Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

Е.В. Каменева

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность

Оренбург

2019

УДК 004.056:351(076.5)
ББК 32.971.3я+67.401.114я7
К18

Рецензент – доцент, кандидат педагогических наук Е. В. Бурькова

К18 **Каменева Е.В.**
Организационное и правовое обеспечение информационной безопасности : методические указания / Е.В. Каменева; Оренбургский гос. ун-т. - Оренбург: ОГУ, 2019.

Методические указания содержат методику работы с основными нормативными и методическими документами в области информационной безопасности, а также рекомендации по разработке организационной подсистемы информационной безопасности предприятия.

Методические указания предназначены для выполнения лабораторных работ студентами, изучающими дисциплину «Организационное и правовое обеспечение информационной безопасности» для обучающихся по направлению подготовки 10.03.01 Информационная безопасность.

УДК 004.056:351(076.5)
ББК 32.971.3я+67.401.114я7

Содержание

Введение

Методические указания предназначены для выполнения лабораторных работ студентами, изучающими дисциплины «Организационное и правовое обеспечение информационной безопасности» обучающихся по направлению подготовки 10.03.01 Информационная безопасность. Каждая работа включает теоретическое изложение материала, порядок выполнения и контрольные вопросы для самоподготовки.

Лабораторный курс содержит четыре работы, при выполнении которых студенты получать навыки:

- работы с методическими и руководящими документами по защите информации;
- применения организационных мер защиты информации;
- работы с нормативно-правовыми актами;
- по выявлению угроз информационной безопасности объекта;
- ведения документов учета, обработки, хранения и передачи конфиденциальной информации;
- организации построения систем защиты информации.

К выполнению лабораторной работы следует приступать после ознакомления с теоретической частью соответствующего раздела и рекомендациями, приведенными в конкретной работе.

Практикум рекомендован преподавателям как вспомогательный материал в организации и проведении занятий, а также студентам - для аудиторного и самостоятельного освоения лабораторной части дисциплины «Организационное и правовое обеспечение информационной безопасности».

1 Лабораторная работа № 1. Закрепление права предприятия на защиту информации в нормативных документах

1.1 Цель работы

Освоение метода правовой защиты информации ограниченного доступа на предприятии.

1.2 Теоретическая часть

Организационно-правовое обеспечение информационной безопасности представляет совокупность законов и других нормативно-правовых актов, а также организационных решений, которые регламентируют как общие вопросы обеспечения *защиты информации*, так и организацию, и функционирование защиты конкретных объектов и систем.

Правовые аспекты организационно-правового обеспечения информационной безопасности направлены на достижение следующих целей:

− формирование правосознания граждан по обязательному соблюдению правил защиты конфиденциальной информации;

− определение мер ответственности за нарушение правил защиты информации;

− придание юридической силы технико-математическим решениям вопросов организационно-правового обеспечения защиты информации;

− придание юридической силы процессуальным процедурам разрешения ситуаций, складывающихся в процессе функционирования системы защиты.

Информационные отношения достигли такой ступени развития, на которой оказалось возможным сформировать самостоятельную отрасль законодательства, регулирующую информационные отношения. В эту отрасль, которая целиком посвящена вопросам информационного законодательства, включаются:

− законодательство об интеллектуальной собственности;

− законодательство о средствах массовой информации;

− законодательство о формировании информационных ресурсов и предоставлении информации из них;

− законодательство о реализации права на поиск, получение и использование информации;

− законодательство о создании и применении информационных технологий и средств их обеспечения.

В отрасли права, акты которых включают информационно-правовые нормы, входят конституционное право, административное право, гражданское право, уголовное право, предпринимательское право.

Формирование законодательства в области информационного права в Российской Федерации (РФ) началось, в основном, со времени появления «Концепции правовой информатизации России», утвержденной Указом Президента РФ от 28.06.93 г. № 966. В основе информационного законодательства находится свобода информации и запретительный принцип права (все, что не запрещено законом - разрешено).

Структура информационного законодательства строится исходя из принципа «верховенства закона»: нормы вышестоящего по иерархии акта обладают более высокой юридической силой и являются определяющими для соответствующих норм всех нижестоящих актов.

Иерархия законодательных документов РФ представлена в таблице 1.1.

Таблица 1.1 – Иерархия законодательных документов РФ

<table>
<tr><td colspan="2">Конституция РФ</td></tr>
<tr><td colspan="2">Федеральные конституционные законы РФ</td></tr>
<tr><td colspan="2">Федеральные законы РФ</td></tr>
<tr><td colspan="2">Указы и распоряжения Президента РФ</td></tr>
<tr><td colspan="2">Законодательные акты субъектов РФ</td></tr>
<tr><td>Постановления и распоряжения Правительства РФ</td><td>Нормативные правовые акты высших органов исполнительной власти субъектов РФ</td></tr>
<tr><td>Нормативные правовые акты федеральных органов исполнительной власти</td><td>Нормативные правовые акты органов исполнительной власти субъектов РФ</td></tr>
<tr><td colspan="2">Правовые акты органов местного самоуправления</td></tr>
</table>

В статье 5, ФЗ «Об информации, информационных технологиях и защите информации» от 27.7.2006 г. № 149-ФЗ, сказано: "Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)".

Общедоступная информация - информация, которую нельзя скрывать от общества. Примером служит информация о состоянии окружающей среды, о деятельности органов государственной власти и органов местного самоуправления, документы, накапливаемые в открытых фондах библиотек и архивов. Так же в эту категорию можно отнести нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, правовое положение организаций и полномочия государственных органов, органов местного самоуправления.

Информацией ограниченного доступа является информация представляющая ценность для ее владельца, доступ к которой ограничивается на законном основании. В свою очередь информация ограниченного доступа подразделяется на информацию, составляющую государственную тайну (ГТ) и информацию, соблюдение конфиденциальности которой установлено федеральным законом (конфиденциальная информация (КИ)).

В соответствии с ФЗ РФ от 21.07.1993 N 5485-1 (ред. от 29.07.2018) «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».

Сведения, которые могут быть отнесены к **государственной тайне,** определены в Указе Президента РФ от 30 ноября 1995 г. № 1203.

К ним относятся сведения:

- в военной области;
- о внешнеполитической и внешнеэкономической деятельности;
- в области экономики, науки и техники;

− в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Нельзя засекречивать информацию в качестве государственной тайны:

− если ее утечка (разглашение и т.п.) не влечет ущерба национальной безопасности страны;

− в нарушение действующих законов;

− если сокрытие информации будет нарушать конституционные и законодательные права граждан;

− для сокрытия деятельности, наносящей ущерб окружающей природной среде, угрожающей жизни и здоровью граждан.

Подробный перечень содержится в ст. 5 Закона РФ «О государственной тайне».

Перечень сведений конфиденциального характера опубликован в Указе Президента РФ от 6.03.97 г. № 188 **«Об утверждении перечня сведений конфиденциального характера».**

Коммерческая тайна - сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;

Персональные данные - сведения о фактах, событиях и обстоятельствах частой жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленном федеральными законами случаях;

Служебная тайна - служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;

Профессиональная тайна - 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 и иных сообщений и т.д.);

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

Тайна следствия и судопроизводства - сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с ФЗ от 20 августа 2004 г. № 119-ФЗ и другими нормативными правовыми актами Российской Федерации;

Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 02.10.2007 № 229-ФЗ «Об исполнительном судопроизводстве». (Указом Президента от 13.07.2015г. № 357 Перечень дополнен 7 пунктом)

1.3 Порядок выполнения работы

1 Определить название организации в соответствии с вариантом, указанным в таблице 1.2.

Таблица 1.2 – Варианты заданий для выполнения лабораторной работы

Вариант	Наименование ОИ	Вариант	Наименование ОИ
1	Отделение ПАО Сбербанка России	11	ГБУЗ «МИАЦ»
2	Страховая компания «Согаз»	12	Газпромэнерго
3	Научно-исследовательский институт «Волга-Урал НИПИГаз»	13	Оренбургский центр занятости населения
4	МФЦ г. Оренбург	14	ОГУ
5	Департамент информационных технологий Оренбургской области	15	Пенсионный фонд Росси по г. Оренбургу
6	МУ МВД «Оренбургское»	16	Оренбургский областной Военный комиссариат
7	Оренбургский областной арбитражный суд	17	Казначейство РФ по Оренбургской области
8	Следственный комитет РФ по Оренбургской области	18	Орский завод холодильного оборудования

Продолжение таблицы 1.2

9	ФНС РФ г. Оренбурга Дзержинского района	19	Медногорский медно-серный комбинат
10	ПАО «Стрела»	20	ОАО РОСТЕЛЕКОМ г.Оренбург

2 Разработать организационную структуру предприятия / организации / учреждения в соответствии с заданным вариантом работы. Описать направления работы организации и основные функции его подразделений. Пример организационной структуры приведен на рисунке 1.1.

Рисунок 1.1 – Организационная структура ООО «Светлинский ферроникелевый завод»

3 Разработать схему информационных потоков предприятия / организации / учреждения. Пример схемы информационные потоков приведен на рисунке 1.2.

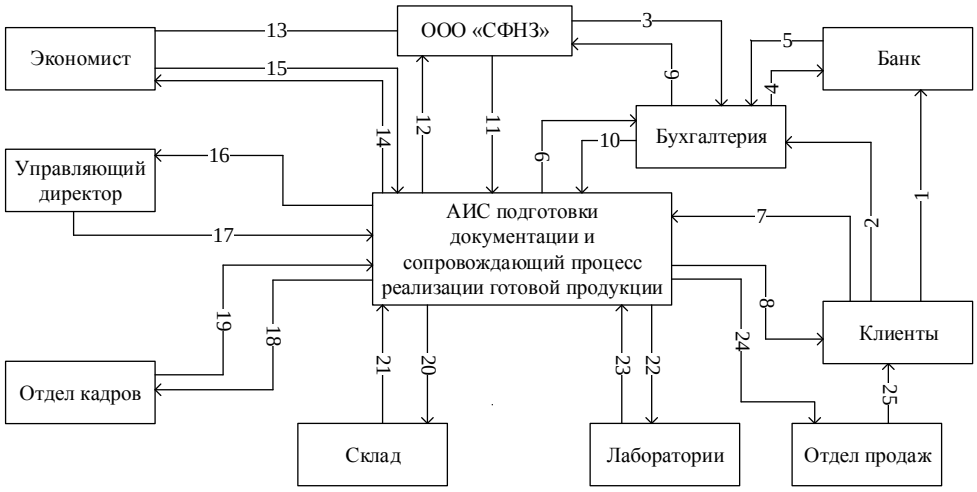

Рисунок 1.2 – Схема информационных потоков организации / предприятия

Схема информационных потоков, в обязательном порядке, сопровождается таблицей (таблица 1.3), в которой приводится их описание и анализ.

Таблица 1.3 – Анализ информационных потоков организации/предприятия

Номер информационного потока	Наименование	Описание
1	Оплата услуг	Производится оплата услуг в Бухгалтерию ООО «СФНЗ» и в банк
2		
3	Запрос финансовой отчетности	Руководство ООО «СФНЗ» запрашивает финансовый отчет в Бухгалтерии
4	Запрос о состоянии счета	Бухгалтерия запрашивает отчет о состоянии счета
⋮	⋮	⋮
25	Продажа	Передача готовой продукции клиентам

4 Провести анализ защищаемых информационных ресурсов предприятия / организации / учреждения.

5 Опираясь на правовую базу в области защиты информации, обосновать право организации/предприятия на защиту информации ограниченного доступа.

1.5 Контрольные вопросы

1 Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне»

2 Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ

3 Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера»

4 Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ

5 С принятием каких законов началось формирование законодательства в информационной сфере?

6 Какие общественные отношения являются предметом правового регулирования в информационной сфере?

7 Какой закон установил принципы правового регулирования отношений, в информационной сфере?

8 Какие документы составляют правовую базу в информационной сфере?

9 Назовите виды информационных ресурсов по принадлежности и по доступности.

10 Относится ли государственная тайна к конфиденциальной информации?

11 Какая информация относится к персональным данным?

12 Существует ли информация, которую запрещено относить к информации ограниченного доступа?

13 Нормативно-правовое регулирование профессиональной тайны в РФ.

14 Признаки и объекты профессиональной тайны.

15 Какие сведения относятся к служебной тайне?

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

17 Чем отличается служебная тайна от профессиональной?

18 Внутренние нормативные документы, которые используются для правовой защиты служебной и КТ.

19 Какой закон регулирует отношения, связанные с отнесением информации к коммерческой тайне?

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

21 Что понимается под убытком в результате разглашения КТ?

22 Определение и виды конкурентной разведки.

23 Какие сведения не могут составлять коммерческую тайну?

24 Какие грифы конфиденциальности может использовать предприятие для обозначения степени важности коммерческой информации?

2 Лабораторная работа №2. Правовые нормы защиты информации в автоматизированных системах

2.1 Цель работы

Освоить порядок классификации автоматизированных систем в защищенном исполнении и методы правовой защиты информации ограниченного доступа, обрабатываемой в них.

2.2 Теоретическая часть

Согласно ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на АС. АС. Термины и определения», под АС понимается система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. В зависимости от вида деятельности выделяют следующие виды АС:

- автоматизированные системы (АС);
- государственные автоматизированные системы (ГАС);
- автоматизированные системы управления (АСУ);
- автоматизированные системы управления технологическим процессом;
- системы автоматизированного проектирования (САПР) и др.

При обработке или хранении в АС информации, не отнесенной к категории секретной, в рамках системы защиты информации (СЗИ) от несанкционированного доступа (НСД) государственным, коллективным, частным и совместным предприятиям, а также частным лицам рекомендуются следующие ***организационные мероприятия***:

- выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;

− определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;

− установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;

− ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;

− получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;

− обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;

− выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;

− организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ от НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;

− разработка СЗИ от НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;

− осуществление приемки СЗИ от НСД в составе АС.

Согласно РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных

систем и требования по защите информации» классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие ***конфиденциальную информацию***.

В целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации АС делят на соответствующие классы по условиям их функционирования.

Дифференциация подхода к выбору методов и средств защиты определяется:

− важностью обрабатываемой информации,

− различием АС по своему составу, структуре, способам обработки информации,

− различием по количественному и качественному составу пользователей и обслуживающего персонала.

Основными этапами классификации АС являются:

− разработка и анализ исходных данных;

− выявление основных признаков АС, необходимых для классификации;

− сравнение выявленных признаков АС с классифицируемыми;

− присвоение АС соответствующего класса защиты информации от НСД.

Необходимыми исходными данными для проведения классификации конкретной АС являются:

− перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

− перечень лиц, имеющих доступ к штатным средствам, АС, с указанием их уровня полномочий;

− матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

− режим обработки данных в АС.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

− наличие в АС информации различного уровня конфиденциальности;

− уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

− режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС. Деление АС по группам представлено на рисунке XX.

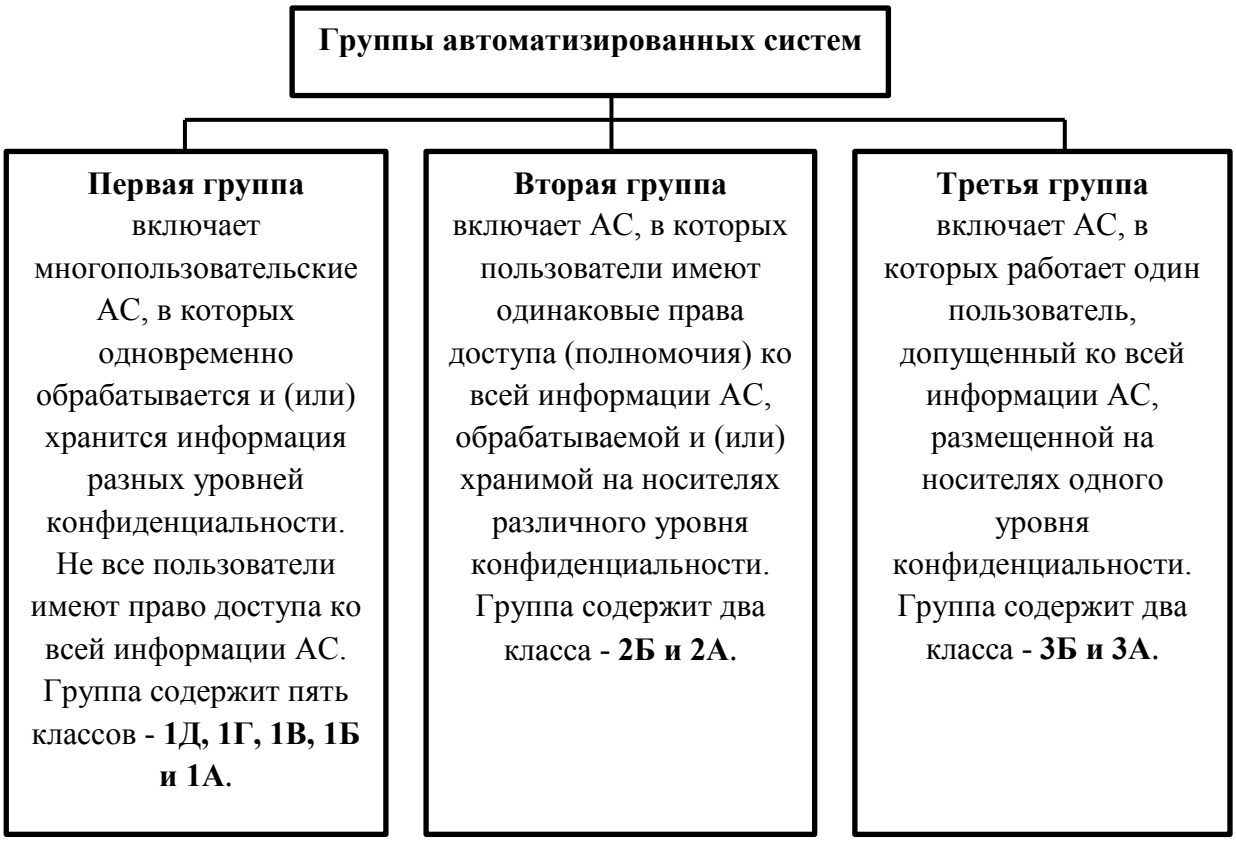

Рисунок 2.1 – Группы автоматизированных систем

В соответствии с РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» устанавливается следующий порядок классификации АС в зависимости от вида сведений конфиденциального/секретного характера:

− АС, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г;

− АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д;

− АС, обрабатывающие информацию, составляющую коммерческую тайну, режим защиты которой определяет ее собственник, по уровню защищенности к классам 3Б, 2Б и не ниже 1Д (если по решению руководителя предприятия не предъявляются более высокие требования);

− АС, обрабатывающие информацию, составляющую государственную тайну, в зависимости от режим обработки данных к классам 3А, 2А, 1В, 1Б, 1А.

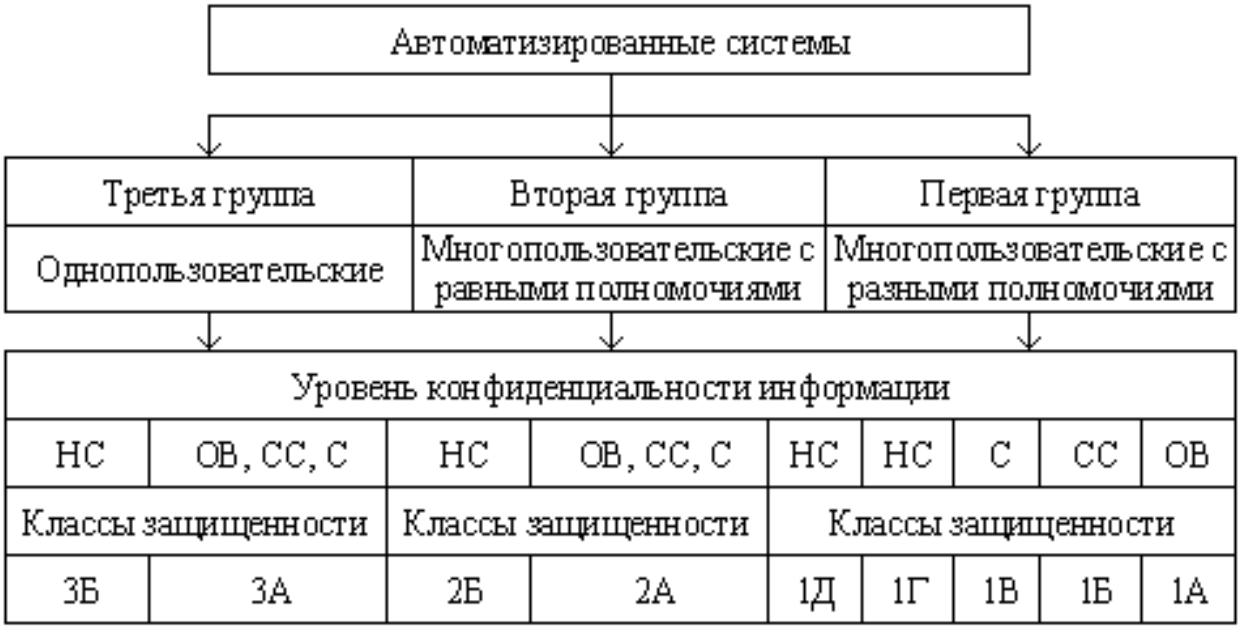

Рисунок 2.2 – Классификация автоматизированных систем

Наибольшие требования по защиты информации, обрабатываемой в АС, предъявляются к АС класса 1А, наименьшие – к 3Б.

Наибольшие требования по защиты информации, обрабатываемой в АС, предъявляются к АС класса 1А, наименьшие – к 3Б.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации в АС от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), которая состоит из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

2.3 Задание на лабораторную работу

1 Разработать структурную схему АС для предприятия / организации / учреждения из лабораторной работы №1. Пример структурной схемы АС приведен на рисунке 2.3

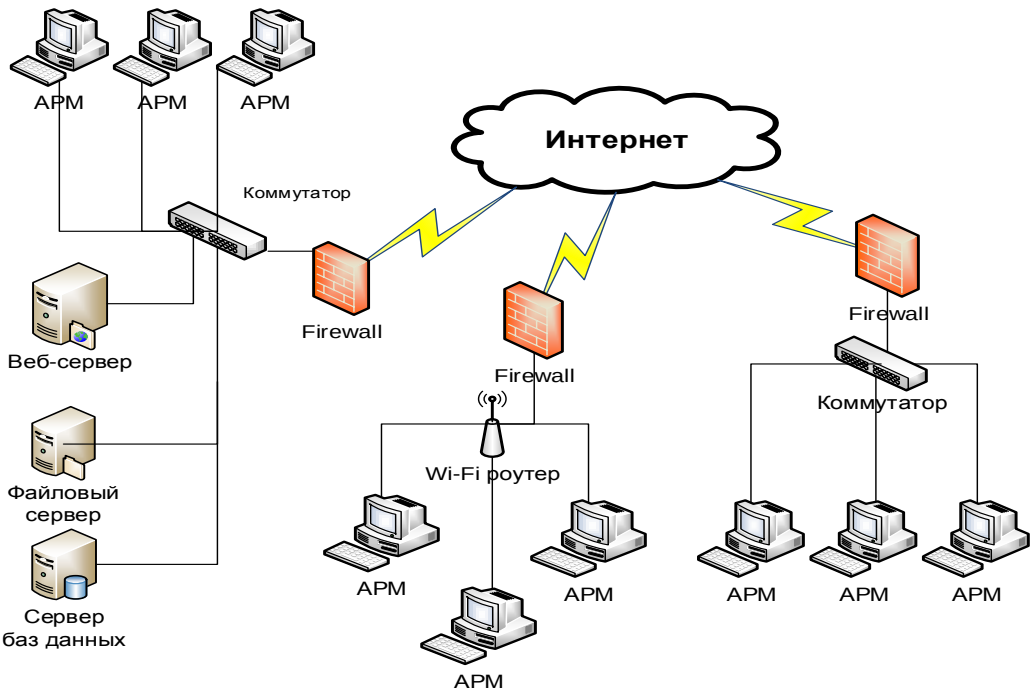

Рисунок 2.3 – Структурная схема АС предприятия / организации / учреждения

2 Проанализировать (составить таблицу) аппаратное обеспечение АС предприятия / организации / учреждения.

3 Проанализировать (составить таблицу) программное обеспечение предприятия / организации / учреждения.

4 Провести классификацию АС предприятия / организации / учреждения.

5 Определить недостатки АС предприятия / организации / учреждения, на основе требований предъявляемых в РД «Автоматизированные системы защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

2.4 Контрольные вопросы

1 РД «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г.

2 РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» от 30 марта 1992 г.

3 Что представляет собой документ «Политика безопасности»?

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

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

6 Какие документы необходимо представить для присвоения класса защищенности?

7 Какие классификационные признаки являются определяющими при установлении класса АС?

8 Сколько классов АС существует и чем они различаются?

9 От чего зависит выбор класса защищенности СВТ для АС, создаваемых на базе защищенных СВТ?

10 Где указаны требования к безопасности компьютерных сетей в РФ?

3 Лабораторная работа №3. Лицензирование деятельности в области защиты информации

3.1 Цель работы

Освоить порядок получения лицензии в области защиты информации.

3.2 Теоретическая часть

Деятельность в области защиты информации ограниченного доступа подлежит обязательному лицензированию. Согласно закону от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», отдельным организациям требуется иметь лицензию ФСТЭК России на оказание услуг в области защиты конфиденциальной информации.

Лицензированием в области защиты информации называется деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации. Государственная политика в области лицензирования отдельных видов деятельности и обеспечения защиты жизненно важных интересов личности, общества и государства определяется Постановление Правительства РФ от 21.11.2011 N 957 (ред. от 18.01.2018) «Об организации лицензирования отдельных видов деятельности»

Лицензией называется разрешение на право проведения работ в области защиты информации. Лицензия выдается на конкретные виды деятельности на три года, по истечении которых осуществляется ее перерегистрация в порядке, установленном для выдачи лицензии.

Лицензия выдается в том случае, если предприятие, подавшее заявку на получение лицензии, имеет условия для проведения лицензирования: производственную и испытательную базу, нормативную и методическую документацию, располагает научным и инженерно-техническим персоналом.

В ст.12 ФЗ перечислены виды деятельности, на которые требуется *лицензия*. В контексте информационной безопасности *лицензия* требуется на следующие виды деятельности:

1) разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

2) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;

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

4) разработка и производство средств защиты конфиденциальной информации;

5) деятельность по технической защите конфиденциальной информации;

6) осуществление работ, связанных с использованием сведений, составляющих государственную тайну (только для юридических лиц);

7) деятельность, связанная с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну (только для юридических лиц);

8) осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (только для юридических лиц).

В таблице 3.1. показано, в какой лицензирующий орган, в зависимости от осуществляемого вида деятельности, необходимо подавать документы.

Таблица 3.1 – Лицензирующие органы в области защиты информации

Вид деятельности	Лицензирующие органы	
	ФСБ	ФСТЭК
1	+	
2	+	
3	+	
4	+	+
5		+
6	+	
7	+	
8	+	

В рамках рассматриваемых видов деятельности были выпущены отдельные постановления Правительства Российской Федерации, разъясняющие порядок лицензирования. Среди них:

− Постановление Правительства РФ от 21.11.2011 N 957 (ред. от 18.01.2018) «Об организации лицензирования отдельных видов деятельности»

− Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации»;

− Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 15.06.2016) «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»;

− Постановление Правительства РФ от 15.04.1995 № 333 (ред. от 23.08.2018 N 984) «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;

− Постановление Правительства РФ от 16.04.2012 № 313 «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»

Для получения лицензии соискатель должен направить в лицензирующий орган заполненное заявление, в котором указываются:

- для юридического лица: полное и сокращенное наименование и организационно-правовая форма, адреса, где планируется ведение лицензируемого вида деятельности, государственный регистрационный номер записи о создании юридического лица и данные документа, подтверждающего внесение в реестр юридических лиц РФ, номера телефонов и адрес электронной почты юр. лица.

- для индивидуального предпринимателя: полное ФИО, место жительства, адреса мест, где планируется ведение лицензируемой деятельности, данные документа, удостоверяющего личность (например, паспорта), государственный регистрационный номер записи о регистрации и данные документа, подтверждающего факт внесения сведений об индивидуальном предпринимателе в единый государственный реестр индивидуальных предпринимателей.

- ИНН и данные документа, подтверждающего постановку соискателя на учет в налоговом органе;

- лицензируемый вид деятельности;

– доказательства уплаты государственной пошлины за получение лицензии;

– реквизиты документов, перечень которых определяется положением о лицензировании конкретного вида деятельности и которые свидетельствуют о соответствии соискателя лицензии лицензионным требованиям.

К заявлению соискатель должен приложить копии документов в соответствии с положением о лицензировании конкретного вида деятельности и опись прилагаемых документов. Следует отметить, что в последних редакциях закона предусмотрена электронная *отправка* документов в лицензирующий орган с электронной подписью соискателя. В течение трех рабочих дней лицензирующий орган принимает решение о соответствии предоставленных документов. В случае принятия документов на рассмотрение в срок не позднее 45 рабочих дней принимается решение об отказе или предоставлении лицензии соискателю. Решение о предоставлении лицензии или об отказе в ее предоставлении оформляется приказом (распоряжением) лицензирующего органа.

Уведомление о принятии решения вручается или отправляется соискателю в письменной форме. Если решение отрицательное, должны указываться причины отказа и реквизиты акта проверки возможности выполнения соискателем лицензии лицензионных требований и условий, если причиной отказа является невозможность выполнения соискателем лицензии указанных требований и условий.

К соискателю лицензии предъявляются следующие требования:

– в штате **по основному месту работы** в соответствии со штатным расписанием руководителя и(или) уполномоченного руководить работами лица, имеющих высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности **не менее 3 лет**, или высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области проводимых работ по лицензируемому виду деятельности **не менее 5 лет**, или иное высшее образование и стаж работы в области проводимых

работ по лицензируемому виду деятельности не менее 5 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов);

– не менее двух инженерно-технических работников имеющих высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности **не менее 3 лет** или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов);

– наличие помещений, принадлежащих на праве собственности или ином законном основании, в которых созданы необходимые условия для осуществления лицензируемого вида деятельности;

– наличие необходимого оборудования, принадлежащего на праве собственности или ином законном основании, в соответствии с перечнем, определяемым ФСТЭК;

– использование принадлежащих лицензиату на праве собственности или ином законном основании автоматизированных систем, предназначенных для обработки конфиденциальной информации, а также средств защиты такой информации, прошедших процедуру оценки соответствия, аттестованных и (или) сертифицированных по требованиям безопасности информации, в соответствии с законодательством Российской Федерации;

– наличие технической и технологической документации, национальных стандартов и методических документов в соответствии с определенным ФСТЭК перечнем.

Следует отметить, что если трактовать ФЗ «О лицензировании отдельных видов деятельности» буквально, то *лицензия* нужна всем организациям, которые

пытаются защитить свою информацию. *По* этому поводу в 2012 г. было много дискуссий и вопросов к регулятору. Результатом стало *информационное сообщение* ФСТЭК от 30 мая 2012 г. N 240/22/2222:

«…получение юридическим лицом лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации является обязательным в случае, если эта деятельность направлена на получение прибыли от выполнения работ или оказания услуг по технической защите конфиденциальной информации и (или) она необходима для достижения целей деятельности, предусмотренных в учредительных документах юридического лица, а также, если это юридическое лицо (уполномоченное лицо) обеспечивает техническую защиту конфиденциальной информации при ее обработке в соответствии с Федеральным законом "Об информации, информационных технологиях и о защите информации" по поручению обладателя информации конфиденциального характера и (или) заказчика информационной системы».

3.3 Порядок выполнения работы

1 Выбрать абстрактную организацию и определить для нее вид деятельности в области информационной безопасности.

2 Разработать пакет документов для получения лицензии по выбранному, виду деятельности, который содержит:

− заявление в лицензирующий орган;

− таблицу, содержащую список сотрудников, их квалификацию, контактные данные;

− правоустанавливающие документы на помещения, предназначенные для осуществления лицензируемого вида деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним (в случае, если такие права зарегистрированы в указанном реестре, - сведения об этих помещениях);

− технические паспорта и аттестаты соответствия защищаемых помещений требованиям безопасности информации;

− технические паспорта автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации (с приложениями), актов классификации автоматизированных систем по требованиям безопасности информации, планов размещения основных и вспомогательных технических средств и систем, аттестатов соответствия автоматизированных систем требованиям безопасности информации или сертификатов соответствия автоматизированных систем требованиям безопасности информации, а также перечень защищаемых в автоматизированных системах ресурсов, описание технологического процесса обработки информации в автоматизированных системах;

− документов, подтверждающих право соискателя лицензии на программы для электронно-вычислительных машин и базы данных, планируемые к использованию при осуществлении лицензируемого вида деятельности;

− документы, содержащие сведения о наличии контрольно-измерительного, производственного и испытательного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемого вида деятельности, с приложением копий документов о поверке (калибровке) и маркировании контрольно-измерительного оборудования, а также документов, подтверждающих права соискателя лицензии на использование указанного оборудования, средств защиты информации и средств контроля защищенности информации;

− документы, содержащие сведения об имеющихся технической и технологической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг, предусмотренных пунктом 4 настоящего Положения, с приложением копий документов, подтверждающих, что документы, содержащие информацию ограниченного доступа, получены в установленном законодательством Российской Федерации порядке;

− если лицензируемый вид деятельности – «услуги по мониторингу информационной безопасности средств и систем информатизации» - копии документов, подтверждающих наличие необходимой системы производственного контроля в соответствии с установленными стандартами.

3.5 Контрольные вопросы

1 Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности».

2 Постановление Правительства РФ от 21.11.2011 N 957 (ред. от 18.01.2018) «Об организации лицензирования отдельных видов деятельности»

3 Нормативно-правовое регулирование деятельности в области защиты конфиденциальной информации

4 Какие виды деятельности в области защиты информации, содержащей государственную тайну, подлежат обязательному лицензированию?

5 Какие виды деятельности в области защиты конфиденциальной информации подлежат обязательному лицензированию?

6 Какие лицензионные требования предъявляются к соискателю лицензии?

7 Порядок лицензирования, срок действия лицензии.

8 Назовите причины, по которым лицензирующий орган может отказать в выдаче лицензии или отозвать ее.

4 Лабораторная работа №4. Создание организационной подсистемы информационной безопасности предприятия

4.1 Цель работы

Освоить методику оформления организационно-распорядительных документов, регламентирующих работу по защите информации в организации.

4.2 Теоретическая часть

Организационная защита информации является основой и важнейшим элементом в общей системе защиты информации предприятия, с высокой эффективностью обеспечивающим ее защиту при условии соблюдения должностными лицами предприятия норм и правил защиты информации, определенных в соответствующих нормативно-методических документах.

Организационная защита информации призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-технические и программно-аппаратные) реализовать на практике спланированные руководством предприятия меры по защите информации.

Цель принимаемых руководством предприятия и должностными лицами организационных мер — исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите.

Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

Используются два примерно равнозначных определения организационной зашиты информации.

Организационная защита информации — составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационная защита информации на предприятии — регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

К основным организационным мероприятиям относят:

1 Организацию режима и охраны. Их цель - исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей.

2 Организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил ЗИ.

3 Организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение.

4 Организацию использования ТС средств сбора, обработки, накопления и хранения конфиденциальной информации.

5 Организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты.

6 Организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Комплексная система защиты информации любой организации строится на базе организационно-распорядительных документов, которые в свою очередь являются элементом подсистемы организационной защиты информации.

Типовая структура организационно-нормативной документации включает в себя следующие документы:

− «Политика безопасности предприятия», предназначен для определения целей и принципов информационной безопасности. Он так же фиксирует перечень объектов информационной безопасности предприятия, а также список необходимых для ее обеспечения внутренних документов. Обычно оформляется в виде положения. Составляется подразделением, отвечающим за безопасность предприятия. Утверждается руководителем предприятия. Актуализируется не реже 1 раза в год или при изменении состава информационных средств.

− «Распределение ответственности за обеспечение безопасности», предназначен для определения ресурсов информационной безопасности и ответственности за доступ к ним. Оформляется в виде распоряжения. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется после изменения политики безопасности или после изменения технологических участков и состава информационных ресурсов.

− «Процесс внедрения новой информационной системы», предназначен для описания процесса внедрения новой информационной системы в действующий бизнес-процесс. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется после изменения политики безопасности предприятия.

− «Инвентаризация ресурсов», предназначен для определения категорий ресурсов, подлежащих инвентаризации. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается

руководителем предприятия. Актуализируется не реже 1 раза в год, перед проведением инвентаризации.

− «Классификация ресурсов», предназначен для классификации ресурсов с точки зрения безопасности. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется не реже 1 раза в год.

− «Безопасность при выборе персонала и работе с ним», предназначен для определения мер по обеспечению безопасности при выборе персонала и работе с ним. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется по необходимости.

− Заключение соглашений о соблюдении режима информационной безопасности со всеми сотрудниками.

− «Реагирование на инциденты в области безопасности, а также на сбои и неисправности», предназначен для определения порядка реагирования на инциденты в области безопасности, на сбои и неисправности информационных систем. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется после возникновения инцидентов, сбоев, неисправностей, а также по необходимости.

− «Должностные инструкции по информационной безопасности», предназначен для установки прав и обязанностей, касающихся информационной безопасности, которые должны быть включены в должностные инструкции сотрудников. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется по необходимости.

− «Процедуры реагирования в случае инцидентов», предназначен для определения порядка реагирования персонала предприятия на возникающие в процессе работы инциденты. Оформляется в виде инструкции. Составляется

подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется по необходимости.

− «Защита от вредоносного ПО (вирусов, троянских коней)», предназначен для определения правил и способов защиты информационных средств от вредоносного ПО. Оформляется в виде инструкции. Составляется подразделением безопасности и подразделением информатизации предприятия. Утверждается руководителем предприятия. Актуализируется при изменении состава информационных ресурсов.

− «Безопасность носителей данных», предназначен для определения правил работы с носителями информации. Оформляется в виде инструкции. Составляется подразделением безопасности. Утверждается руководителем предприятия. Актуализируется по необходимости.

Методические документы, на базе которых проводится разработка пакета организационно-нормативной документации:

– Российское законодательство;

– стандарты в области информационной безопасности РФ и рекомендации регулирующих органов;

– отраслевые стандарты;

– система технических регламентов;

– нормативные документы национальной системы стандартизации;

– ГОСТы по стандартизации;

– требования ФСБ России, ФСТЭК России, МВД и Минобороны;

– международные стандарты (такие как ISO 27001, ISO 27002 и др.).

4.3 Порядок выполнения работы

Для организации из лабораторной работы №1 разработать пакет организационно-распорядительных документов:

− Положение «Политика безопасности предприятия»;

− Распоряжение о распределении ответственности за обеспечение безопасности;

− Инструкцию по внедрении новой информационной системы;

− Инструкцию по инвентаризации ресурсов;

− Заключение соглашения о соблюдении режима информационной безопасности со всеми сотрудниками;

− Инструкция о порядке реагирования на инциденты в области информационной безопасности, а также на сбои и неисправности;

− Инструкцию по защите от вредоносного ПО (вирусов, троянских коней);

− Инструкцию о безопасности носителей данных.

Состав организационно-распорядительных документов приводится в приложении.

4.4 Контрольные вопросы

1 Каким законом регулируются вопросы создания и деятельности частных СБ?

2 Кем выдаются лицензии на осуществление частной детективной и охранной деятельности?

3 Какое оружие и специальные средства могут применяться при осуществлении частной охраной деятельности?

4 Могут ли частные охранники использовать специальные технические средства, предназначенные для негласного получения информации?

5 Правовые основы использования специальных технических средств сбора и защиты информации?

6 Цели и задачи организационной защиты информации, ее связь с правовой защитой информации.

7 Виды угроз информационной безопасности объекту зашиты.

8 Обеспечение режима секретности при проведении НИОКР по секретной (конфиденциальной) тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве.

9 Понятия допуска к секретной (конфиденциальной) информации

10 Понятие доступа к (конфиденциальным) работам, документам и изделиям.

11 Организация работ по защите информации при опубликовании открытых материалов.

12 Обеспечение режима секретности при хранении и транспортировке объектов.

13 Назначение и требования внутриобъектового режима.

14 Цели и задачи пропускного режима.

15 Порядок оформления и выдачи пропусков.

16 Порядок организации информационной безопасности объекта при осуществлении международного научно-технического и экономического сотрудничества.

17 Организация обеспечения режима секретности при проведении служебного совещания.

18 Планирование работ по защите информации в организации

Список использованных источников

1 Организационно-правовое обеспечение информационной безопасности [Текст] : учеб. пособие для студентов вузов, обучающихся по специальностям 090102 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммукационных систем" / [А. А. Стрельцов и др.]; под ред. А. А. Стрельцова. - М.: Академия, 2008. - 256 с.

2 Романов, О. А. Организационное обеспечение информационной безопасности [Текст] : учеб. для вузов / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с. - (Высшее профессиональное образование). - Библиогр.: с. 185.

3 Основы организационного обеспечения информационной безопасности объектов информатизации [Текст] : учеб. пособие / С. Н. Семкин [и др.]. - М. : Гелиос АРВ, 2005. - 192 с.

4 Правовое обеспечение информационной безопасности [Текст] : учеб. пособие для вузов / под ред. С. Я. Казанцева.- 2-е изд., испр. и доп. - М. : Академия, 2007. - 240 с.

5 Федеральной службы по техническому и экспортному контролю (ФСТЭК России). [Официальный сайт]. Режим доступа : http://www.fstec.ru

6 Федеральная Служба безопасности Российской Федерации. [Официальный сайт]. Режим доступа : http://www.fsb.ru

7 Центр по лицензированию, сертификации и защите государственной тайны ФСБ России. [Официальный сайт]. Режим доступа : http://clsz.fsb.ru

8 Общероссийская Сеть распространения правовой информации КонсультантПлюс. [Официальный сайт]. Режим доступа : http://www.consultant.ru

Приложение А

Состав организационно-распорядительных документов

А.1. Документ «Политика безопасности предприятия».

Состав документа:

Определение информационной безопасности, перечень ее составляющих.

Определить понятие информационной безопасности, перечислить объекты информационной безопасности предприятия.

Краткое разъяснение политики безопасности, принципов ее построения и соответствия стандартам и требованиям, имеющим особое значение для организации.

Разъяснение соответствия положений политики местному и международному законодательству.

Требования по обучению персонала вопросам безопасности.

Требования по обнаружению и блокированию вирусов и других вредоносных программ.

Требования обеспечения непрерывность ведения бизнеса.

Ответственность за нарушения политики безопасности.

А.2. Документ «Распределение ответственности за обеспечение безопасности»

Состав документа:

Определение ресурсов, имеющих отношение к информационной безопасности, по каждой системе.

Для каждого ресурса (или процесса) должен быть назначен ответственный сотрудник из числа руководителей. Разграничение ответственности должно быть закреплено документально.

Разграничение ответственности определяется отдельным Приказом или Распоряжением по предприятию.

Для каждого ресурса должен быть определен и закреплен документально список прав доступа (матрица доступа).

А.3. Документ «Процесс внедрения новой информационной системы»

Состав документа:

Соответствие новой системы существующей политике управления пользователями.

Проверка всех внедряемых компонентов на совместимость с существующими частями системы.

А.4. Документ «Инвентаризация ресурсов»

Состав документа.

Информационные ресурсы

Базы данных и файлы данных, системная документация, пользовательская документация, учебные материалы, инструкции по эксплуатации или по поддержке,

планы по поддержанию непрерывности бизнеса, мероприятия по устранению неисправностей, архивы информации или данных

Программные ресурсы

Приложения, операционные системы и системное программное обеспечение, средства разработки

Физические ресурсы

Вычислительная техника, коммуникационное оборудование (маршрутизаторы, телефонные станции, факсы, автоответчики, модемы), магнитные носители (кассеты и диски), другое техническое оборудование (источники питания, кондиционеры).

А.5. Заключение соглашений о соблюдении режима информационной безопасности со всеми сотрудниками

Условия трудового соглашения с работником

- письменная формулировка их должностных обязанностей
- письменная формулировка прав доступа к ресурсам компании (в том числе и информационным)
- соглашение о конфиденциальности
- специальные соглашения о перлюстрации всех видов служебной корреспонденции (мониторинг сетевых данных, телефонных переговоров, факсов и т.д.).

Включение задачи обеспечения безопасности в служебные обязанности всех сотрудников.

А.6. Документ «Реагирование на инциденты в области безопасности, а также на сбои и неисправности»

Предназначен для определения порядка реагирования на инциденты в области безопасности, на сбои и неисправности информационных систем.

Состав документа:

Отчеты об инцидентах

Отчеты о недостатках в системе безопасности

Отчеты о сбоях и неисправностях компьютерных систем

В случае обнаружения нестандартной ситуации необходимо:

- записать все симптомы ее появления;
- компьютер должен быть изолирован и если возможно его использование приостановлено;
- о факте должно быть немедленно сообщено непосредственному руководителю и службе информационной безопасности, они же должны быть проинформированы о результатах анализа причин произошедшего;

Изучение инцидента

Дисциплинарные меры (в российской специфике это, в зависимости от последствий: дисциплинарные, административные или даже уголовные)

Регулярное обучение персонала по вопросам безопасности

А.7. Документ «Защита от вредоносного ПО (вирусов, троянских коней)»

Состав документа.

Состав программных средств.

Обязательность применения только лицензионного программного обеспечения и запрет использования неутвержденного программного обеспечения должны быть закреплены документально

Получение программного ПО

Применяемое антивирусное ПО

Контроль целостности ПО

Антивирусный контроль входящей информации

Правила восстановления системы после вирусных атак

Мониторинг всей информации, касающейся вредоносного программного обеспечения.

А.8. Документ «Безопасность носителей данных»

Состав документа.

Управление съемными носителями

- порядок уничтожения съёмных носителей;
- порядок выноса съёмных носителей за пределы предприятия
- хранение съёмных носителей

Хранение и обращение с носителями

- бумажные документы
- записи на кассетах
- копировальная бумага
- отчеты
- картриджи
- магнитные ленты
- съемные диски или кассеты
- оптические носители
- листинги программ
- тестовые данные
- системная документация

Процедуры обращения с информацией и ее хранения

- учет и маркировка всех носителей
- ограничение доступа
- протоколирование доступа и защита данных из спулинга (например, которые ожидают распечатки).