ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Кафедра мультисервисных сетей и информационной безопасности

А.В. Крыжановский

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические указания к лабораторным занятиям

Самара

2018

УДК 681.3.067

ББК 32.973-018.2

К

Рекомендовано к изданию методическим советом ПГУТИ, протокол №62, от 15.05.2018 г.

Рецензент:

заведующий кафедрой АЭС ФГБОУ ВО ПГУТИ,

д.т.н., проф. Росляков А.В.

Крыжановский, А.В.

К Организационное и правовое обеспечение информационной безопасности: методические указания к лабораторным занятиям/ А.В. Крыжановский– Самара: ПГУТИ, 2018. – 56 с.

Методические указания разработаны в соответствии ФГОС ВО направлений подготовки 10.05.02 (ИБТС) и 10.03.01 (ИБ) и предназначены студентам факультета ТР для методического обеспечения проведения лабораторных работ по дисциплине «Организационное и правовое обеспечение информационной безопасности» с целью закрепления полученных теоретических знаний, выработки умения применять действующую законодательную базу в области информационной безопасности, а также получения практических навыков по созданию систем защиты информации.

Содержится материал по организационным и правовым аспектам защиты информации, раскрывающий основные положения нормативно-правовых актов информационного права, принципы и методы создания систем информационной безопасности, организацию профотбора персонала, работу подразделений защиты информации, входящих в состав службы безопасности предприятия.

Содержание

Введение

Надежное обеспечение защиты информации современного предприятия возможно только при условии комплексного подхода к созданию системы информационной безопасности (ИБ). Такой подход включает использование правовых, организационных и технических механизмов обеспечения ИБ. Причем, пределы величины необходимого уровня защищенности охраняемых активов определяются как нормативно-правовой базой, так и вопросами экономической целесообразности вложения средств.

Наличие различных источников угроз, ведение бумажного и электронного делопроизводства конфиденциального характера требуют разграничения доступа к информации, создания структурных подразделений ИБ, а также установления мер административной, гражданской и уголовной ответственности за нарушения в информационной сфере.

Наиболее вероятными источниками утечки информации являются:

- персонал, имеющий доступ к информации;

- документы, содержащие эту информацию;

- технические средства и системы обработки информации, в том числе линии связи, по которым она передается.

В качестве потенциальных угроз безопасности информации могут выступать стихийные бедствия, неблагоприятная внешняя среда, катастрофы, политическая нестабильность, террористическая деятельность, ошибки и неисправности компьютерных программ, компьютерная преступность.

Обеспечение целостности, конфиденциальности и доступности информационных ресурсов предприятия возможно при активном участии и сотрудничестве государства, органов государственной власти и служб безопасности коммерческих структур.

Вопросы государственного регулирования ИБ лежат в плоскости со-

здания эффективной правовой базы информационного законодательства, определения перечня сведений конфиденциального характера и создания государственной системы лицензирования и сертификации в области защиты конфиденциальной информации.

Коммерческие предприятия в своей деятельности должны использовать международные и российские стандарты безопасности, современные подходы к профотбору персонала, рекомендации по организации внутриобъектового режима секретности и охране материально-технических, людских и информационных активов.

Лабораторная работа №1

Закрепление права предприятия на защиту информации в нормативных документах

1 Цель лабораторной работы

Изучение методов правовой защиты служебной и коммерческой тайны на предприятии и разработка внутренних документов выбранного предприятия, предназначенных для организации правовой защиты коммерческих секретов.

2 Основные понятия

Должностная служебная тайна связана с интересами государственной службы и службы в органах местного самоуправления. К служебной тайне (в соответствии с Указом Президента РФ от 6 марта 1997г. №188) относятся служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации (ГК РФ) и федеральными законами (служебная тайна).Доступ к профессиональным сведениям закрытого характера связан с должностным статусом лица, которому эти сведения стали известны по службе. Поэтому при утечке этой секретной информации страдают интересы предприятия.Защита прав обладателя коммерческих секретов осуществляется способами, предусмотренными ГК РФ и другими законами. Среди них можно выделить следующие: пресечение действий, нарушающих право или создающих угрозу его нарушения; возмещение убытков, в том числе и упущенной выгоды (ст. 12 ГК РФ).

Конкурентная разведка – это сбор и обработка информации законными способами. На данный момент в нашей стране под конкурентной разведкой подразумеваются четыре различных направления сбора инфор-

мации:

-о партнерах и клиентах (для предотвращения мошенничеств с их стороны);

- о потенциальных партнерах и сотрудниках;

- выполнение услуг, предусмотренных "Законом о частной детективной и охранной деятельности" (поиск имущества должника и т.п.);

- сбор информации маркетингового характера.

Добывание коммерческих секретов с нарушением существующего законодательства классифицируется как промышленный шпионаж.

Ответственность за промышленный шпионаж определена в статье 183 Уголовного кодекса Российской Федерации (УК РФ).

3 Домашнее задание

1 Ознакомиться с основными положениями правового обеспечения защиты конфиденциальной информации [1].

2 Ознакомиться с основными положениями правового обеспечения защиты коммерческой и служебной тайны [2,3].

3 Ознакомиться с понятиями конкурентная разведка и промышленный шпионаж и основными положениями законодательства [4].

4 Варианты заданий на выполнение работы

1Из Приложения 1 выберите вариант предприятия, деятельность которого связана с использованием сведений, относящихся к коммерческой или служебной тайне. Номер варианта предприятия с указанием видов деятельности должен совпадать с номером бригады учебной группы.

2 Руководствуясь положениями Федерального законодательства Российской Федерации [1-3] (Приложение 2) составьте план мероприятий по

защите коммерческой или служебной тайны для выбранного предприятия.

3 Составьте перечень сведений, составляющих коммерческую или служебную тайну выбранного предприятия.

4 Составьте перечень внутренних документов, используемых в целях правовой защиты секретов выбранного предприятия.

5 Разработайте внутренние документы, которые будут использоваться для правовой защиты секретов выбранного предприятия. Образцы соответствующих документов приведены в Приложении 3.

6 Руководствуясь положениями законодательства [4] и материалами Приложения 4 опишите методы конкурентной разведки, которые могут использоваться информационно-аналитической службой предприятия.

5 Порядок выполнения лабораторной работы

1 Изучите особенности выбранного предприятия, которое занимается видами деятельности, связанной с использованием коммерческой тайны.

2 Наименование видов деятельности занесите в табл.1.

Таблица 1

№ п/п	Наименование видов деятельности	Примечание
1	Направление деятельности 1	
2	Направление деятельности 2	
……	……	
N	Направление деятельности N	

3 При разработке плана мероприятий по защите коммерческих секретов предприятия можно воспользоваться следующими методическими указаниями.

3.1 Определение целей плана по защите коммерческой тайны. Ими

могут быть:

- предотвращение кражи коммерческих секретов;

- предотвращение разглашения коммерческих секретов сотрудниками или их утечки через технические каналы.

3.2 Анализ сведений, составляющих коммерческую тайну, для чего необходимо:

- определить, какие сведения на предприятии (технологические и деловые) являются коммерческой тайной;

- установить места их накопления и хранения;

- оценить возможности по перекрытию каналов утечки;

- проанализировать соотношение затрат на защиту и возможных потерь при утере информации, если использованы различные технологии, обеспечивающие защиту коммерческой тайны;

- назначить сотрудников, персонально ответственных за каждый участок системы обеспечения безопасности.

3.3 Обеспечить реализацию деятельности системы по следующим направлениям:

- контроль сооружений и оборудования предприятия (обеспечение безопасности производственных и конторских помещений, охрана фото- и иного копировального оборудования, контроль посещений предприятия);

- работа с персоналом предприятия, в том числе проведение бесед при приеме на работу; инструктаж вновь потупивших на работу по правилам и процедурам, принятым для защиты коммерческой тайны на предприятии; обучение сотрудников правилам сохранения коммерческих секретов; стимулирование соблюдения конфиденциальности;

- беседы с сотрудниками, увольняющимися из предприятия;

- организация работы с конфиденциальными документами (установление порядка и правил ведения делопроизводства, контроль за конфиденциальными документами, контроль за публикациями, контроль и учет тех-

нических носителей конфиденциальных сведений, рассекречивание и уничтожение конфиденциальных документов, охрана чужих секретов);

- работа с конфиденциальной информацией, циркулирующей в технических средствах и системах, которые обеспечивают трудовую деятельность (создание системы предотвращения утечки информации через технические каналы);

- работа с конфиденциальной информацией, накопленной в компьютерных системах (создание системы защиты электронной информации от несанкционированного доступа к ней; обеспечение контроля за использованием ЭВМ);

- защита коммерческой тайны предприятия в организационно-правовых документах, в процессе заключения контрактов и договоров с коллективом, сотрудниками, смежниками, поставщиками и т. д. Здесь важно четко определить круг лиц, имеющих отношение к этой работе.

После составления перечня определяются те мероприятия плана, которые выполняются специализированной организацией (наличие квалифицированных специалистов в конкретной области, техническая и методическая оснащенность) и те из них, которые осуществляются силами и средствами собственной службы безопасности (знание оперативной обстановки, динамичность). При такой работе достигаются оптимальные результаты с точки зрения финансовых затрат и качества защиты.

3.4 Разработайте пакет внутрифирменных документов, ориентированных на защиту корпоративной конфиденциальной информации. Для этого ознакомьтесь с образцами подобных документов, которые приведёны в Приложении 2. В разрабатываемый пакет включите документы, которые Вы считаете наиболее актуальными для обеспечения режима коммерческой тайны Вашего предприятия.

6 Содержание отчёта

1 Цель работы.

2 Отчет о выполненной работе оформляется в соответствии с общепринятыми требованиями и предоставляется в виде распечатки контрольного листа из файла. **Обязательным требованием является наличие титульного листа отчёта.**

7 Список контрольных вопросов

1 Нормативно-правовое регулирование профессиональной тайны в РФ.

2 Признаки и объекты профессиональной тайны.

3 Какие сведения относятся к служебной тайне?

4 На каких правовых актах основана защита служебной и коммерческой информации на предприятии?

5 Чем отличается служебная тайна от профессиональной?

6 Какие внутренние нормативные документы используются для правовой защиты служебной и КТ?

7 В какие виды договоров включаются условия о неразглашении служебной тайны?

8 Что понимается под ущербом в результате разглашения КТ?

9 Определение и виды конкурентной разведки.

8 Список литературы

Основная

1 Федеральный закон от 27.07.2006 № 149-ФЗ « Об информации, информационных технологиях и о защите информации» [Электронный ресурс] / КонсультантПлюс.- Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=183056;fld=134;dst=1000000001,0;rnd=0.741186022442

0134, свободный.-Загл. с экрана.

2 Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне" [Электронный ресурс] / КонсультантПлюс.- Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=160225;fld=134;dst=1000000001,0;rnd=0.33993384323544973 , свободный.-Загл. с экрана.

3 Федеральный закон "О служебной тайне" (Проект № 124871-4) [Электронный ресурс] / КонсультантПлюс.- Режим доступа: http://iso27000.ru/zakonodatelstvo/federalnye-zakony-rf/federalnyi-zakon-o-sluzhebnoi-taine-proekt-No-124871-4, свободный.-Загл. с экрана.

Дополнительная

4 Закон Российской Федерации от 11.03.1992 №2487-1 «О частной детективной и охранной деятельности в Российской Федерации» [Электронный ресурс] /КонсультантПлюс.-Режим доступа: http://docs.cntd.ru/ document/9004238, свободный.- Загл. с экрана.

Лабораторная работа №2

Лицензирование деятельности и сертификация средств

в области защиты государственной тайны и конфиденциальной информации

1 Цель лабораторной работы

1 Изучение основных норм законодательства, устанавливающего порядок лицензирования деятельности и сертификации средств в области защиты государственной тайны и конфиденциальной информации.

2 Разработать внутренние документы выбранного предприятия, предназначенные для организации лицензирования деятельности предприятия и сертификации средств защиты информации, отнесённой к государственной тайне и конфиденциальной.

2 Основные понятия

2.1 Государственная система защиты информации в РФ

Для обеспечения защиты информации ограниченного доступа действует Государственная система защиты информации в РФ (ГСЗИ), которая включает:

-совокупность органов (ФСБ, ФСТЭК, СВР), сил и средств, осуществляющих деятельность в области защиты информации (ЗИ);

-систему лицензирования деятельности в области ЗИ;

-систему сертификации средств ЗИ;

-систему подготовки и переподготовки специалистов в области ЗИ.

2.2 Правовая основа системы лицензирования и сертификации в РФ

Лицензирование - это процесс передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ. Получить право или разрешение на определенную деятельность может не каждый субъект, а только отвечающий определенным критериям в соответствии с правилами лицензирования.

Лицензия - документ, дающий право на осуществление указанного видадеятельности в течение определенного времени.

Перечень видов деятельности в области защиты информации ограниченного доступа, на которые требуются лицензии, определен в [2, статья 12].

К ним, в частности, относится разработка, производство, реализация и сервисное обслуживание:

-шифровальных средств;

-защищенных систем телекоммуникаций;

-программных средств;

-специальных технических средств ЗИ;

- подготовка и переподготовка кадров.

Сертификация - это подтверждение соответствия продукции или услуг установленным требованиям или стандартам.

Сертификат - документ, подтверждающий соответствие средства ЗИ требованиям по безопасности информации.

Законодательной и нормативной базой лицензирования и сертификации в области ЗИ ограниченного доступа (отнесённой к государственной тайне и конфиденциальной) являются.

1) Федеральные законы РФ:

-«О государственной тайне» [1];

-«О лицензировании отдельных видов деятельности»[2] ;

-«О техническом регулировании» [5]

2) Постановления Правительства РФ:

– «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны (в ред. Постановлений Правительства РФ от 23.04.96 N 509, от 30.04.97 N 513, от 29.07.98 N 854)» от 15.04.1995 N 333 [3];

– «О лицензировании деятельности по технической защите конфиденциальной информации» от 03.02.2012 N 79 [4];

– «О сертификации средств защиты информации» (в ред. Постановлений Правительства РФ от 23.04.1996 N 509,от 29.03.1999 N 342, от 17.12.2004 N 808, от 21.04.2010 N 266) от 26.06.1995 № 608 [8];

– « О внесении дополнений в некоторые решения Правительства Российской Федерации» от 23.04.1996 № 509.

3) Приказы ФСБ и Гостехкомиссии:

– приказ ФСБ «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия» от 13 ноября 1999 г. N 564 [6];

– «Положение о сертификации средств защиты информации по требованиям безопасности информации». Утверждено приказом председателя Гостехкомиссии РФ от 27.10.1995 N 199 [7].

2. 3 Лицензирования деятельности по защите государственной тайны

Общие нормы, устанавливающие порядок организации и осуществления этой деятельности, содержатся в статье 27 Федерального Закона «О государственной тайне» [1].

Основные положения данной статьи:

– лицензия выдается только на основании результатов специальной экспертизы (проверки готовности организации к работе со сведениями, составляющими государственную тайну);

– в структуре организации должно быть подразделения по защите государственной тайны (ГТ) и специально подготовленные сотрудники;

– организация должна иметь сертифицированные средства защиты информации;

– необходима государственная аттестация руководителей организации, ответственных за защиту государственных секретов.

Постановлением Правительства РФ от 15.04.95 №333 утверждено «Положение о лицензировании деятельности предприятий…» [3], в котором установлено, что:

– лицензия разрешает осуществление конкретного вида деятельности в течение установленного срока на всей территории Российской Федерации, а также в учреждениях Российской Федерации, находящихся за границей;

– органами, уполномоченными на ведение лицензионной деятельности, являются:

– по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, - Федеральная служба безопасности Российской Федерации (ФСБ) и ее территориальные органы (на территории Российской Федерации), Служба внешней разведки Российской Федерации (СВР) (за рубежом);

– на право проведения работ, связанных с созданием средств защиты

информации – Федеральная служба технического и экспортного контроля (ФСТЭК), ФСБ;

– на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны – ФСБ, ФСТЭК, СВР.

Лицензирование деятельности предприятий ФСБ, МО (министерства обороны), СВР и ФСТЭК по допуску к проведению работ, связанных с использованием сведений, составляющих государственную тайну, осуществляется руководителями министерств и ведомств Российской Федерации, которым подчинены указанные предприятия.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не может быть менее трех и более пяти лет. Продление срока действия лицензии производится в порядке, установленном для ее получения. На каждый вид деятельности выдается отдельная лицензия.

Основанием для отказа в выдаче лицензии является:

– наличие в представленных документах недостоверной или искаженной информации;

– отрицательное заключение экспертизы;

– отрицательное заключение по результатам государственной аттестации руководителя предприятия.

Специальные экспертизы предприятий выполняются по следующим направлениям:

– режим секретности;

– противодействие иностранной технической разведке;

– защита информации от утечки по техническим каналам.

Экспертные комиссии формируются при ФСБ, ФСТЭК и их органах на местах и аттестационных центрах.

2.3.1 Принципы лицензирования

1 Лицензирование в области защиты ГТ является обязательным.

2 Деятельность в области ЗИ лиц, не прошедших лицензирование, запрещена (с применением соответствующих статей гражданского и уголовного кодексов к нарушителям).

3 Лицензии на право деятельности в области ЗИ выдаются только юридическим лицам независимо от организационно - правовой формы (физические лица не в состоянии удовлетворить указанным требованиям).

4 Лицензии выдаются только предприятиям, зарегистрированным на территории РФ на основании специальной экспертизы заявителя.

Для получения лицензии предприятие обязано предъявить следующий перечень документов.

К заявлению на получение лицензии необходимо приложить следующие документы:

– копия свидетельства о государственной регистрации предприятия;

– копии учредительных документов, заверенных нотариусом;

– копии документов на право собственности или аренды имущества, необходимого для ведения заявленной деятельности;

– справка налогового органа о постановке на учет;

– представление органов государственной власти РФ с ходатайством о выдаче лицензии;

– документ, подтверждающий оплату рассмотрения заявления.

Проведение экспертизы осуществляется экспертными комиссиями Лицензионного центра либо аттестационными центрами.

Например, коммерческому банку, претендующему на получение лицензии на эксплуатацию шифровальных средств для защиты конфиденциальной информации предъявляются требования по:

– наличию и составу необходимых аппаратно-программных средств и помещений;

– размещению, охране и специальному оборудованию помещений, в которых находятся средства криптографической ЗИ;

– обеспечению режима и порядка доступа к средствам криптографической ЗИ;

– обеспечению необходимой технической и эксплуатационной документацией;

– уровню квалификации и подготовленности специалистов в области защиты и эксплуатации АС;

– режиму эксплуатации и хранения средств криптографической ЗИ.

2.3.2 Государственная аттестация руководителей, ответственных за ГТ

Основная цель государственной аттестации – повысить компетентность руководителей в части обеспечения сохранности сведений, составляющих государственную тайну.

Документом, по организации государственной аттестации руководителей является «Инструкция о порядке проведения государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну», утвержденная Председателем Гостехкомиссии России 17.10.95 г.

Государственное аттестование проводится методом собеседования аттестационной комиссии с руководителем предприятия.

К аттестуемому предъявляются следующие требования.

***Должен знать*:**

– законодательные акты Российской Федерации по вопросам защиты государственной тайны;

– нормативные документы, утверждаемые Правительством Российской Федерации,

– по обеспечению защиты сведений, составляющих государственную тайну;

– -нормативно-методические документы по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, утверждаемые ФСБ и ФСТЭК;

– перечень продукции предприятия, подлежащей защите от разведок, основные охраняемые сведения о предприятии и выпускаемой продукции;

– возможные каналы утечки информации по всему технологическому циклу разработки, изготовления и испытаний продукции предприятия;

– деловые и моральные качества сотрудников структурного подразделения предприятия по защите государственной тайны.

***Должен уметь организовывать*:**

– разработку мероприятий по защите сведений о предприятии и выпускаемой продукции, составляющих государственную тайну, и оценку их достаточности;

– проведение анализа возможностей разведки по добыванию сведений, составляющих государственную тайну;

– аттестование рабочих мест по всему технологическому циклу разработки, изготовления и испытания продукции;

– комплексный контроль выполнения принимаемых мер по защите сведений, составляющих государственную тайну.

***Быть ознакомленным*:**

– с государственной системой лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений,составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны;

– с возможностями иностранных разведок по добыванию сведений, составляющих государственную тайну;

– с методиками контроля выполнения норм противодействия иностранным техническим разведкам.

2.4 Сертификация средств защиты информации, составляющей государственную тайну

Национальный орган по сертификации определяется Правительством РФ. В настоящее время эти функции выполняет Федеральное агентство по техническому регулированию и метрологии.

Сертификация средств защиты информации, прежде всего, подразумевает проверку их качественных характеристик для реализации основной функции – защиты информации на основании государственных стандартов и требований по безопасности информации.

Общие принципы сертификации средств защиты ГТ определены нормами статьи 28 Закона «О государственной тайне» [1] - средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на ФСТЭК, ФСБ и Министерство обороны в соответствии с функциями, возложенными на них законодательством Российской Федерации. Сертификация осуществляется на основании требований государственных стандартов Российской Федерации и иных нормативных документов, утверждаемых Правительством Российской Федерации.

Законодательной базой сертификации СЗИ по требованиям безопасности для сведений, составляющих государственную тайну, является:

– «Положение о сертификации средств защиты информации…» утверждено постановлением Правительства Российской Федерации от

26.06.95 г. № 608 [8]. Это положение зарегистрировано Госстандартом России в Государственном реестре 20 марта 1995 г. (Свидетельство № РОСС RU. 0001. 01БИ00);

– «Положение о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (система сертификации СЗИ-ГТ)». Утверждено приказом ФСБ от 13.11. 1999 г. N 564 [6].

2.4.1 Принципы сертификации

1 Сертификация изделий, обеспечивающих защиту ГТ, является обязательной.

2 Обязательность использования криптографических алгоритмов, являющихся стандартами.

3 Принятие на сертификацию изделий только от заявителей, имеющих лицензию.

В соответствии с вышеназванными документами, государственным организациям и предприятиям запрещено использование в информационных системах шифровальных средств, не имеющих сертификата.

Кроме этого в области информационных технологий действуют системы добровольной сертификации банковских технологий (МЕКАС) и средств связи.

2.4.2 Порядок сертификации

1 В Центральный орган по сертификации подается заявление и полный комплект технической документации.

2 Центральный орган назначает испытательный центр (лабораторию) для проведения испытания.

3 Испытания проводятся на основании хозяйственного договора между заявителем и испытательным центром.

4 Сертификация (экспертиза материалов и подготовка документов для выдачи) осуществляется Центральным органом.

Сертификат выдается на срок до 5 лет.

2.5 Лицензирование и сертификация в области защиты конфиденциальной информации

Лицензирование деятельности в области защиты конфиденциальной информации основано на:

– Федеральном законе от 04.05.2011 N 99-ФЗ (ред. от 13.07.2015, с изм. от 30.12.2015) "О лицензировании отдельных видов деятельности" (с изм. и доп., вступ. в силу с 10.01.2016) [2];

– «Положении о лицензировании деятельности по технической защите конфиденциальной информации». Утверждено Постановлением Правительства РФ от 03.02.2012 N 79 .

Действие данного закона не распространяется на следующие виды деятельности, связанные с ЗИ:

– деятельность, связанная с защитой государственной тайны;

– деятельность в области связи;

– использование результатов интеллектуальной деятельности.

В соответствии с настоящим Федеральным законом лицензированию подлежат следующие виды деятельности в области ЗИ:

– разработка, производство, распространение, техническое обслуживание и предоставление услуг в области шифрования информации; шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

– деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;

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

– деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

– деятельность по технической защите конфиденциальной информации;

– разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Срок действия лицензии не может быть менее чем пять лет и может быть продлен по заявлению лицензиата.

Продление срока действия лицензии осуществляется в порядке переоформления документа, подтверждающего наличие лицензии.

В систему сертификации могут входить организации независимо от форм собственности, а также общественные объединения.

Постановление Правительства РФ от 23.04.96 N 509 устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом. Это технические, криптографические, программные и другие средства, предназначенные для защиты сведений,

составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Системы сертификации создаются ФСТЭК, ФСБ, Министерством обороны и СВР.

Система сертификации средств защиты информации в РФ осуществляется по требованиям безопасности информации, определенным ФСТЭК.

«Положение о сертификации средств защиты информации по требованиям безопасности информации» утверждено приказом Председателя Гостехкомиссии России от 27 октября 1995 г. № 199 [6] . В соответствии с [6] обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для защиты информации, составляющей государственную тайну, и другой информации с ограниченным доступом, а также средства, использующиеся в управлении экологически опасными объектами. В остальных случаях сертификация носит добровольный характер (добровольная сертификация) и осуществляется по инициативе разработчика, изготовителя или потребителя средства защиты информации.

Сертификационные испытания средств защиты в рамках данной системы сертификации предусматривают комплекс мероприятий по проверке соответствия этих средств формальным базовым требованиям по обеспечению безопасности информации, изложенным в нормативных документах ФСТЭК.

3 Домашнее задание

1 Изучить нормы, устанавливающие порядок лицензирования деятельности, связанной с использованием сведений, составляющих государственную тайну[1, статья 27 (Приложение 1)], [2 (Приложение 2)], [3 (Приложение 3)].

2 Изучить нормы, устанавливающие порядок лицензирования деятельности в области технической защиты конфиденциальной информации [4 (Приложение 4)].

3 Изучить порядок сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (система сертификации СЗИ-ГТ) [1,статья 28 (Приложение 1)], [6 (Приложение 6)].

4 Изучить порядок сертификации средств защиты информации по требованиям безопасности информации [7 (Приложение 7)].

5 Внимательно ознакомиться с материалом раздела 8 настоящих методических указаний и усвоенные сведения использовать при выполнении работы .

4 Порядок выполнения лабораторной работы

1 Из Приложения 9 выберите вариант предприятия, деятельность которого связана с использованием сведений, относящихся к коммерческой или служебной тайне. Номер варианта предприятия с указанием видов деятельности должен совпадать с номером бригады учебной группы.

2 Обоснуйте необходимость проведения лицензирования выбранного вида деятельности на выбранном предприятии. Для обоснования необходимости лицензирования деятельности, связанной с ЗИ ограниченного доступа, следует руководствоваться положениями законодательства [1-4] и материалом раздела 2.

Если на выбранном предприятии не окажется лицензируемых по требованиям защиты информации видов деятельности, то их нужно ввести, учитывая упомянутое законодательство.

3 В соответствии с законодательством [1-4] составьте перечень документов, необходимых для получения лицензии на выбранный вид деятельности.

4 В соответствии с Приложением 1 в [7] составьте перечень сертифи-

цируемых СЗИ.

5 В соответствии с законодательством [5-8] укажите порядок и необходимость (обязательная или добровольная) сертификации выбранных СЗИ. Укажите перечень сертификационных документов, необходимых для выбранных средств ЗИ.

6 Составьте для выбранного предприятия документы для лицензирования и сертификации с использованием образцов, содержащихся в папке «Образцы документов» **(**Приложение 11**).**

7 При разработке документов с использованием предлагаемых образцов учтите, что в соответствии с Указом Президента Российской Федерации от 16.08.2004 № 1085 термин «Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия)» заменён термином «Федеральная служба по техническому и экспортному контролю (ФСТЭК России)».

5 Содержание отчёта

1 Цель работы.

2 Краткие сведения о правовой основе системы лицензирования и сертификации в РФ.

3 Обоснование необходимости проведения лицензирования выбранного вида деятельности выбранного предприятия со ссылкой на законодательство.

5 Перечень документов на получение лицензии.

6 Перечень средств защиты информации (СЗИ), подлежащих сертификации.

7 Перечень сертификационных документов.

8 Разработанные документы, необходимые для получения лицензий и сертификатов СЗИ.

9 Выводы.

10 Отчёт о выполненной работе оформляется в электронном и рас-

печатанном виде в соответствии с требованиями РД ПГУТИ и сдаётся преподавателю. **Обязательным требованием является наличие титульного листа отчёта (Приложение 10).**

6 Список контрольных вопросов

1Сущность нормативно-правового регулирования деятельности в области защиты конфиденциальной информации.

2 Какие виды деятельности в области защиты конфиденциальной информации подлежат лицензированию?

3 Порядок лицензирования, срок действия лицензии.

4Организационная структура системы сертификации в области защиты конфиденциальной информации.

5 При каких организациях созданы системы сертификации в РФ?

6Порядок и требования при осуществлении сертификации средств защиты информации.

7 В каких случаях сертификация носит добровольный характер?

8 Кем устанавливаются формы сертификата и знака соответствия?

9 Назовите российские и международные стандарты безопасности.

7 Список литературы

1 Закон РФ от 21.07.1993 N 5485-1(ред. от 08.03.2015) "О государственной тайне" [Электронный ресурс] / КонсультантПлюс. Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=176315;fld=134;dst=1000000001,0;rnd=0.7843954091451089, свободный.-Загл. с экрана.

2 Федеральный закон от 04.05.2011 N 99-ФЗ (ред. от 13.07.2015, с изм. от 30.12.2015) "О лицензировании отдельных видов деятельности" (с

изм. и доп., вступ. в силу с 10.01.2016) [Электронный ресурс] / КонсультантПлюс.- Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=182965;fld=134;from=1826928;rnd=189271.888332858215142;;ts=01892716936347046655005, свободный.-Загл. с экрана.

3 Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны. (в ред. Постановлений Правительства РФ от 23.04.96 N 509, от 30.04.97 N 513, от 29.07.98 N 854) . Утверждено Постановлением Правительства РФ от 15.04.95 N 333.

4 Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено Постановлением Правительства РФ от 03.02.2012 N 79 .

5 Федеральный закон от 27.12.2002 N 184-ФЗ (ред. от 28.11.2015) "О техническом регулировании" [Электронный ресурс] / Консультант Плюс.- Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=189650;fld=134;from=1783471141;rnd=189271.8708743195056309;;ts=01892719230594523930271, свободный.-Загл. с экрана.

6 Положение о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (система сертификации СЗИ-ГТ). Утверждено приказом ФСБ от 13.11. 1999 г. N 564. [Электронный ресурс] / Режим доступа: http://www.libertarium.ru/15571?PRINT_VIEW=YES, свободный.-Загл. с экрана.

7 Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом пред-

седателя Гостехкомиссии РФ от 27.10.1995 N 199. [Электронный ресурс]/ Режим доступа : http://iso27000.ru/zakonodatelstvo/normativnye-dokumenty-fstek-rossii/polozhenie-o-sertifikacii-sredstv-zaschity-informacii-po-trebovaniyam-bezopasnosti-informacii, свободный.-Загл. с экрана.

8 Положение о сертификации средств защиты информации (в ред. Постановлений Правительства РФ от 23.04.1996 N 509, от 29.03.1999 N 342, от 17.12.2004 N 808, от 21.04.2010 N 266). Утверждено Постановлением Правительства РФ от 26.06.95 № 608.

Лабораторная работа № 3
Правовые нормы защиты информации в автоматизированных системах

1 Цель работы

Изучение правовой основы обеспечения защиты информации в автоматизированных системах (АС) и средствах вычислительной техники (СВТ). Разработать внутренние документы выбранного предприятия, учитываемых при разработке «Политики безопасности».

2 Основные понятия

Правовое обеспечение защиты информации в АС – это совокупность законодательных актов, нормативно-правовых документов, положений, инструкций, руководств, требования которых обязательны в системе защиты информации, включающих следующие нормы.

Для корпоративных сетей с большим количеством пользователей составляется документ, регламентирующий работу в сети, – «Политика безопасности». Этот документ учитывает услуги, предоставляемые Интернет , и требования информационной безопасности и основан на стандарте ISO/ IEC 17799.

«Политика безопасности» обеспечивает выполнение таких правил безопасности информации, как: идентификация, разделение полномочий, регистрация и учет работы, шифрование, применение цифровой подписи, обеспечение антивирусной защиты и контроль целостности информации.

В общем случае система защиты информации в компьютерной сети реализуется в три этапа: анализ риска, реализация политики безопасности и поддержание политики безопасности.

Требования к безопасности компьютерных сетей в РФ разработаны ГТК. Эти требования обязательны для государственных и коммерческих предприятий, допущенных к сведениям, составляющим ГТ. В остальных случаях они носят рекомендательный характер. К таким документам относится, например, РД ГТК «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» от 30.03.92.

Требования к безопасности АС устанавливаются в соответствии с классом защищенности. Показатели защищенности средств вычислительной техники от НСД даны в РД ГТК «Средства ВТ. Защита от НСД. Показатели защищенности от НСД к информации» от 30.03.92.

3 Домашнее задание

1 Ознакомиться с текстом руководящих документов ГТК [1-5]. Тексты документов приведены в Приложении.

2 Внимательно ознакомиться с материалом раздела 2 настоящих методических указаний и усвоенные сведения использовать при выполнении работы.

4 Порядок выполнения лабораторной работы

1 Аналогично предыдущим лабораторным работам выберите вариант предприятия, деятельность которого связана с использованием сведений, относящихся к коммерческой или служебной тайне. Номер вариан-

та предприятия с указанием видов деятельности должен совпадать с номером бригады учебной группы.

2 Оцените угрозы конфиденциальным ресурсам выбранного предприятия и составьте перечень актуальных угроз.

Некоторые возможные угрозы безопасности информации :

- утечка защищаемой информации по штатным или искусственным техническим каналам;
- несанкционированный доступ к защищаемой информации;
- деструктивное (разрушительное) воздействие на информацию и средства её обработки;
- недекларированные возможности программного обеспечения;
- внедрение устройств негласного съёма информации.

3 Разработайте и обоснуйте мероприятия для создания системы защиты АС и СВТ выбранного предприятия.

4 Укажите перечень РД ГТК, учитываемых при разработке «Политики безопасности» на вашем предприятии.

5 Определите и обоснуйте требования по защите конфиденциальной информации выбранного предприятия : группу и класс защищённости АС и СВТ от НСД с использованием НПА [1-5], тексты которых находятся в Приложении.

6 Разработайте внутренние документы выбранного предприятия, учитываемые при разработке «Политики безопасности»:

а) акт классификации автоматизированной системы обработки информации;

б) аттестат соответствия автоматизированной системы требованиям по безопасности информации;

в) аттестат соответствия защищаемого помещения требованиям по безопасности информации;

г) форма технического паспорта на защищаемое помещение;

д) форма технического паспорта на автоматизированную систему;

е) пример документального оформления перечня сведений конфиденциального характера;

ж) классы защищенности от несанкционированного доступа к информации;

з) основные нормативные правовые акты и методические документы по защите конфиденциальной информации.

Образцы указанных документов приведены в [5].

5 Содержание отчёта

1 Цель работы.

2 Перечень актуальных угроз информационным ресурсам выбранного предприятия.

3 Перечень предлагаемых мероприятий для создания системы защиты АС и СВТ выбранного предприятия.

4 Перечень документов, учитываемых при разработке «Политики безопасности» на выбранном предприятии .

5 Обоснованные требования по защите конфиденциальной информации выбранного предприятия :группу и класс защищённости АС и СВТ.

6 Образцы разработанных документов.

7 Выводы.

8 Отчёт о выполненной работе оформляется в электронном и распечатанном виде в соответствии с требованиями РД ПГУТИ и сдаётся преподавателю. **Обязательным требованием является наличие титульного листа отчёта.**

6 Список контрольных вопросов

1 Назовите особенности расследования компьютерных преступлений.

2 Какие задачи решаются судебно-бухгалтерской и программно-технической экспертизами при проведении следственных действий?

3 Существующая классификация компьютерных преступлений.

4 Методы и приемы предупреждения компьютерных преступлений. Анализ компьютерных преступлений.

5 В каких документах представлены нормы правового обеспечения защиты информации в АС?

6 Что представляет собой документ «Политика безопасности»?

7 Какие документы необходимо представить для присвоения класса защищенности АС?

8 От чего зависит выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ?

9 Выполнение каких правил безопасности обеспечивается путем реализации «Политики безопасности»?

9 Где указаны требования к безопасности компьютерных сетей в РФ?

7 Список литературы

1Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

2Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.

3Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решени-

ем председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

4Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации .Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

5Нормативно- методический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом ГТК России от 30 августа 2002 г. № 282.

Лабораторная работа № 4
Построение информационной системы персональных данных (ИСПДн) предприятия

1 Цель лабораторной работы

Изучение правовой основы обеспечения безопасности персональных данных (ПДн) в информационной системе персональных данных (ИСПДн) выбранного предприятия. Разработка внутренних документов ИСПДн выбранного предприятия на основе типовых форм, приведённых в Приложении.

2 Основные понятия

2.1 Установление уровня защищенности ПДн

Установление уровня защищенности (УЗ) ПДн осуществляется в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [3].

Уровень защищенности ПДн — это комплексный показатель, который характеризует выполнение требований, нейтрализующих угрозы безопасности ИСПДн. Требованиями к защите ПДн при их обработке в информационных системах установлены 4 УЗ ПДн, различающихся перечнем необходимых к выполнению требований по защите информационных систем.

Для определения уровня защищенности необходимо установить категории обрабатываемых ПДн субъектов (физических лиц), вид обработки по форме отношений между субъектами и организацией, количество субъектов, а также тип угроз, актуальных для информационной системы.

Категории обрабатываемых ПДн, подразделяются на 4 группы:

– 1 группа — специальные категории ПДн, к которым относятся информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта;

– 2 группа — биометрические ПДн, то есть данные, характеризующие биологические или физиологические особенности субъекта, например фотография или отпечатки пальцев;

– 3 группа — общедоступные ПДн, то есть сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;

– 4 группа — иные категории ПДн, не представленные в трех предыдущих группах.

По форме отношений между организацией и субъектами обработка подразделяется на 2 вида:

– обработка ПДн работников (субъектов, с которыми данная организация связана трудовыми отношениями);

– обработка ПДн субъектов, не являющихся работниками данной организации.

По количеству субъектов, ПДн которых обрабатываются, определены 2 категории:

– менее 100 000 субъектов;

– более 100 000 субъектов;

И наконец, типы актуальных угроз:

– угрозы 1-го типа связаны с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн;

– угрозы 2-го типа связаны с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн;

– угрозы 3-го типа не связаны с наличием недекларированных возможностей в ПО, используемом в ИСПДн.

Установив исходные данные, для конкретной ИСПДн определяется УЗ ПДн.

Определим, для примера, уровень защищенности для ИСПДн «Бухгалтерия» (рис. 4.1).

Исходные данные ИСПДн «Бухгалтерия»:

1. Категория обрабатываемых ПДн – иные;
2. В ИС обрабатываются ПДн сотрудников;
3. Количество субъектов – 190 (менее 100 000);
4. Системное ПО сертифицировано – тип актуальных угроз – 2.

Уровень защищенности системы определяется в соответствии с методикой, представленной в [3], где определены типы угроз, а также требования по уровню защищенности в соответствии с вышеприведенными критериями.

Категории ПДн		Специальные			Биометрические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Рис. 4.1- Определение уровня защищенности ИСПДн «Бухгалтерия»

Уровень защищенности ПДн ИСПДн «Бухгалтерия» – 3 УЗ

В данном случае системное ПО сертифицировано, а следовательно для системы будут актуальны угрозы 2-го типа: «Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе» - выдержка из 6-го пункта [3].

2.2Определение актуальных угроз ИСПДн

Оценка актуальности той или иной угрозы производится на основании:

– коэффициента вероятности реализации угрозы;

– показателя опасности (ущерба).

Для определения коэффициента вероятности реализации угрозы применяются два показателя:

– уровень исходной защищенности ИСПДн;

– возможность реализации рассматриваемой угрозы.

1. *Под уровнем исходной защищенности* понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС. Показатели исходной защищенности определяются по табл. П4 Приложения 6. Необходимые характеристики для каждого варианта отображены в табл.П 2 Приложения 6. В табл. 4.1 для примера представлены уровни защищенности ИСПДн «Бухгалтерия».Уровень исходной защищенности ИСПДн определяется на основании технических и эксплуатационных характеристик (по 7 признакам) путем подсчета в % соотношении Высоких, Средних и Низких показателей защищенности ИСПДн.

Таблица 4.1

Исходная защищенность ИСПДн «Бухгалтерия»

№	Технические и эксплуатационные характеристики	Уровень защищенности
1	По территориальному размещению.	Высокий

Продолжение табл.4.1

2	По наличию соединения с сетями общего пользования.	Низкий
3	По встроенным (легальным) операциям с записями баз персональных данных.	Низкий
4	По разграничению доступа к персональным данным.	Средний
5	По наличию соединений с другими базами ПДн иных ИСПДн.	Высокий
6	По уровню (обезличивания) ПДн.	Низкий
7	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки.	Средний

Для определения исходного уровня защищенности ИСПДн можно воспользоваться табл. 4.2.

Таблица 4.2

Определение исходного уровня защищенности ИСПДн (U_1)

Уровень исходной защищенности ИСПДн (U_1)	Высокий	Средний	Низкий	U_1
Высокий	70%	30%	0	0
Средний	70%		30%	5
Низкий	иначе			10

Для ИС «Бухгалтерия» Высоких - 2 из 7 показателей (менее 70%), Высоких и Средних - 4 из 7 показателей (менее 70%). Следовательно, *уро-*

вень исходной защищенности для данной ИС «Бухгалтерия» – Низкий, U_1 *=10.*

2. Обращаемся к [5] и определяем *модель угроз выбранной ИСПДн.* Для ИСПДн «Бухгалтерия» подходит «Типовая модель угроз безопасности ПДн, обрабатываемых в локальных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена».

При обработке ПДн данной ИС, возможна реализация следующих угроз безопасности ПДн:

– угрозы утечки информации по техническим каналам;

– угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам мы не рассматриваем, так как ранее установили, что среди них для нас нет актуальных.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена. Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн, включают в себя следующие угрозы:

– угрозы, реализуемые в ходе загрузки ОС и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

– угрозы, реализуемые после загрузки ОС и направленные на выполнение НСД с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) ОС или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД

программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);

– угрозы внедрения вредоносных программ.

– угрозы из внешних сетей включают в себя:

– угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;

– угрозы сканирования, направленные на выявление типа ОС ИС-ПДн, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;

– угрозы выявления паролей;

– угрозы получения НСД путем подмены доверенного объекта;

– угрозы типа «Отказ в обслуживании»;

– угрозы удаленного запуска приложений;

– угрозы внедрения по сети вредоносных программ.

3. Теперь определяем *вероятность реализации каждой угрозы ПДн* ($\mathbf{U_2}$).

Числовой коэффициент ($\mathbf{U_2}$) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

– маловероятно – отсутствуют объективные предпосылки для осуществления угрозы ($\mathbf{U_2}$ = 0);

– низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($\mathbf{U_2}$ = 2);

– средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны ($\mathbf{U_2}$ = 5);

– высокая вероятность – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности не приняты ($\mathbf{U_2}$

= 10).

Предполагаем, что экспертным путем уже определены вероятности реализуемости угроз для выбранной ИСПДн. В табл. П4 Приложения 6 для каждого варианта даны наиболее вероятные угрозы (вероятность возникновения $U_2 > 0$). Другие существующие угрозы считаем как маловероятные ($U_2 = 0$).

Оценку вероятности реализации угроз ИСПДн «Бухгалтерия» можно посмотреть в табл. 4.3.

Таблица 4.3

Оценка вероятности реализации угроз ИСПДн «Бухгалтерия»

Угрозы НСД	Вероятность реализации угрозы	Оценка вероятности реализации угрозы (U_2)
1. Угрозы уничтожения, хищения аппаратных средств ИС носителей информации путем физического доступа к элементам ИС.		
1.1. Кража ПЭВМ.	Маловероятно	0
1.2. Кража носителей информации.	Маловероятно	0
1.3. Кража ключей и атрибутов доступа.	Маловероятно	0
1.4. Кража, модификация, уничтожение информации.	Маловероятно	0
1.5. Вывод из строя узлов ПЭВМ, каналов связи.	Маловероятно	0
1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ.	Маловероятно	0
1.7. Несанкционированное отключение средств защиты.	Маловероятно	0
2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
2.1. Действия вредоносных программ (вирусов).	Низкая вероятность	2
2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных.	Маловероятно	0
2.3. Установка ПО, не связанного с исполнением служебных обязанностей.	Маловероятно	0

Продолжение табл.4.3

Угрозы НСД	Вероятность реализации угрозы	Оценка вероятности реализации угрозы (U_2)
3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и системы защиты в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.		
3.1. Утрата ключей и атрибутов доступа.	Низкая вероятность	2
3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками.	Низкая вероятность	2
3.3. Непреднамеренное отключение средств защиты.	Маловероятно	0
3.4. Выход из строя аппаратно-программных средств.	Низкая вероятность	2
3.5. Сбой системы электроснабжения.	Маловероятно	0
3.6. Стихийное бедствие.	Маловероятно	0
4. Угрозы преднамеренных действий внутренних нарушителей.		
4.1. Доступ к информации, ее модификация или уничтожение лицами, не допущенными к ее обработке.	Маловероятно	0
4.2. Разглашение информации, ее модификация или уничтожение сотрудниками, допущенными к ее обработке.	Низкая вероятность	2
5.Угрозы несанкционированного доступа по каналам связи.		
5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИС и принимаемой из внешних сетей информации:		
5.1.1. Перехват за переделами контролируемой зоны.	Низкая вероятность	2
5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями.	Маловероятно	0
5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	0

Продолжение табл.4.3

Угрозы НСД	Вероятность реализации угрозы	Оценка вероятности реализации угрозы (U_2)
5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИС, топологии сети, открытых портов и служб, открытых соединений и др.	Низкая вероятность	2
5.3.Угрозы выявления паролей по сети.	Низкая вероятность	2
5.4.Угрозы навязывание ложного маршрута сети.	Низкая вероятность	2
5.5.Угрозы подмены доверенного объекта в сети.	Низкая вероятность	2
5.6.Угрозы внедрения ложного объекта как в ИС, так и во внешних сетях.	Низкая вероятность	2
5.7.Угрозы удаленного запуска приложений.	Низкая вероятность	2
5.8.Угрозы внедрения по сети вредоносных программ.	Низкая вероятность	2

4. По итогам оценки исходного уровня защищенности (U_1) и вероятности реализации угрозы (U_2), рассчитывается *коэффициент реализуемости угрозы* (U) и определяется *возможность реализации угрозы.*

Коэффициент реализуемости угрозы U определяется соотношением:

$$U = (U_1 + U_2) / 20.$$

Возможность реализации угрозы определяется по табл. П5 Приложения 6.

Возможность реализации угроз ИСПДн «Бухгалтерия» представлена в табл. 4.4.

Таблица 4.4

Реализуемость угроз ИСПДн «Бухгалтерия» (U)

Угрозы НСД	Коэффициент реализуемости угрозы	Возможность реализации угрозы
1. Угрозы уничтожения, хищения аппаратных средств ИС носителей информации путем физического доступа к элементам ИС.		
1.1. Кража ПЭВМ.	0,5	средняя
1.2. Кража носителей информации.	0,5	средняя
1.3. Кража ключей и атрибутов доступа.	0,5	средняя
1.4. Кража, модификация, уничтожение информации.	0,5	средняя
1.5. Вывод из строя узлов ПЭВМ, каналов связи.	0,5	средняя
1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ.	0,5	средняя
1.7. Несанкционированное отключение средств защиты.	0,5	средняя
2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
2.1. Действия вредоносных программ (вирусов).	0,6	средняя
2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных.	0,5	средняя
2.3. Установка ПО, не связанного с исполнением служебных обязанностей.	0,5	средняя
3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и системы защиты в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.		
3.1. Утрата ключей и атрибутов доступа.	0,6	средняя
3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками.	0,6	средняя
3.3. Непреднамеренное отключение средств защиты.	0,5	средняя
3.4. Выход из строя аппаратно-программных средств.	0,6	средняя

Продолжение табл.4.4

Угрозы НСД	Коэффициент реализуемости угрозы	Возможность реализации угрозы
3.5. Сбой системы электроснабжения.	0,5	средняя

3.6. Стихийное бедствие.	0,5	средняя
4. Угрозы преднамеренных действий внутренних нарушителей.		
4.1. Доступ к информации, ее модификация или уничтожение лицами, не допущенными к ее обработке.	0,5	средняя
4.2. Разглашение информации, ее модификация или уничтожение сотрудниками, допущенными к ее обработке.	0,6	средняя
5.Угрозы несанкционированного доступа по каналам связи.		
5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИС и принимаемой из внешних сетей информации:		
5.1.1. Перехват за переделами контролируемой зоны.	0,6	средняя
5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями.	0,5	средняя
5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0,5	средняя
5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИС, топологии сети, открытых портов и служб, открытых соединений и др.	0,6	средняя
5.3.Угрозы выявления паролей по сети.	0,6	средняя
5.4.Угрозы навязывание ложного маршрута сети.	0,6	средняя
5.5.Угрозы подмены доверенного объекта в сети.	0,6	средняя
5.6.Угрозы внедрения ложного объекта как в ИС, так и во внешних сетях.	0,6	средняя
5.7.Угрозы удаленного запуска приложений.	0,6	средняя
5.8.Угрозы внедрения по сети вредоносных программ.	0,6	средняя

5. *Оценка опасности угроз* производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

– низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;

– средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов ПДн;

– высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

Предполагаем, что оценка опасности угроз произведена. Данные о последствиях реализации угроз берутся из табл. П3 Приложения 6. Считаем, что для остальных угроз, где U_2 = 0, показатель опасности угроз низкий или средний.

Оценка опасности угроз для ИСПДн «Бухгалтерия» представлена в табл. 4.5.

Таблица 4.5

Оценка опасности угроз безопасности ИСПДн «Бухгалтерия»

Угрозы НСД	Опасность угрозы
1. Угрозы уничтожения, хищения аппаратных средств ИС носителей информации путем физического доступа к элементам ИС.	
1.1. Кража ПЭВМ.	низкая
1.2. Кража носителей информации.	низкая
1.3. Кража ключей и атрибутов доступа.	низкая
1.4. Кража, модификация, уничтожение информации.	низкая
1.5. Вывод из строя узлов ПЭВМ, каналов связи.	низкая
1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ.	низкая
1.7. Несанкционированное отключение средств защиты.	средняя

Продолжение табл.4.5

Угрозы НСД	Опасность угрозы
2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.1. Действия вредоносных программ (вирусов).	низкая
2.2. Недекларированные возможности системного ПО и ПО для обработки	низкая

персональных данных.	
2.3. Установка ПО, не связанного с исполнением служебных обязанностей.	средняя
3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и системы защиты в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
3.1. Утрата ключей и атрибутов доступа.	низкая
3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками.	средняя
3.3. Непреднамеренное отключение средств защиты.	низкая
3.4. Выход из строя аппаратно-программных средств.	низкая
3.5. Сбой системы электроснабжения.	средняя
3.6. Стихийное бедствие.	низкая
4. Угрозы преднамеренных действий внутренних нарушителей.	
4.1. Доступ к информации, ее модификация или уничтожение лицами, не допущенными к ее обработке.	низкая
4.2. Разглашение информации, ее модификация или уничтожение сотрудниками, допущенными к ее обработке.	средняя
5.Угрозы несанкционированного доступа по каналам связи.	
5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИС и принимаемой из внешних сетей информации:	
5.1.1. Перехват за переделами контролируемой зоны.	низкая
5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями.	низкая
5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая

Продолжение табл.4.5

Угрозы НСД	Опасность угрозы
5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИС, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
5.3.Угрозы выявления паролей по сети.	низкая
5.4.Угрозы навязывание ложного маршрута сети.	низкая
5.5.Угрозы подмены доверенного объекта в сети.	низкая

5.6.Угрозы внедрения ложного объекта как в ИС, так и во внешних сетях.	низкая
5.7.Угрозы удаленного запуска приложений.	низкая
5.8.Угрозы внедрения по сети вредоносных программ.	низкая

6. В соответствии с правилами отнесения угрозы безопасности к актуальной (табл. 4.6), *определяются актуальные и неактуальные угрозы.*

Таблица 4.6

Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

На основе проведённого исследования ИСПДн «Бухгалтерия», для данной системы принимается решение об актуальности следующих угроз:

– несанкционированное отключение средств защиты;

– установка ПО, не связанного с исполнением служебных обязанностей;

– непреднамеренная модификация (уничтожение) информации сотрудниками;

– сбой системы электроснабжения;

– разглашение информации, ее модификация или уничтожение. Как пример, для ИСПДн «Бухгалтерия» ниже представлены меры по устранению угроз, актуальных для данной системы:

– введение контроля доступа в помещения, закрытие дверей на замок, проведение пользователям ИСПДн инструктажа о работе с ПДн;

– проведение пользователям инструктажа о политике установки ПО, осуществление необходимого контроля;

– осуществление резервного копирования обрабатываемых ПДн и проведение необходимого инструктажа;

– подключение ко всем ключевым элементам ИСПДн источников бесперебойного питания;

– осведомление пользователей о порядке работы с ПДн, а так же подписание «Соглашения о неразглашении».

3 Домашнее задание

1 Изучить материалы рекомендуемых источников информации, текст которых вынесен в Приложения 1-5.

2 Внимательно ознакомиться с материалом раздела 2 настоящих методических указаний и эти сведения использовать при выполнении работы.

4 Порядок выполнения лабораторной работы

1. Выбрать вариант, в котором представлена ИСПДн с соответствующими ей исходными данными (Приложение 6, табл.П1). Номер выбранного варианта должен совпадать с номером бригады учебной группы.

2. По методике, описанной выше и представленной в [3], определить УЗ ПДн. Для наглядности можно воспользоваться табл. 4.7.

Таблица 4.7

Определение уровня защищенности ПДн

Категории ПДн	Специальные			Биометрические	Иные			Общедоступные		
Собственные работники	нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов	>100	<100			>100	<100		>100	<100	

		тыс.	тыс.			тыс.	тыс.		тыс.	тыс.	
Тип актуальных угроз	1	1УЗ	1УЗ	1УЗ	1УЗ	1УЗ	2УЗ	2УЗ	2УЗ	2УЗ	2УЗ
	2	1УЗ	2УЗ	2УЗ	2УЗ	2УЗ	3УЗ	3УЗ	2УЗ	3УЗ	3УЗ
	3	2УЗ	3УЗ	3УЗ	3УЗ	3УЗ	4УЗ	4УЗ	4УЗ	4УЗ	4УЗ

В зависимости от уровня защищенности ПДн определяется перечень требований, выполнение которых необходимо для нейтрализации угроз безопасности ПДн.

3. На основе исходных данных выбранной ИСПДн (Приложение 6, табл.П2-П6) и методике, представленной в [4-5], определить актуальные угрозы ИСПДн и описать методы и средства их предотвращения.

4. Для определения актуальных угроз выбранной ИСПДн воспользуйтесь методикой , результатами рассмотренного примера для ИСПДн «Бухгалтерия» и получите следующие результаты:

– рассчитайте уровень исходной защищенности выбранной ИСПДн (с.40-42);

– обоснуйте выбор модели угроз рассматриваемой ИСПДн (с 42-43);

– рассчитайте вероятность реализации каждой угрозы ПДн (с.43-46);

– рассчитайте коэффициент реализуемости угрозы (U) и определите возможность реализации угрозы (с.46-48);

– выполните оценку опасности угроз (с.48-50);

– на основании выполненных расчётов определите актуальные и неактуальные угрозы (с.50-52).

5 Разработайте пакет внутренних документов, регламентирующих обработку и защиту ПДн. Примерный перечень «Организационно-распорядительной, регламентной и информационно-справочной документации ИСПДн» помещён в Приложение 7.

5 Содержание отчёта

1 Цель работы.

2 Технические характеристики корпоративной ИСПДн, подлежащей защите (по результатам п.1 лабораторного задания).

3 Описание методики и результаты расчёта УЗ ПДн (по результатам п.2 лабораторного задания).

4 Перечень требований, выполнение которых необходимо для нейтрализации угроз безопасности ПДн в зависимости от уровня защищенности ПДн .

5 Обоснованный перечень актуальных угроз ИСПДн, методы и средства их предотвращения.

6 В качестве обоснования представьте следующие результаты:

– уровень исходной защищенности выбранной ИСПДн;

– обоснование выбора модели угроз рассматриваемой ИСПДн;

– методика и результаты расчёта вероятности реализации каждой угрозы ПДн;

– методика и результаты расчёта коэффициента реализуемости угрозы (U) и возможность реализации угрозы;

– выполненная оценка опасности угроз;

– на основании выполненных расчётов список актуальных и неактуальных угроз .

7 Разработанный пакет внутренних документов, регламентирующих обработку и защиту ПДн.

8 Выводы.

9 Отчёт о выполненной работе оформляется в электронном и распечатанном виде в соответствии с требованиями РД ПГУТИ и сдаётся преподавателю. **Обязательным требованием является наличие титульного листа отчёта.**

6 Список контрольных вопросов

1 Законодательная и нормативная база правового регулирования вопросов защиты персональных данных.

2 Руководящие документы по защите персональных данных.

3 Основные термины, определения и общие положения в области защиты персональных данных.

4 Понятие и классификация информационных систем персональных данных с составлением соответствующего акта.

5 Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

6 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

7 Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных.

7 Список литературы

1 Федеральный закон РФ от 27.07.2006 № 152-ФЗ "О персональных данных" [Электронный ресурс] / Официальный сайт ФСТЭК - Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/107-zakony/365, свободный. – Загл. С экрана.

2 Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс] / Официальный сайт ФСТЭК - Режим доступа: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691, свободный. – Загл. с экрана.

3 Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке

в информационных системах персональных данных" [Электронный ресурс] / Официальный сайт компании «КонсультантПлюс» - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/, свободный. – Загл. с экрана.

4 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 14 февраля 2008 [Электронный ресурс] / Официальный сайт ФСТЭК - Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380, свободный. – Загл. с экрана.

5 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15 февраля 2008 [Электронный ресурс] / Официальный сайт ФСТЭК - Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379, свободный. – Загл. с экрана.