УДК

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

Кафедра радиоэлектроники и защиты информации

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению практических работ по организационному обеспечению информационной безопасности

Для студентов специальностей 090103 и 090104

Томск 2011

УДК

Составитель Л.А. Белицкая

Методические указания для практических занятий по организационному обеспечению информационной безопасности. – Томск: Изд-во ТУСУР, 2011.– 22 с.

Методические указания предназначены для проведения практических занятий по курсам «Организационное обеспечение информационной безопасности» и «Организационная защита информации» с целью закрепления полученных теоретических знаний, выработки умения применять действующую законодательную базу в области информационной безопасности, а также получения практических навыков по проектированию, исследованию и эксплуатацией систем защиты информации.

Содержится материал по организационно-правовым аспектам защиты информации, принципы и методы создания систем информационной безопасности, по организации работы с персоналом, обладающим конфиденциальной информацией, по работе подразделений защиты информации (технологии и методы защиты документов и продукции), по организации службы безопасности предприятия (охраны и допуска).

Библиогр.: 15 назв.

Рецензент

ВВЕДЕНИЕ

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

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

Наиболее вероятными источниками утечки информации являются:

- персонал, имеющий доступ к информации;
- документы, содержащие эту информацию;
- технические средства и системы обработки информации, в том числе линии связи, по которым она передается.

Угрозы безопасности информации определяются естественными факторами: стихийные бедствия (ураганы, наводнения, землетрясения), несчастные случаи (катастрофы, пожары, аварии), ошибки в процессе обработки информации (ошибки пользователя, ошибки оператора, сбои аппаратуры) и умышленными (хищение носителей информации, подключение к каналам связи, перехват ЭМИ, несанкционированный доступ, разглашение информации, копирование данных). Источники угроз: люди, технические устройства, модели (алгоритмы, программы), технологические схемы обработки, внешняя среда.

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

Вопросы государственного регулирования ИБ лежат в плоскости создания эффективной правовой базы информационного законодательства, определения перечня сведений конфиденциального характера и создания государственной системы лицензирования и сертификации в области защиты конфиденциальной информации.

Коммерческие предприятия в своей деятельности должны использовать международные и российские стандарты безопасности, современные подходы к профотбору персонала, рекомендации по организации внутриобъектового и пропускного режима, публикаторской и рекламной деятельности, охране материально-технических, людских и информационных активов, знать порядок засекречивания и рассекречивания сведений документов и продукции, передачи документов изделий от одного должностного лица другому или другой организации или другому государству.

ПРАКТИЧЕСКАЯ РАБОТА № 1
ЗАКРЕПЛЕНИЕ ПРАВА ПРЕДПРИЯТИЯ НА ЗАЩИТУ ИНФОРМАЦИИ В НОРМАТИВНЫХ ДОКУМЕНТАХ

1.1. Направления обеспечения информационной безопасности

Направления обеспечения информационной безопасности – это нормативно-правовые категории, ориентированные на обеспечение комплексной защиты информации от внутренних и внешних угроз.

Выделяют следующие направления защиты информации:

- правовая защита – это специальные законы, нормативные акты, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям;
- инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности.

Защита прав обладателя информации ограниченного доступа осуществляется способами, предусмотренными Гражданским кодексом Российской Федерации и законами РФ по информатизации и защите информации. Среди них можно выделить следующие: «Об информации, информатизации и защите информации», «Об участии в международном обмене», «О связи», «О государственной тайне», «О правовой охране программ ЭВМ и топологии микросхем», «Об информационном обеспечении экономического и социального развития», «О коммерческой тайне», «Об органах государственной безопасности», «О патентах», «Об авторском праве и смежных правах», «Об архивах». Действия по защите информации от утечки по техническим каналам регламентируются следующими правовыми документами: ГОСТ 29339-92 «Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ», ГОСТ Р 50752 «Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники. Методы испытаний», Указы президента РФ «О создании государственной технической комиссии при президенте РФ», «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам связи», «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», «Положение о государственной системе защиты информации в РФ».

1.2. Конкурентная разведка и промышленный шпионаж

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

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

- о потенциальных партнерах и сотрудниках;

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

- сбор информации маркетингового характера.

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

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

1.3. Исходные данные для проведения работы

1.3.1. Цель работы. Освоение метода правовой защиты служебной или коммерческой тайны на предприятии.

1.3.2. Для проведения ПР № 1 используется следующая игровая ситуация:

Вы работаете на предприятии, которое занимается одним из следующих видов деятельности, связанной с использованием коммерческой или служебной тайны (варианты видов деятельности):

Таблица 1

№ варианта	Вид и область деятельности	Количество человек
1	НПЦ	Более 500
2	ОАО	100-500
3	ООО	200-300
4	НПО	Не более 800
5	ОАО	300-500
6	ЧП	50-100
7	ФГУП	До 1000
8	ИП	20-50
9	ООО	До 100
10	ЗАО	300-500

1.3.3. Нормативно-правовые документы, ориентированные на обеспечение информационной безопасности на предприятии.

1.3.4. Лекционный материал.

1.4. Задание

1.4.1. Определите название фирмы, выберите вид и область деятельности из перечисленных в таблице 1, обоснуйте выбор. Укажите общие данные о предприятии (профиль деятельности, форма собственности, число клиентов, профиль клиентской базы, объем продаж или оборот, основные стратегические задачи предприятия, конкурентные компании их доля присутствия на рынке).

На основе анализа штатной структуры предприятия составьте предварительный список должностей, имеющих отношение к конфиденциальной информации (КИ) предприятия.

1.4.2. Составьте план мероприятий по защите КИ (в соответствии с законом РФ «О коммерческой тайне»).

1.4.3. Укажите перечень внутрифирменных нормативно-правовых документов, которые будут использоваться в целях правовой защиты секретов вашей фирмы. Составьте 1-2 документа.

1.4.4. Составьте перечень сведений, составляющих коммерческую тайну вашей фирмы.

1.4.5. Опишите методы конкурентной разведки, которые будут использоваться вашей информационно-аналитической службой.

1.4.6. Отчет о выполненной работе оформляется в соответствии с общепринятыми требованиями и предоставляется в письменном (или распечатанном виде).

Контрольные вопросы

1. Нормативно-правовое регулирование профессиональной тайны в РФ.
2. Признаки и объекты профессиональной тайны.
3. Какие сведения относятся к служебной тайне?
4. На каких правовых актах основана защита служебной и коммерческой информации на предприятии?
5. Чем отличается служебная тайна от профессиональной?
6. Какие внутренние нормативные документы используются для правовой защиты служебной и коммерческой тайны?
7. В какие виды договоров включаются условия о неразглашении служебной тайны?
8. Что понимается под убытком в результате разглашения коммерческой тайны?
9. Определение и виды конкурентной разведки.

ПРАКТИЧЕСКАЯ РАБОТА № 2
ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ И СЕРТИФИКАЦИЯ СРЕДСТВ В ОБЛАСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

2.1. Государственная система защиты информации в РФ

В зависимости от характера информации, ее доступности для заинтересованных потребителей, а также экономической целесообразности конкретных защитных мер могут быть выбраны следующие формы защиты информации:

- патентование;
- авторское право;
- признание сведений конфиденциальными;
- товарные знаки;

- лицензирование;
- сертификация.

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.

Вопросы лицензирования в области защиты конфиденциальной информации рассмотрены в законе РФ «О лицензировании отдельных видов деятельности» от 8 августа 2001 г. № 128-ФЗ (ред. от 11 марта 2003 г. № 32-ФЗ).

Вопросы сертификации в области защиты конфиденциальной информации рассмотрены в законе РФ «О сертификации продукции и услуг» от 10 июня 1993 г. N 5151-1 (ред. от 31 июля 1998г. № 154-ФЗ).

Вопросы защиты интеллектуальной собственности рассмотрены в законах РФ «О патентах», «Об авторском праве» и «О товарных знаках».

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

Постановление Правительства РФ от 23.04.96 № 509 устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом. Это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Системы сертификации создаются Государственной технической комиссией при Президенте Российской Федерации (ГТК), Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, Службой внешней разведки Российской Федерации.

Системы сертификации средств защиты информации в РФ осуществляется по требованиям безопасности информации, определенным ГТК. К нормативным документам относятся руководящие документы ГТК – по требованиям к автоматизированным системам, к средствам ВТ, к межсетевым экранам.

2.2. Исходные данные для проведения работы

2.2.1. Цель работы. Освоение методов защиты КИ при использовании государственных систем лицензирования и сертификации.

2.2.2. Условия работы фирмы аналогичны указанным в ПР №1.

2.2.3. Лекционный материал.

2.3. Задание

2.3.1. Обоснуйте необходимость проведения лицензирования выбранного (см. ПР № 1) вида деятельности.

2.3.2. Укажите порядок и необходимость (обязательная или добровольная) сертификации средств, используемых в выбранном виде деятельности.

2.3.3. Укажите перечень сертификационных документов, необходимых для выбранной деятельности фирмы.

2.3.4. Составьте для вашей фирмы документы, необходимые для осуществления заданного вида деятельности (используя самостоятельный поиск).

2.3.5. Отчет о выполненной работе оформляется в письменном (или распечатанном виде).

Контрольные вопросы

1. Нормативно-правовое регулирование деятельности в области защиты конфиденциальной информации.
2. Какие виды деятельности в области защиты конфиденциальной информации подлежат лицензированию?
3. Порядок лицензирования, срок действия лицензии.
4. Организационная структура системы сертификации в области защиты конфиденциальной информации.
5. При каких организациях созданы системы сертификации в РФ?
6. Порядок и требования при осуществлении сертификации средств защиты информации.
7. В каких случаях сертификация носит добровольный характер?
8. Кем устанавливаются формы сертификата и знака соответствия?
9. Назовите российские и международные стандарты безопасности.
10. Назовите различия между авторским правом и коммерческой тайной?
11. Какая взаимосвязь между патентом и коммерческой тайной?

ПРАКТИЧЕСКАЯ РАБОТА № 3
ОРГАНИЗАЦИЯ ПРОПУСКНОГО РЕЖИМА НА ПРЕДПРИЯТИИ

3.1. Внутриобъектовый и пропускной режимы

Внутриобъектовый и пропускной режимы устанавливаются, как правило, на предприятиях, осуществляющих в предусмотренном законодательством Российской Федерации порядке работу со сведениями, составляющими государственную тайну. Вместе с тем нормы и правила внутриобъектового режима могут быть применимы в случаях, когда предприятие выполняет работы и с иными видами информации с ограниченным доступом (например, конфиденциальной информацией).

Внутриобъектовый режим — комплекс мероприятий, направленных на обеспечение установленного режима секретности непосредственно в структурных подразделениях, на объектах и в служебных помещениях предприятия.

Пропускной режим — это совокупность норм и правил, регламентирующих порядок входа на территорию предприятия и выхода лиц, въезда и выезда транспортных средств, вноса и выноса, ввоза и вывоза носителей сведений кон-

фиденциального характера, а также мероприятий по реализации названных норм и правил с использованием имеющихся сил и средств.

Основными элементами системы организации пропускного режима являются:

- режимно-секретное подразделение;
- служба безопасности предприятия;
- бюро пропусков;
- контрольно-пропускные пункты и т.д.

3.2. Исходные данные для проведения работы

3.2.1. Цель работы. Освоение методов организации охраны защищаемой информации на предприятии.

3.2.2. Условия работы фирмы аналогичны указанным в ПР № 1.

3.3.3. Лекционный материал.

3.3. Задание

3.3.1. Определите основные объекты охраны.

3.3.2. Укажите перечень задач и функций службы безопасности.

3.3.3. Укажите основные направления работы по организации внутриобъектового режима на предприятии.

3.3.4. Определите и обоснуйте способы охраны территории предприятия и его объектов; укажите количество постов, мест несения дежурства по охране объектов, участки (зоны, территории) охраны; количество и виды контрольно-пропускных пунктов, порядок и особенности несения дежурства на этих пунктах сотрудниками охраны; порядок и особенности действий личного состава охраны во всех случаях (в том числе в экстренных ситуациях); порядок и особенности применения (использования) технических средств обнаружения и охраны на каждом участке (зоне, территории) охраны.

3.3.5. Отчет о выполненной работе оформляется в письменном (или распечатанном виде).

Контрольные вопросы

1. Система охраны предприятия.
2. Что такое «несанкционированное действие»?
3. Взаимосвязь внутриобъектового и пропускного режимов.
4. Что подразумевается под физической защитой предприятия?
5. Инженерно-технические средства защиты предприятия.
6. Виды пропусков на предприятие.
7. Формы допуска по степеням секретности сведений, составляющих государственную тайну, и грифы секретности их носителей.
8. Меры пресечения несанкционированного доступа.
9. Мероприятия по предупреждению разглашения конфиденциальной информации.

ПРАКТИЧЕСКАЯ РАБОТА № 4
НОРМАТИВНО-ПРАВОВЫЕ НОРМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

4.1. Нормативно-правовое обеспечение защиты информации в АС

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

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

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

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

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

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

4.2. Исходные данные для проведения работы

4.2.1. Цель работы. Освоение методов защиты информации в автоматизированных системах.

4.2.2. Условия работы фирмы аналогичны указанным в ПР №1.

4.3.3. Тексты руководящих документов ГТК РФ.

4.3.4. Лекционный материал.

4.3. Задание

4.3.1. Оцените угрозы вашим информационным ресурсам (укажите наиболее вероятные виды компьютерных преступлений).

4.3.2. Укажите мероприятия, проводимые при создании системы защиты информации в вашей компьютерной сети.

4.3.3. Укажите перечень руководящих документов ГТК, учитываемых при разработке «Политики безопасности» на вашем предприятии.

4.3.4. Определите и обоснуйте требования по защите вашей конфиденциальной информации – группу и класс защищенности средств вычислительной техники от НСД (с использованием РД ГТК, поиск самостоятельно).

4.3.5. Отчет о выполненной работе оформляется в письменном (или распечатанном виде).

Контрольные вопросы

1. Назовите особенности расследования компьютерных преступлений.
2. Какие задачи решаются судебно-бухгалтерской и программно-технической экспертизами при проведении следственных действий?
3. Существующая классификация компьютерных преступлений. Методы НСД.
4. Методы и приемы предупреждения компьютерных преступлений. Анализ компьютерных преступлений.
5. В каких документах представлены нормы правового обеспечения защиты информации в АС?
6. Что представляет собой документ «Политика безопасности»?
7. Какие документы необходимо представить для присвоения класса защищенности АС?
8. От чего зависит выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ?
9. Выполнение каких правил безопасности обеспечивается путем реализации «Политики безопасности»?
10. Где указаны требования к безопасности компьютерных сетей в РФ?

ПРАКТИЧЕСКАЯ РАБОТА № 5
СОЗДАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

5.1. Концепция информационной безопасности

Практические (организационные) мероприятия по созданию системы информационной безопасности предприятия (ИБП) включают следующие этапы: разработка политики безопасности, проведение анализа рисков, планирование обеспечения информационной безопасности; планирование действий в чрезвычайных ситуациях и подбор механизмов и средств обеспечения информационной безопасности.

Первые два этапа обычно трактуются как выработка политики безопасности и составляют так называемый административный уровень системы ИБП.

Третий и четвертый этапы заключаются в разработке процедур безопасности. На этих этапах формируется уровень планирования системы ИБП.

В указанном документе конкретизируются стратегические принципы безопасности (вытекающие из целей и задач ИБП). В качестве примера можно привести две стратегии ответных действий на нарушение безопасности:

- «защититься и продолжить», когда организация опасается за уязвимость информационных ресурсов и оказывает максимальное противодействие нарушению;

- «выследить и наказать», когда злоумышленнику позволяют продолжить действия с целью его компрометации и наказания.

5.2. Проведение анализа риска

Анализ риска необходим главным образом для выявления уязвимости АС и ее системы защиты, определения необходимых и достаточных затрат на ИБП. Основу процесса анализа риска составляет определение того, что надо защищать, от кого и как. Для этого выявляются активы – компоненты АС, нуждающиеся в защите.

Количественную оценку риска можно получить на базе экспертного опроса, статистически или по некоторой математической зависимости, адекватной конкретной угрозе конкретному активу. Кроме вероятности осуществления угрозы, важен размер ожидаемых потерь. В общем случае ожидаемые потери рассчитываются по следующей формуле:

$$E = P \cdot V,$$

где P – вероятность проявления угрозы;

V – величина ущерба при реализации угрозы.

Если на предприятии создана система защиты информационных ресурсов в АС с известной степенью защиты, то величина ущерба будет пропорциональна степени незащищенности АС.

5.3. Исходные данные

5.3.1. Цель работы. Освоение этапов разработки концепции и создания системы информационной безопасности в АС предприятия.

5.3.2. Условия работы фирмы аналогичны указанным в ПР №1.

5.3.3. Лекционный материал.

5.4. Задание

5.4.1. Указать цель обеспечения ИБП.

5.4.2. Задать величину степени защищенности (в процентах) создаваемой на объекте системы защиты информации и стоимость (S) используемых активов АС.

5.4.3. Выбрать и обосновать стратегические принципы безопасности АС.

5.4.4. Оценить величину ущерба (V) активам АС при реализации угроз.

5.4.5. Рассчитать ожидаемые потери (Е) после создания системы информационной безопасности (заполнить таблицу 2).

Таблица 2

Категории активов	S [руб.]	V [руб.]	P	E [руб.]
Аппаратное обеспечение				
Программное обеспечение				
Информационное обеспечение				
Персонал				
Документация				
Расходные материалы				

5.4.6. Отчет о выполненной работе оформляется в письменном (или распечатанном виде).

Примечание. Вероятность возникновения угроз (Р) взять из известных в литературе данных или принять среднее значение – 0,5.

Контрольные вопросы

1. Этапы создания системы ИБП.
2. Реализация на практике концепции ИБП.
3. На основе каких документов разрабатывается политика безопасности?
4. Исходя из чего выбирают стратегические принципы безопасности?
5. Уровни политики безопасности и ответственные за них.
6. Зачем проводится анализ риска? Методы оценки рисков.
7. Категории защищаемых активов АС, классификация угроз.
8. Содержание плана защиты АС.
9. Содержание плана обеспечения непрерывной работы и восстановления АС.

ПРАКТИЧЕСКАЯ РАБОТА № 6
ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ РАБОТЕ С КАДРАМИ

6.1. Персонал фирмы и его роль в утечке информации

В целях обеспечения информационной безопасности необходимо уделять особое внимание подбору и изучению кадров, проверке любой информации, указывающей на их сомнительное поведение и компрометирующие связи. В настоящее время ведущие коммерческие структуры имеют строго разработанные и утвержденные руководством организационные структуры и функции управления для каждого подразделения. Используются оргсхемы или организационные чертежи, на которых графически изображается каждое рабочее место, прописываются должностные обязанности и определяются информационные потоки для отдельного исполнителя.

Кроме того, для большей конкретизации этих процедур на каждое рабочее место составляются профессиограммы. Профессиограмма – это перечень личностных качеств с оценочной шкалой, которыми должен обладать потенциальный сотрудник.

6.2. Основные рекомендации при организации проверки и отбора кандидатов на работу в коммерческие предприятия

С точки зрения обеспечения стратегических интересов коммерческой структуры являются обязательными следующие основные функции по отбору кандидатов на работу:

- определение степени вероятности формирования у кандидата преступных наклонностей в случаях возникновения в его окружении определенных благоприятных обстоятельств;
- выявление имевших место ранее преступных наклонностей, судимостей, связей с криминальной средой.

Для добывания подобной информации используются возможности различных подразделений коммерческих структур, а также некоторых сторонних организаций, например детективных агентств, бюро по занятости населения, диспансеров. Используются тщательно подготовленные процедуры приема и увольнения персонала.

6.3. Исходные данные

6.3.1. Цель работы. Освоение методов защиты информации при профотборе.

6.3.2. Ваша фирма (см. условия ПР № 1) собирается уволить двух сотрудников – руководителя производственного отдела и рекламного агента и принять на их место новых работников.

6.3.3. Лекционный материал.

6.3.4. Примеры тестов профориентации.

6.4. Задание

6.4.1. Укажите основные мероприятия комплексного профотбора, проводимые службами безопасности фирмы в каждом случае.

6.4.2. Сделайте выбор тестов (поиск осуществляется самотоятельно), которые будут использоваться для проверки каждого из кандидатов.

6.4.3. Укажите особенности процедуры увольнения прежних работников с точки зрения обеспечения сохранности коммерческих секретов, оформите соответствующие документы.

6.4.4. Составьте профили требований (профессиограммы) к данным сотрудникам (таблица 3).

6.4.5. Отчет о выполненной работе оформляется в виде распечатки контрольного листа из файла.

Таблица 3

Качества работника		Оценочная шкала						
		1	2	3	4	5	6	7
Административные								
Межличностные								
Интеллектуальные								
Психологическая устойчивость								
Деловые								

Контрольные вопросы

1. С какой целью вводятся процедуры психологического профотбора?
2. Что включает в себя комплексный подход при профотборе кадров?
3. Какие структуры используются для сбора сведений о кандидатах?
4. Какие методы используются для сбора сведений о кандидатах?
5. Назовите тестовые приемы и другие научные методики проверки кандидатов.
6. Особенности проведения итоговой беседы с кандидатами.
7. Какие меры целесообразно предпринять до беседы с увольняемым сотрудником?
8. Какие формы может принимать беседа с увольняемым сотрудником, и каким образом должен быть построен разговор?
9. Какие существуют варианты сохранения в тайне коммерческих сведений при увольнении сотрудников?

ПРАКТИЧЕСКАЯ РАБОТА № 7
ЗАЩИТА ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА

7.1. Организация международного сотрудничества

Изменения последних лет в области внешней политики России привели к росту числа международных контактов, их глубины и многогранности. Информационное обеспечение международных договоренностей, в том числе с использованием сведений, составляющих государственную тайну, и конфиденциальной информации осуществлялось и ранее. Тем не менее, в нынешних условиях развития нашего государства решение проблемы обеспечения должного уровня национальной безопасности требует создания стройной организации процесса защиты информации во всех сферах деятельности государства.

Основными элементами системы международного сотрудничества являются:

- передача другим государствам сведений, составляющих государственную или иную тайну;
- прием на предприятии иностранных представителей;
- выезд персонала, осведомленного в сведениях, составляющих государственную или иную тайну, за границу.

При организации международного сотрудничества необходимо руководствоваться: законом РФ «О государственной тайне» от 21 июля 1993 г. № 5485-1 (ред. от 24 сентября 1997 г.); ФЗ «О коммерческой тайне» от 02 февраля 2006 г. № 19; ФЗ «Об участии в международном информационном обмене» от 5 июня 1996 г.; Положением правительства РФ «О подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. № 973 (ред. от 24.09.2010 г. № 746); ФЗ «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию»; «Положение о Межведомственной комиссии по защите государственной тайны» и др.

7.2. Исходные данные для проведения работы

3.2.1. Цель работы. Освоение методов организации защиты информации при международном сотрудничестве.

3.2.2. Условия работы фирмы аналогичны указанным в ПР № 1.

3.3.3. Лекционный материал.

7.3. Задание

3.3.1. Организуйте прием иностранной делегации на предприятии. Для этого определите тематику мероприятия и составьте: программу приема; план мероприятий по защите информации; списки сотрудников, уполномоченных участвовать в приеме; уведомление о приеме иностранных граждан; отчет о проведении приема; журнал учета приема иностранных граждан.

3.3.2. Укажите перечень задач и функций службы безопасности при подготовке и приеме иностранных представителей.

3.3.3. Укажите основные направления работы по подготовке служебных помещений или административных территорий, выделенных для приема иностранных делегаций.

3.3.4. Определите обязанности сотрудников, участвующих в мероприятиях по приему иностранных представителей.

3.3.5. Отчет о выполненной работе оформляется в письменном (или распечатанном виде).

Контрольные вопросы

1. Действующие нормативно-правовые акты в сфере международных отношений.

2. Роль Межведомственной комиссии по защите государственной тайны?

3. Что должен содержать проект межправительственного договора (соглашения) по взаимной защите передаваемых сведений?

4. Каким ФЗ устанавливается срок ограничения права выезда из РФ?

5. Какой в общей сложности срок ограничения права гражданина на выезд из РФ, при допуске к сведениям разных степеней секретности?

6. Порядок передачи другим государствам сведений, составляющих государственную или иную тайну.

7. Порядок выезд персонала, осведомленного в сведениях, составляющих государственную или иную тайну, за границу.

ПРАКТИЧЕСКАЯ РАБОТА № 8
ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ РЕКЛАМНОЙ И ПУБЛИКАТОРСКОЙ ДЕЯТЕЛЬНОСТИ

8.1. Общие положения

Работу современного предприятия невозможно представить без публикаторской деятельности и рекламных акций различного характера. Вместе с тем, если предприятие работает с конфиденциальной информацией, такие виды деятельности могут привести к возникновению возможных каналов утечки этой информации.

Мероприятия по защите информации в процессе подготовки и реализации рекламных и публикаторских (издательских) проектов должны занимать особое место в повседневной деятельности предприятия.

При подготовке материалов к открытому опубликованию необходимо руководствоваться:

- перечнем сведений, отнесенных к государственной тайне (закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-1 (ред. от 24 сентября 1997 г.);
- перечнем сведений, конфиденциального характера (Указ президента РФ от 6 марта 1997 г. № 188);
- ФЗ «О коммерческой тайне» от 02 февраля 2006 г. № 19;
- перечнем сведений, составляющих коммерческую тайну предприятия;
- законом РФ «О рекламе» от 13 марта 2006 г. № 38-ФЗ (ред. от 28 сентября 2010 г.);
- основным нормативным правовым актом, определяющим общие принципы свободы массовой информации и регулирующим вопросы деятельности СМИ в Российской Федерации – законом РФ «О средствах массовой информации» от 27 декабря 1991 г. № 2124-1 и др.

8.2. Исходные данные для проведения работы

3.2.1. Цель работы. Освоение методов организации защиты информации при рекламной и публикаторской деятельности.

3.2.2. Условия работы фирмы аналогичны указанным в ПР № 1.

3.2.3. Для проведения ПР № 8 используется следующая ситуация: ваша организация решила провести научно-практическую конференцию и рекламную акцию (таблица 4).

Таблица 4

№ варианта	Вид деятельности	Примечание
1	Наружная реклама	
2	Реклама на телевидении и радио	
3	Реклама в периодических печатных изданиях	
4	Пресс-конференция	На территории предприятия
5	Подготовка пресс-релизов	
6	Подготовка официальных комментариев	
7	Брифинг	
8	Встреча с представителями СМИ	
9	Проведение пресс-конференции	На территории предприятия
10	Подготовка сообщений для СМИ	

3.3.4. Лекционный материал.

8.3. Задание

3.3.1. Выберите один из видов деятельности для вашего предприятия (таблица 4). Составьте текст публикации (сообщений).

3.3.2. Укажите основные направления защиты информации в ходе выбранной вами деятельности.

3.3.3. Укажите основные организационные работы по подготовке и проведению научно-практической конференции на территории предприятия, направленные на исключение утечки конфиденциальной информации.

3.3.4. Составьте экспертное заключение о возможности открытой публикации материалов конференции.

3.3.5. Отчет о выполненной работе оформляется в письменном (или распечатанном виде).

Контрольные вопросы

1. Обязанности членов экспертной комиссии при подготовке и проведении экспертизы.
2. Кто включается в состав экспертной комиссии?
3. Что такое разглашение конфиденциальной информации?
4. Основные направления деятельности по пресечению утечки конфиденциальной информации?

5. Какие факты и обстоятельства могут привести к разглашению информации?

6. Каналы распространения информации.

7. Мероприятия, направленные на исключение открытого опубликования информации с ограниченным доступом.

8. Что такое цензура массовой информации?

9. Какие формы должна принимать беседа с журналистом, и каким образом должен быть построен разговор, чтобы исключить утечку конфиденциальной информации?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Копылов В.А. Информационное право: Учебник. – М.: Юристъ, 2003.
2. Рассолов М.М. Информационное право. – М.: Юристъ, 1999.
3. Позняков Е.Н. Защита объектов (рекомендации для руководящих и сотрудников служб безопасности). – М.: Концерн «Банковский деловой центр», 1997.
4. Организация и современные методы защиты информации / Под общей редакцией С.А. Диева и А.Г. Шаваева. – М.: Концерн «Банковский деловой центр», 1998.
5. Ярочкин В.И. Служба безопасности коммерческого предприятия. Организационные вопросы. – М.: «Ось-89», 1995.
6. Климов В.А. Методология формирования перечня сведений, относящихся к служебной или коммерческой тайне // Конфидент. 1997. №4. С. 11–22.
7. Вехов В.Е. Компьютерные преступления: Способы совершения и раскрытия. – М.: Право и закон, 1996.
8. Беззубцев О.А., Ковалев А.Н. Лицензирование и сертификация в области защиты информации: Учебное пособие. – М.: МИФИ, 1996. – 108с.
9. Гасанов Р.М. Промышленный шпионаж на службе монополий. – М., 1986.
10. Барсуков В.В., Водолазкий В.В. Соверменные технологии безопасности. Интегральный подход. - М.: «Нолидж», 2000.
11. Семкин С.Н., Беляков ЭВ., Гребнев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. – М.: Гелиос АРВ, 2005. – 192 с.
12. Струков В.И. Организационно-правовое обеспечение информационной безопасности: Методическое пособие. – Таганрог: ТРТУ, 2004. – 14 с.
13. Ярочкин В.И. Информационная безопасность. Учебное пособие. М.: Междунар. отношения, 2000. – 400 с.
14. Струков В.И. Правовое обеспечение защиты информации: Методическое пособие. – Таганрог: ТРТУ, 1999. – 75 с.
15. Струков В.И., Кухаренко А.П. Основы защиты информации в предпринимательской деятельности: Методическое пособие. – Таганрог: ТРТУ, 2000. –110 с.

ОГЛАВЛЕНИЕ

Белицкая Лилия Анатольевна

Методические указания к выполнению практических работ по организационному обеспечению информационной безопасности

Для студентов специальностей
090103 и 090104

Ответственный за выпуск Белицкая Л.А.
Редактор
Корректор

ПР 2011 г.
Формат 60x84 1/16
Печать офсетная.
Заказ №

Подписано к печати
Бумага офсетная.
Усл. п.л. – 0,9. Уч. – изд. л. – 0,8.
Тираж 100 экз.

«С»

Издательство Томского государственного университета систем управления и радиоэлектроники
Типография Томского государственного университета систем управления и радиоэлектроники