МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«4» 04 2022г.

Организационное и правовое обеспечение информационной безопасности

Методические указания по выполнению практических работ для студентов специальностей и направлений подготовки 10.03.01, 10.05.02

Курск 2022

УДК 004.725.7

Составители: А.Л. Марухленко

Рецензент
Кандидат технических наук, доцент кафедры информационной безопасности М.А.Ефремов

Организационное и правовое обеспечение информационной безопасностии:методические указания к выполнению практических работ / Юго-Зап. гос. ун-т, сост.: А. Л. Марухленко. Курск, 2022. 14 с. Библиогр.: с. 13

Излагаются методические рекомендации по подготовке к практическим занятиям по дисциплине «Организационное и правовое обеспечение информационной безопасности».

Методические указания по выполнению практических работ для студентов специальностей и направлений подготовки 10.03.01, 10.05.02 очной формы обучения.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по направлению подготовки «Информационная безопасность» и «Информационная безопасность телекоммуникационных систем».

Текст печатается в авторской редакции

Подписано в печать Формат 60x84 1/16.
Усл. печ. л. . Уч. –изд. л. . Тираж 50 экз. Заказ 1496
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

Практические занятие №1 Организационные источники и каналы утечки информации

Рефераты:

1) Понятие, проблемы и структура экономической безопасность предпринимательской деятельности (на примере фирм различных типов).
2) Классификация информационных ресурсов ограниченного доступа к ним персонала фирмы, характеристика каждой группы.
3) Информационная безопасность, история формирования.

Теоретическая часть:

Каналы распространения информации носят объективный характер, отличаются активностью и включают в себя:

1) деловые, управленческие, торговые, научные и другие коммуникативные регламентированные связи;
2) информационные сети;
3) естественные технические каналы излучения, создания фона. Канал распространения информации представляет собой путь перемещения сведений из одного источника в другой в санкционированном (разрешенном, законном) режиме или в силу объективных закономерностей. Например: обсуждение важного вопроса на закрытом совещании, запись на бумаге содержания изобретения, переговоры с потенциальным партнером, работа на ЭВМ и т.д.

Угрозы сохранности, целостности и конфиденциальности информационных ресурсов ограниченного доступа практически реализуются через риск образования канала несанкционированного получения (добывания) кем-то ценной информации и документов.

Этот канал представляет собой совокупность незащищенных или слабо защищенных фирмой направлений возможной утраты конфиденциальной информации, которые злоумышленник использует для получения необходимых сведений, преднамеренного незаконного доступа к защищаемой информации.

Каждая конкретная фирма обладает своим набором каналов несанкционированного доступа к информации, что зависит от множества

моментов — профиля деятельности, объемов защищаемой информации, профессионального уровня персонала, местоположения здания и т.п.

В отличие от третьего лица злоумышленник или его сообщник целенаправленно охотятся за конкретной информацией и преднамеренно, противоправно устанавливают контакт с источником этой информации или преобразуют канал ее объективного распространения в канал ее разглашения или утечки. Такие каналы всегда являются тайной злоумышленника.

Каналы несанкционированного доступа могут быть двух типов: организационные и технические. Обеспечиваются они легальными и нелегальными методами.

Организационные каналы разглашения информации отличаются большим разнообразием видов и основаны на установлении разнообразных, в том числе законных, взаимоотношений злоумышленника с фирмой или ее сотрудником для последующего несанкционированного доступа к интересующей информации.

Организационные каналы утечки конфиденциальной информации принято классифицировать по следующим признакам:

1) по каналам коммуникации и источникам конфиденциальной информации; по источникам угроз;
2) по времени воздействия и месту их возникновения;
3) по направлениям деятельности организации и характеру конфиденциальной информации;
4) по характеру взаимоотношений с партнерами;
5) по способам и средствам несанкционированного доступа к конфиденциальной информации;
6) по способам, средствам и методам защиты информации от утечки и несанкционированного доступа к ней;
7) по степени формализации каналов утечки и т. д.

Основные организационные каналы утечки и несанкционированного доступа к информации:

1) разглашение информации персоналом организации;
2) разглашение информации при осуществлении сотрудничества с другими организациями, в частности в ходе переговоров, при проведении совещаний, при приеме в организации посетителей;
3) при осуществлении рекламной и публикаторской деятельности.

Практические занятие №2 Технические средства защиты информации

Рефераты:

1) Концепция информационной безопасности.
2) Основы экономической безопасности предпринимательской деятельности.
3) Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

Теоретическая часть:

- ***Технические*** (аппаратные) средства. Это различные по типу устройства (мех анические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защитыинформации. Они либо препятствуют физ ическому проникновению, либо, если проникновение все жесостоялось, дост упу к информации, в том числе с помощью ее маскировки. Первую часть зада чи решаютзамки, решетки на окнах, защитная сигнализация и др.
- Вторую генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств,
  «перекрывающих» потенциальные каналыутечки информации или позволяю щих их обнаружить. Преимущества технических средств связаны с ихнадежн остью, независимостью от субъективных факторов, высокой устойчивостью к модификации.
- Слабыестороны: недостаточная гибкость, относительно большие объем и ма сса, высокая стоимость. Инженерно техническая защита сведений предприятия начинается с ограничения доступа посторонних лиц на территорию путем создания контролируемых зон: периметр здания и близлежащей территории, все здания предприятия, отдельные кабинеты и помещения. Руководитель компании должен создать специальную службу безопасности. Инженерно-техническая группа будет проводить постоянный контроль и охрану всех зон.
  Следующим этапом защиты информации станет закупка и установка технических средств, которые работают с конфиденциальными данными (телефония, разноуровневые системы связи, громкоговоритель, диспетчерская связь, звукозаписывающие и звуковоспроизводящие средства). Обезопасить компанию от воздействия прослушивающих технических средств, найти во всех контролируемых зонах слабые места, в которых злоумышленник сможет добраться до информативных акустических, электрических или магнитных сигналов. Выявить все возможные системы, к которым может быть совершен несанкционированный доступ (несекретная телефонная линия, пожарная или звуковая сигнализация, системы охранной сигнализации, средства наблюдения и другие). Выявленные слабые места по возможности устранить или уменьшить их количество. Определить и разграничить помещения по группам важности и секретности (залы, переговорные помещения, кабинеты). На основе всех собранных данных комиссия, проводящая обследование компании, составляет протокол, по фактам которого формируется акт и утверждается руководителем компании. После проверки должен быть составлен план всего

здания, его помещений, зон контроля. В кабинетах и других помещениях повышенного уровня безопасности производят ТЗИ (некриптографический способ защиты технических каналов от утечки информации)

Практические занятие №3 Защита персональных данных
Рефераты:

1) Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
2) Информационная безопасность (по материалам зарубежных источников литературы).
3) Правовые основы защиты конфиденциальной информации.

Теоретическая часть:

Этапы работ по защите персональных данных

Обязательные (в том числе предварительные) этапы работ по защите персональных данных:

Определить все ситуации, когда требуется проводить обработку персональных данных (ПДн).

Выделить бизнес-процессы, в которых обрабатываются персональные данные.

Выбрать ограниченное число бизнес-процессов для проведения аналитики. На этом этапе формируется перечень подразделений и сотрудников компании, участвующих в обработке ПДн в рамках своей служебной деятельности.

Определить круг информационных систем и совокупность обрабатываемых ПДн.

Провести категорирование ПДн и предварительную классификацию информационных систем (ИС).

Выработать меры по снижению категорий обрабатываемых ПДн.

Сформировать актуальную модель угроз для каждой информационной системы обработки персональных данных (ИСПДн).

Подготовить техническое задание (ТЗ) по созданию требуемой системы защиты.

Провести уточнение классов ИС, с последующей подготовкой рекомендаций по использованию технических средств защиты ПДн.

Подать уведомление о начале обработки персональных данных в Уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) для регистрации в качестве оператора ПДн.

Отправить заявку на получение экземпляров руководящих документов ФСТЭК России по организации системы защиты.

Разработать требования для конкретной ИСПДн, с учетом присвоенного класса защиты.

Подготовить технический проект по защите ИСПДн и помещений.

Разработать пакет организационно-распорядительных документов для СЗПДн (положения, приказы, инструкции, регламенты);

Спроектировать и внедрить систему защиты персональных данных (СЗПДн);

Взять согласия на обработку ПДн с субъектов персональных данных;

Проводить контрольные мероприятия по выявлению нарушений защиты персональных данных.

Проверить при трансграничной передаче находится ли получатель персональных данных в стране, где осуществляется надлежащая защита персональных данных.

Практические занятие №4 Разработка организационно-распорядительной документации для объекта информации

Рефераты:

1) Экономические основы защиты конфиденциальной информации.
2) Организационные основы защиты конфиденциальной информации.
3) Структура, содержание и методика составления перечня сведений, составляющих предпринимательскую тайну.

Теоретическая часть:

Разработка организационно-распорядительной документации для объекта информатизации

Защита информации включает в себя комплекс организационных и технических мер, направленных на обеспечение безопасности свойств информации (конфиденциальность, целостность, доступность). Очевидно, что базисом системы защиты информации являются организационные меры, которые должны быть задокументированы в форме приказов, перечней, регламентов, инструкций, положений, руководств, регламентов, стандартов и т.д. Но и технические меры также предваряются разработкой документации, например: технический паспорт, модель угроз, техническое задание на разработку системы защиты информации, технический проект и т.д.

Разработка организационно-распорядительной и технической документации, отвечающей требованиям безопасности информации, регламентирующей процессы системы защиты информации на всех этапах её существования, сложная и трудоёмкая задача. Во многих организациях или отсутствует документация, или это набор документов — шаблонов, наличие которых не влияет на процессы, связанные с деятельностью по защите информации.
Перечень необходимых документов может меняться в зависимости от специфики объектов информатизации, на которых планируется обрабатывать защищаемую информацию.Первоначально определяются защищаемые объекты, назначаются лица, ответственные за организацию защиты информации, устанавливаются угрозы безопасности защищаемой информации, разрабатывается техническое задание на создание защищённого объекта информатизации. На следующих этапах выполняется проектирование, ввод в действие и сопровождение объекта. На каждом из этапов разрабатывается соответствующая документация: эскизный проект; технический проект; рабочая документация, материалы по аттестации объекта информатизации и т.д.

Практические занятие №5 Анализ эффективности применения средств защиты информации на объекте информатизации

Рефераты:

1) Построение и функционирование защищенного документооборота.
2) Анализ инструкции по обработке и хранению конфиденциальных документов.
3) Направления и методы защиты документов на бумажных носителях.

Теоретическая часть:

Основные организационно-технические мероприятия по защите информации

1. Лицензирование деятельности предприятий в области защиты информации.

2. Аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности.

3. Сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам.

4.Категорирование вооружения и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной, экономической, политической, научно-технической и других сферах деятельности.

5. Обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений.

6. Оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов (перехват информации, подлежащей защите), расположенных на территории России.

7. Введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите.
8. Создание и применение информационных и автоматизированных систем управления в защищенном исполнении.
9. Разработка и внедрение технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи.
10. Разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование.
11. Применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам электросвязи.

Практические занятие №6 Организация внутриобъектового режима
Рефераты:

1) Направления и методы защиты машиночитаемых документов.
2) Направления и методы защиты электронных документов.
3) Архивное хранение конфиденциальных документов.

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

Основными направлениями работы по организации внутриобъектового режима *на предприятии являются:*
определение общих требований режима секретности на предприятии в соответствии с положениями нормативных правовых актов и указаний вышестоящих органов государственной власти организаций); ограничение круга лиц, допускаемых к сведениям, составляющим государственную тайну, и их носителям;регламентация непосредственной работы сотрудников предприятия, а также командированных лиц, с носителями сведений, составляющих государственную тайну;планирование комплекса мероприятий, направленных на исключение утечки сведений, составляющих государственную тайну, и утрат носителей этих сведений; организация контроля со стороны должностных лиц предприятия и структурных подразделений по защите государственной тайны за выполнением требований по режиму секретности на предприятии;организация работы с персоналом предприятия, допущенным к сведениям, составляющим государственную тайну, а также вновь принимаемыми на работу гражданами.

Задачи по организации внутриобъектового режима на предприятии возлагаются, как правило, на заместителя руководителя предприятия,

отвечающего за вопросы защиты государственной тайны. Заместитель руководителя предприятия работу по формированию системы внутриобъектового режима организует на основе всестороннего анализа возможных каналов утечки сведений, составляющих государственную тайну, при проведении предприятием всех видов работ.

В ходе выполнения этой работы руководством предприятия используются следующие основные подходы к организации внутриобъектового режима*:* определение ответственности руководителей подразделений должностных лиц за защиту государственной тайны;четкое разграничение функций, возлагаемых на соответствующие структурные подразделения предприятия (служба безопасности, режимно-секретное подразделение, подразделение противодействия иностранным техническим разведкам, служба охраны и др.);

создание эффективной системы контроля за выполнением мероприятий по режиму секретности и обеспечению сохранности Носителей сведений, составляющих государственную тайну.

Руководитель предприятия и соответствующие должностные лица должны обеспечить соблюдение основных принципов формирования системы внутриобъектового режима: принципа персональной ответственности руководителей структурных подразделений, других должностных лиц и сотрудников предприятия за выполнение задач в области защиты государственной тайны; принципа комплексного использования имеющихся сил и средств для решения задач по защите государственной тайны;принципа полного охвата всех направлений деятельности предприятия, в ходе работы по которым возможна утечка сведений, составляющих государственную тайну, или утрата носителей этих сведений.

Практические занятие №7 Организация пропускного режима

Рефераты:

1) Направления и методы защиты аудио и визуальных документов.
2) Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
3) Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

Теоретическая часть:

Контрольно-пропускной режим (как часть системы безопасности) должен соответствовать действующему законодательству, уставу предприятия, а также иным нормативно-правовым актам, регулирующим деятельность предприятия.

Основными целями создания контрольно-пропускного режима являются:

защита законных интересов предприятия, поддержание порядка внутреннего управления;
защита собственности предприятия, ее рациональное и эффективное использование;
ост прибылей предприятия;
внутренняя и внешняя стабильность предприятия;
защита коммерческих секретов и прав на интеллектуальную собственность.

Контрольно-пропускной режим как часть системы безопасности позволяет решить следующие задачи:
обеспечение санкционированного прохода сотрудников и посетителей, ввоза (вывоза) продукции и материальных ценностей, ритмичной работы предприятия;
предотвращение бесконтрольного проникновения посторонних лиц и транспортных средств на охраняемые территории и в отдельные здания (помещения);
своевременное выявление угроз интересам предприятия, а также потенциально опасных условий, способствующих нанесению предприятию материального и морального ущерба;
создание надежных гарантий поддержания организационной стабильности внешних и внутренних связей предприятия, отработка механизма оперативного реагирования на угрозы и негативные тенденции;
пресечение посягательств на законные интересы предприятия, использование юридических, экономических, организационных, социально-психологических, технических и иных средств для выявления и ослабления источников угроз безопасности предприятия.

Контрольно-пропускной режим можно определить как систему обеспечения нормативных, организационных и материальных гарантий выявления, предупреждения и пресечения посягательств на законные права предприятия, его имущество, интеллектуальную собственность, производственную дисциплину, технологическое лидерство, научные достижения и охраняемую информацию и как совокупность организационноправовых ограничений и правил, устанавливающих порядок пропуска через контрольно-пропускные пункты сотрудников объекта, посетителей, транспорта и материальных ценностей.
Нормативные гарантии заключаются в толковании и реализации норм права, уяснении пределов их действия, в формировании необходимых правоотношений, определении и обеспечении правомерной деятельности подразделений и работников фирмы по поводу ее безопасности, использования ограничительных мер, применения санкций к физическим и юридическим лицам, посягающим на законные интересы фирмы.
Организационные гарантии формируются путем разработки, построения и поддержания высокой работоспособности общей организационной структуры управления процессом выявления и подавления угроз

деятельности фирмы, использования эффективного механизма стимулирования ее оптимального функционирования, соответствующей подготовки кадров.

Практические занятие №8 Разработка модели угроз информационной безопасности

Рефераты:

1) Соотношение источников, каналов распространения и каналов утечки информации.
2) Анализ опыта защиты информации в зарубежных странах.
3) Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

Теоретическая часть:

Модель угроз безопасности информации содержит следующие разделы:

1. Общие положения.
2. Описание информационной системы и особенностей ее функционирования.
2.1. Цель и задачи, решаемые информационной системой.
2.2. Описание структурно-функциональных характеристик информационной системы.
2.3. Описание технологии обработки информации.
3. Возможности нарушителей (модель нарушителя).
3.1. Типы и виды нарушителей.
3.2. Возможные цели и потенциал нарушителей.
3.3. Возможные способы реализации угроз безопасности информации.
4. Актуальные угрозы безопасности информации. Приложения (при необходимости).

Раздел «Общие положения» содержит назначение и область действия документа, информацию о полном наименовании информационной системы, для которой разработана модель угроз безопасности информации, а также информацию об использованных для разработки модели угроз безопасности информации нормативных и методических документах, национальных стандартах. В данный раздел также включается информация об используемых данных и источниках, на основе которых определяются угрозы безопасности информации (документация, исходные тексты программ, опросы персонала, журналы регистрации средств защиты, отчеты об аудите и иные источники).

Раздел «Описание информационной системы и особенностей ее функционирования» содержит общую характеристику информационной системы, описание структурнофункциональных характеристик информационной системы, описание взаимосвязей между сегментами информационной системы, описание взаимосвязей с другими информационными системами и информационнотелекоммуникационными

сетями, описание технологии обработки информации. Также в данном разделе приводятся предположения, касающиеся информационной системы и особенностей ее функционирования (в частности предположения об отсутствии неучтенных беспроводных каналов доступа или динамичность выделения адресов узлам информационной системы, иные предположения). В раздел включаются любые ограничения, касающиеся информационной системы и особенностей ее функционирования.

Раздел «Возможности нарушителей (модель нарушителя)» содержит описание типов, видов, потенциала и мотивации нарушителей, от которых необходимо обеспечить защиту информации в информационной системе, способов реализации угроз безопасности информации. В данный раздел также включаются предположения, касающиеся нарушителей (в частности предположение об отсутствии у нарушителя возможности доступа к оборудованию, сделанному на заказ и применяемому при реализации угрозы, предположение о наличии (отсутствии) сговора между внешними и внутренними нарушителями или иные предположения). В раздел включаются любые ограничения, касающиеся определения нарушителей (в частности исключение администраторов информационной си- стемы или администраторов безопасности из числа потенциальных нарушителей или иные предположения).

Раздел «Актуальные угрозы безопасности информации» содержит описа- ние актуальных угроз безопасности, включающее наименование угрозы безопасности информации, возможности нарушителя по реализации угрозы, используе- мые уязвимости информационной системы, описание способов реализации угрозы безопасности информации, объекты воздействия, возможные результат и по- следствия от реализации угрозы безопасности информации.

Основная учебная литература

1. А. П. Фисун. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие - Курск : ЮЗГУ, 2013 -.Ч. 1 / Минобрнауки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - 150 с. : ил., табл. - Имеется электрон. аналог. - Библиогр.: с. 137-149.
2. А. А. Гребеньков, И. А. Шуклин, Е. О. Ефимова. Организационно-правовые механизмы обеспечения информационной безопасности [Электронный ресурс]: методические рекомендации по подготовке к практическим занятиям для специальности 090900.68 «Информационная безопасность» для студентов всех форм обучения /

Юго-Западный государственный университет, Кафедра теоретической механики и мехатроники ; Курск : ЮЗГУ, 2013. - 28 с.

3. Фисун А.П. Основы правового обеспечения информационной безопасности[Электронный ресурс] : учебное пособие - Курск : ЮЗГУ, 2013 - .Ч. 1 / Минобрнауки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - 149 с. : ил., табл. - Имеется печ. аналог. - Библиогр.: с. 137-149.

4. А. П. Фисун. Основы правового обеспечения информационной безопасности [Электронный ресурс] : учебное пособие - Курск : ЮЗГУ, 2013 - .Ч. 2 / Минобрнауки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - 302 с.

Дополнительная учебная литература

1. Ишейнов В.Я., Мецатуанян М.В. Защита конфиденциальной информации. М.: Форум, 2013. – 256с.
2. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности, – СПб: СПб НИУ ИТМО, 2014. – 173с.
3. Лыньков Л.М., Голиков В.Ф., Борботько Т.В. Основы защиты информациии управления интеллектуальной собственностью [Текст] : учебно-методическое пособие. — Минск: БГУИР, 2013. — 243 с.

4. Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно- правовое и методическое обеспечение информационной безопасности / Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с.