИ):

1) АИ, связанные с составлением и уточнением перечня сведений, подлежащих защите;

2) АИ, проводимые в целях принятия решения о необходимости разработки и внедрения дополнительных режимных мероприятий перед началом новых работ или в связи с изменением оперативной обстановки;

3) АИ фактической эффективности и надежности мер по защите сведений, отнесенных к тому или иному виду тайн, при проведении конкретных работ со сведениями, составляющими тот или иной вид тайны, по конкретной теме НИОКР, проблеме, заказу, конкретному проекту и т. п.;

4) АИ тех сторон деятельности предприятия, которые имеют существенное значение для обеспеченности сохранности защищаемых сведений (анализ открытых публикаций, транспортировки спецпродукции, приема командированных лиц, осуществления международных связей и т. д.).

Аналитической работой по выявлению и предупреждению возможной утечки охраняемой в интересах государства информации начали заниматься в Советском Союзе в первой половине 60-х годов. Первые штатные аналитические подразделения появились в 1968 году в Министерстве среднего машиностроения (МСМ). На предприятиях, подведомственных министерству, были созданы аналитические службы, которые получили название «специальные научно-технические подразделения» (СНТП).

Информационно-аналитическое обеспечение безопасности бизнеса предназначено для выявления угроз и минимизации предпринимательских рисков. Экономическое благополучие предприятия во многом обеспечивается хорошо организованной системой сбора деловой информации, ее своевременной обработкой и распределением.

Информационно-аналитическая деятельность осуществляется самостоятельными службами, например, Службой деловой разведки (ДР), являющейся составляющей частью системы экономической безопасности. Основными задачами такой службы являются:

- сбор и оперативное использование информации по гражданскому, уголовному и хозяйственному законодательству;
- подготовка и анализ заключаемых договоров, а также подготовка рекомендаций по вопросам правовой защиты от противоправных действий;
- работы с вкладчиками, акционерами, финансовыми брокерами и дилерами с использованием методов деловой разведки;
- подготовка и проведение рекламной кампании;
- разработка мероприятий по участию организации в процессах лоббирования, схем поведения по отношению к политическим партиям и общественным движениям;
- сбор и анализ коммерческой информации, в явном или неявном виде присутствующей в средствах массовой информации;

- анализ процессов и тенденций в инвестиционно-финансовой сфере внутри Федерации и за рубежом;
- сбор информации по конкурирующим фирмам, а также составление психологических портретов их лидеров;
- разработка концепции стратегического развития организации, подготовка, экспертиза и реализация отдельных организационно-финансовых проектов и технологий.

Состав всех ресурсов (материальных, кадровых, информационных) определяется в процессе экономического обоснования затрат на защиту информации на предприятии, поэтому остановимся на этом подробнее.

13.3. Финансовые ресурсы

Практическая работа по проектированию, созданию и сопровождению системы защиты информации невозможна без экономического обоснования затрат на их реализацию. Является фактом, что данная работа осуществляется в сложных условиях, при этом факторами сложности являются: конкуренция в области безопасности (часто недобросовестная), желание Подрядчика получить большую выгоду с минимальными затратами, некачественное выполнение работ по безопасности и другие.

Показателем зрелости руководства хозяйствующего субъекта по отношению к вопросам безопасности является проведение сравнительного анализа затрат, понесенных хозяйствующим субъектом на обеспечение безопасности в сравнении с эффектом (техническим, экономическим, организационным и прочим), полученным от реализации мероприятий безопасности. Таким образом, необходимым процессом в современной управленческой деятельности является оценка эффективности и оптимизация затрат на реализацию мероприятий по защите информации.

По оценкам экспертов, для обеспечения своей информационной безопасности организация должна иметь специальное структурное подразделение по обеспечению информационной безопасности и в среднем ежемесячно затрачивать на обеспечение его функционирования 15–20 % от получаемой ежемесячно прибыли.

Систематические затраты на обслуживание системы безопасности (затраты на предупредительные мероприятия) можно разбить на следующие группы:

1. Управление системой защиты информации:

- затраты на планирование системы защиты информации предприятия;
- затраты на изучение возможностей информационной инфраструктуры предприятия по обеспечению безопасности информации ограниченного распространения;

- затраты на осуществление технической поддержки производственного персонала при внедрении средств защиты и процедур, а также планов по защите информации;
- проверка сотрудников на лояльность, выявление угроз безопасности;
- организация системы допуска исполнителей и сотрудников конфиденциального делопроизводства с соответствующими штатами и оргтехникой.

2. Регламентное обслуживание средств защиты информации:

- затраты, связанные с обслуживанием и настройкой программно-технических средств защиты, операционных систем и используемого сетевого оборудования;
- затраты, связанные с организацией сетевого взаимодействия и безопасного использования информационных систем;
- затраты на поддержание системы резервного копирования и ведение архива данных;
- проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, средств вычислительной техники и другого оборудования.

3. Аудит системы безопасности:

- затраты на контроль изменений состояния информационной среды предприятия;
- затраты на систему контроля за действиями исполнителей.

4. Обеспечение должного качества информационных технологий:

- затраты на обеспечение соответствия требованиям качества информационных технологий, в том числе анализ возможных негативных аспектов информационных технологий, которые влияют на целостность и доступность информации;
- затраты на доставку (обмен) конфиденциальной информации;
- удовлетворение субъективных требований пользователей: стиль, удобство интерфейсов и др.

5. Обеспечение требований стандартов:

- Затраты на обеспечение соответствия принятым стандартам и требованиям, достоверности информации, эффективности средств защиты.

6. Обучение персонала:

- повышение квалификации сотрудников предприятия в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности;
- развитие нормативной базы службы безопасности.

7. Затраты на контроль:

- плановые проверки и испытания;

- затраты на проверки и испытания программно-технических средств защиты информации;
- затраты на проверку навыков эксплуатации средств защиты персоналом предприятия;
- затраты на обеспечение работы лиц, ответственных за реализацию конкретных процедур безопасности по подразделениям;
- оплата работ по контролю правильности ввода данных в прикладные системы;
- оплата инспекторов по контролю требований, предъявляемых к защитным средствам при разработке любых систем (контроль выполняется на стадии проектирования и спецификации требований).

8. Внеплановые проверки и испытания:

- оплата работы испытательного персонала специализированных организаций;
- обеспечение испытательного персонала (внутреннего и внешнего) материально-техническими средствами.

9. Контроль за соблюдением политики ИБ:

- затраты на контроль реализации функций, обеспечивающих управление защитой коммерческой тайны;
- затраты на организацию временного взаимодействия и координации между подразделениями для решения повседневных конкретных задач;
- затраты на проведение аудита безопасности по каждой автоматизированной информационной системе, выделенной в информационной среде предприятия;
- материально-техническое обеспечение системы контроля доступа к объектам и ресурсам предприятия.

10. Затраты на внешний аудит:

- затраты на контрольно-проверочные мероприятия, связанные с лицензионно-разрешительной деятельностью в сфере защиты информации.

11. Пересмотр политики информационной безопасности предприятия (проводится периодически):

- затраты на идентификацию угроз безопасности;
- затраты на поиск уязвимостей системы защиты информации;
- оплата работы специалистов-аналитиков, выполняющих работы по определению возможного ущерба и переоценке степени риска.

12. Затраты на ликвидацию последствий нарушения режима ИБ:

- восстановление системы безопасности до соответствия требованиям политики безопасности;
- установка последних версий программных средств защиты информации;
- приобретение технических средств, взамен пришедших в негодность;

- проведение дополнительных испытаний и проверок технологических информационных систем;
- затраты на утилизацию скомпрометированных ресурсов.

13. Восстановление информационных ресурсов предприятия:

- затраты на восстановление баз данных и прочих информационных массивов;
- затраты на проведение мероприятий по контролю достоверности данных, подвергшихся атаке на целостность.

14. Затраты на выявление причин нарушения политики безопасности:

- затраты на проведение расследований нарушений политики безопасности (сбор данных о способах совершения, механизме и способах сокрытия неправомерного деяния, поиск следов, орудий и предметов посягательства; выявление мотивов неправомерных действий и др.);
- затраты на обновление планов обеспечения непрерывности деятельности службы безопасности.

15. Затраты на переделки:

- Затраты на внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности;
- Затраты на повторные проверки и испытания системы защиты информации.

16. Внешние затраты на ликвидацию последствий нарушения политики безопасности:

- обязательства перед государством и партнерами;
- затраты на юридические споры и выплаты компенсаций;
- потери в результате разрыва деловых отношений с партнерами.

17. Потеря новаторства:

- затраты на проведение дополнительных исследований и разработки новой рыночной стратегии;
- отказ от организационных, научно-технических или коммерческих решений, ставших неэффективными в результате утечки сведений и затраты на разработку новых средств ведения конкурентной борьбы;
- потери от снижения приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения.

18. Прочие затраты:

- заработная плата секретарей и служащих, организационные и прочие расходы, которые непосредственно связаны с предупредительными мероприятиями;
- другие виды возможного ущерба предприятию, в том числе связанные с невозможностью выполнения функциональных задач, определенных его Уставом.

Ответственность за сбор и анализ информации по затратам на информационную безопасность несут экономический отдел и служба безопасности предприятия.

В настоящее время российскими производителями разработано программное обеспечение по управлению обеспечением (в том числе, финансовым) информационной безопасности: программные комплексы компании Digital Security, Программный комплекс Гриф, Система Кондор, Специализированная сметная программа «X-Link» и др.

Рекомендуемые источники и литература

1. Алавердов, А.Р. Управление кадровой безопасностью организации / А.Р. Алавердов. – М.: Маркет ДС, 2008. – 176 с.
2. Астахов, А.М. Искусство управления информационными рисками / А.М. Астахов. – М.: ДМК, 2010. – 312 с.
3. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.
4. Баяндин, Н.И. Основы деловой разведки / Н.И. Баяндин; под ред. Л.М. Кунбутаева. – М.: Изд. МЭИ, 2005. – 320 с.
5. Официальный сайт фирмы Digital Security. – http://www.dsec.ru – Загл. с экрана.
6. Самоукина, Н.В. Незаменимый сотрудник и кадровая безопасность / Н.В. Самоукина. – М.: Вершина, 2008. – 176 с.
7. Северин, В.А. Правовое обеспечение информационной безопасности предприятия: учебно-практическое пособие / В.А. Северин. – М.: Городец, 2000. – 192 с.
8. Управление рисками: обзор употребительных подходов / В.А. Галатенко – http://www.citforum.ru/security/articles/ risk_management/ – Загл. с экрана.
9. Что такое кадровая безопасность компании? – http://www.it2b.ru/ it2b3.view2.page32.html. – Загл. с экрана.
10. Управление безопасностью: учеб. пособие / Л.П. Гончаренко, Е.С. Куценко; Рос. экон. акад. им. Г.В. Плеханова. – М.: КноРус, 2010. – 272 с.
11. Основы управления информационной безопасностью: учебное пособие / А.П. Курило, Н.Г. Милославская , М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2014. – 244 с.
12. Милославская, Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2014. – 166 с.

13. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2013. – 214 с.

14. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2014. – 170 с.

15. Милославская, Н.Г. Управление рисками информационной безопасности: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И.Толстой. – М.: Горячая линия – Телеком, 2014. – 130 с.

16. Войтик, А.В. Экономика информационной безопасности / А.В. Войтик, В.Г. Прожерин. – СПБ.: ИТМО, 2012. –120 с.

17. Блюмин, А.М. Мировые информационные ресурсы: учеб. пособие для вузов в области мировых информ. ресурсов / А.М. Блюмин, Н.А. Феоктистов; Ин-т гос. упр., права и инновацион. технологий. – М.: Дашков и К°, 2011. – 295 с.

Тема 14. Создание системы защиты информации в организации

14.1. Этапы создания системы защиты информации.
14.2. Классификация организационно-технологических мероприятий по защите информации.
14.3. Общие требования к системе защиты информации.

14.1. Этапы создания системы защиты информации

Организация работ по созданию и эксплуатации объектов защиты информации отражается в разрабатываемом на предприятии «Руководстве по защите информации» или в «Политике информационной безопасности».

Выделяются следующие стадии создания системы защиты информации (СЗИ):

1. Предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание.

2. Стадия проектирования (разработки проектов) и реализации объекта информатизации, включающая разработку СЗИ в составе объекта информатизации.

3. Стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также ат-

тестацию объекта информатизации на соответствие требованиям безопасности информации.

Каждая стадия предполагает создание ряда документов.

1. Предпроектное обследование.

- аналитическое обоснование необходимости создания СЗИ;
- техническое (частное техническое) задание на разработку СЗИ;
- акт классификации автоматизированной системы обработки информации.

2. На стадии проектирования и создания объекта информатизации и СЗИ в его составе на основе предъявляемых требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:

- разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) объекта информатизации в соответствии с требованиями технического (частного технического) задания на разработку СЗИ;
- разработка раздела технического проекта на объект информатизации в части защиты информации;
- строительно-монтажные работы в соответствии с проектной документацией, утвержденной заказчиком, размещением и монтажом технических средств и систем;
- разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации, либо их сертификация;
- закупка сертифицированных технических, программных и программно-технических (в т.ч. криптографических) средств защиты информации и их установка;
- разработка (доработка) или закупка и последующая сертификация по требованиям безопасности информации программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные программные средства;
- организация охраны и физической защиты помещений объекта информатизации, исключающих несанкционированный доступ к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;
- разработка и реализация разрешительной системы доступа пользователей и эксплуатационного персонала к обрабатываемой (обсуждаемой) на объекте информатизации информации;
- определение заказчиком подразделений и лиц, ответственных за эксплуатацию средств и мер защиты информации, обучение назначенных

лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации;

- выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;
- разработка эксплуатационной документации на объект информатизации и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);
- выполнение других мероприятий, специфичных для конкретных объектов информатизации и направлений защиты информации.

Задание на проектирование оформляется отдельным документом, согласовывается с проектной организацией, службой (специалистом) безопасности предприятия-заказчика в части достаточности мер по технической защите информации и утверждается заказчиком.

На стадии проектирования и создания объекта информатизации оформляются также технический (техно-рабочий) проект и эксплуатационная документация СЗИ, состоящие:

- из пояснительной записки с изложением решений по комплексу организационных мер и программно-техническим (в том числе криптографическим) средствам обеспечения безопасности информации, состава средств защиты информации с указанием их соответствия требованиям ТЗ;
- описания технического, программного, информационного обеспечения и технологии обработки (передачи) информации;
- плана организационно-технических мероприятий по подготовке объекта информатизации к внедрению средств и мер защиты информации;
- технического паспорта объекта информатизации;
- инструкций и руководств по эксплуатации технических и программных средств защиты для пользователей, администраторов системы, а также для работников службы защиты информации.

3. На стадии ввода в действие объекта информатизации и СЗИ осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком (поставщиком) и заказчиком;
- аттестация объекта информатизации по требованиям безопасности информации.

На этой стадии оформляются:

- акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний;
- предъявительский акт к проведению аттестационных испытаний;
- заключение по результатам аттестационных испытаний.

При положительных результатах аттестации на объект информатизации оформляется «Аттестат соответствия» требованиям по безопасности информации.

Кроме вышеуказанной документации в учреждении (на предприятии) оформляются приказы, указания и решения:

- о проектировании объекта информатизации, создании соответствующих подразделений разработки и назначении ответственных исполнителей;
- о формировании группы обследования и назначении ее руководителя;
- о заключении соответствующих договоров на проведение работ;
- о назначении лиц, ответственных за эксплуатацию объекта информатизации;
- о начале обработки в АС (обсуждения в защищаемом помещении) конфиденциальной информации.

14.2. Классификация организационно-технологических мероприятий по защите информации

К мероприятиям по защите информации относятся:

1. Лицензирование деятельности предприятий в области защиты информации.
2. Аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности.
3. Сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам.
4. Категорирование вооружения и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной, экономической, политической, научно-технической и других сферах деятельности.
5. Обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений.
6. Оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов (перехват информации, подлежащей защите), расположенных на территории России.
7. Введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите.

8. Создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

9. Разработка и внедрение технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи.

10. Разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование.

11. Применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам электросвязи.

12. Аудит (контроль) состояния защиты информации – это специальная проверка организации и эффективности защиты информации установленным требованиям и/или нормам.

К контрольным мероприятиям относятся:

1. Аттестация объектов информатизации по требованиям безопасности информации:

- аттестация автоматизированных систем, средств связи, обработки и передачи информации;
- аттестация помещений, предназначенных для ведения секретных и конфиденциальных переговоров;
- аттестация технических средств, установленных в выделенных помещениях.

Сертификат соответствия (далее – сертификат) – документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям;

Сертификация продукции (далее – сертификация) – это деятельность по подтверждению соответствия продукции установленным требованиям.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России. Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленными в «Аттестате соответствия».

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации:

- от несанкционированного доступа, в том числе от компьютерных вирусов;
- от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие);
- от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

2. Контроль защищенности информации ограниченного доступа:

- выявление технических каналов утечки информации и способов несанкционированного доступа к ней;
- контроль эффективности применяемых средств защиты информации.

3. Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок (ПЭМИН):

- персональные ЭВМ, средства связи и обработки информации;
- локальные вычислительные системы;
- оформление результатов исследований в соответствии с требованиями ФСТЭК РФ.

4. Проектирование объектов в защищенном исполнении:

- разработка концепции информационной безопасности;
- проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении;
- проектирование помещений, предназначенных для ведения секретных и конфиденциальных переговоров.

14.3. Общие требования к системе защиты информации

Наиболее общими требованиями к системе защиты информации являются следующие.

1. Система защиты информации должна быть представлена как нечто целое. Целостность системы будет выражаться в наличии: единой цели ее функционирования, информационных связей между элементами системы,

иерархичность построения подсистемы управления системой защиты информации. Ни одна ее часть не может быть изъята без ущерба для всей системы.

2. Система защиты информации должна обеспечивать:

- безопасность информации,
- средств информации,
- защиту интересов участников информационных отношений.

3. Система защиты информации должна обеспечивать информационные связи внутри системы между ее элементами, обеспечивающие их согласованное функционирование, и связи с внешней средой, перед которой система проявляет свою целостность и выступает как единое целое.

4. Система защиты информации должна охватывать весь технологический комплекс информационной деятельности.

5. Система защиты информации быть разнообразной по используемым средствам, многоуровневой с иерархической последовательностью доступа.

6. Система защиты информации должна быть открытой для изменения и дополнения мер обеспечения безопасности информации.

7. Система защиты информации должна быть нестандартной. При выборе средств защиты нельзя рассчитывать на неосведомленность злоумышленников относительно ее возможностей.

8. Система защиты информации должна быть простой для технического обслуживания и удобной для эксплуатации пользователями.

9. Система защиты информации должна быть надежной. Любые поломки технических средств являются причиной появления неконтролируемых каналов утечки информации.

Комплексная система защиты информации (КСЗИ) – это совокупность сил, средств, методов и мероприятий, используемых во взаимодействии и дополнении друг друга и предназначенных для обеспечения на регулярной основе и на заданном уровне защиты информации на этом объекте.

Рекомендуемые источники и литература

1. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: конспект лекций / Л.В. Астахова. – Челябинск, 2006. – 361 с.

2. Бардаев, Э.А. Документоведение: учебник / Э.А. Бардаев, В.Б. Кравченко. – М.: Издательский центр «Академия», 2008. – 304 с.

3. Грибунин, В.Г. Комплексная система защиты информации на предприятии / В.Г. Грибунин, В.В. Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.

4. Петренко, С. Информационная безопасность: экономические аспекты / С. Петренко, С. Симонов, Р. Кислов. – http://www.citforum.ru/security/articles/ sec/index.shtml – Загл. с экрана.

5. Курило, А.П. Аудит информационной безопасности / А.П. Курило, С.Л. Зефиров; под общ. ред. А. П. Курило. – М.: БДЦ-пресс, 2006. – 304 с.

6. Пора заняться аудитом / С. Баричев. – http://www.cio-world.ru/offline/2004/32/37225// – Загл. с экрана.

7. Семенов, А.Н. Методы аудита информационной безопасности / А.Н. Семенов. – М.: Гардарика, 2003.

8. Гришина, Н.В. Комплексная система защиты информации на предприятии: учеб. пособие для вузов / Н.В. Гришина. – М.: Форум, 2011. – 238 с.

ЗАКЛЮЧЕНИЕ

В данном учебном пособии рассмотрены основы теории информационной безопасности и методологии защиты информации.

В первом разделе освещены базовые понятия в области информационной безопасности, их соотношения друг с другом, организация системы обеспечения информационной безопасности в России, вопросы государственной политики в области информационной безопасности Российской Федерации**.** Второй раздел посвящен информации как предмету и объекту защиты: понятию защищаемой информации, критериям отнесения информации ограниченного доступа и общедоступной информации к защищаемой. Особое внимание уделено видам защищаемой информации ограниченного доступа, к которым относятся государственная тайна, служебная тайна, коммерческая тайна, профессиональная тайна, персональные данные, объекты интеллектуальной собственности. Третий раздел включает в себя вопросы понятия и классификации угроз защищаемой информации. В ней уделено внимание видам и способам дестабилизирующего воздействия на защищаемую информацию со стороны разных источников: людей; технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи; систем обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации; технологических процессов отдельных промышленных объектов; природных явлений. Отдельно освещены каналы и методы несанкционированного доступа к конфиденциальной информации. Четвертый раздел характеризует методологию защиты информации: виды, методы, средства защиты информации, ее ресурсное обеспечение, ключевые моменты создания комплексной системы защиты информации.

СПИСОК ИСТОЧНИКОВ И РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Источники

1. ISO/IEC 27006:2007 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью. – М.: Изд-во стандартов, 2007.

2. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005). – М.: Изд-во стандартов, 2005.

3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2006.

4. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. – М.: Изд-во стандартов, 2000.

5. ГОСТ Р ИСО/МЭК 15408-1-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. – М.: Изд-во стандартов, 2002.

6. ГОСТ Р ИСО/МЭК 15408-2-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – М.: Изд-во стандартов, 2002.

7. ГОСТ Р ИСО/МЭК 15408-3-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Требования доверия к безопасности. – М.: Изд-во стандартов, 2002.

8. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью. – М.: Изд-во стандартов, 2005.

9. Гражданский кодекс Российской Федерации. Часть вторая: Кодекс Рос. Федерации от 26 янв. 1996 г. № 14-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 22 дек. 1995 г.: Ввод. Федер. законом Рос. Федерации от 26 янв. 1996 г. № 15-ФЗ // Рос. газ. – 1996. – 6–8, 10 февр.

10. Гражданский кодекс Российской Федерации. Часть четвертая: Кодекс Рос. Федерации от 18 декабря 2006 г. № 230-ФЗ // Рос. газ. – 2006. – 22 дек.

11. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 09 сентября 2000 г. – М., 2000.

12. Конституция Российской Федерации: Конституция: Принята всенар. голосованием 12 дек. 1993 г. // Рос. газ. – 1993. – 25 дек.

13. Концепция защиты государственной тайны от 17 июня 1998 г.

14. Концепция национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 10 января 2000 г. № 24 // СЗ РФ. – 2000. – № 2. – ст. 170.

15. Об авторском праве и смежных правах: Закон Рос. Федерации от 9 июля 1993 г. № 5351-I // Рос. газ. – 1993. – 3 авг.

16. О банках и банковской деятельности в РСФСР: Закон Рос. Совет. Федератив. Социалист. Респ. от 2 дек. 1990 г. № 395-I // Рос. газ. – 1990. – 11 дек.

17. О безопасности: Закон Рос. Федерации от 5 марта 1992 г. № 2446-I // Рос. газ. – 1992. – 6 мая.

18. Об информации, информатизации и защите информации: Федер. закон Рос. Федерации от 20 февр. 1995 г. № 24-ФЗ // Рос. газ. – 1995. – 22 февр.

19. Об информации, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 24-ФЗ // Рос. газ. – 2006. – 29 июля.

20. Об оперативно-розыскной деятельности: Федер. закон Рос. Федерации от 12 авг. 1995 г. № 144-ФЗ // Рос. газ. – 1995. – 18 авг.

21. Об утверждении перечня сведений конфиденциального характера: Указ Президента Рос. Федерации от 6 марта 1997 г. № 188 // Рос. газ. – 1997. – 14 марта.

22. Об участии в международном информационном обмене: Федер. закон Рос. Федерации от 4 июля 1996 г. № 85-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 5 июня 1996 г. // Рос. газ. – 1996. – 11 июля.

23. О внесении изменений и дополнений в Закон Российской Федерации «О государственной тайне»: Федер. закон Рос. Федерации от 6 окт. 1997 г. № 131-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 19 сент. 1997 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 24 сент. 1997 г. // Рос. газ. – 1997. – 9 окт.

24. О внешней разведке: Федер. закон Рос. Федерации от 10 янв. 1996 г. № 5-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 8 дек. 1995 г. // Рос. газ. – 1996. – 17 янв.

25. О государственной тайне: Закон Рос. Федерации от 21 июля 1993 г. № 5485-I // Рос. газ. – 1993. – 21 сент.

26. О коммерческой тайне: Федер. закон Рос. Федерации от 29 июля 2004 г. № 98-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 9 июля 2004 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 15 июля 2004 г. // Рос. газ. – 2004. – 5 авг.

27. О персональных данных: Федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Рос. газ. – 2006. – 29 июля.

28. О служебной тайне и порядке обращения с конфиденциальной информацией в государственных органах и органах местного самоуправления: Проект Федерального закона. – М., 2003.

29. Основы законодательства Российской Федерации об охране здоровья граждан: Основы законодательства Рос. Федерации от 22 июля 1993 г. № 5487-I // Рос. газ. – 1993. – 18 авг.

30. Основы законодательства Российской Федерации о нотариате: Основы законодательства Рос. Федерации от 11 февр. 1993 г. № 4462-I // Рос. газ. – 1993. – 13 марта.

31. О техническом регулировании: Федер. закон Рос. Федерации от 27 дек. 2002 г. № 184-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 15 дек. 2002 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 18 дек. 2002 г. // Рос. газ. – 2002. – 31 дек.

32. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: Постановление правительства РФ от 3 ноября 1994 г. № 1233 // Собр. законодательства Рос.Федерации. – 2005. – № 30 (ч. II), ст. 3165.

33. Профессиональный кодекс нотариусов Российской Федерации, принятый 18 апреля 2001 года (с изм. от 31.03. 2006) // Собрание представителей нотариальных палат субъектов Российской Федерации. – 2006.

34. Трудовой кодекс Российской Федерации: Кодекс Рос. Федерации от 30 дек. 2001 г. № 197-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 21 дек. 2001 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 26 дек. 2001 г. // Рос. газ. – 2001. – 31 дек.

35. Уголовный кодекс Российской Федерации: Кодекс Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: Принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: Одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г.: Ввод. Федер. законом Рос. Федерации от 13 июня 1996 г. № 64-ФЗ // Рос. газ. – 1996. – 25 июня.

Литература

1. Алексенцев, А.И. О классификации конфиденциальной информации по видам тайны / А.И. Алексенцев // Безопасность информационных технологий. – 1999. – № 3.

2. Алексенцев, А.И. О концепции защиты информации / А.И. Алексенцев // Безопасность информационных технологий. – 1998. – № 4.

3. Алексенцев, А.И. О составе защищаемой информации / А.И. Алексенцев // Безопасность информационных технологий. – 1999. – № 2.

4. Алексенцев, А.И. Понятие и назначение комплексной системы защиты информации / А.И. Алексенцев // Вопросы защиты информации. – 1996. – № 2.

5. Алексенцев, А.И. Понятие и структура угроз защищаемой информации / А.И. Алексенцев // Безопасность информационных технологий. – 2000. – №3.

6. Алексенцев, А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» / А.И. Алексенцев // Безопасность информационных технологий. – М., 1999. – № 1.

7. Астахова, Л.В. Информационная безопасность: герменевтический подход: монография/Л.В.Астахова; ВАК, Министерство обороны Российской Федерации и др. – М.: РАН, 2010. – 192 с.

8. Астахова, Л.В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации / Л.В. Астахова // Вестник ЮУрГУ. Серия Компьютерные технологии, управление и радиоэлектроника. – 2013. – Т. 13, №.1. – С. 79–83.

9. Астахова, Л.В. Понятие культуры информационной безопасности / Л.В. Астахова // НТИ. Сер. 1. Орг. и методика информ. работы. – 2014. – № 2. – С.1-8.

10. Бачило, И.Л. Информационное право: учебник / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов; под ред. Б.Н. Топорнина. – СПб.: Юридический центрПресс, 2001. – 787 с.

11. Баяндин, Н.И. Основы деловой разведки / Н.И. Баяндин; под ред. Л.М. Кунбутаева. – М.: Изд. МЭИ, 2005. – 320 с.

12. Галатенко, В.А. Основы информационной безопасности / В.А. Галатенко. – М.: Интернет-университет информационных технологий – ИНТУИТ.ру, 2005. – 358 с.

13. Галатенко, В.А. Стандарты информационной безопасности / В.А. Галатенко. – М.: Интернет-университет информационных технологий. – ИНТУИТ.ру, 2005. – 324 с.

14. Герасименко, В.А. Основы защиты информации: учебник / В.А. Герасименко, А.А. Малюк. – М., 1997. – 538 с.

15. Гришина, Н.В. Комплексная система защиты информации на предприятии: учеб. пособие для вузов по специальностям 090103 «Орг. и технология защиты информ.» и 090104 «Комплекс. защита объектов информ.» / Н.В. Гришина. – М.: Форум, 2011. – 238 с.

16. Доронин, А.И. Бизнес-разведка / А.И. Доронин. – М.: Изд-во «Ось-89», 2003. – 384 с.

17. Основы управления информационной безопасностью: учебное пособие / А.П. Курило, Н.Г. Милославская , М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2014. – 244 с.

18. Левин, В.И. Носители информации в цифровом веке / В.И. Левин.– М.: КомпьютерПресс, 2000. – 256 с.

19. Милославская, Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью: учебное пособие / Н.Г. Милослав-

ская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2014. – 166 с.

20. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2013. – 214 с.

21. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2014. – 170 с.

22. Милославская, Н.Г. Управление рисками информационной безопасности: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2014. – 130 с.

23. Романов, О.А. Организационное обеспечение информационной безопасности: учебник / О.А. Романов, С.А. Бабин, С.Г. Жданов. – М.: Издательский центр «Академия», 2008. – 240 с.

24. Северин, В.А. Правовое обеспечение информационной безопасности предприятия: учебно-практическое пособие / В.А. Северин. – М.: Городец, 2000. – 192 с.

25. Соловьев, Э.Я. Коммерческая тайна и ее защита / Э.Я. Соловьев. – 2-е изд., перераб. и доп.– М.: Ось-89, 2002. – 128 с.

26. Стрельцов, А.А., Горбатов, В.С., Полякова, Т.А. и др. Организационно-правовое обеспечение информационной безопасности: учебное пособие / А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова, и др.; под ред. А.А. Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.

27. Теоретические основы компьютерной безопасности: учеб. пособие для вузов по специальности 090100 «Информационная безопасность» / А.А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М.: Академия, 2009. – 267 с.

28. Тихонов, В.А. Информационная безопасность: организационные, правовые и технические аспекты / В.А. Тихонов, В.В. Райх. – М.: Гелиос АРВ, 2006. – 516 с.

29. Право и информационная безопасность: учебное пособие // Ю.А. Белевская, Ю.А. Глоба, А.Н. Касилов и др.; под ред.А.Л. Фисуна и Ю.А. Белевской. – М.: Приор-издат, 2005. – С. 140.

30. Чумарин, И.Г. Тайна предприятия: что и как защищать / И.Г. Чумарин.– СПб.: ООО «Издательство ДНК», 2001. – 160 с.

31. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.:ДМК ПРЕСС, 2012. – 592 с.

32. Шиверский, А.А. Защита информации: проблемы теории и практики / А.А. Шиверский. – М.: Юристъ, 1996. – 112 с.

ПРИЛОЖЕНИЯ

Приложение 1

Словарь терминов

Аттестация объекта защиты:

– официальное подтверждение органом по сертификации или другим специально уполномоченным органом наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований и норм эффективности защиты информации.

Безопасность информации:

– состояние защищенности информации... от внутренних или внешних угроз;

– состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации [подделки], несанкционированного копирования, блокирования информации и т. п.;

– состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение;

– обеспечение защиты информации от случайного или преднамеренного доступа лиц, не имеющих право на ее получение, раскрытие, модификацию или разрушение;

– защита информации от случайного или преднамеренного доступа лиц, не имеющих на это права, ее получения, раскрытия, модификации или разрушения. реализация требований и правил по защите информации, поддержанию информационных систем в защищенном состоянии, эксплуатация специальных средств защиты и обеспечение организационных и инженерно-технических мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляется службами безопасности информации.

Блокирование информации:

– прекращение или затруднение доступа законных пользователей к информации.

Владелец информации (информационных ресурсов):

– субъект, осуществляющий владение и пользование {информационными ресурсами} и реализующий полномочия распоряжения в пределах, установленных законом;

– субъект, реализующий полномочия владения, пользования и распоряжения {информационными ресурсами} в объеме, устанавливаемом собственником;

– субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;

– субъект информационных отношений, обладающий правом владения, распоряжения и пользования информационным ресурсом по договору с собственником информации;

– юридическое или физическое лицо, которое имеет полномочия владеть, пользоваться и распоряжаться данной информацией по договору с собственником, в силу закона или решения административных органов;

– субъект, в непосредственном ведении которого в соответствии с законом находится информация.

Государственная тайна:

– защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности российской федерации;

– особой важности, совершенно секретные и секретные сведения военного, экономического, политического и иного характера, охраняемые государством.

Гриф конфиденциальности:

– специальная отметка на носителе информации либо в сопроводительных документах на него, свидетельствующая о том, что носитель содержит конфиденциальную информацию.

Гриф секретности:

– реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

– идентифицированный уровень конфиденциальности информации, который должен обеспечиваться в процессе обработки и использования защищаемой информации;

– обозначение на документе (надпись, штамп и др.), определяющее степень секретности содержащихся в нем сведений.

Дезинформация:

– сознательное искажение передаваемых сведений с целью создания ложного представления у лиц, использующих эти сведения; передача ложной информации;

– способ маскировки, заключающийся в преднамеренном распространении ложных сведений об объектах, их составе и деятельности, а также имитации их деятельности в соответствии с этими сведениями;

– один из методов защиты информации, заключающийся в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности, положении дел на предприятии и т. д.

Доступ к информации:

– получение субъектом возможности ознакомления с информацией, в том числе с помощью технических средств;

– ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации;

– право на ознакомление с конкретными сведениями, составляющими государственную или коммерческую тайну, и документами с соответствующим грифом, реализуемое в соответствии с разрешительной системой;

– санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную или коммерческую тайну.

Защита информации:

– деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

– комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т. п.;

– организационные, программные и технические методы и средства, направленные на удовлетворение ограничений, установленных для типов или экземпляров данных в системе обработки данных;

– совокупность мероприятий, обеспечивающих предупреждение несанкционированного доступа к конфиденциальной информации, к охраняемым сведениям промышленного, экономического, торгового, финансового и технологического характера;

– деятельность собственника информации или уполномоченных им лиц по: обеспечению своих прав на владение, распоряжение и управление защищаемой информацией; предотвращению утечки и утраты информации; сохранению полноты, достоверности, целостности защищаемой информации, ее массивов и программ обработки; сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами;

– совокупность мероприятий, обеспечивающих предупреждение разглашения, утечки и несанкционированного доступа к конфиденциальной информации.

Защищаемая информация:

– любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу;

– информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

– сведения, на использование и распространение которых введены ограничения их собственником.

Информационная безопасность:

– состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства;

– способность системы противостоять случайным или преднамеренным внутренним или внешним информационным воздействиям, следствием которых могут быть ее нежелательное состояние или поведение;

– проведение правовых, организационных и инженерно-технических мероприятий при формировании и использовании информационных технологий, инфраструктуры и информационных ресурсов, защите информации высокой значимости и прав субъектов, участвующих в информационной деятельности.

Информация:

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

– совокупность знаний о фактических данных и зависимостях между ними;

– совокупность сведений (данных), циркулирующих в обществе, биологических и технических системах;

– сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), отраженные на материальных носителях, используемые в целях получения знаний и практических решений;

– сведения о лицах, предметах, событиях, явлениях и процессах независимо от формы их представления, используемые в целях получения знаний, принятия решений.

Искажение информации:

– преднамеренное действие по созданию ложной информации в технических средствах ее обработки.

Канал утечки информации:

– такие дестабилизирующие факторы, следствием проявления которых может быть получение (или опасность получения) защищаемой информации лицами или процессами, не имеющих на это законных полномочий;

– варианты технологии несанкционированного доступа к информации;

– физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка охраняемых сведений;

– неконтролируемый физический путь от источника информации за пределы организации или круга лиц, обладающих охраняемыми сведениями, посредством которого возможно неправомерное овладение злоумышленниками конфиденциальной информацией. для образования канала утечки необходимы определенные пространственные, временные и энерге-

тические условия и соответствующие средства приема, накопления и обработки информации на стороне злоумышленников.

Категорирование защищаемой информации:

– установление градации важности защищаемой информации.

Кодирование информации:

– отождествление данных с их кодовыми комбинациями; установление соответствия между элементом данных и совокупностью символов, называемой кодовой комбинацией (словом кода);

– преобразование с помощью кодов открытого текста в условный с целью скрыть от злоумышленника содержание передаваемой по каналам связи информации;

– метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи, направлении письменного сообщения, когда есть угроза, что оно может попасть в руки соперника, а также при обработке и хранении информации в СВТ.

Коммерческая тайна:

– не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам;

– информация составляет ... коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности;

– управленческая, производственная, научно-техническая, финансовая, торговая и иная документированная информация, используемая для достижения целей предпринимательской деятельности, распространение которой может нанести ущерб этой деятельности;

– защищаемые предприятием сведения в области производства, новых технологий, организационной, коммерческой и иной деятельности, имеющие для предприятия действительную или потенциальную коммерческую ценность в силу неизвестности ее другим лицам, раскрытие (утечка, разглашение) которых может нанести ущерб интересам предприятия.

Комплексная система защиты информации:

– система, полно и всесторонне охватывающая все предметы, процессы и факторы, которые обеспечивают безопасность всей защищаемой информации;

– совокупность сил, средств, методов и мероприятий, используемых во взаимодействии и дополнении друг друга и предназначенные для обеспе-

чения на регулярной основе и на заданном уровне защиты информации на этом объекте.

Контроль состояния защиты информации:

– проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации;

– мероприятия, обеспечивающие соблюдение требований по обеспечению защиты информации, проверку состояния и работоспособности всех средств и механизмов системы защиты информации.

Конфиденциальная информация:

– документированная информация, доступ к которой ограничивается в соответствии с законодательством российской федерации;

– информация, требующая защиты;

– служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственником на основе законов о коммерческой, профессиональной [промышленной] тайне, государственной службе и других законодательных актов – требует защиты.

Концепция зашиты информации:

– система взглядов и общих технических требований по защите информации;

– система взглядов, насущность, цели, принципы и организацию защиты информации;

– система взглядов, требований и условий организации защиты охраняемых сведений от разглашения, утечки и несанкционированного доступа к ним через различные каналы.

Лицензирование в области защиты информации:

– деятельность, заключающаяся в передаче или в получении прав на проведение работ в области защиты информации.

Личная тайна:

– защищаемая физическим лицом информация личного характера, распространение которой может нанести моральный или материальный ущерб отдельному физическому лицу.

Математическая защита информации:

– математические и криптографические средства, используемые для кодирования, шифрования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления некоторой специальной информации и ее обратного преобразования.

Мероприятие по защите информации:

– совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

Многоуровневая защита:

– защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности;

– защита, обеспечивающая разграничение доступа к объектам различных уровней конфиденциальности.

Модель защиты:

– абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

Модификация:

– любые изменения, не меняющие сущности объекта.

Нарушитель безопасности информации:

– физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами.

Непреднамеренное воздействие на информацию:

– ошибка пользователя информацией, сбой технических и программных средств информационных систем, а также природное явление или иное нецеленаправленное на изменение информации воздействие, связанное с функционированием технических средств, систем или с деятельностью людей, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированное воздействие на информацию:

– воздействие на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящее к искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированный доступ к информации:

– получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

– доступ к информации, нарушающий правила разграничения доступа...;

– преднамеренное обращение к конфиденциальной информации лицами, не имеющими права доступа к определенным сведениям;

– неправомерный преднамеренный доступ к источникам конфиденциальной информации лицами, не имеющими права доступа к ним. основными способами НСД являются: сотрудничество, выведывание, подслушивание, наблюдение, хищение, копирование, подделка, уничтожение, перехват, фотографирование и др.

Носители информации:

– физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

– материальных объект, предназначенный для хранения данных;

– материальные объекты, в том числе физические поля, в которых, информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, создавая тем самым возможность для ее накопления, хранения, передачи и использования.

Объект защиты:

– информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации;

– информация, технические средства и технология ее обработки, в отношении которых необходимо обеспечить безопасность информации.

Организационная защита информации:

– регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет организационных мероприятий.

Организация защиты информации:

– содержание и порядок действий по обеспечению защиты информации.

Пользователь информации:

– субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею;

– субъект, обращающийся к собственнику или владельцу за получением необходимых ему информационных продуктов... и пользующийся ими;

– субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

– юридическое или фактическое лицо [средство], обладающее полномочиями доступа к конфиденциальной информации;

– субъект, обращающийся к информационной системе, посреднику за получением необходимой ему информации.

Правовая защита информации:

– специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

Программная защита информации:

– система специальных программ, включаемых в состав программного обеспечения, реализующих функции защиты информации.

Разглашение информации:

– несанкционированное доведение защищаемой информации до неконтролируемого количества получателей информации;

– несанкционированное ознакомление с этой информацией лиц, не имеющих законного доступа к ней, лицом, которому эти сведения были доверены или стали известны по службе или работе;

– умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшее к не вызванному служебной необходимостью оглашению охраняемых сведений, а также передача таких сведений по открытым техническим каналам или обработка их на некатегорированных ЭВМ;

– умышленные или неосторожные действия должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по службе или работе, приведшие к ознакомлению с ними лиц, не допущенных к этим сведениям.

Разграничение доступа к информации:

– система мероприятий, обеспечивающих предоставление пользователям только той информации, которая необходима им для выполнения их работы.

Распространение защищаемой информации:

– открытое использование... сведений.

Режим конфиденциальности:

– комплекс мер, обеспечивающих реализацию системы защиты информации на конкретном предприятии, в его структурном подразделении или при выполнении конкретной работы в зависимости от степени секретности или конфиденциальности имеющейся на данном предприятии информации и других факторов, оказывающих влияние на построение системы защиты информации;

– защищенный законодательством страны порядок обеспечения безопасности носителей конфиденциальной информации.

Санкционированный доступ к информации:

– доступ к информации, не нарушающий правила разграничения доступа.

Система защиты информации:

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

– организованная совокупность органов и объектов защиты информации, используемых методов и средств защиты, а также осуществляемых защитных мероприятий;

– организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых)... для решения... выбранной задачи защиты;

– организованная совокупность мероприятий, методов, органов и средств, создаваемых с целью защиты информации.

Служебная тайна:

– информация, относящаяся к деятельности органов государственной власти и управления, предприятий, учреждений, организаций, доступ граждан [субъектов, лиц] к которой ограничивается в интересах обеспечения их функционирования;

– несекретные сведения служебного характера.

Собственник информации [информационных ресурсов]:

– субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения (информационными ресурсами);

– субъект реализующий полномочия владения, пользования, распоряжения (информационными ресурсами) в объеме, устанавливаемом законом;

– субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;

– юридическое или физическое лицо, владеющее информацией в соответствии с законом о собственности;

– субъект информационных отношений, обладающий юридическим правом владения, распоряжения и пользования информационным ресурсом;

– юридическое или физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией.

Способ защиты информации:

– порядок и правила применения определенных принципов и средств защиты информации.

Способы несанкционированного доступа:

– совокупность приемов и порядок действий с целью получения (добывания) охраняемых сведений незаконным, противоправным путем;

– приемы и порядок действий с целью получения [добывания] охраняемых сведений незаконным путем.

Средства защиты информации:

– технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации;

– техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации;

– аппаратные, программные, криптографические и другие средства, предотвращающие несанкционированный доступ к информации;

– ресурсы системы, выделяемые для организации и обеспечения защиты информации;

– совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и техниче-

ских систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации;

– технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную [коммерческую] тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Субъект доступа:

– лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Техническая защита информации:

– совокупность мероприятий и технических средств (механических, оптических, электрических и радиотехнических), обеспечивающих защиту информации.

Угроза безопасности информации:

– мера возможности возникновения такого явления или события, следствием которого могут быть нежелательные воздействия на информацию: нарушение (или опасность нарушения) физической целостности, логической структуры, несанкционированная модификация (или опасность такой модификации) информации, несанкционированное получение (или опасность такого получения) информации, несанкционированное размножение информации;

– потенциально существующая опасность случайного или преднамеренного нарушения безопасности информации, обусловленная особенностями ее хранения и обработки;

– реальные или потенциальные возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации...

Утечка информации:

– неконтролируемое распространение защищаемой информации;

– неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена;

– несанкционированное, неправомерное завладение соперником этой информацией и получение тем самым возможности использования этой информации в своих, в ущерб интересам, собственника [владельца] информации целях;

– бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена по службе или стала известна в процессе работы;

– не контролируемый выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена.

Уязвимость информации:

– событие, возникающее как результат стечения обстоятельств, когда в силу каких-то причин используемые... средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторов и нежелательного их воздействия на защищаемую информацию.

Целостность информации:

– способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

– состояние данных, когда они сохраняют свое информационное содержание и однозначность интерпретации в условиях случайных воздействий;

– неизменность информации в условиях случайных или преднамеренных действий в процессе эксплуатации ИС.

Шифрование информации:

– алгоритмическое (криптографическое) преобразование данных, выполняемое в посимвольном порядке с целью получения шифрованного текста;

– математическое, алгоритмическое (криптографическое) преобразование данных с целью получения шифрованного текста;

– метод защиты информации, используемый чаще при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником. шифрование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если перехвативший не имеет сведений (ключа) для раскрытия шифра.

Эффективность защиты информации:

– степень соответствия результатов защиты информации поставленной цели;

– степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

Приложение 2

Перечень нормативно-правовых актов по информационной безопасности и защите информации

№	Сокращение	Полное наименование	Редакция
1	2	3	4
1	Конституция РФ	«Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993)	с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ
2	ГК РФ	«Гражданский кодекс Российской Федерации (часть вторая)» от 26.01.1996 N 14-ФЗ (ред. от 02.12.2013) «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013)	
3	КоАП	«Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ	ред. от 28.12.2013 (с изм. и доп., вступ. в силу с 21.01.2014)
4	НК РФ	«Налоговый кодекс Российской Федерации (часть первая)» от 31.07.1998 N 146-ФЗ (ред. от 28.12.2013)	
5	СК РФ	«Семейный кодекс Российской Федерации» от 29.12.1995 N 223-ФЗ	ред. от 25.11.2013
6	ТК РФ	«Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ	ред. от 28.12.2013
7	УК РФ	«Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ	ред. от 28.12.2013 (с изм. и доп., вступ. в силу с 21.01.2014)
8	УП №1203	Указ Президента РФ от 30.11.1995 N 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»	ред. от 26.09.2013
9	УП №188	Указ Президента РФ от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера»	ред. от 23.09.2005
10	ФЗ № 3185-1	Закон РФ от 02.07.1992 N 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании»	ред. от 28.12.2013
11	ФЗ №395-1	Федеральный закон от 02.12.1990 N 395-1 «О банках и банковской деятельности»	ред. от 30.09.2013 (с изм. и доп., вступающими в силу с 01.01.2014)

Окончание прил. 2

1	2	3	4
12	ФЗ №5485-1	Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне»	ред. от 21.12.2013
13	63-ФЗ	Федеральный закон от 31.05.2002 N 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»	ред. от 02.07.2013
14	98-ФЗ	Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»	ред. от 11.07.2011
15	125-ФЗ	Федеральный закон от 24.07.1998 N 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»	ред. от 28.12.2013 (с изм. и доп., вступ. в силу с 03.01.2014)
16	126-ФЗ	Федеральный закон от 07.07.2003 N 126-ФЗ «О связи»	ред. от 28.12.2013
17	149-ФЗ	Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»	ред. от 28.12.2013
18	152-ФЗ	Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»	ред. от 23.07.2013
19	212-ФЗ	Федеральный закон от 24.07.2009 N 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования»	ред. от 28.12.2013 (с изм. и доп., вступ. в силу с 03.01.2014)
20	218-ФЗ	Федеральный закон от 30.12.2004 N 218-ФЗ «О кредитных историях»	ред. от 23.07.2013
21	224-ФЗ	Федеральный закон от 27.07.2010 N 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»	ред. от 23.07.2013 (с изм. и доп., вступающими в силу с 01.01.2014)

Приложение 3

Правовая защита информации ограниченного доступа (А. Прозоров // www.infowatch.ru)

№	Сведения	Ссылка на НПА	Наказание за разглашение	Термин / Комментарии
1	2	3	4	5
1	**Государственная тайна**	Конституция РФ ст. 29 п. 4 ФЗ № 5485-1 ст. 5 УП № 1203 149-ФЗ ст. 9 п. 3	УК РФ ст. 275, 276, 283, 283.1, 284 ТК РФ ст. 81 6)в) (разглашение охраняемой законом тайны) ТК РФ ст. 243 7) (случаи полной материальной ответственности) КоАП ст. 13.12 п. 7 (нарушение правил защиты информации)	**«Государственная тайна –** защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ» – ФЗ №5485-1. Общий перечень сведений представлен в «ФЗ о ГТ», детализированный представлен в перечне, утвержденном Указом Президента РФ
2	**Коммерческая тайна Секрет производства (ноу-хау)**	98-ФЗ ГК РФ IV ст. 1465 149-ФЗ ст. 9 п. 4 УП №188 п. 5, 6	УК РФ ст. 183 УК РФ ст. 147 ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6 (нарушение правил защиты информации) КоАП ст. 13.14 (разглашение информации с огр. доступом) КоАП ст. 7.12 (нарушение авторских и смежных прав, изобретательских и патент ных прав)	98-ФЗ «…режим КТ в отношении информации, составляющей секрет производства (ноу-хау)». **«Коммерческая тайна –** режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду» **–** 98-ФЗ. **«Информация, составляющая коммерческую тайну (секрет производства) –** сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу

Продолжение прил. 3

1	2	3	4	5
				неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны» – 98-ФЗ
3	**Персональные данные**	152-ФЗ 149-ФЗ ст. 9 п. 9 УП №188 п. 1	УК РФ ст. 137 ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14 КоАП ст. 13.11 (нарушение правил обработки ПДн)	**Персональные данные –** любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) – 152-ФЗ. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (**персональные данные**), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях – УП 188
4	**Банковская тайна (тайна банковских вкладов)**	ФЗ № 395-1 ст.26 ГК РФ II, ст. 857	УК РФ ст. 183 ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	«Тайна об операциях, о счетах и вкладах своих клиентов и корреспондентов» – ФЗ № 395-1 «Тайна банковского счета и банковского вклада, операций по счету и сведений о клиенте» – ГК РФ
5	**Тайна кредитной истории**	218-ФЗ ст. 6 и 7, содержание кредитной истории – ст. 4	ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	«**Кредитная история –** информация, состав которой определен настоящим Федеральным законом и которая характеризует исполнение заемщиком принятых на себя обязательств по договорам займа (кредита) и хранится в бюро кредитных историй» – 218 ФЗ. Состав сведений определен в п. 4 218-ФЗ
6	**Служебная тайна**	149-ФЗ ст. 9 п. 4 УП № 188 п. 3 ТК РФ ст. 349.1 ПП 1233 (узкая область действия)	ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	«Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (**служебная тайна**)» – УП 188. «К служебной информации ограниченного распространения относится несекретная информация,

Продолжение прил. 3

1	2	3	4	5
				касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью.» – ПП 1233 «Работнику государственной корпорации или государственной компании в случаях запрещается ... разглашать или использовать сведения, отнесенные законодательством РФ к сведениям конфиденциального характера, или служебную информацию, а также сведения, ставшие ему известными в связи с исполнением трудовых обязанностей» – ТК РФ Ст. 139 «Служебная и коммерческая тайна» ГК РФ утратила силу с 01.01.2008; N 119-ФЗ «Об основах государственной службы РФ» утратил силу; ПП 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» существенно сократил область действия, стал про «использование атомной энергии» Термин четко не определен, есть мнения юристов, что «под служебной тайной следует понимать информацию, которая стала доступна гражданину при исполнении им своих служебных (трудовых) обязанностей, акцентирует внимание на том, что попытки ограничить понятие «служебной тайны» взаимоотношениями, возникающими только в рамках государственных организаций, не только не находят опоры в законе, но и неверны по самой своей сути»
7	**Тайна связи**	Конституция РФ ст.23 п.2 126-ФЗ ст.63 УП №188 п.4	УК РФ ст.138 ТК РФ ст.81, 243 КоАП ст.13.12 п.6, 13.14	«Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи» – 126-ФЗ

Продолжение прил. 3

1	2	3	4	5
8	**Инсайдерская информация**	224-ФЗ	ТК РФ ст. 81, 243 КоАП ст.13.12 п. 6, 13.14	«**Инсайдерская информация –** точная и конкретная информация, которая не была распространена или предоставлена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну), распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров …» – 224-ФЗ
9	**Налоговая тайна**	НК РФ ст. 102	УК РФ ст. 183, ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	«**Налоговую тайну** составляют любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением ряда сведений …» – НК РФ
10	**Врачебная тайна**	323-ФЗ ст.13 УП №188 п.4 ФЗ № 3185-1 СК РФ ст.15	УК РФ ст. 137 ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	«Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют **врачебную тайну**» – 323-ФЗ
11	**Нотариальная тайна**	Основы зак-ва РФ о нотариате №4462-1 ст.16 и 28 154-ФЗ ст.26 УП № 188 п. 4	ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	«Нотариус обязан хранить в тайне сведения, которые стали ему известны в связи с осуществлением его профессиональной деятельности» – №4462-1 «..тайна совершения нотариальных действий…» – ст. 26 154-ФЗ
12	**Адвокатская тайна**	63-ФЗ ст. 8 УП № 188 п. 4	ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	«Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю»
13	**Аудиторская тайна**	307-ФЗ ст.9	ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	«Аудиторскую тайну составляют любые сведения и документы, полученные и (или) составленные аудиторской организацией и ее работниками, а также индивидуальным

Окончание прил. 3

1	2	3	4	5
				аудитором и работниками, с которыми им заключены трудовые договоры, при оказании услуг, предусмотренных настоящим Федеральным законом, за исключением ряда сведений…» – 307-ФЗ
14	**Тайна страхования**	ГК РФ II, ст. 946 326-ФЗ ст. 47 212-ФЗ ст. 32 125-ФЗ ст. 18	ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	«Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц» – ГК РФ
15	**Личная и семейная тайна**	Конституция РФ ст. 23 п. 1 ГК РФ ст. 150 п. 1 149-ФЗ ст. 9 п. 8	УК РФ ст. 137 ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	Понятие в явном виде не определено
16	**Журналистская тайна**	2124-1-ФЗ ст. 41 и 49	ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	«Журналист обязан сохранять конфиденциальность информации и (или) ее источника» – 2124-1-ФЗ Понятие в явном виде не определено
17	**Профессиональная тайна**	149-ФЗ ст.9 п. 4 УП №188 п. 4	ТК РФ ст. 81, 243 КоАП ст. 13.12 п. 6, 13.14	Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна) – 149-ФЗ Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее) – УП № 188

ОГЛАВЛЕНИЕ

Учебное издание

Астахова Людмила Викторовна

ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
И МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Техн. редактор *А.В. Миних*

Издательский центр Южно-Уральского государственного университета

Подписано в печать 17.12.2014. Формат 60×84 1/16. Печать цифровая.
Усл. печ. л. 8,14. Тираж 100 экз. Заказ 666/343.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В.И. Ленина, 76.