Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

А. Г. Жестовский

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие по выполнению
практических работ для студентов специальности
10.05.03 «Информационная безопасность
автоматизированных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2023

УДК 004.9(075)

Рецензент
заведующий кафедрой информационной безопасности
Института цифровых технологий ФГБОУ ВО
«Калининградский государственный технический университет»,
кандидат физико-математических наук, доцент
Н. Я. Великите

Жестовский, А. Г.

Организационное и правовое обеспечение информационной безопасности: учебно-методическое пособие по выполнению практических работ для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / А. Г. Жестовский. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2023. – 66 с.

В учебно-методическом пособии приведены требования к оцениванию знаний при текущей и промежуточной аттестации студентов, проводимых в соответствии с учебным планом.

Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы модуля «Методы и средства обеспечения информационной безопасности автоматизированных систем» 10.05.03 Информационная безопасность автоматизированных систем.

Рис. 1, список лит. – 64 наименования

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала кафедрой информационной безопасности института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 30 июня 2023 г., протокол № 11

Учебно-методическое пособие по рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией ИЦТ 05 июля 2023 г., протокол № 8

УДК 004.9(075)

ОГЛАВЛЕНИЕ

1. Введение 4
2. Практическое занятие № 1 Работа с нормативно-правовыми документами, регламентирующими вопросы правового регулирования защиты государственной тайны 5
3. Практическое занятие № 2 Изучение порядка осуществления лицензирования и сертификации в области защиты информации 14
4. Практическое занятие № 3 Изучение вопросов защиты интеллектуальной собственности в российской федерации 21
5. Практическое занятие № 4 Состав компьютерных преступлений. Нормы ответственности за правонарушения в информационной сфере..... 31
6. Практическое занятие № 5 Правовое регулирование взаимоотношений администрации и персонала в области защиты информации..... 40
7. Практическое занятие № 6 Правовые основы использования организационных средств защиты информации 44
8. Практическое занятие № 7 Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных 47
9. Практическое занятие № 8 Правовое регулирование защиты информации с использованием технических средств и противодействия угрозам информационной безопасности 52
10. Литература 59
11. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» 64

1. ВВЕДЕНИЕ

В настоящее время при решении задач защиты конфиденциальной информации в органе государственной власти, на предприятии, в коммерческой организации или в учреждении наиболее значимую роль играют меры организационного характера, способные по своей сути объединить в комплексе все имеющиеся способы и методы защиты информации на основе действующих норм и правил. Это обусловлено, прежде всего, вполне объяснимым стремлением руководителей организаций и предприятий создать и на необходимом уровне поддерживать эффективную систему защиты информации, способную в каждом конкретном случае с учетом специфики деятельности предприятия определить необходимую совокупность сил и средств, а также мероприятий, используемых при решении задач по защите информации.

Организаторские функции руководителей предприятия играют важную роль в достижении основных целей его деятельности. Не случайно выбор управленческих решений не может быть эффективным без строгой системы применения нормативно-методических документов на основе опыта работы предприятия в той или иной области, в нашем случае, – в области, связанной с защитой конфиденциальной информации. Многообразие функций и задач, решаемых предприятиями различных сфер деятельности и организационно-правовых форм, требует постоянного совершенствования системы защиты конфиденциальной информации, принятия новых нормативных актов, методических документов, инструкций и руководств для работников предприятия.

Объединить в себе всю имеющуюся информацию по вопросам защиты конфиденциальной информации, четко определить направления ее защиты и расставить в нужный момент приоритеты в использовании необходимых сил и средств, способов и методов ее защиты – приоритетная задача организационной составляющей системы защиты конфиденциальной информации.

Для решения данной задачи необходимы разносторонние знания нормативно-правовых основ защиты информации, направлений деятельности предприятий, очередности и порядка принятия управленческих решений в зависимости от выбранного комплекса мероприятий.

2. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1. РАБОТА С НОРМАТИВНО-ПРАВОВЫМИ ДОКУМЕНТАМИ, РЕГЛАМЕНТИРУЮЩИМИ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ

2.1. Общие сведения

Цель:

1. Закрепить и углубить изучаемый материал студентами.

2. Определить проблемные вопросы в организации допуска и доступа к сведениям, составляющим коммерческую тайну и изложить свою позицию по совершенствованию контроля над обеспечением режима при работе с конфиденциальной информацией.

3. Изучить мероприятия по обеспечению защиты и сохранности документов, дел и изделий содержащие сведения государственной и коммерческой тайны.

Учебные вопросы:

1. Нормативно-правовые документы по защите государственной тайны.
2. Нормативно-методические документы по государственной тайны.
3. Федеральный ФЗ № 5485-1 «О государственной тайне».
4. Нормативно-правовые документы по защите коммерческой тайны.
5. Нормативно-методические документы по защите коммерческой тайны.
6. Федеральный закон N 98-ФЗ «О коммерческой тайне».

2.2. Теоретическое введение

Общественные отношения, связанные с отнесением информации к государственной тайне (ГТ), а также с операциями по доступу, обработки и рассекречиванию подобной информации, регламентируются ФЗ РФ «О государственной тайне». В нем даются базовые определения:

– 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:

– система защиты государственной тайны – совокупность органов защиты ГТ, используемых ими средств и методов защиты сведений, составляющих ГТ, и их носителей, а также мероприятий, проводимых в этих целях;

– средства защиты информации (относимой к ГТ) – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих ГТ, средства, в которых они реализованы, а также средства контроля эффективности защиты информации».

Перечень сведений, относимых к ГТ, утверждается Указом Президента РФ.

В Законе определяется, что не подлежат засекречиванию следующие све-

дения:

1. Сведения о чрезвычайных происшествиях, катастрофах, угрожающих безопасности и здоровью граждан.

2. Сведения о состоянии экологии, здравоохранения, демографии, образования, культуры, сельского хозяйства и преступности.

3. Сведения о привилегиях, компенсациях, льготах, предоставляемых всем субъектам.

4. Сведения о фактах нарушения прав и свобод человека и гражданина.

5. Сведения о ресурсах золотого запаса и государственных валютных резервов.

6. Сведения о состоянии здоровья высших должностных лиц.

7. Сведения о фактах нарушения здравоохранения органами государственной власти и должностными лицами.

Определены Степени секретности засекречиваемой информации:

1. Особая важность (ОВ) – сведения, разглашение которых может нанести ущерб интересам РФ.

2. Совершенно секретно (СС) – сведения, разглашение которых может нанести ущерб министерствам и ведомствам.

3. Секретно (С) – сведения, разглашение которых может нанести ущерб предприятиям, учреждениям, организациям.

Необходимо отметить, что многие документы, регламентирующие защиту информации, относимой к ГТ, сами имеют грифы секретности.

Регуляторами в сфере контроля защиты ГТ являются следующие государственные органы: ФСБ, ФСТЭК, СВР, межведомственная комиссия по защите ГТ.

В соответствии с указом Президента РФ «Об утверждении Перечня сведений конфиденциального характера», к сведениям конфиденциального характера относят:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные).

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью (профессиональная тайна).

5. Сведения, связанные с коммерческой деятельностью (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них (ноу-хау).

Существуют следующие признаки отнесения сведений к служебной тайне:

1) сведения, содержащие служебную информацию о деятельности государственных органов или подведомственных им предприятий, организаций, запрет на распространение которых установлен законом или диктуется служебной необходимостью;

2) сведения, являющиеся конфиденциальной информацией для других лиц, но ставшие известными представителям государственных органов в силу исполнения ими служебных обязанностей.

Служебная тайна – защищаемая законом конфиденциальная информация, ставшая известной в государственных органах или органах местного самоуправления на законных основаниях, в силу исполнения ими служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен законом или в силу служебной необходимости.

Критерии охраноспособности информации, составляющей служебную тайну:

1) информация, составляющая служебную информацию о деятельности самого органа власти;

2) охраноспособная конфиденциальная информация, составляющая коммерческую, банковскую, профессиональную тайну, тайну частной жизни – «чужая тайна»;

3) сведения, не являющиеся ГТ и не подпадающие под перечень сведений, доступ к которым не может быть ограничен;

4) получена информация в силу исполнения служебных обязанностей.

Объекты служебной тайны:

1. Военная тайна.

2. Тайна следствия.

3. Судебная тайна (тайна совещания судей и присяжных).

4. Налоговая тайна.

5. Таможенная тайна.

Обычно на документы, относящиеся к служебной тайне, наносится гриф «Для служебного пользования» (ДСП).

ФЗ РФ «О коммерческой тайне» выделяет следующие признаки относимости информации к коммерческой тайне:

- информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;
- отсутствует свободный доступ к информации;
- обладатель информации принимает мерь к охране ее конфиденциальности.

Коммерческая тайна (ФЗ РФ от 29.07.2004 N 98-ФЗ) – конфиденциальность информации, позволяющая ее обладателю при существующих или воз-

можных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

К коммерческой тайне не могут быть отнесены следующие сведения:

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

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

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

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

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

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

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

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

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

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

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

Для введения режима коммерческой тайны в организации в обязательном порядке должно быть выполнено:

1) определение перечня информации, составляющей коммерческую тайну;

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

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

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

5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации.

При этом гриф коммерческой тайны должен содержать следующие сведения:

• для юридических лиц – полное наименование и место нахождения;

• для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства.

Информация, относимая к коммерческой тайне, может категорироваться локальными нормативными актами организации (по аналогии со степенями секретности). Соответственно могут использоваться несколько грифов, например: «Конфиденциально», «Строго конфиденциально».

2.3. Методические указания и порядок выполнения работы

При подготовке к занятию (задание на самостоятельную работу)

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы № 2 «Правовые основы защиты государственной тайны», используя литературу, а также конспект лекций.

В ходе самостоятельной работы необходимо:

– проверить нормативно-правовые документы в СПС «Консультант Плюс» на соответствие действующему законодательству ***(приложение № 1).***

Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического занятия:

– изучить и составить ответы на контрольные вопросы *(вопросы из **приложения № 2)***, представить ответы на вопросы в отчёте практического занятия

(устно).

Приложение № 1

Для группы № 1с номерами 1-10 по списку в журнале

Перечень нормативно-правовых документов:

1. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне».

2. Указ Президента РФ от 30.11.1995 Г\I 1203 «Об утв. Перечня сведений, отнесенных к гостайне».

3. Указ Президента РФ от 6 октября 2(104 г. N 1286 «Вопросы межведомственной комиссии по защите ГТ'».

4. Распоряжение Президента РФ от 1б.04.2005 N 151-рп «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к ГТ».

5. Постановление Правительства РФ от 20.02.1995 N 170 «Об установлении порядка рассекречивания и продления сроков засекречивания архивных документов Правительства СССР».

6. Постановление Правительства РФ от 15.04.1995 N 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих ГТ, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите ГТ».

7. Постановление Правительства РФ от 04.09.1995 N 870 «Об утв. Правил отнесения сведений, составляющих ГТ, к различным степеням секретности».

8. Постановление Правительства РФ от 02.08.1997 N 973. «Об утв. Положения о подготовке и передаче сведений, составляющих ГТ, другим государствам или Международным организациям».

9. Постановление Правительства РФ от 22.08.1998 N 1003 «Об утв. Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к ГТ».

10. Постановление Правительства РФ от 02.04.2002 N 210 «Об утв. списка стратегических видов полезных ископаемых, сведения о которых составляют ГТ».

11. Постановление Правительства РФ от 23.07.2005 N 443 «Об утв. Правил разработки перечня сведений, отнесенных к ГТ».

12. Постановление Правительства РФ от 31.07.2007 N 491 «Об утв. Положения о ведении реестра государственных или муниципальных контрактов, в которые включаются сведения, касающиеся размещения заказов и составляющие ГТ».

13. Постановление Правительства РФ от 24.12.2007 N 928 «О порядке проведения проверни наличия в заявках на выдачу патента на изобретение или

полезную модель, созданные в РФ, сведений, составляющих ГТ».

14. Постановление Правительства РФ от 06.02.2010 N 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан РФ к ГТ».

Для Группы № 2 с номерами 11-20 по списку в журнале

Перечень нормативно-правовых документов, регламентирующих обработку и защиту информации, относимой к коммерческой тайне:

1. Федеральный закон от 29.07.2004 N 98 ФЗ «О коммерческой тайне».
2. Указ Президента РФ от 06.03.1997 N 188 «Об утв. Перечня сведений конфиденциального характера».
3. Постановление Правительства РСФСР от 05.12.1991 N 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

Перечень нормативно-правовых документов, регламентирующих обработку и защиту служебной информации ограниченного распространения:

1. «Уголовно-процессуальный кодекс РФ» от 18.12.2001 N 174-ФЗ.
2. «Арбитражный процессуальный кодекс РФ» от 24.07.2002 N 95-ФЗ.
3. «Гражданский процессуальный кодекс РФ» от 14.11.2002 N 138-ФЗ.
4. «Таможенный кодекс РФ» от 28.05.2003 N 61-ФЗ.
5. Федеральный закон от 17.12.1994 N 67-ФЗ «О федеральной фельдъегерской связи».
6. Федеральный закон от 27.05.1996 N 57-ФЗ «О государственной охране».
7. Федеральный закон от 21.07.1997 N 114-ФЗ «О службе в таможенных органах РФ».
8. Федеральный закон от 27.07.2004 N 79-ФЗ «О государственной гражданской службе РФ».
9. Постановление Правительства РФ от 03.11.1994 N 1233 «Об утв. Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
10. Постановление Правительства РФ от 22.09.2009 N 754 «Об утверждении Положения о системе межведомственного электронного документооборота».
11. Распоряжение Пр-ва РФ от 02.10.2009 N 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти».
12. Приказ МНС РФ от 03.03.2003 N БГ•3-28/96 «Об утв. Порядка доступа к конфиденциальной информации налоговых органов» (зарег. в Минюсте РФ 26.03.2003 N 4335).

Перечень нормативно-методических документов:

1. РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». (Гостехкомиссия России, 1992).

2. РД «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». (Гостехномиссия России, 1992).

3. РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». (Гостехкомиссия России, 1992).

4. РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». (Гостехкомиссия России, 1992).

Для Группы № 3 с номерами 21-30 по списку в журнале

Перечень нормативно-методических документов:

1. РД «Зашита от несанкционированного доступа к информации; Термины и определения». (Гостехкомиссия России, 1992).

2. РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». (Гостехкомиссия России, 1997).

3. РД «Защита информации. Специальные защитные знаки. Классификация и общие требования». (Гостехкомиссия России, 1997).

4. РД «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». (утв. приказом Гостехкомиссии России от 04.06.1999 N 114).

5. РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий». (утв. приказом Гостехкомиссии России от 19.06.2002 N 187) (часть 1, 2, 3).

6. РД «Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности». (Гостехкомиссия России, 2003).

7. РД «Безопасность информационных технологий. Руководство по регистрации профилей защиты». (Гостехкомиссия России, 2003).

8. РД «Безопасность информационных технологий. Руководство по формированию семейств профилей защиты». (Гостехкомиссия России, 2003).

9. РД «Руководство по разработке профилей защиты и заданий по безопасности». (Гостехкомиссия России, 2003).

10. РД «Временная методика оценки защищенности основных технических средств и систем, предназначенных ДЛЯ обработки, хранения и (или) передачи по линиям связи конфиденциальной информации». (Гостехкомиссия России, 2002).

11. РД «Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации». (Гостехкомиссия России, 2002).

12. РД «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам». (Гостехкомиссия России, 2002).

13. РД «Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во, вспомогательных технических средствах и системах». (Гостехкомиссия России, 2002).

14. Нормативно-методический документ. «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К) (утв. приказом Гостехкомиссии России от 30.08.2002 N 282).

15. «Методические рекомендации по технической защите информации, составляющей коммерческую тайну» (утв. Зам. директора ФСТЭК России 25.12.2006).

16. «Базовая модель угроз безопасности информации в ключевых системах информационной структуры» (утв. зам. директора ФСТЭК России 18.05.2007).

17. «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. Зам. директора ФСТЭК России 18.05.2007).

18. «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. Зам. директора ФСТЭК России 18.05.2007).

19. «Положение о Реестре ключевых систем информационной инфраструктуры» (утв. приказом ФСТЭК России №74 от 04.03.2009. Зарег. в Минюсте России 07.04.2009).

Приложение № 2

Контрольные вопросы

1. Перечень документов, ведущихся на предприятии по защите государственной тайны.

2. Перечень документов, ведущихся на предприятии по защите коммерческой тайны.

3. Разработать вариант Приказа «Об организации работ с информацией,

составляющей коммерческую тайну».

4. Порядок допуска сотрудников и других лиц к сведениям, составляющим государственную тайну.

5. Порядок допуска сотрудников и других лиц к сведениям, составляющим коммерческую тайну предприятия.

6. Перечень сведений, составляющих коммерческую тайну предприятия.

7. Ответственность за разглашение сведений, составляющих коммерческую тайну.

8. Ответственность за разглашение сведений, составляющих государственную тайну.

9. Разработать перечень мероприятий по контролю над обеспечением режима при работе со сведениями, содержащими коммерческую тайну.

10. Определить порядок работы с документами с грифом «Коммерческая тайна» (учет, хранение, размножение, пересылка, уничтожение).

3. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2. ИЗУЧЕНИЕ ПОРЯДКА ОСУЩЕСТВЛЕНИЯ ЛИЦЕНЗИРОВАНИЯ И СЕРТИФИКАЦИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Общие сведения

Цель – закрепление теоретических знаний в области обеспечения информационной безопасности.

Учебные вопросы

1. Организационная структура системы государственного лицензирования в области защиты информации.

2. Общий порядок проведения лицензирования в области защиты информации.

3. Система сертификации средств защиты информации по требованиям безопасности информации.

4. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.

5. Виды и схемы сертификации средств защиты информации.

6. Порядок проведения сертификации и контроля.

7. Перечень средств защиты информации, подлежащих сертификации.

3.2. Теоретическое введение

Для обеспечения защиты государственной и служебной тайны действует Государственная система защиты информации в РФ, которая включает:

– совокупность государственных органов, 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.

Рынок средств и систем информатизации в России сейчас настолько разнообразен, что в подавляющем большинстве случаев потребитель не в состоянии самостоятельно убедиться в соответствии приобретаемой им продукции установленным на государственном уровне нормам и правилам. Положение усугубляется тем обстоятельством, что российский рынок заполнен импортными изделиями. Для этих изделий производители и поставщики в лучшем случае декларируют соответствие отдельным зарубежным стандартам, о содержании которых у вас, как правило, нет никакой информации.

На бытовом уровне логичным путем решения этой проблемы является обращение к некоторому третьему лицу, являющемуся специалистом в данной области и заведомо независимому от поставщика продукции, которое может дать заключение о соответствии продукции установленным требованиям. На государственном уровне аналогичная процедура называется сертификацией.

Сертификация – процедура, выполняемая третьей стороной, независимой от изготовителя (продавца) и потребителя продукции или услуг, по подтверждению соответствия этих продукции или услуг установленным требованиям.

Результатом выполнения процедуры сертификации является так называемый сертификат соответствия.

Сертификат соответствия – документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Общие правовые основы сертификации продукции и услуг в Российской Федерации установлены Законом «О сертификации продукции и услуг», где определены права и ответственность в области сертификации органов государственного управления, а также изготовителей (продавцов, исполнителей) и других участников сертификации.

Сертификация средств и систем информатизации является элементом общей системы сертификации продукции в Российской Федерации.

Основными целями сертификации средств информатизации, информационных технологий и услуг являются:

• защита пользователей средств и систем информатизации от приобретения средств и систем, в том числе импортных, которые представляют опасность для жизни, здоровья, имущества, а также для окружающей среды;

• обеспечение разработчиков систем, а также широкого круга пользователей этих систем достоверной информацией о состоянии отечественного и зарубежного рынков средств информатизации, телекоммуникаций, информационных технологий и услуг;

• обеспечение информационного обмена между государственными систе-

мами информатизации;

• обеспечение условий для информационного взаимодействия субъектов негосударственной принадлежности с субъектами государственной принадлежности;

• содействие повышению научно-технического уровня и конкурентоспособности отечественных систем информатизации, информационных технологий и услуг;

• содействие созданию условий для вхождения России в мировое информационное пространство.

Необходимо отметить, что сертификация средств информатизации не только обеспечивает удовлетворение интересов потребителя, но приносит определенные выгоды и изготовителю (поставщику) продукции. Так, в частности, сертификация способствует расширению рынка сбыта (распространению продукции в тех районах, где потребителю неизвестна репутация фирмы) и обеспечивает подтверждение качества продукции фирмы по сравнению с продукцией конкурентов. С точки зрения организации торговых взаимосвязей сертификация способствует созданию доверительных отношений между производителями (поставщиками) и потребителями продукции. Необходимо иметь в виду, что только имеющее место и объективно подтвержденное качество конкретных видов отечественной информационной продукции и средств информатизации может сделать их конкурентоспособными и реально обеспечить спрос на них.

Говоря о сертификации, нельзя не отметить ее тесную взаимосвязь со стандартизацией в сфере информатизации.

Во-первых, как уже говорилось выше, суть процедуры сертификации заключается в подтверждении соответствия средств информатизации установленным требованиям. Документами, содержащими эти требования, являются стандарты, разрабатываемые в процессе стандартизации.

Во-вторых, собственно процедура сертификации регламентируется действующими нормативными документами (стандартами).

В соответствии с принятой терминологией "информатизация" как предметная область представляет собой организационный социально-экономический и научно-технический процесс создания условий для удовлетворения информационных потребностей, базирующийся на массовом применении новых информационных технологий. В интересах государства и граждан отдельные виды предпринимательской деятельности в области информатизации целесообразно ограничить, т. е. на определенных условиях ввести разрешительную систему (лицензирование).

Лицензирование должно ограничивать следующие виды деятельности:

• создание и применение информационных технологий, включая про-

граммы для ЭВМ и другие компоненты средств информатизации;

• формирование информационных ресурсов на основе использования современных информационных технологий;

• оказание услуг по информационному обеспечению потребителей информационных ресурсов при соблюдении требований безопасности для государства, организаций, граждан, необходимых для предотвращения и ликвидации техногенных, информационных и экономических угроз и их последствий в сфере информатизации.

За рубежом большое внимание уделяется вопросам защиты государственных информационных ресурсов, где обязательному лицензированию подлежат виды деятельности по защите информации и информационных ресурсов, организации доступа к базам данных и сетям передачи данных. Кроме того, лицензируется предоставление услуг в части использования программных продуктов.

Принятый в России Закон «О лицензировании отдельных видов деятельности» не распространяется на отношения, возникающие в связи с использованием результатов интеллектуальной деятельности. Поэтому в настоящее время разрешительная система на определенных условиях для вышеперечисленных видов деятельности регламентируется законодательством, регулирующим сертификацию, патентным законодательством, законами об авторском праве и смежных правах, а также законом, определяющим участие в международном информационном обмене.

Проблема лицензирования отдельных элементов деятельности в сфере информатизации поставлена в Законе «Об информации, информатизации и защите информации»:

• в п. 4 ст. 7 указано, что для решения проблемы качественного формирования государственных информационных ресурсов необходимо разработать и внедрить в практику порядок лицензирования деятельности организаций, специализирующихся на формировании государственных информационных ресурсов на основе договоров с соответствующими органами власти;

• в п. 4 ст. 11 указано, что осуществление лицензионной деятельности в области работы с персональными данными в связи с особенностями этой деятельности нуждается в дополнительном правовом регулировании;

• в п. 3 ст. 19 указано, что организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, должны получать лицензию на этот вид деятельности.

Указанными статьями установлено, что порядок лицензирования определяется законодательством Российской Федерации.

В тех случаях, когда разрешение на использование технических решений (изобретений, ноу-хау) дается не государством, а коллективным или индивиду-

альным субъектом – собственником или, по поручению последнего, владельцем технического решения, применяется такая юридическая форма, как лицензионный договор.

Основным отличием процесса лицензирования от процесса сертификации является состав категорий, по отношению к которым они применяются. В процессе лицензирования фигурируют такие категории, как «деятельность» (подразумеваются виды или направления деятельности) и «субъект» (физическое лицо, предприятие, организация или иное юридическое лицо).

В соответствии с действующим законодательством в Российской Федерации отдельные виды деятельности осуществляются предприятиями, организациями и учреждениями независимо от организационно-правовой формы, а также физическими лицами, осуществляющими предпринимательскую деятельность без образования юридического лица, на основании лицензии – специального разрешения органов, уполномоченных на ведение лицензирования.

Лицензия является официальным документом, который разрешает осуществление указанного в нем вида деятельности в течение установленного срока, а также определяет условия его осуществления.

Основу нормативно-правовой базы лицензирования в сфере информатизации составляют Законы «О лицензировании отдельных видов деятельности», «Об информации, информатизации и защите информации» и «Об участии в международном информационном обмене».

Общие принципы лицензирования видов деятельности в сфере информатизации России можно сформулировать следующим образом:

• целью лицензирования является защита интересов государства и граждан от неумышленного или сознательного некачественного выполнения работ, соответствующих определенным видам деятельности в сфере информатизации;

• виды деятельности в сфере информатизации, подлежащие лицензированию, а также органы, осуществляющие лицензирование конкретных видов деятельности в различных областях информатизации, определены рядом нормативных документов;

• право на осуществление деятельности, подлежащей лицензированию, может получить субъект, отвечающий определенным критериям, которые заранее определяются правилами проведения лицензирования и являющимися их неотъемлемой частью требованиями к предприятию-заявителю.

Таким образом, субъектом лицензирования становится лишь то физическое или юридическое лицо, которое представляет все необходимые и правильно оформленные документы и удовлетворяет соответствующим требованиям.

За органом, уполномоченным на проведение лицензионной деятельности, закрепляется право на осуществление контроля за деятельностью лицензиата.

3.3. Методические указания и порядок выполнения работы

При подготовке к занятию (задание на самостоятельную работу)

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы раздела 4 «Правовое регулирование деятельности организаций в области информационной безопасности», используя литературу, а также конспект лекций.

В ходе самостоятельной работы необходимо:

– проверить нормативно-правовые документы в СПС «Консультант Плюс» на соответствие действующему законодательству ***(приложение № 1).***

Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы лицензирования в области защиты конфиденциальной информации и вопросы сертификации в области защиты конфиденциальной информации, лично отрабатывают контрольные вопросы практического занятия ***(приложение № 2).***

Приложение № 1.
Законодательная и нормативная база в области обеспечения ИБ РФ

А) Дополнить список нормативно-правовыми актами, используемыми для руководства вопросами обеспечения информационной безопасности всех ветвей власти и деятельности организации (предприятия).

Б) Уточнить наименование и дату издания представленных документов, используя одну из информационно-справочных систем.

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. № 149-ФЗ.
2. О связи: Федеральный закон от 07.07.2003 г. № 126-ФЗ.
3. Об электронной цифровой подписи: Федеральный закон от 10.01.2002 г. № 1-ФЗ.
4. О коммерческой тайне: Федеральный закон от 29.07.2004 г. № 98-ФЗ.
5. О персональных данных: Федеральный закон от 27.07.2006 г. № 152-ФЗ.
6. О лицензировании отдельных видов деятельности: Федеральный закон от 08.08.2001 г. № 128-ФЗ.
7. Об утверждении перечня сведений конфиденциального характера: Указ Президента Российской Федерации от 06.03.1997 г. № 188.
8. О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена: Указ Президента Российской Федерации от 12 мая 2004 года № 611 (в редакции Указов Прези-

дента Российской Федерации от 22.03.2005 № 329 и от 03.03.2006 г. № 175).

9. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: Постановление Правительства Российской Федерации от 03.11.1994 г. № 1233.

10. Указ Президента Российской Федерации от 12 мая 2009 г. N 537. О стратегии национальной безопасности Российской Федерации до 2020 года.

Приложение № 2

Контрольные вопросы

1. Согласно Закону «О сертификации продукции и услуг», для каких целей проводится сертификация?
2. Какие группы документов входят в нормативную базу сертификации средств и систем информатизации?
3. В каких основных направлениях проводится сертификация средств информатизации?
4. Перечислите средства информатизации, которые подлежат обязательной сертификации согласно нормативному документу «Номенклатура продукции и услуг, подлежащих обязательной сертификации в Российской Федерации».
5. Ознакомьтесь с Законом «Об информации, информатизации и защите информации». Какие цели защиты информации определяет данный Закон?
6. Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
7. Организационная структура системы государственного лицензирования в области защиты информации.
8. Что включает в себя деятельность по международному информационному обмену?
9. Права и обязанности лицензиатов.
10. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
11. Назовите случаи приостановления или прекращения действия лицензии.
12. В каких случаях предприятию отказывают в выдаче лицензии?
13. Какие документы предоставляются для получения лицензии?
14. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
15. Какие средства относятся к шифровальным?
16. Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?

17. Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.

18. Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

19. Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.

20. Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

21. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.

22. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.

23. Назовите виды и схемы сертификации средств защиты информации.

24. Каковы функции ФСТЭК в области сертификации средств защиты информации?

25. Каковы функции органов сертификации средств защиты информации?

26. Каковы функции испытательных лабораторий (центров).

27. Каковы функции заявителей?

28. Общий порядок проведения сертификации средств защиты информации.

29. Виды контроля в области сертификации средств защиты информации.

30. Чем определяются сроки проведения сертификационных испытаний?

31. На какой срок выдается сертификат?

32. Назовите причины приостановления или аннулирования действия сертификата.

33. Порядок проведения аттестации объектов информатизации. Этапы аттестации.

34. Какие сведения в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» запрещено относить к конфиденциальной информации?

4. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3. ИЗУЧЕНИЕ ВОПРОСОВ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

4.1. Общие сведения

Цель: Изучить основы законодательства РФ об авторском и патентном праве.

Учебные вопросы

1. Международная охрана авторских прав.
2. Нормативно-правовые документы по защите результатов интеллектуальной деятельности.
3. Нормативно-методические документы по защите результатов интеллектуальной деятельности.
4. Основные положения Гражданского кодекса по защите результатов интеллектуальной деятельности.

4.2. Теоретическое введение

Основы правового регулирования в области ИС закреплены Конституцией РФ 1993 г. (с изменениями от 01 июля 2020 г.) в качестве конституционного права: “Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом” (ст. 44).

Формируется государственная политика в этой области. Указ Президента РФ от 22.06.98 № 863 «О государственной политике по вовлечению в хозяйственный оборот результатов научно-технической деятельности и объектов и объектов интеллектуальной собственности в сфере науки и технологии» в качестве приоритетных выделяет следующие направления:

- государственное стимулирование процессов создания, правовой охраны и использования интеллектуальной собственности, обеспечивающих повышение конкурентоспособности отечественной продукции;
- обеспечение сбалансированности прав и законных интересов субъектов правоотношений в области интеллектуальной собственности, создающее условия заинтересованности этих субъектов при создании, правовой охране и использовании интеллектуальной собственности (ст.1 п.1).

Новое законодательство создало необходимые предпосылки для реализации такой политики. Оно регулирует имущественные и связанные с ними личные неимущественные правоотношения, возникающие в связи с созданием, правовой охраной, регистрацией и использованием объектов интеллектуальной собственности. Новое законодательство юридически закрепило, а в части патентного права – восстановило традиционное в мировой правовой и экономической практике положение, в соответствии с которым права на объекты интеллектуальной собственности (изобретения, полезные модели, промышленные

образцы, товарные знаки, секреты производства, программы для ЭВМ, произведения науки, литературы и искусства и другие результаты научных исследований и творческого труда), созданные в связи с выполнением работником служебных обязанностей, становятся собственностью работодателя и специфическим товаром, который, как и всякий товар может быть введен в хозяйственный оборот на внутреннем и внешнем рынках. Неслужебные объекты интеллектуальной собственности являются собственностью авторов или их правопреемников.

Формами введения в хозяйственный оборот могут быть различные формы использования объектов интеллектуальной собственности: для изобретений, полезных моделей, промышленных объектов, товарных знаков – изготовление, применение, ввоз, предложение к продаже, продажа и иное введение в хозяйственный оборот продукта или товара, содержащего запатентованный объект интеллектуальной собственности; для селекционных достижений – производство, воспроизведение, предложение к продаже и иные формы сбыта; для программ для ЭВМ, баз данных, произведений науки, литературы и искусства – выход в свет (опубликование), воспроизведение (изготовление), распространение (продажа, прокат, аренда и т. п.) и др.

Понятие права интеллектуальной собственности

Под интеллектуальной собственностью по действующему законодательству понимается исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, продукции и выполняемых работ или услуг (фирменное наименование, товарный знак, знак обслуживания и т. п.). Использование третьими лицами таких результатов интеллектуальной деятельности и средств индивидуализации, которые являются объектами исключительных прав, возможно, только с согласия правообладателя.

Таким образом, права на объекты интеллектуальной собственности являются исключительными правами в отношении третьих лиц, что означает, что только Университет или иной правообладатель, являющийся собственником прав на конкретный объект интеллектуальной собственности, вправе его использовать по своему усмотрению, запрещая такие действия всем третьим лицам без разрешения правообладателя. Такое разрешение может быть дано в форме лицензионного договора.

Нарушение прав интеллектуальной собственности

Любые формы несанкционированного использования объектов интеллектуальной собственности признаются нарушением прав правообладателя, а любое юридическое или физическое лицо, несанкционированно использующее правоохраняемый объект интеллектуальной собственности, является нарушителем таких прав. Такое нарушение по требованию правообладателя должно

быть прекращено, а лицо, совершившее противоправное действие, обязано возместить ему причиненные убытки.

Возникшие споры рассматриваются в судебном порядке. К ним относятся следующие споры:

- об авторстве на объект ИС;
- об установлении патентообладателя (правообладателя);
- о нарушении исключительного права на использование охраняемого объекта ИС и других имущественных прав патентообладателя (правообладателя);
- о заключении и исполнении лицензионных договоров на использование охраняемого объекта ИС;
- о праве преждепользования;
- о выплате работодателем вознаграждения работнику – автору о выплате компенсаций, предусмотренных Патентным Законом;
- другие споры, связанные с охраной прав на объект ИС.

К противоправным действиям, влекущим за собой административную ответственность, относится недобросовестная конкуренция, формами которой в отношении объектов интеллектуальной собственности являются: продажа товаров с незаконным использованием результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации юридического лица, продукции, работ и услуг (фирменное наименование, товарный знак, знак обслуживания и т. п.); получение, использование, разглашение научно-технической, производственной или торговой информации, в том числе коммерческой тайны, без согласия ее владельца (ст. 10).

За наиболее общественно опасные правонарушения предусмотрена уголовная ответственность. К ним относятся:

– незаконное использование объектов авторского права, товарных знаков, изобретений, полезных моделей, промышленных образцов, разглашение сущности последних до официальной публикации сведений о них без согласия автора или заявителя;

– незаконный экспорт технологий, научно-технической информации и услуг, используемых при создании оружия массового поражения, вооружения и военной техники.

Права на объекты интеллектуальной собственности ограничены территорией государства, выдавшего охранный документ или регламентировавшего другие формы охраны, и носят срочный характер. Так для объектов промышленной собственности законодательством РФ установлены следующие сроки действия охранных документов: патент на изобретение – 20 лет; свидетельство на полезную модель – 5 лет; патент на промышленный образец – 10 лет; свидетельство на товарный знак – 10 лет с даты подачи соответствующей заявки в

Роспатент; патент на селекционное достижение – 30 лет с даты регистрации; авторское право на произведение науки, литературы и искусства, включая программы для ЭВМ и базы данных – в течение всей жизни автора и 50 лет после его смерти.

Объектами интеллектуальной собственности являются:

- изобретения, полезные модели и промышленные образцы;
- товарные знаки, знаки обслуживания, наименования мест происхождения товаров;
- программы для ЭВМ и базы данных;
- топологии интегральных микросхем;
- секреты производства (ноу-хау);
- селекционные достижения;
- произведения науки, литературы и искусства.

Изобретением является неизвестное ранее знание о том, как решить (удовлетворить) определенную общественную (утилитарную) проблему (потребность). Изобретению предоставляется правовая охрана, если оно является новым, имеет изобретательский уровень и промышленно применимо.

К полезным моделям относится конструктивное выполнение средств производства и предметов потребления, а также их составных частей. Полезной модели предоставляется правовая охрана, если она является новой и промышленно применимой.

Промышленным образцом является художественно-конструкторское решение изделия, определяющее его внешний вид. Промышленному образцу предоставляется правовая охрана, если он является новым, оригинальным и промышленно применимым.

Товарные знаки и знаки обслуживания – это обозначения, способные отличать соответственно товары и услуги одних юридических или физических лиц от однородных товаров и услуг других юридических или физических лиц.

Наименование места происхождения товара – это название страны, населенного пункта, местности или другого географического объекта, используемое для обозначения товара, особые свойства которого исключительно или главным образом определяются характерными для данного географического объекта природными условиями или людскими факторами либо природными условиями и людскими факторами одновременно.

Под программой для ЭВМ действующее законодательство понимает объективную форму представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, а также подготовительные материалы, полученные в ходе ее разработки, и порождаемые программой аудиовизуальные отображения.

База данных – это объективная форма представления и организации совокупности данных (например, статей, расчетов) систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ.

Топологией интегральной микросхемы является зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы и связей между ними.

Под секретами производства (ноу-хау) следует понимать не относящийся к государственным секретам особый вид информации, составляющий служебную или коммерческую тайну, при условии, если информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней отсутствует свободный доступ на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

К селекционным достижениям относят сорта растений и породы животных.

К произведениям науки, литературы и искусства относятся все охраняемые авторским правом результаты творческой деятельности, обнародованные и необнародованные, но выраженные в какой-либо объективной форме, независимо от назначения и достоинства произведения.

В отношении этих объектов вуз должен осуществлять комплекс необходимых и достаточных действий по их правовой охраны и коммерческой реализации.

4.3. Методические указания и порядок выполнения работы

При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы раздела № 3 «Правовые основы защиты конфиденциальной информации», используя литературу, а также конспект лекций.

В ходе самостоятельной работы необходимо:

– проверить нормативно-правовые документы в СПС «Консультант Плюс» на соответствие действующему законодательству ***(приложение № 1)***.

Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся положений Конституции РФ, Доктрины информационной безопасности РФ и федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического занятия:

– изучить и составить ответы на контрольные вопросы *(вопросы из **при-***

ложения № 2), представить ответы на вопросы в отчёте практического занятия.

Приложение № 1.

Законодательная и нормативная база в области обеспечения ИБ РФ

Для группы № 1 с номерами 1-3 по списку в журнале

- Патентный закон РФ от 23.09.92 № 3517-1.
- Закон РФ «О товарных знаках, знаках обслуживания и наименовании мест происхождения товаров» от 23.09.92 № 3520-1.
- Закон РФ «О правовой охране программ для ЭВМ и баз данных» от 23.09.92 № 3523-1.

Для группы № 2 с номерами 4-6 по списку в журнале

- Закон РФ «О правовой охране топологии интегральных микросхем» от 23.09.97 №3526-1.
- Закон РФ «О конкуренции и ограничении монополистической деятельности на товарных рынках» (в редакции законов РФ от 24.06.92 № 3119-1, от 15.07.92 № 3310-1, ФЗ от 25.05.95 №83-ФЗ, ФЗ от 6.05.98 № 70-ФЗ).

Для Группы № 3 с номерами 7-9 по списку в журнале

- Закон РФ «Об авторском праве и смежных правах» от 09.07.93 № 5351-1.
- Закон РФ «О селекционных достижениях» от 06.08.93 № 5605-1.
- Федеральный Закон РФ «О ратификации Евразийской патентной конвенции» от 01.06.95 № 85-ФЗ.

Для группы № 4 с номерами 9-11 по списку в журнале

- Гражданский кодекс РФ. Ч. I. Федеральный закон от 30.11.94 № 5-ФЗ.
- Гражданский кодекс РФ. Ч. II. Федеральный закон от 26.01.96 № 15-ФЗ.
- Уголовный кодекс. РФ Федеральный закон от 13.06.96 № 63-ФЗ.

Для группы № 5 с номерами 12-14 по списку в журнале

- Указ Президента РФ от 22.07.98 № 863 «О государственной политике по вовлечению в хозяйственный оборот результатов научно-технической деятельности и объектов и объектов интеллектуальной собственности в сфере науки и технологии».
- Указ Президента РФ от 14.05.98 № 556 «О правовой защите результатов научно-исследовательских, опытно – конструкторских и технологических работ военного, специального и двойного назначения».

Для группы № 6 с номерами 15-17 по списку в журнале

- Постановление правительства РФ от 29.09.98 № 1132 «О первоочередных мерах по правовой защите интересов государства в процессе экономического и гражданско-правового оборота результатов научно-исследовательских, опытно-конструкторских и технологических работ военно-

го, специального и двойного назначения».

- Постановление правительства РФ от 2.09.99 № 982 «Об использовании результатов научно-технической деятельности». Постановление правительства РФ от 29.09.98 № 1132 «О первоочередных мерах по правовой защите интересов государства в процессе экономического и гражданско-правового оборота результатов научно-исследовательских, опытно-конструкторских и технологических работ военного, специального и двойного назначения».
- Постановление правительства РФ от 2.09.99 № 982 «Об использовании результатов научно-технической деятельности».

Для группы № 7 с номерами 18-20 по списку в журнале

- Конституция Российской Федерации от 12.12.93.
- Постановление Верховного Совета Российской Федерации «О введении в действие Закона РФ «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров»» от 23.09.93 № 3521-1.

Для группы № 8 с номерами 21-23 по списку в журнале

- Постановление Верховного Совета Российской Федерации «О введении в действие Закона РФ «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров»» от 23.09.93 № 3521-1.
- «Правила подачи и рассмотрения ходатайств о прекращении действия на территории РФ авторских свидетельств СССР на изобретения, свидетельств СССР на промышленные образцы, а также патентов СССР, выданных на имя Государственного фонда изобретений СССР, и выдачи патентов Российской Федерации на оставшийся срок», утвержденные приказом Комитета РФ по патентам и товарным знакам от 25.06.93 № 35 с изменениями в соответствии с приказом Роспатента от 30.10.96 № 125.

Для группы № 9 с номерами 24-26 по списку в журнале

- Указ Президента РФ от 6.03.97 № 188 «Об утверждении перечня конфиденциального характера», «Перечень сведений конфиденциального характера».
- Постановление Совета Министров – Правительства РФ от 12.07.93 № 648 «О порядке использования изобретений и промышленных образцов, охраняемых действующими на территории РФ авторскими свидетельствами на изобретение и свидетельствами на промышленный образец, и выплаты их авторам вознаграждения».

Для группы № 10 с номерами 27-29 по списку в журнале

- Постановление Верховного Совета СССР от 31.05.91 «О введении в действие Закона СССР «Об изобретениях в СССР»».
- Закон СССР «Об изобретениях в СССР» от 31.05.91.
- Закон СССР «О промышленных образцах» от 10.06.91.

Для группы № 11 с номерами 30-33 по списку в журнале

- Распоряжение Правительства РФ от 20.04.95 № 540-р «О мероприятиях по совершенствованию системы создания и защиты научных и технологических достижений и механизмов их использования в РФ».
- Федеральный закон «Об информации, информатизации и защите информации» от 20.02.95 № 24-ФЗ.

Приложение № 2

Содержание отчёта (контрольные вопросы):

1. Интеллектуальная собственность и ее понятие. Значение интеллектуальной собственности в современном обществе.

1. Общая характеристика интеллектуальной собственности и ее понятие.
2. Исключительный характер права интеллектуальной собственности.
3. Особенности и специфика объектов интеллектуальной собственности как объектов гражданских прав.

2. Источники права интеллектуальной собственности. Основные институты права интеллектуальной собственности.

1. Законодательство Российской Федерации в области права интеллектуальной собственности.
2. Основные международные договоры в области правовой охраны интеллектуальной собственности. Классификация объектов интеллектуальной собственности.
3. Институт авторского и смежных прав. Институт патентного права.

3. Институт авторского и смежных прав. Авторское право и его объекты. Виды, признаки и классификация объектов авторского права.

1. Законодательство Российской Федерации об авторском праве.
2. Правовая охрана авторских прав.
3. Классификация объектов авторского права.

4. Субъекты авторского и смежных прав и классификация.

1. Авторы произведений. Правоспособность авторов.
2. Исключительная природа авторских прав. Соавторство. Правопреемство.
3. Личные неимущественные права автора: право авторства, право на имя, право на защиту репутации автора, право на обнародование.

5. Договорные отношения в области создания, использования и передачи прав на объекты авторского права.

1. Типология правоотношений в процессе создания, использования передачи прав на объекты авторского права.
2. Виды авторских договоров и их классификация. Структура авторского договора и его существенные условия.
3. Порядок заключения авторского договора.

6. Патентное право

1. Понятие и принципы патентного права.

2. Изобретательское право: понятие, признаки, объекты и их защита.

3. Полезные модели: признаки и правовая защита. Промышленные образцы: признаки и правовая защита.

7. Субъекты права промышленной собственности, их характеристика. Передача прав на объекты промышленной собственности.

1. Источники права, регулирующие имущественные и личные неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием объектов промышленной собственности.

2. Автор изобретения, полезной модели, промышленного образца.

3. Понятие патентообладателя. Передача прав на патент. Виды и способы передачи прав.

8. Средства индивидуализации участников гражданского оборота

1. Фирменные наименования: содержание и государственная регистрация.

2. Товарные знаки и знаки обслуживания: назначение, функции и их правовая защита.

3. Средства индивидуализации участников гражданского оборота и передача прав на использование этих объектов.

9. Институт специальной правовой охраны объектов интеллектуальной собственности

1. Понятие специальной правовой охраны объектов интеллектуальной собственности.

2. Источники права специальной охраны. Объекты специальной правовой охраны.

3. Особенности правового регулирования отношений по созданию и использованию объектов специальной правовой охраны.

10. Защита права интеллектуальной собственности.

1. Законодательство Российской Федерации о защите авторских и смежных прав.

2. Виды правонарушений в области авторского права. Контрафактные экземпляры произведений.

3. Гражданская, администрация и уголовная ответственность за нарушение авторских прав.

11. Информационное право

1. Общие сведения об информации и информационном праве и его источниках.

2. Охрана «ноу-хау».

3. Информационное законодательство: состав и источники.

12. Международная охрана авторских прав

1. Женевская Всемирная конвенция об авторском праве 1952 г.

2. Присоединение России к Бернской конвенции об охране литературных и художественных произведений к Женевской Всемирной конвенции об авторском праве в редакции

3. Перспективы участия России во Всемирной торговой организации.

13. Патентное право в сфере информационных технологий.

1. Официальная регистрация программ для ЭВМ и баз данных.

2. Основы патентного права. Условия патентоспособности изобретений, полезных моделей и промышленных образцов.

3. Права автора и патентообладателя.

14. Патентное право в сфере информационных технологий.

1. Получение патента.

2. Регистрация и выдача патента на секретное изобретение.

3. Ответственность за нарушения законодательства в сфере патентных прав.

5. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4. СОСТАВ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ. НОРМЫ ОТВЕТСТВЕННОСТИ ЗА ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

5.1. Общие сведения

Цели:

1. Закрепить и углубить изучаемый материал студентами.

2. Формирование твердых теоретических знаний и практических навыков в области квалификации преступлений в сфере компьютерной информации.

3. Приобретение систематизированных знаний в области квалификации преступлений в сфере компьютерной информации.

4. Ознакомление с действующей в правоохранительных органах и судах практикой применения норм Уголовного кодекса РФ, закрепляющих ответственность за преступления в сфере компьютерной информации.

5. Углубление навыков и умений практического использования этих знаний, подготовка к компетентному решению профессиональных задач в сфере борьбы с компьютерными преступлениями.

6. Реализация системы практических задач и упражнений по использованию уголовно-правовых знаний.

Учебные вопросы:

1. Понятие и значение квалификации преступлений в сфере компьютерной информации.

2. Понятие и виды преступлений в сфере компьютерной информации по действующему российскому уголовному законодательству.

5.2. Теоретическое введение

Преступления в сфере компьютерной информации – предусмотренные уголовным законом общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов.

К указанным преступлениям относятся: неправомерный доступ к компьютерной информации (ст. 272 УК); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).

Неправомерный доступ к компьютерной информации (ст. 272 УК) имеет предметом охраняемую законом компьютерную информацию, т.е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (примечание 1 к данной статье).

Для признания информации охраняемой законом необходимо, чтобы:

а) закон (иной нормативный правовой акт) давал основание для защиты данных от несанкционированного доступа;

б) законный обладатель информации предпринимал меры по ее охране.

Доступ к компьютерной информации означает получение возможности знакомиться с информацией и использовать ее. Принципиальным является доступ именно к информации, а не только к ее носителю.

Получение сведений происходит посредством проникновения в ЭВМ, систему ЭВМ или их сеть (непосредственно или через удаленный доступ) либо путем перехвата компьютерной информации (подключение к коммуникационным каналам или узлам передачи данных; улавливание остаточного излучения монитора, принтера, других устройств).

Неправомерность доступа означает, что субъект не имеет права получать и использовать информацию. Наличие или отсутствие такого права может не зависеть от воли законного обладателя сведений. Например, разрешение банковского служащего на получение и использование информации о состоянии счетов клиентов не исключает ответственности за доступ к этим данным.

Деяние признается преступлением, если повлекло уничтожение компьютерной информации, ее блокирование, модификацию либо копирование.

Под уничтожением компьютерной информации понимается ее исчезновение с носителя без возможности восстановления. Блокирование сведений предполагает невозможность законного доступа к ним при их сохранности. Модификацией информации являются любые ее изменения, кроме трансформации компьютерной программы или базы данных, осуществляемой в целях их

функционирования на конкретных технических средствах пользователя или под управлением конкретных программ пользователя. Копирование данных означает их дублирование. Физическое выражение и формат копии могут отличаться от оригинала. Это возможно при фотографировании сведений с монитора, переписывании от руки.

Наказание за совершение вышеуказанного преступления предусматривается вплоть до лишения свободы сроком до 7 лет.

Деяние подпадает под признаки ст. 272 УК РФ, если:

– речь идет именно о компьютерной информации, которая, к тому же, относится к категории охраняемой законом;

– речь идет об отнесении доступа к конфиденциальной компьютерной информации к разряду несанкционированного (неправомерного);

– речь идет о наличии наступивших вредных последствий, а именно модификации, блокирования, копирования или уничтожения информации, к которой осуществлялся неправомерный доступ;

– речь идет о наличии причинно-следственной связи между осуществленным неправомерным доступом и причиненными вредными последствиями.

Влияние ясности понятий, выработанных законодателем, на правильную квалификацию деяний. В большинстве случаев требуется расширительное толкование норм права, поскольку в законодательстве отсутствуют необходимые ссылки на специфику защиты прав (например, авторских прав в Интернете).

Основные понятия: информация; неправомерный доступ; охраняемая законом информация; компьютерная информация; машинный носитель; электронно-вычислительная машина (ЭВМ); система ЭВМ; сеть ЭВМ; уничтожение, блокирование, модификация, копирование информации; нарушение работы ЭВМ, системы ЭВМ или их сети.

Роль Федерального закона «О правовой охране программ для электронных вычислительных машин и баз данных» (23 сентября 1992 года № 3523-1), который в 2002 году был принят в новой редакции (ред. Федерального закона от 24.12.2002 № 177-ФЗ).

Федеральный закон «Об авторском праве и смежных правах» (от 9 июля 1993 года№ 5351-1 в ред. Федеральных законов от 19.07.1995 № 110-ФЗ, от 20.07.2004 № 72-ФЗ).

Особенности научного и законодательного толкования таких понятий как:

- «информация; компьютерная информация; машинный носитель»,
- «неправомерный доступ; охраняемая законом информация; уничтожение, блокирование, модификация, копирование информации; нарушение работы ЭВМ, системы ЭВМ или их сети»;
- «модификация информации»;

- «адаптация программы для ЭВМ или базы данных»;
- «уничтожение информации»;
- «блокирование информации»;
- «копирование информации»;
- «нарушение работы ЭВМ, системы ЭВМ или их сети»;
- «электронно-вычислительная машина (ЭВМ); система ЭВМ; сеть ЭВМ».

Характеристика неправомерного доступа к компьютерной информации.

Особенности субъектов преступления. В ст. 272 УК РФ можно выделить несколько категорий субъектов преступления:

1. Лица, осуществляющие неправомерный доступ к компьютерной информации, ч. 1 от. 272 УК РФ (общий субъект).

2. Лица, осуществляющие неправомерный доступ к компьютерной информации с использованием своего служебного положения, ч. 2 ст. 272 УК РФ.

3. Лица, имеющие доступ к ЭВМ, системе ЭВМ или их сети, но осуществляющие неправомерный доступ к компьютерной информации, ч. 2 ст. 272 УК РФ.

Задачи для самоконтроля

Задача 1.

В ООО, оказывающем парикмахерские услуги, под руководством и по указанию директора ООО одним из кассиров систематически в конце каждой вечерней смены информация фискальной памяти контрольно-кассовой машины уничтожалась посредством подключения к внешнему порту некого корректирующего устройства, обнуляющего всю информацию о «пробитых» суммах. После этого вручную набивалась новая информация о продажах, которая была меньше первоначальной.

Определите правомерность данного деяния и квалифицируйте его.

Задача 2.

Провайдеры спутникового Интернета предлагают клиентам полноценные тюнеры, через которые можно смотреть спутниковые телеканалы. Моделей таких тюнеров выпущено значительное количество и для одной из них – SkyStar1 – (помимо прочего, этот PCI-тюнер может записывать MPEG-видеопоток на винчестер компьютера, как цифровой видеомагнитофон) хакеры написали программы, открывающие кодированные телеканалы так же, как это делают карты-эмуляторы. При этом картинка выводится на монитор, звук – на аудиокарту, а вся дешифрация сигнала выполняется программно, центральным процессором компьютера. Не нужна ни карта-эмулятор, ни даже CAM-модуль (декодер). При этом обращаем внимание, что одних программ и PCI-тюнера недостаточно, так как для просмотра каждого закрытого канала надо достать его

уникальные ключи (которые можно взять из смарт-карты).

Каким образом можно расценить указанный способ доступа к перехваченному кодированному видеосигналу? Дайте уголовно-правовую характеристику.

Задача 3.

Современные цифровые телетюнеры не выдают на экран закодированную картинку, но многие модели имеют встроенный жесткий диск и способны записывать на не принимаемые передачи. Фирмы-производители прямо указывают, что их телетюнеры позволяют записать кодированный поток. Очевидно, что, обладая таким тюнером, для просмотра записанных кодированных программ можно пользоваться одной смарт-картой на несколько человек или обмениваться не самой картой, а лог-файлами ее «переговоров» с CAM-модулем (декодером).

Каким образом можно расценить указанный способ доступа к перехваченному кодированному видеосигналу? Дайте уголовно правовую характеристику.

Задача 4.

Вместо точного копирования всего программного обеспечения смарт-карты, берется только та его минимальная составляющая, которая позволяет в действующий период времени просматривать телеканал. При этом неважно, будет ли программное обеспечение в какой-то степени совпадать с имеющимся на карте или нет, главное, оно должно суметь декодировать телесигнал, закодированный определенным, действующим на данный момент кодом. В классическом варианте пиратские эмуляторы – это самодельные карты с маленьким компьютером на одном кристалле. Будучи вставленными в CAM-модуль (декодер), они выполняют работу легальных смарт-карт.

Дайте уголовно-правовую характеристику деяния.

Задача 5.

Способ заключается в тиражировании точных копий легальной карты – клонов. Если смотреть программное обеспечение, то оно у всех карт, включая подлинную, абсолютно идентично. Внешний видеокарт клона роли не играет: она может копировать оригинал, быть на него похожа или иметь свой собственный дизайн.

Каким образом можно расценить указанный способ? Дайте уголовно правовую квалификацию.

Задача 6.

Сотрудник крупнооптовой фирмы-импортера компьютерных комплектующих, работая старшим менеджером по закупкам в США, большую часть переговоров с партнерами вел по ICQ. Его ICQ-номер был зарегистрирован более семи лет назад. При регистрации он указал абстрактный e-mail –

qwert@kjlkj.asdfghjk.com (возможно, у него тогда его еще не было или он не хотел его давать). По подбору знаков похоже, что это случайная последовательность расположенных рядом на клавиатуре знаков. Даже доменного имени asdfghjk.com не существовало. Злоумышленник зарегистрировал доменное имя asdfghjk.com, создал в домене компьютер kjlkj.asdfghjk.com и завел на нем пользователя qwert. После этого в фирму Mirabilis (владельцы системы ICQ) была направлена просьба выслать, якобы, утраченный пароль на адрес, который был назван при регистрации. Пароль был выслан.

Квалифицируйте деяния злоумышленника. Что будет, если, зная пароль, злоумышленник его сменит (то есть сделает невозможным пользование данным номером для легального адресата)?

Как можно квалифицировать действия злоумышленника, если он получит всю информацию (список компаний, у которых закупается товар – информация конфиденциальная; цены и объем закупок – средне-конфиденциальная)? Если бы он уведомил поставщиков об изменении адреса поставок и направил поставки на несуществующие адреса?

Задача 7.

Системный администратор М. Увлекался бразильскими песнями. Сообщения М. на открытых форумах были проанализированы. В результате были сделаны выводы о пристрастиях М. Был создан русский сайт, полностью удовлетворяющий запросам М. На М. была осуществлена социальная атака: плакат с рекламой сайта был трижды опущен ему в почтовый ящик, повешен на дверь подъезда, положен под дворники машины, послан спам с рекламой сайта. Аналогичные меры были предприняты в отношении его подруги. М. зашел с рабочего компьютера на созданный специально под него сайт.

Как квалифицировать действия, если М. будет продан специальный модифицированный диск, несущий программы – закладки?

Как квалифицировать действия, если пока М. переписывает музыкальные файлы, сам сайт, пользуясь «прорехой» в программном обеспечении компьютера М., переписал несколько файлов с сетевых дисков фирмы?

Задача 8.

Студент заочного отделения Шабалин решил использовать компьютер из компьютерного класса академии для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема – одного из элементов компьютерной системы.

Подлежит ли уголовной ответственности Шабалин?

Дайте анализ состава преступления, предусмотренного ст.274 УК РФ.

Что понимается под информационно-телекоммуникационными сетями и

оконечным оборудованием в смысле ст. 274 УК РФ? Какие виды оконечного оборудования возможны?

Относится ли к оконечному оборудованию телефонный модем?

Задача 9.

Аспирант университета Хохлов, 24-ти лет, занимался исследовательской работой по компьютерной «вирусологии». Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы, так называемые «сетевые черви», проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате этого были полностью уничтожены списки сотрудников университета, расчеты бухгалтерии по зарплате, повреждены материалы научно-исследовательской работы, в том числе «пропали» две кандидатские и одна докторская диссертации.

Решите вопрос о правомерности действий Хохлова. В чем заключается субъективная сторона преступлений в сфере компьютерной информации?

5.3. Методические указания и порядок выполнения работы

При подготовке к занятию (задание на самостоятельную работу)

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы № 8 «Электронная цифровая подпись. Защита прав и законных интересов субъектов информационной сферы», используя литературу, а также конспект лекций.

В ходе самостоятельной работы необходимо:

– проверить нормативно-правовые документы в СПС «Консультант Плюс» на соответствие действующему законодательству ***(приложение № 1).***

Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся положений Конституции РФ, Доктрины информационной безопасности РФ и федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического занятия:

– изучить и составить ответы на контрольные вопросы *(вопросы из **приложения № 2)***, представить ответы на вопросы в отчёте практического занятия (устно).

– быть в готовности к проведению тестирования по темам № 7, № 8.

Приложение № 1.

Законодательная и нормативная база в области обеспечения ИБ РФ

Перечень нормативно-правовых документов:

1. Конституция Российской Федерации принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // Собрание законодательства РФ, 26.01.2009, N 4, ст. 445.

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (02.06.2016) // Собрание законодательства РФ, 17.06.1996, N 25, ст. 2954.

3. Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 N 1-ФЗ (ред. от 28.11.2015) (с изм. и доп., вступ. в силу с 01.01.2016) // Собрание законодательства РФ, 13.01.1997, N 2, ст. 198.

4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 01.05.2016) // Собрание законодательства РФ, 24.12.2001, N 52 (ч. I), ст. 4921.

Приложение № 2

Содержание отчёта (контрольные вопросы):

1. Проблемы предупреждения, выявления, документирования и расследования преступлений в сфере компьютерной информации.

2. Особенности становления и совершенствования законодательства России и зарубежных стран, касающегося регулирования отношений в сфере компьютерной информации.

3. Понятия «преступление в сфере компьютерной информации», «компьютерные преступления», «информационные преступления», их сходство и различия.

4. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ): особенности предупреждения, выявления и расследования.

5. Роль Федерального закона «О правовой охране программ для электронных вычислительных машин и баз данных» и Федерального закона «Об авторском праве и смежных правах».

6. Особенности научного и законодательного толкования таких понятий, как «информация; компьютерная информация; машинный носитель», «нарушение работы ЭВМ, системы ЭВМ или их сети»; «электронно-вычислительная машина (ЭВМ); система ЭВМ; сеть ЭВМ».

7. Особенности научного и законодательного толкования таких понятий, как «неправомерный доступ»; «охраняемая законом информация»; «модификация информации»; «адаптация программы для ЭВМ или базы данных»; «уничтожение информации»; «блокирование информации»; «копирование информации».

8. Особенности субъектов преступления. Виды хакеров.

9. Роль потерпевшей стороны в совершении преступлений рассматриваемой категории.

10. Способы совершения неправомерного доступа к компьютерной информации.

11. Способ непосредственного (активного) перехвата.

12. Способ несанкционированного доступа.

13. Манипуляции с компьютерной информацией.

14. Особенности выявления и расследования мошенничеств, совершаемых с использованием сети Интернет.

15. Понятие мошенничества с использованием сети Интернет.

16. Способы совершения мошенничеств и особенности их выявления и расследования. Онлайн-аукционы.

17. Способы совершения мошенничеств и особенности их выявления и расследования. Доставка товаров.

18. Способы совершения мошенничеств и особенности их выявления и расследования. Pay Pal и электронные платежные системы.

19. Способы совершения мошенничеств и особенности их выявления и расследования. Партнерские программы.

20. Способы совершения мошенничеств и особенности их выявления и расследования. Предложение несуществующих услуг и товаров.

21. Способы совершения мошенничеств и особенности их выявления и расследования. Мошенничество с платежными банковскими картами.

22. Способы совершения мошенничеств и особенности их выявления и расследования. Мошенничество с использованием фирм-однодневок.

23. Особенности предупреждения, выявления и расследования создания, использования и распространения вредоносных программ для ЭВМ (ст. 273 УК РФ).

24. Особенности криминологической характеристики создания, использования и распространения вредоносных программ для ЭВМ.

25. Способы совершения создания, использования и распространения вредоносных программ для ЭВМ.

26. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ).

27. Действия служб безопасности в зависимости от способа проникновения в сеть и последующей кражи информации.

28. Роль администратора сети в выявлении несанкционированного доступа к информации.

29. Передача информации с помощью стеганографии. Особая роль администратора сети.

30. Роль специальных познаний в выявлении расследовании преступлений, связанных с информационными технологиями.

31. Понятие «электронного документа». Доказательственное значение информации, записанной цифровым способом.

32. Особенности назначения и производства предварительных исследований и судебных экспертиз. Принципы оценки экспертных исследований.

33. Новые методы анализа, используемые при выявлении преступлений в сфере высоких технологий.

34. Роль психологических методов в защите информации.

35. Принципы исследования защищенности компьютерных систем.

6. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ВЗАИМООТНОШЕНИЙ АДМИНИСТРАЦИИ И ПЕРСОНАЛА В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Общие сведения

Цели:

1. Закрепить и углубить изучаемый лекционный материал студентами.

2. Определить мероприятия, связанные с подготовкой и проведением совещаний и заседаний по конфиденциальным вопросам, а также при работе с посетителями и изложить свою позицию по совершенствованию этой работы.

3. Рассмотреть виды переговоров, цели и задачи переговоров, вопросы планирования и подготовка переговоров.

4. Дать некоторые рекомендации по защите информации в ходе издательской и рекламной деятельности предприятия.

Учебные вопросы

1. Нормативная база для работы с конфиденциальными документами.

2. Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства (ноу-хау) и служебный секрет производства.

3. Режим обмена конфиденциальной документированной информацией.

4. Режим конфиденциальности при проведении совещаний и переговоров.

5. Классификация угроз информационной безопасности.

6.2. Теоретическое введение

Для сохранения конфиденциальности информации, и ее защиты необходимо регулировать отношения между администрацией и персоналом, опираясь на правовые нормы. Регулирование информационных отношений с помощью права осуществляется посредством установления определенных информационно-правовых норм, т. е. путем установления правил поведения субъектов информационных отношений и применения норм информационного права.

Разработка мер и обеспечение защиты информации осуществляются подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководством предприятия (учреждения) для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии ФСТЭК России и/или ФАПСИ на право оказания услуг в области защиты информации.

Право – это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определённых сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Правовые нормы обеспечения безопасности и защиты информации на

любом предприятии (фирме, организации) отражаются в совокупности учредительных, организационных и функциональных документов.

В процессе своей работы предприятие должно руководствоваться определенными документами, регулирующими взаимоотношения между администрацией и работниками. Состав нормативно-правовой базы предприятия по защите информации:

- перечень сведений, ограниченного доступа;
- положение о порядке обеспечения безопасности информации;
- должностные инструкции сотрудников, допущенных к работе;
- памятку работнику о защите информации;
- договорное обязательство при приеме на работу сотрудника;
- соглашения, подготавливаемые на случай возможного увольнения работников, имеющих доступ к сведениям, ограниченного доступа.

Перечень сведений, составляющих коммерческую тайну, определяется руководителем предприятия. Структурно этот перечень должен включать несколько частей, соответствующих различным видам тайны (концептуальной, организационной, технологической, параметрической и эксплуатационной).

Положение о порядке обеспечения безопасности информации включает в себя следующие разделы: порядок определения грифа, ограничивающего распространение информации; порядок допуска сотрудников к работе с информацией, составляющей тайну; обязанности сотрудников, допущенных к работе с информацией, составляющей тайну; принципы организации режима работы с информацией, составляющей коммерческую тайну.

Должностные инструкции: Допуск сотрудников к работе с информацией, осуществляется первым лицом предприятия (директором, президентом и т. д.) и его заместителями и руководителями структурных подразделений. Для принятия решения о допуске работника к информации, составляющей тайну, необходимо его предварительно проверить в течение испытательного срока.

К работе с информацией допускаются работники, прошедшие испытательный срок, только после изучения ими требований соответствующих документов по защите тайны предприятия, сдачи зачетов на знание изложенных в них требований, оформления ими в письменном виде обязательств по ее неразглашению.

Обязанности работников, допущенных к работе с информацией, состоят в следующем:

- в строгом сохранении тайны, ставшей им известной в связи с выполнением служебных обязанностей, либо от других работников фирмы;
- в принятии мер по пресечению действий других лиц, которые могут привести к утечке информации;
- в немедленном информировании непосредственного руководителя и

сотрудника службы безопасности предприятия обо всех фактах несанкционированного доступа к охраняемой информации, либо о создании предпосылок к этому;

- в неиспользовании секретов предприятия в личных целях;
- в ознакомлении только с теми закрытыми документами, к которым получен допуск в связи с выполнением служебных обязанностей;
- в доведении до минимально необходимого числа лиц, участвующих в подготовке документов, содержащих коммерческую тайну;
- в неукоснительном соблюдении порядка учета и хранения носителей информации (печатные документы, магнитные носители, образцы и т. д.).

Памятка работнику о защите информации должна содержать в очень краткой форме:

- основные обязанности и права работника в связи с необходимостью защиты коммерческой тайны;
- ключевые моменты, определяющие режим секретности проводимых работ;
- перечень основных документов предприятия, регламентирующих порядок обеспечения безопасности тайны.

В *трудовом договоре* с работником при приеме на работу вносятся следующие обязательства:

- в период работы на предприятии не разглашать информацию, которая стала известны работнику в связи с выполнением им служебных обязанностей;
- выполнять относящиеся к работнику требования приказов и иных документов по защите информации, с которой он ознакомлен;
- в случае увольнения не разглашать и не использовать известные работнику сведения в личных интересах, или в интересах других физических или юридических лиц.

Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действуют требования по защите информации, вытекающие из нормативно-правовых документов предприятия. При заключении трудового договора и оформлении приказа о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент включения данного лица в механизм обеспечения информационной безопасности.

Также должна быть запись о том, что работник предупрежден о материальной, дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством.

Документы, подготавливаемые на случай возможного увольнения работников, имеющих доступ к информации, предназначены для предотвращения

разглашения защищаемых сведений и имеют форму соглашения, анкеты, заявления, либо иную.

Обязанности по сохранению информации возлагаются и на руководителя организации. Для этого в контракт, заключаемый с руководителем, вводятся соответствующие положения:

- обязательство руководителя хранить информацию и не использовать ее в ущерб организации;
- о персональной ответственности за создание необходимых условий для сохранности информации;
- об ответственности руководителя за нарушения режима защиты информации и возможных последствиях.

6.3. Методические указания и порядок выполнения работы

Задание (выполнить письменно):

1. Составить перечень возможных угроз со стороны конкурентов (злоумышленников) безопасности коммерческой фирмы.
2. Определить мероприятия по защите конфиденциальной информации фирмы при приеме посетителей, клиентов, партнеров, представителей органов власти.
3. Определить мероприятия по защите конфиденциальной информации фирмы при работе со СМИ.
4. Сформулировать мероприятия (задачи) направленные на обеспечение безопасности проведения деловых встреч по конфиденциальным вопросам.
5. Сформулировать мероприятия (задачи) направленные на обеспечение безопасности проведения совещаний по конфиденциальным вопросам.
6. Изложить взгляды на совершенствование работы службы безопасности предприятия по защите конфиденциальной информации фирмы при приеме посетителей.

Контрольные вопросы (подготовить устные ответы):

1. Виды переговоров и цели и задачи переговоров.
2. Планирование и подготовка переговоров (раскрыть план переговоров).
3. Особенности подготовки и проведения деловых встреч и бесед на улице, в ресторане, гостиничном номере.
4. Особенности передачи конфиденциальной информации зарубежным партнерам во время проведения закрытых совещаний и переговоров.
5. Мероприятия, проводимые службой безопасности по защите конфиденциальной информации при проведении переговоров.
6. Меры противодействия утечки коммерческих секретов при приеме посетителей.
7. Правила взаимоотношений с официальными лицами при посещении ими коммерческого предприятия.

8. Дайте определение термина «документооборот».

9. Что вы понимаете под корпоративным конфиденциальным электронным документооборотом?

10. Что включает в себя организация работы с конфиденциальными электронными документами?

11. Какие возможности должна предусматривать система электронного конфиденциального документооборота?

7. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6. ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ОРГАНИЗАЦИОННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

7.1. Общие сведения

Цели:

1. Закрепить и углубить изучаемый материал студентами.

2. Определить проблемные вопросы организационной защиты информации в органах управления, в организациях и на предприятиях различной формы собственности и изложить свою позицию по совершенствованию организационных мероприятий защиты информации.

3. Рассмотреть роль и место организационной защиты в системе комплексной безопасности предпринимательской деятельности, основные цели принципы, функции, задачи и мероприятия организационной защиты информации, политика информационной безопасности; изучаются силы и средства защиты информации на предприятиях различной формы собственности.

Учебные вопросы:

1. Роль и место организационной защиты в системе комплексной безопасности предпринимательской деятельности.

2. Понятие, цели, основные функции, задачи и мероприятия организационной защиты информации.

3. Основные принципы организационной защиты информации.

4. Политика информационной безопасности.

5. Силы и средства защиты информации.

6. Организационное обеспечение комплексной безопасности предпринимательства.

7.2. Методические указания и порядок выполнения работы

При подготовке к занятию (задание на самостоятельную работу)

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы № 7 «Правовые основы использования организационных средств защиты информации», используя литературу, а также конспект лекций.

Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического занятия:

- изучить и составить ответы на контрольные вопросы, представить ответы на вопросы в отчёте практического занятия (устно);
- составить логическую схему базы знаний по содержанию блока;
- составить терминологический словарь и перечень персоналий.

Приложение № 1.

Дать письменные ответы по ситуациям № 1–6.

Номер по списку	1-5	6-10	11-15	16-20	21-25	26-30
Номер задания	1	2	3	4	5	6

Ситуация 1

По государственному заказу ОАО «Машзавод» разрабатывает и поставляет различные современные комплексы для Российской Армии, аналогов которых в мире нет. Разведки многих иностранные государств, стремятся заполучить образцы и технологию производства этих комплексов.

Определите, какие органы осуществляют защиту государственной тайны, объекты защиты? Какие организационные мероприятия необходимо проводить на предприятии с целью обеспечения защиты объектов информационной безопасности? Какие принципы организации и функционирования организационной защиты информации необходимо учитывать на предприятии?

Ситуация 2

Один из научно-исследовательских институтов (условно Ненецкий НИИ проблем ядерных технологий), занимается проектированием новых ядерных реакторов. Все работы засекречены.

Определите, в чьей компетенции находится контроль за состоянием защиты информации в НИИ, а также какие органы, силы и средства должны осуществлять защиту государственной тайны?

Ситуация 3

На предприятие, занимающееся производством оптических приборов во-

енного назначения (условно «Мост») на должность системного администратора рассматривается кандидатура Петрова А. И., который до этого работал ведущим программистом на другом режимном предприятии и был допущен к государственным секретам. На вопрос: «Причина увольнения с прежней работы? Ответил, что не удовлетворён заработной платой».

Какие и кем должны быть проведены мероприятия в отношении Петрова А.И. на этапе рассмотрения его кандидатуры, в период испытательного срока и при дальнейшей работе на должности системного администратора?

Ситуация 4

На заседании у губернатора с главами районных администраций, представителей силовых структур, руководителей крупных промышленных предприятий области, представители общественности, журналисты (условно N-ой области) рассматривались хозяйственные вопрос. Затем после небольшого перерыва, губернатор перешел к обсуждению вопросов, связанных с мобилизационной готовность в области, о переходе экономики области на военный режим работы?

Кто, по вашему мнению, имел право принимать участие в обсуждении вопросов после перерыва? Как должен быть осуществлен режим защиты государственных секретов?

Ситуация 5

Предприятие (условно «Зенит») занимается выпуском продукции двойного назначения (например, системы навигации для самолетов). Ряд узлов и деталей этой системы засекречены или же отнесены к коммерческой тайне?

Как, по вашему мнению, должен осуществляться производственный процесс изготовления этих систем: вместе коммерческие и государственные секреты, но под охраной государственных органов; раздельно – секретные и коммерческие узлы и агрегаты и т. д. в определенных цехах, но под охраной государственных органов или же как-то иначе?

Ситуация 6

После проведения маркетинговых исследований одна из коммерческих фирм, занимающаяся освоением рынка пластиковых труб решила открыть свой филиал в г. Морском?

Какая информация может быть отнесена к коммерческой тайне? Как и какими силами и средствами фирма должна защищать свои коммерческие секреты, какие для этого необходимо провести организационные мероприятия?

Контрольные вопросы (подготовиться к ответам – устно):

1. Роль и место организационной защиты в системе комплексной безопасности предпринимательской деятельности.

2. Понятие, цели, основные функции, задачи и мероприятия организаци-

онной защиты информации.

3. Основные принципы организационной защиты информации.

4. Политика информационной безопасности.

5. Силы и средства физической защиты информации.

6. Силы и средства технической защиты информации.

7. Силы и средства специальной защиты информации.

8. Силы и средства информационно-коммерческой защиты информации.

9. Система организационного обеспечение комплексной безопасности предпринимательства.

8. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7. ПОРЯДОК ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Общие сведения

*Цель***:** изучить основы организации защиты персональных данных (ПДн) и основное содержание разрабатываемых документов по защите ПДн.

Учебные вопросы

1. Нормативно-правовые документы по защите ПД.

2. Нормативно-методические документы по защите ПД.

3. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».

8.2. Теоретическое введение

В соответствии с пунктом 1 статьи 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

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

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Говоря о защите информации в целом, прежде всего, следует различать требования, предъявляемые к защите сведений: составляющих государственную тайну; признаваемые коммерческой тайной; персонального характера. Российское законодательство о защите персональных данных является относительно новым и существует множество нерешенных вопросов, что зачастую препятствует выполнению операторами персональных данных необходимых требований действующего законодательства о персональных данных.

Однако, несмотря на значительный комплекс проблем необходимо понимать, что:

1. Все без исключения физические лица являются субъектами ПДн.

2. Все без исключения организации являются операторами персональных данных и должны рассматривать требования Закона о персональных данных с точки зрения обеспечения наших прав и свобод, закрепленных Конституцией РФ.

3. Четкое выполнение требований регуляторов (Роскомнадзор, ФСТЭК России, ФСБ России) – уменьшение рисков манипулирования со стороны персонала и конкурентов.

Рекомендации по проведению комплекса необходимых мероприятий по защите ПДн

Для соблюдения минимальных требований и недопущения серьезных претензий со стороны регуляторов (в первую очередь Роскомнадзора) рекомендуется проведение следующего комплекса мероприятий:

1. Создание комиссии по проведению комплекса мероприятий по защите ПДн. Учитывая, что проведение данных работ включает широкий круг вопросов, в состав комиссии привлекаются лица, обладающие знаниями в сфере защиты информации, в области юриспруденции, работника кадровой службы, бухгалтера, системного администратора.

2. Начинать работу по проведению комплекса мер по защите ПДн следует с проведения категорирования обрабатываемых персональных данных. Проще говоря, задачей данного этапа работы является выявление всех данных персонального характера, обрабатываемых в организации. Также на данном этапе необходимо оценить наличие согласий субъектов ПДн на обработку данных, проанализировать требуется ли для нужд организации хранение всех сведений персонального характера, а также определить перечень ответственных лиц.

3. Определение характеристики ИСПДн. На данном этапе необходимо определить конфигурации и топологии ИСПДн, физические, функциональные и технологические связи как внутри системы, так и с другими системами различного уровня и назначения, определить технические и программные средства, используемые в ИСПДн.

4. Определение перечня угроз в части соблюдения безопасности информации, их актуальность (рекомендуется привлечение экспертов по информационной безопасности), разработка модели угроз и определение класса ИСПДн.

5. Подготовка и направление уведомление в Роскомнадзор с целью включения в реестр операторов.

6. Разработка порядка работы с ПДн. В случае необходимости разработать и провести комплекс дополнительных мероприятий по защите ПДн, в том числе по технической защите ПДн (приобрести и настроить необходимые технические средства и программное обеспечение). Разработанный порядок должен обеспечивать своевременное предоставление информации в случае полу-

чения запросов из Роскомнадзора (7 раб. дней) или непосредственно от физических лиц – субъектов ПДн (10 раб. дней).

7. Подготовка и утверждение комплекта организационно-распорядительной документации. В наличии должны быть:

– приказ о назначении ответственного должностного лица/подразделения;

– положение о защите ПДн;

– приказы о допуске, перечень допущенных сотрудников;

– журналы учета носителей информации.

8. Доведение до сотрудников порядка работы со сведениями о персональных данных, в том числе обучение сотрудников.

9. Планирование и проведение контрольных мероприятий по защите ПДн.

8.3. Методические указания и порядок выполнения работы

При подготовке к занятию (задание на самостоятельную работу)

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы № 8.1, используя литературу, а также конспект лекций.

В ходе самостоятельной работы необходимо:

– проверить нормативно-правовые документы в СПС «Консультант Плюс» на соответствие действующему законодательству ***(Приложение № 1).***

Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию. Затем студенты последовательно усваивают учебные вопросы, касающиеся федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического занятия:

– изучить и разработать один из документов в области защиты ПД *(по номеру в списке журнала преподавателя из* ***Приложение № 2)***, представить вариант документа в отчёте практического занятия.

– разработать 5 тестовых заданий по ФЗ №152 *(распределение заданий – Приложение № 3).*

Приложение № 1.

Законодательная и нормативная база в области обеспечения ИБ РФ:

1. Доктрина информационной безопасности Российской Федерации: утверждена Президентом Российской Федерации 5 декабря 2016 г. № .646.

2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (с изменениями от 25 апреля, 25 июля, 30, 31 октября, 31 декабря 2002 г., 30 июня, 4 июля, 11 ноября, 8, 23 декабря 2003 г., 9 мая, 26, 28 июля, 20 августа, 25 октября, 28, 30 декабря 2004 г.,

7, 21 марта, 22 апреля, 9 мая, 2, 21, 22 июля 2005 г.).

3. Федеральный закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».

4. Федеральный закон РФ от 7 июля 2003 г. № 126-ФЗ «О связи» (с изменениями от 23 декабря 2003 г., 22 августа, 2 ноября 2004 г., 9 мая 2005 г.).

5. Федеральный закон РФ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

6. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

7. Федеральный закон РФ от 18 июля 1999 г. № 183-ФЗ «Об экспортном контроле».

8. Указ Президента РФ от 14.05.1998 № 147 «О правовой защите результатов научно-исследовательских, опытно-конструкторских и технологических работ военного, специального и двойного назначения».

9. Указ Президента РФ от 24.01.1998 № 61 «О перечне сведений, отнесенных к государственной тайне».

Приложение № 2

Задание для самостоятельной работы.

Для всех: перечень документов, разрабатываемых на предприятии по защите ПД.

Персонально каждому: создайте или найдите в сети Интернет и адаптируйте под свою организацию (в нашем случае – это ФГБОУ ВО «КГТУ») следующие документы:

1. – «Согласие на обработку персональных данных».

– «Согласие на обработку персональных данных (в случае получения данных у третьих лиц/передачи данных третьим лицам)».

2. – «Отзыв согласия на обработку персональных данных».

– «Журнал учета согласий субъектов персональных данных».

3. – «Журнал учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных».

– «Уведомление об обработке (о намерении осуществлять обработку) персональных данных», направляемое в Роскомнадзор.

4. «Приказ о создании комиссии по проведению категорирования персональных данных и проведению инвентаризации/обследования информационных систем».

5. – «Опросный лист для сбора исходных данных об ИСПДн».

– акт категорирования персональных данных (перечень персональных данных»).

6. – «Перечень информационных систем, обрабатывающих ПДн».

– акт классификации информационной системы, обрабатывающей ПДн».

7. – «Положение о защите персональных данных».

– «План мероприятий по защите персональных данных».

8. «Приказы о допуске к работе с ПД».

9. – Обязательство о неразглашении сведений персонального характера».

– «Журнал учета защищаемых носителей информации».

10. – «Акт на списание и уничтожение электронных носителей информации».

– перечень мероприятия, предусмотренные по обеспечению безопасности ПДн при их обработке в информационных системах.

Алгоритм классификации ИСПДн приведён на рисунке 1.

Контрольные вопросы:

1. В какой степени законодательная база РФ обеспечивает защиту прав личности на доступ к информации?
2. Какие государственные гарантии реализации права на доступ к информации определяет Закон Российской Федерации «Об информации, информационных технологиях и о защите информации»?
3. В какой степени законодательная база РФ обеспечивает защиту права на неприкосновенность частной жизни?
4. Раскройте понятие «персональные данные» и дайте их классификацию.
5. В какой степени законодательная база РФ обеспечивает защиту личности от воздействия «вредной» информации?
6. Перечислите современные технологии защиты от утечки конфиденциальной информации.
7. Перечислите каналы утечки конфиденциальной информации.
8. Перечислите средства контентного анализа исходящих пакетов данных.
9. Перечислите средства криптографической защиты конфиденциальной информации.
10. Перечислите современные технологии защиты от утечки конфиденциальной информации.

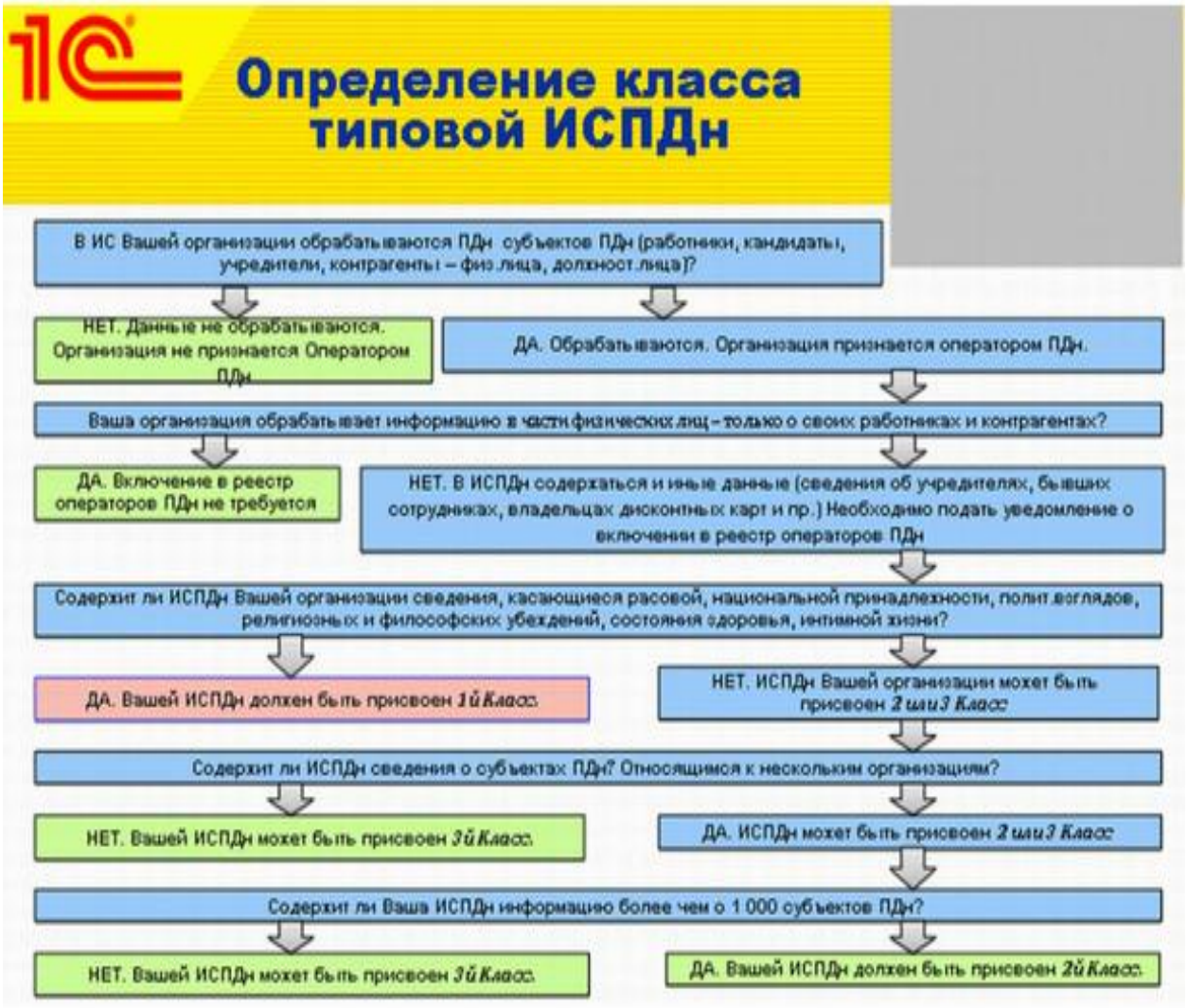

Рисунок 1. Определение класса типовой ИСПДн

9. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.1. Общие сведения

Цель: закрепление теоретических знаний в области обеспечения информационной безопасности.

Учебные вопросы:

1. Нормативные правовые документы по технической защите информации.
2. Организационно-распорядительные документы по технической защите информации
3. Нормативные и методические документы по технической защите ин-

формации Государственные стандарты.

4. Отраслевые нормативные документы по технической защите информации.

9.2. Теоретическое введение

Общедоступная информация определяется в ФЗ РФ «Об информации, информационных технологиях и защите информации» как «общеизвестные сведения и иная информация, доступ к которой не ограничен».

Принципами правового регулирования отношений в сфере информации, информационных технологий и защиты информации являются:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов РФ при создании информационных систем и их эксплуатации;

5) обеспечение безопасности РФ при создании информационных систем, их эксплуатации и защите, содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия; 8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Правовое регулирование отношений в сфере оборота общедоступной информации определяется контролю за деятельностью, связанной с обращением информации.

Так выделяют общественные отношения в сфере:

1. средств массовой информации и рекламы;

2. информационных ресурсов (архивные, музейные, библиотечные фонды);

3. информационных систем федерального, регионального, муниципального уровня;

4. доступа к информации (обязательной к обнародованию или предоставлению по запросам граждан, компетентных органов);

5. международного обмена информацией.

9.3. Методические указания и порядок выполнения работы

При подготовке к занятию (задание на самостоятельную работу)

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы 9.1 «Средства и методы физической защиты объектов», используя литературу, а также конспект лекций.

В ходе самостоятельной работы необходимо:

проверить документы в СПС «Консультант Плюс» на соответствие действующему законодательству ***(приложение № 1).***

Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию. Затем студенты последовательно усваивают учебные вопросы, касающиеся федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического занятия и готовят ответы на контрольные вопросы *(вопросы из **приложения № 2** – устно)*.

Приложение № 1.

Законодательная и нормативная база в области обеспечения ИБ РФ

По списку в журнале с 1 по 5 номер

Федеральные законы по технической защите информации

В РФ разработаны и введены в действие следующие федеральные законы в области обеспечения ИБ:

1. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
2. Федеральный закон РФ от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
3. Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи».
4. Федеральный закон РФ от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
5. Федеральный закон РФ от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных».
8. Федеральный закон РФ от № 390-ФЗ от 28.12.2010 «О безопасности».

По списку в журнале с 6 по 11 номер

Указы и распоряжения Президента РФ по технической защите информации

Президентом РФ подписаны следующие указы в области обеспечения ИБ:

1. Указ Президента РФ от 16.08.2004 № 1085 «Вопросы федеральной службы по техническому и экспортному контролю».

2. Указ Президента РФ от 30.11.1995 №1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».

3. Указ Президента РФ от 23.09.2005 № 1111 «Об утверждении перечня сведений конфиденциального характера».

4. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

5. Указ Президента Российской Федерации от 16.08.2004 № 1085 «Положение о Федеральной службе по техническому и экспортному контролю».

По списку в журнале с 12 по 17 номер

Постановления Правительства РФ по технической защите информации

1. Постановление Совета министров-правительства РФ от 15.09.1993 года № 912-51 «Положение о государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам».

2. Постановление Правительства РФ от 03.101994 года № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

3. Постановление Правительства РФ от 15.04.1995 года № 333 «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».

4. Постановление Правительства РФ от 26.06.1995 № 608 "О сертификации средств защиты информации».

5. Постановление Правительства РФ от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности».

6. Постановление Правительства РФ от 31.08.2006 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты кон-

фиденциальной информации».

7. Постановление Правительства РФ от 03.02.2012 № 79 «Лицензировании деятельности по технической защите конфиденциальной информации».

8. 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)».

По списку в журнале с 18 по 23 номер

Приказы ФСТЭК

В рамках обеспечения технической защиты информации ФСТЭК выпустил следующие приказы.

1. Приказ ФСТЭК России от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

2. Приказ ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

Организационно-распорядительные документы по технической защите информации

К организационно-распорядительным документам по технической защите информации относятся:

1. Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная Указом Президента РФ от 12.05.2009 № 537.

2. Доктрина информационной безопасности Российской Федерации: утверждена Президентом Российской Федерации 5 декабря 2016 г. № 646.

3. Положение «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 ...», утвержденное постановлени-

ем Правительства РФ от 16 апреля 2012 г. № 313.

4. Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Государственной технической комиссии при Президенте РФ 25.11.1994.

По списку в журнале с 24 по 30 номер

Нормативные и методические документы по технической защите информации Государственные стандарты

1. ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».

2. ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

3. ГОСТ Р 51188-98. «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство».

4. ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».

5. ГОСТ Р 51583-2000. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования».

6. ГОСТ Р 52447-2005. «Защита информации. Техника защиты информации. Номенклатура показателей качества».

7. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

8. ГОСТ Р 51241-2008. «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».

9. ГОСТ Р ИСО/МЭК ТО 18044. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

10. ГОСТ Р ИСО/МЭК 18045. «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

11. ГОСТ Р ИСО/МЭК ТО 19791. «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».

12. ГОСТ Р ИСО/МЭК ТО 15446. «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».

13. ГОСТ Р ИСО/МЭК 18028-1. «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности».

Приложение № 2

Контрольные вопросы:

1. Основной объект информационного права.
2. Определение информационного общества.
3. Дополнительные объекты информационного права.
4. Предмет и метод информационного права.
5. Источники информационного права.
6. Система информационного права.
7. Связь информационной безопасности с другими отраслями права.
8. В каких случаях нельзя относить информацию к государственной тайне?
9. Какие государственные органы занимаются вопросами обеспечения безопасности информации, и какие задачи они решают?
10. Охарактеризуйте место правовых мер в системе комплексной защиты информации.
11. Законодательная и нормативная база по информационной безопасности в Российской Федерации (показать схемой).
12. Нормативные правовые документы по технической защите информации (уточнить содержание и представить перечень).
13. Организационно-распорядительные документы по технической защите информации (уточнить содержание и представить перечень).
14. Нормативные и методические документы по технической защите информации Государственные стандарты. (уточнить содержание и представить перечень).
15. Требования международных стандартов к ИБ (уточнить содержание и представить перечень).

10. ЛИТЕРАТУРА

Основная учебная литература

1. Ищейнов, В. Я. Защита конфиденциальной информации: учеб. пособие / В. Я. Ищейнов, М. В. Мецатунян. – Москва: ФОРУМ, 2013. – 256 с.

2. Кузнецов, А. В. Основы защиты информации: учеб. пособие / В. А. Иванов, О. П. Пономарев, И. А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 122 с.

3. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью. / учеб. пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой – Москва: Горячая линия-Телеком, 2012. – 214 с.

4. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва: Издательство Юрайт, 2018. – 309 с

5. Ярочкин, В. И. Служба безопасности коммерческого предприятия. Москва: 3-е изд., перераб. и доп. – Москва: Ось-89, 2003. – 352 с.

6. Корнеев И.К., Степанов Е.А. Защита информации в офисе: учебник. – Москва: ТК Велби, Изд-во Проспект, 2008. – 336 с.

7. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин. – Санкт-Петербург: СПбНИУИТМО, 2014. – 173 с.

Дополнительная учебная литература

1. Организационно-правовое обеспечение информационной безопасности: учеб. пособие / А. А. Стрельцов [и др.]; под общ. ред. А. А. Стрельцова. – Москва: Академия, 2008. – 256 с. (наличие в библиотеке БГАРФ – 12 экз.)

2. Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие для студентов, обучающихся по спец. «Комплексное обеспечение информационной безопасности автоматизированных систем» / Ю. А. Родичев. – Санкт-Петербург: Питер, 2008. – 272 с.

3. Галатенко, В. А. Стандарты информационной безопасности: курс лекций: учеб. пособие для вузов / В. А. Галатенко; ред. В. Б. Бетелин. – 2-е изд. – Москва: Интернет-Ун-т Информац. Технологий, 2006. – 262 с.

4. Основы информационной безопасности [Электронный ресурс]: учеб. пособие для вузов / Е. Б. Белов [и др.]. – Электрон. текстовые дан. – Москва: Горячая линия-Телеком, 2011. – 544 с. – Режим доступа: 23 http://www.iprbookshop.ru/12014.html.

5. Ярочкин, В. И. Информационная безопасность: учебник для вузов / В. И. Ярочкин. – Москва: Акад. проект, 2008. – 542 с.

6. Просис, Крис. Расследование компьютерных преступлений / К. Про-

сис, К. Мандиа; пер. О. Труфанов. – Москва: ЛОРИ, 2013. – 76 с.

7. Расследование и раскрытие преступлений, совершенных посредством SMS-сообщений: методические рекомендации / ДГСК МВД России; сост. Н. А. Жукова (и др.). – Москва, 2014.

8. Болсуновская, Л. Мошенничество в сфере компьютерной информации: анализ судебной практики // Уголовное право. – 2016. – N 2. – С.12–16.

9. Евдокимов, К. Н. Вредоносные компьютерные программы как орудие и средство совершения преступлений: онтологические и гносеологические аспекты // Рос. юстиция. – 2020. – N 3. – С.56–58.

10. Поддубная, Е. Проблемы квалификации преступлений, связанных с хищением денежных средств в системах интернет-банкинга / Е. Поддубная, Е. Фернандес Гонсалес // Защита информации. – 2013. – N 2. – С.28–31.

11. Степанов-Егиянц, В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации: монография. – Москва: Статут, 2016. – 190 с.

12. Комментарий к Уголовному кодексу Российской Федерации (постатейный) с практическими разъяснениями официальных органов и постатейными материалами. 2-е издание. Автор комментариев и составитель В. С. Чижевский – Москва: Книжный мир, 2017. – 684 с.

13. Криминалистика: учебник для студентов вузов / под ред. А. Ф. Волынского, В. П. Лаврова. – 2-е изд., перераб. и доп. – Москва: ЮНИТИ-ДАНА: Закон и право, 2015. – 943 с.

14. Егоров, В. П. Конфиденциальное делопроизводство [Электрон. ресурс]: учеб. пособие / В. П. Егоров, А. В. Слиньков. – Москва: Юридический институт МИИТа, 2015. – 178 с.

15. Мэггс, П. Б. Интеллектуальная собственность [Электрон. ресурс]. / П. Б. Мэггс, А. П. Сергеев. – Москва: Юристъ, 2000. – 400 с.

16. Современные методы защиты информации [Электрон. ресурс] // Camafon.ru [сайт]. [2019]. URL: https://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi.

17. Астахова, А. В. Информационные системы в экономике и защита информации на предприятиях – участниках ВЭД: учеб. пособие / А. В. Астахова. – Санкт-Петербург: Троицкий мост, 2014.

18. Чеботарева, А. А. Информационное право: учеб. пособие / А. А. Чеботарева. – Москва: Юридический институт МИИТа, 2014.

19. Груздева, Л. М. Информационные технологии в профессиональной деятельности: метод. указания по выполнению практических работ / Л. М. Груздева, С. Л. Лобачев, А. А. Чеботарева. – Москва: Юридический институт МИИТа, 2015.

20. Карпов, В. И Основы теории обеспечения безопасности личности,

общества и государства: учеб. пособие / В. И. Карпов, О. Н. Новокшанов, Д. Б. Павлов. – Москва: Юридический институт МИИТа, 2010.

Периодические издания

1. Лачихина, А. Б. Подходы и методы управления информационной безопасностью в процессе управления промышленным предприятием / А. Б. Лачихина, А. А. Петраков. // Вопросы радиоэлектроники. – 2017. – № 11. – С.48–51.

2. Домуховский, Н. А. Обзор закона «О безопасности критической информационной инфраструктуры Российской Федерации» / Н. А. Домуховский. // Защита информации. Инсайд. – 2017. – № 6. – С.8–13.

Справочная литература

1. Доктрина информационной безопасности Российской Федерации: утверждена Президентом Российской Федерации 5 декабря 2016 г. № 646.

2. Стратегия развития информационного общества в Российской Федерации: утверждена Президентом Российской Федерации 07.02.2008 № Пр-212. // Консультант Плюс. – 2014. С. 2–7.

3. Стратегия национальной безопасности Российской Федерации до 2020 года: указ Президента Российской Федерации от 12 мая 2009 г. № 537 (в ред. указа Президента РФ от 01.07.2014 N 483) // Консультант Плюс. – 2014. – С. 2–19.

4. О безопасности: федеральный закон РФ от 28 декабря 2010 г № 390-ФЗ. // Консультант Плюс. – 2014. – С. 2–8.

5. Об информации, информационных технологиях и о защите и информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ (в ред. федерального закона от 21.07.2014 N 222-ФЗ) // Консультант Плюс. – 2014. – С. 2–19.

6. О лицензировании отдельных видов деятельности: федеральный закон от 4 мая 2011 г. № 99-ФЗ (в ред. федерального закона от 14.10.2014 N 307-ФЗ) // Консультант Плюс. – 2014. – С. 2–26.

7. О техническом регулировании: федеральный закон от 27 декабря 2002 г. № 184-ФЗ (в ред. федерального закона от 23.06.2014 N 160-ФЗ) // Консультант Плюс. – 2014. – С. 2–46.

8. О коммерческой тайне: федеральный закон РФ от 29 июля 2004 г № 98-ФЗ (в ред. федерального закона от 12.03.2014 N 35-ФЗ) // Консультант Плюс. – 2014. – С. 2–7.

9. Об организации лицензирования отдельных видов деятельности: постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 (в ред. постановления Правительства РФ от 28.10.2013 N 966) // Консультант Плюс. – 2013. – С. 2–9.

10. Конвенция о преступности в сфере компьютерной информации ETS № 185 (заключена в г. Будапеште 23.11.2001).

11. Конституция Российской Федерации/ Принята 12 декабря 1993 г. все-

народным голосованием (с изменениями от 01 июля 2020 г.)

12. Уголовный кодекс Российской Федерации от 13.06.1996 года №63-ФЗ.

13. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.

14. Гражданский кодекс Российской Федерации (часть 4) от 06.04.2011 № 63-ФЗ.

15. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».

16. Федеральный закон РФ от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».

17. Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи».

18. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

19. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

20. Постановление Правительства Российской Федерации от 03 февраля 2012 г. № 79 (ред. от 15 июня 2016 г.) «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»).

21. Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

22. Федеральный закон от 27.12.2009 г. № 363-ФЗ «О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных».

23. Трудовой кодекс Российской Федерации (Федеральный закон от 30.12.2001 № 197-ФЗ), гл. 14.

24. Указ Президента Российской Федерации от 3 декабря 2008 года № 1715 «О некоторых вопросах государственного управления в сфере связи, информационных технологий и массовых коммуникаций».

25. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

26. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

27. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям био-

метрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

28. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

29. Порядок проведения классификации информационных систем персональных данных. Совместный приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20. Зарегистрирован в Минюсте России 3 апреля 2008 г., регистрационный № 11462.

30. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

31. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.

32. Положение о методах и способах защиты информации в информационных системах персональных данных. Приказ ФСТЭК России от 5 февраля 2010 г. № 58, зарегистрировано в Минюсте РФ 19 февраля 2010 г. № 16456.

33. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. № 149/54-144, 2008 г. ФСБ России.

34. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005). Приказ ФСБ России от 9 февраля 2005 г. № 66 (зарегистрировано в Минюсте Российской Федерации 3 марта 2005 г. № 6382).

35. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) от 16 июля 2010 г. № 482 «Об утверждении образца формы уведомления об обработке персональных данных».

11. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

1. http://www.inside-zi.ru — сайт журнала «защита информации».
2. http://www.inside-zi.ru — сайт журнала «Инсайд».
3. http://www.xakep.ru — сайт журнала «Хакер».
4. http://garant.ru — Гарант: законодательство РФ.
5. http://www.consultant.ru — Консультант +: законодательство РФ.
6. http://fstec.ru/ — официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России).
7. http://www.scrf.gov.ru/ — официальный сайт Совета безопасности Российской Федерации.
8. http://fsb.ru — официальный сайт Федеральной службы безопасности Российской Федерации (ФСБ России).
9. http://www.kremlin.ru/acts – официальный сайт Президента РФ.
10. http://www.government.ru – официальный сайт Правительства России.
11. http://www.mvd.ru – официальный сайт Министерства внутренних дел Российской Федерации.
12. http://ombudsmanrf.org – официальный сайт Уполномоченного по правам человека в Российской Федерации.
13. http://www.infosait.ru – библиотека гостов, стандартов и нормативов.
14. http://www.altx-soft.ru – правовые и организационно-распорядительные документы по технической защите информации.
15. http://avoidance.ru – правовые аспекты обеспечения информационной безопасности.
16. http://www.rg.ru/dok/ [On-line] – опубликованные нормативные-правовые акты РФ.
17. http://www.iqlib.ru – электронная интернет библиотека.
18. http://www.biblioclub.ru – полнотекстовая электронная библиотека.
19. http://www.elibrary.ru – научная электронная библиотека.

Электронный методический материал

Александр Георгиевич Жестовский

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Редактор С. Кондрашова

Уч.-изд. л. 4,7. Печ. л. 4,1.

Издательство федерального государственного бюджетного образовательного учреждения высшего образования «Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1