МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ **"РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)"**

Кафедра «Управление и защита информации»

А.А.ПРИВАЛОВ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПРОЕКТИРОВАНИЯ, СОЗДАНИЯ, МОДЕРНИЗАЦИИ ОБЪЕКТОВ ИНФОРМАЦИИ НА БАЗЕ КОМПЬЮТЕРНЫХ СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

Учебно-методическое пособие
для студентов специальности
10.05.01 «Компьютерная безопасность»

Москва – 2018

УДК 004
П-75

Привалов А.А. Обеспечение информационной безопасности, проектирования, создания, модернизации объектов информации на базе компьютерных систем в защищённом исполнении: Учебно-методическое пособие к курсовому проекту. -М.: РУТ (МИИТ), 2018. – 52с.

Данное учебно-методическое пособие призвано помочь студенту при написания практических работ и курсового проекта по дисциплине «Обеспечение информационной безопасности, проектирования, создание, модернизации объектов информации на базе компьютерных систем в защищённом исполнении». Помимо этого, разъясняются, цели, задачи и требования к оформлению практической работы и курсового проекта.

В составлении учебно-методического пособия участвовали студенты группы ТКИ-511: Кудряшов К.А., Юдакин В.А., Трофимов С.С., Соловьев А.И., Хоружевский С.О.

Рецензент: д.т.н., профессор кафедры «Управление и защита информации» РУТ (МИИТ)Алексеев В.М.

Содержание

Перечень сокращений и определений

КП – курсовой проект - работа, которая подразумевает технический анализ какого-то варианта инженерного решения по конкретной теме в течение всего семестра. Также она часто включает экономическую часть, которая показывает эффект внедрения инноваций, предложенных студентом, на предприятие;

ПО – Программное обеспечение - продукт интеллектуальной деятельности, включающий в себя информацию, выраженную через средства поддержки;

ИБ – Информационная безопасность — состояние сохранности информационных ресурсов и защищённости законных прав личности и общества в информационной сфере;

ФЗ – Федеральный закон — закон, установленный федеральными законодательными органами федеративного государства;

РД – Руководящий документ - нормативно-технический документ, устанавливающий нормы, правила, требования организационно-методического и общетехнического характера;

ОС – Операционная система — комплекс программ, обеспечивающий управление аппаратными средствами компьютера, организующий работу с файлами и выполнение прикладных программ, осуществляющий ввод и вывод данных**;**

ФСТЭК –Федеральная служба по техническому и экспортному контролю — федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности**;**

СЗИ –Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации;

СТР-К – Специальные требования и рекомендации по технической защите конфиденциальной информации;

ВТСС – Вспомогательные технические средства и системы. Технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с ТСПИ и находящиеся в зоне, создаваемого ими электромагнитного поля.

Введение

Данное учебно-методическое пособие призвано помочь студенту при написании практической работы и курсового проекта по дисциплине «Обеспечение информационной безопасности, проектирования, создание, модернизации объектов информации на базе компьютерных систем в защищённом исполнении».

Практическая работа –это подробный анализ нормативной документации, относящейся к сфере информационной безопасности и рассматриваемой темы курсового проекта, в частности. В ходе выполнения практической работы, студенту требуется рассмотреть такие базовые материалы, как межгосударственные стандарты качества (ГОСТ), специальные требования и рекомендации по технической защите, федеральные законы, приказы ФСБ и т.д. Российской Федерации.

Курсовой проект - самостоятельная научная работа, в которой должен быть технический проект по заданной теме. Помимо этого, в курсовом проекте обычно присутствует графические элементы, схемы, чертежи и графики. Курсовой проект строго индивидуален для каждого студента и служит для развития не только профессиональных, но и творческих навыков. Как и при выполнении практической работы для создания курсового проекта необходимо использовать научно-техническую литературу и нормативные документы.

Глава I. Практическая работа
Оформление и содержание практической работы

Вне зависимости от темы, практическая работа должна содержать:

1. Титульный лист
2. Содержание
3. Перечень сокращений и аббревиатур
4. Основная часть (документы, связанные с выбранной темой)
5. Заключение (краткое изложение результата проведённого анализа нормативной документации
6. Список использованных материалов (литература или интернет-источники)

При написании практической работы в ПО Word, нужно использовать шрифт – TimesNewRoman, интервал междустрочный должен быть равен 1.5, размер шрифта – 14. Отступы по краям должны быть «обычными», абзацы должны начинаться с «красной» строки (1.5 см).

Оформление практической работы должно производиться согласно ГОСТу 7.32-2017 и должно включать в себя:

1. Введение
2. Главы
3. Заключение;
4. Список литературы;
5. Приложения

Рассмотрим каждый пункт практической работы.

Титульный лист

В титульном листе оформление производится по указанию ГОСТа 7.32-2017 (см. приложение Г). В этом листе указывается название института, тема, которую рассматривает студен, название предмета (дисциплина), ФИО студента, ФИО преподавателя, город и текущий год.

Перечень сокращений и аббревиатур

В перечне сокращений и аббревиатур указываются все технические и юридические сокращения и аббревиатуры с их расшифровкой и их описанием. Предпочтительно указывать все элементы перечня в алфавитном порядке.

Пример

КП – курсовой проект — работа, которая подразумевает технический анализ какого-то варианта инженерного решения по конкретной теме в течение всего семестра. Также она часто включает экономическую часть, которая показывает эффект внедрения инноваций, предложенных студентом, на предприятие;

ПО – Программное обеспечение — продукт интеллектуальной деятельности, включающий в себя информацию, выраженную через средства поддержки;

ИБ – Информационная безопасность — состояние сохранности информационных ресурсов и защищённости законных прав личности и общества в информационной сфере;

ФЗ – Федеральный закон — закон, установленный федеральными законодательными органами федеративного государства.

Содержание

В ***содержании*** указывается сама структура курсового проекта или практической работы (см. приложение Д). Оно должно содержать в обязательном порядке введение, темы, которые студент рассматривает, заключение, список используемых источников и если необходимо использовать дополнительное материалы, например, блок-схемы, код приложения и т.д., то их нужно указать как приложения. (пример в приложении Е)

Главы, посвящённые проверенным документам, связанным с выбранной темой

В главах, посвящённых документам, связанным с выбранной темой, необходимо выделить следующие аспекты:

– Основные положения документов, в которых описаны их функции

– Отношения и понятия, которые закреплены документом/законом РФ

– Определяющий смысл закона

– Сущностные аспекты закона, определяющие политику безопасности конкретной организации и позволяющие дать рекомендации по классификации объектов защиты.

Пример

Функции Закона (Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации")

Основные функции закона:

– регулирование отношений, возникающих при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;

– создание и использование информационных технологий и средств их обеспечения;

– защита информации, прав субъектов, участвующих в информационных процессах и информатизации.

Отношения, регулируемые Законом

Настоящий Федеральный закон регулирует отношения, возникающие при:

–формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;

–создании и использовании информационных технологий и средств их обеспечения;

–защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Закон не затрагивает отношений, регулируемых Законом Российской Федерации "Об авторском праве и смежных правах".

Понятия, закреплённые Законом

Данный закон подробно раскрывает следующие понятия: информация, информатизация, документированная информация (документ), информационные процессы, информационная система, информационные ресурсы, информация о гражданах (персональные данные), конфиденциальная информация, средства обеспечения автоматизированных информационных систем и их технологий, собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения, владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения, пользователь (потребитель) информации.

Определяющий смысл Закона

Законом определяется государственная политика в сфере формирования информационных ресурсов и информатизации, и её направлений. Например: создание и развитие федеральных и региональных информационных систем и сетей (Глава 2), обеспечение их совместимости и взаимодействия в едином информационном пространстве Российской Федерации, формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учётом современного мирового уровня развития информационных технологий (Глава 4), а также развитие законодательства в сфере информационных процессов (Глава 4), информатизации и защиты информации (Глава 5).

Закон определяет и правовой режим информационных ресурсов, который включает в себя: порядок документирования информации, право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных

системах, категорию информации по уровню доступа к ней, порядок правовой защиты информации.

Заключение

В ***заключении***, студент должен дать представление о сути и итогах проделанного анализа без прочтения всего текста, подчеркнув ключевые моменты каждого из документов. Как и введение, заключение не должно превышать не более двух страниц.

Пример

Рассмотренные нормативно-правовые документы необходимы при проведении аттестации СЗИ, в том числе СЗИ-ГТ, согласно требованиям ФСБ РФ. В ходе анализа документации в основополагающем для этого вопроса документе, в приказе ФСБ РФ от 13 ноября 1999 г. N 564 "Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о её знаках соответствия" были найдены некоторые недочёты. Справедливо заметить, что они не умаляют значимость приказа, не мешают его исполнению, однако оставляют недосказанность.

Проведение аттестационных испытаний СЗИ является актуальной мерой обеспечения информационной безопасности.

Список использованных литературы, источников

В ***списке используемых источников***, студент должен перечислить все источники, которые он использовал при

написании практической работы. Предпочтительно алфавитное перечисление источников, но допустимо представление по мере появления текстовых отсылок. Если используются в качестве источников сайты, то их тоже необходимо включить в этот список и дать ссылку на этот сайт.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. «Безопасность корпоративных сетей.» - Шаньгин В.Ф., – СПб.: Спб ГУ ИТМО, 2004. – 161 с.
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
3. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
4. Указ Президента Российской Федерации от 6 марта 1997 г. N 188 "Об утверждении Перечня сведений конфиденциального характера"
5. Постановление Правительства Российской Федерации от 30.04.2002 N 290 "О лицензировании деятельности по технической защите конфиденциальной информации"
6. Руководящий документ. Приказ председателя Гостехкомиссии России от 19 июня 2002 г. N 187 "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий"

Глава II. Курсовой проект

Содержание курсового проекта

Вне зависимости от темы, курсовой проект, выполненный в полной мере, должен включать в себя:

1. Титульный лист;
2. Содержание;
3. Перечень сокращений и определений касающейся только той темы, которую рассматривается;
4. Введение;
5. Актуальность работы;
6. Анализ актуальных нормативных документов;
7. Формулировка проблемы;
8. Рассмотрение объекта в курсовом проекте.
9. Пути решения проблемы, описанной в курсовом проекте;
10. Заключение;
11. Список использованных источников;
12. Приложения

Согласно ГОСТу 7.32-2017 курсовой проект должен содержать:

1. Введение
2. Главы
3. Заключение;
4. Список литературы;
5. Приложения.

Если в курсовом проекте имеются все указанные пункты, то можно утверждать, что студент изучил тему своего проекта, проанализировал разносторонние источники и актуальные документы, и на основании этого сформулировал проблему и пути её решения.

При написания практической работы в ПО Word, нужно использовать шрифт – TimesNewRoman, интервал междустрочный должен быть равен 1.5, размер шрифта – 14. Отступы по краям должны быть «обычными», абзацы должны начинаться с «красной» строки (1.5 см).

Рассмотрим каждый пункт в отдельности.

Титульный лист

В ***титульном листе*** оформление производится по указанию ГОСТа 7.32-2017. В этом листе указывается название института, тема, которую рассматривает студент, название предмета (дисциплина), ФИО студента, ФИО преподавателя, город и текущий год. Пример титульного листа для курсового проекта представлен в приложении Г.

Содержание

В ***содержании*** указывается сама структура курсового проекта или практической работы (см. приложение Д). Оно должно содержать в обязательном порядке введение, темы, которые студент рассматривает, заключение, список используемых источников и если необходимо использовать дополнительное материалы, например, блок-схемы, код приложения и т.д., то их нужно указать как приложения. (пример в приложении Е)

Для того, чтобы оформить так как показано в приложении Д, нужно в ПО Word пакета Microsoft, перейти на вкладку «Ссылки», на левой части этой вкладки в «Оглавлении» нажать на «Оглавление» и выбрать необходимый стиль. После этого на пустой странице появляется пустое «Содержание». Что бы заполнить «Содержание», нужно выделить тему главы курсового проекта или практической работы, перейти на вкладку «Ссылки» в «Оглавлении» находится «Добавить текст», в нём мы выбираем «Уровень 1». После этого

нужно обновить «Содержание», это можно сделать в «Оглавлении» или при выделении содержания, после этого в содержании появляется тема и указывается, автоматически, страница на которой находится выбранная тема. Если тема имеет подпункты, то необходимо выбрать в «Добавить текст» «Уровень 2» и обновить.

Пример

Содержание:

Перечень сокращений и аббревиатур

В перечне сокращений и аббревиатур указываются все технические и юридические сокращения и аббревиатуры с их расшифровкой и их описанием. Предпочтительно указывать все элементы перечня в алфавитном порядке.

Пример

СЗИ – Средства защиты информации

ИБ – Информационная безопасность

ПО – Программное обеспечение

ФСБ – Федеральная служба безопасности

Введение курсового проекта.

В ***введении*** обосновывается выбор, студентом, темы курсового проекта, формируются проблема и круг вопросов, необходимых для её решения. В конце этого раздела определяется цель работы и взаимосвязанный комплекс задач, подлежащих решению для достижения цели работы и раскрытия темы. Размер введения не должен превышать двух страниц.

Пример

ВВЕДЕНИЕ

Одним из инструментов государственной системы обеспечения информационной безопасности является сертификация СЗИ. Сертификация средств защиты информации (СЗИ) - форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Координация работ по организации сертификации средств защиты информации возлагается на межведомственную комиссию по защите государственной тайны. В развитии Закона РФ «О государственной тайне» постановлением Правительства РФ от 26 июня 1995 г. № 608 утверждено Положение о сертификации средств защиты информации. Данное Положение устанавливает общий порядок сертификации средств защиты

информации в Российской Федерации и её учреждениях за рубежом. Согласно положению, средствами защиты информации являются 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. Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ России.

Данная работа рассматривает процесс сертификации и роль ФСБ РФ в нём.

Актуальность работы.

В ***актуальности работы*** приводятся аргументы её актуальности, должна быть дана оценка современного состояния решаемой проблемы. Показана научная новизна темы, связь выполненной работы с другими научно-исследовательскими работами, её практическая значимость.

Актуальность – это важная часть КП, которая помогает студенту раскрыть необходимость изучения выбранной темы. Она должна отвечать на вопросы: «Почему нужно заниматься исследованием это темы?» и «Почему она так важна?». Определить, действительно ли, выбранная тема актуальна, студент должен еще задолго до начала написания курсового проекта. Если выбранная тема не будет актуальной, то и выполнение данного проекта практически не имеет смысла и сил, которые потребуется при написании.

Актуальность КП должна быть подробно обоснована. Студенту необходимо показать, действительно ли, избранная им тема востребована в современном мире. Если же тема КП не представляет ценности, то и её написание не поможет студенту стать лучшим профессионалом на избранном им пути. Чтобы рассмотрение темы актуальности КП пошло на пользу студенту, нужно показать: как это исследование может помочь улучшить существующую ныне ситуацию в той области развития современного общества, которая была бы прямо или косвенно связана с темой экзаменационной работы.

Для того чтобы обоснование актуальности КП прошло успешно, автор должен умело объяснять, чем определяются цели проведения его исследования конкретно в текущий период времени и необходимо обратить внимание на то, в какой мере актуальность темы курсовой связана с:

- состоянием научного развития;
- появлением новейших обучающих методов и иных дополнительных сведений, непосредственно связанных с темой исследования.

Также, следует пояснить:

- насколько связана выбранная тема с выявленными недостатками в ранее проводившихся исследованиях;
- обуславливается ли тема стремлением воспользоваться новейшими методами исследования;
- имеется ли необходимость в проведении данного исследования в связи с изменением экономических условий и пр.

Пример

В настоящее время одной из наиболее актуальных проблем в области информационной безопасности является проблема защиты от утечки конфиденциальной информации. Технические варианты решения данной проблемы, рассмотренные в курсовом проекте, могут быть сгруппированы в два типа. Первый тип предполагает изменение топологии защищаемой АС путём создания изолированной системы обработки конфиденциальной информации, либо выделения в составе АС сегмента терминального доступа к конфиденциальным данным. Второй вариант технических решений заключается в применении различных средств защиты АС, включая средства активного мониторинга, контентного анализа, а также средства криптографической защиты информации. В данном курсовом проекте будут рассмотрены особенности утечки информации в закрытых сетях и основные способы защиты от подобных утечек.

Анализ нормативных документов и средств защиты информации курсового проекта

В ***анализе нормативных документов*** должен быть приведён список использованных нормативных документов вместе с их кратким анализом, раскрывающего область её применения.

В данном разделе курсового проекта рассматривается список нормативной документации, которая относится к рассматриваемой студентом теме курсового проекта. К нормативной документации могут относиться такие базовые материалы, как межгосударственные стандарты качества (ГОСТ), специальные требования и рекомендации по технической защите, федеральные законы, приказы ФСБ и т.д. Российской федерации.

В ходе анализа нормативной документации, требуется рассмотреть основные положения, функции и требования рассматриваемых документов, на которые опирается тема курсового проекта. Кроме этого, необходимо учесть, на какие документы опирается предложенная документация и выделить ключевые аспекты, определяющие политику безопасности конкретной организации и позволяющие дать рекомендации по классификации объектов защиты.

Рекомендуется обратить особое внимание на следующие документы:

- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)

- Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ

- Доктрина информационной безопасности РФ

- ФЗ №149 “Об информации, информационных технологиях и о защите информации”

- Закон РФ "О государственной тайне" от 21.07.1993г. №5485-1 (с изм. и доп., вступающими в силу с 15.12.2007)

- ФЗ РФ "О персональных данных" от 27 июля 2006 г. N 152-ФЗ

- ФЗ РФ "Об электронной подписи" от 6 апреля 2011 г. N 63-ФЗ

- Приказ ФСТЭК №58 от 5.02.2010г. "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных"

- Закон РФ "О безопасности" от 05.03.1992г.№2446-1

- Приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

Пример

Анализ нормативных документов

К защищаемой информации относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Это, как правило, информация ограниченного доступа, содержащая сведения, отнесённые к государственной тайне, а также сведения конфиденциального характера.

Защита информации от утечки в закрытой сети осуществляется на основе Конституции Российской Федерации, а также следующих документов:

Специальные требования и рекомендации по технической защите конфиденциальной информации" (СТР-К) 2001г

Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об

утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 июля 2013 г. № 240/22/2637 РД 50.715–92. Методические указания Госстандарта России. Информационная технология. Защита информации от утечки за счёт ПЭМИН при её обработке средствами вычислительной техники. Порядок организации работ при разработке и изготовлении.

РД 50.716–92. Методические указания Госстандарта России. Информационная технология. Защити информации от утечки за счёт ПЭМИН при её обработке средствами вычислительной техники. Правила разработки, построения, изложения, оформления документов.

ГОСТ Р ИСО/МЭК 8631–94. Информационные технологии. Программные конструктивы и условные обозначения для их представления.

ГОСТ Р 50840–95. Методы оценки качества, разборчивости и узнаваемости.

ГОСТ Р 50922–96. Защита информации. Основные термины и определения.

ГОСТ Р 50972–96. Защита информации. Радиомикрофон. Технические требования к защите от утечки секретной информации.

Средства защиты

В ***средствах защиты информации*** (СЗИ) студент должен проанализировать все виды СЗИ и выбрать ту или иную СЗИ, которая относится к рассматриваемой студентом теме курсового проекта. К разновидностям СЗИ относятся:

1. **Технические средства защиты информации,**

включая средства контроля эффективности принятых мер защиты информации:

1.1. Средства защиты информации от перехвата оптических сигналов (изображений) в видимом, инфракрасном и ультрафиолетовом диапазонах волн.

1.2. Средства защиты информации от перехвата акустических сигналов, распространяющихся в воздушной, водной, твердой средах.

1.3. Средства защиты информации от перехвата электромагнитных сигналов, в том числе от перехвата побочных электромагнитных излучений и наводок (ПЭМИН), возникающих при работе технических средств регистрации, хранения, обработки и документирования информации.

1.4. Средства защиты информации от перехвата электрических сигналов, возникающих в токопроводящих коммуникациях:

- за счёт ПЭМИН при работе технических средств регистрации, хранения, обработки и документирования информации;

- вследствие эффекта электроакустического преобразования сигналов вспомогательными техническими средствами и системами.

1.5. Средства защиты информации от деятельности радиационной разведки по получению сведений за счёт изменения естественного радиационного фона окружающей среды, возникающего при

функционировании объекта защиты.

1.6. Средства защиты информации от деятельности химической разведки по получению сведений за счёт изменения химического состава окружающей среды, возникающего при функционировании объекта защиты.

1.7. Средства защиты информации от возможности получения сведений магнитометрической разведкой за счёт изменения локальной структуры магнитного поля Земли, возникающего вследствие деятельности объекта защиты.

1.8 Технические средства обнаружения и выявления специальных технических средств, предназначенных для негласного получения информации, устанавливаемых в конструкциях зданий и объектов (помещения, транспортные средства), инженерно-технических коммуникациях, интерьере, в бытовой технике, в технических средствах регистрации, хранения, обработки и документирования информации, системах связи и на открытой территории.

2. Технические средства и системы в защищённом исполнении, в том числе:

2.1. Средства скремблирования, маскирования или шифрования телематической информации, передаваемой по каналам связи.

2.2. Аппаратура передачи видеоинформации по оптическому каналу.

В результате рассмотрения вышеприведённых СЗИ и нормативных документов, студент может выбрать ту или иную СЗИ, которая связана с его темой курсового проекта и сформулировать общие рекомендации по защите информации, циркулирующей в помещениях, а также рекомендации по предотвращению утечки информации по изученным каналам.

Основное внимание на предприятии должно быть уделено ЗИ, в отношении которой угрозы реализуются без применения сложных технических средств перехвата, а именно речевой информации, циркулирующей в защищаемых помещениях; информации, выводимой на экраны видеомониторов; информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны.

Пример

Средства защиты от утечки информации

1. Технические средства — электрические, электромеханические, электронные и др. типа устройства. Преимущества технических средств связаны с их надёжностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объём и масса, высокая стоимость. Технические средства подразделяются на:

– аппаратные — устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой локальных сетей по стандартному интерфейсу (схемы контроля информации по чётности, схемы защиты полей памяти по ключу, специальные регистры);

– физические — реализуются в виде автономных устройств и систем (электронно-механическое

оборудование охранной сигнализации и наблюдения. Замки на дверях, решётки на окнах).

2. Программные средства — программы, специально предназначенные для выполнения функций, связанных с защитой информации. А именно программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации наподобие временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надёжность, простота установки, способность к модификации и развитию.

Недостатки— ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

3.Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

4. Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учётом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития.

Недостатки— высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

В ходе развития концепции защиты информации специалисты пришли к выводу, что использование какого-либо одного из выше указанных способов защиты, не обеспечивает надёжного сохранения информации. Необходим комплексный подход к использованию и развитию всех средств и способов защиты информации.

Формирование проблем курсового проекта

В данном пункте студент должен описать проблемы своей темы курсового проекта, на основе анализа источников и нормативных документов.

Пример

Проблема утечки информации

Известно, что до 70–80% утечки информации связаны с действием сотрудников компании, работающих на предприятии, а также уволенными сотрудниками. Практика показывает, что мотивация совершения подобных действий может быть самой различной. С повышением значимости и ценности информации растет и важность её защиты.

Утечка или утрата информации влечёт за собой материальный ущерб. Кроме того, информация – это фактор управления. Несанкционированное вмешательство в управление может привести к катастрофическим последствиям в объекте управления – производстве и транспорте. Если в организации присутствует конфиденциальная информация, то в ней, в первую очередь, должны быть приняты меры по защите информации от различных угроз.

Ущерб от раскрытия конфиденциальной информации может выражаться в потере преимуществ, упущенной коммерческой выгоде, санкциях со стороны органов управления, административной и уголовной ответственности, ухудшении морального климата в коллективе вследствие раскрытия информации о заработной плате работников, о планируемых кадровых перестановках и т.п.

Конфиденциальная информация – это информация, доступ к которой ограничен кругом доверенных пользователей.

Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Защита от утечки конфиденциальной информации – задача достаточно сложная.

Возрастающее использование электронной почты, интернет-пейджеров и других средств передачи данных, распространённость мобильных устройств, с помощью которых сотрудники могут выносить важную информацию за пределы организации – все это значительно осложняет контроль над потоками данных.

Рассмотрение объекта в курсовом проекте.

В этом разделе курсового проекта студент приводит объект, соответствующий выбранной теме КП, который будет рассмотрен в его работе.

Пример объекта, рассматриваемого в КП

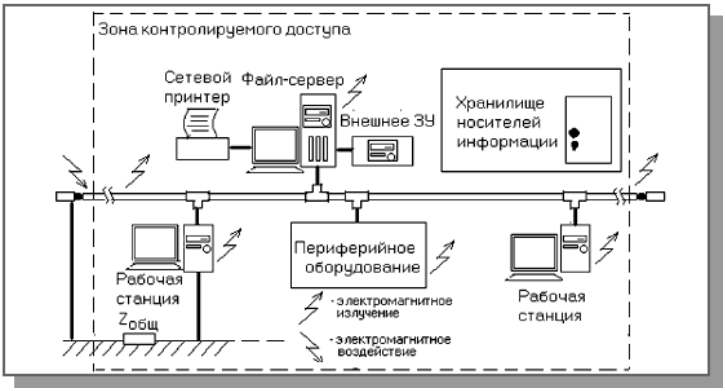

Рисунок 1 – Отдел оценки уязвимости и категорирования

В сети имеется много физических мест и каналов несанкционированного доступа к информации в сети. Каждое устройство в сети является потенциальным источником электромагнитного излучения из-за того, что соответствующие поля, особенно на высоких частотах, экранированы неидеально. Система заземления вместе с кабельной системой и сетью электропитания может служить каналом доступа к информации в сети, в том числе на участках, находящихся вне зоны контролируемого доступа и потому особенно уязвимых. Кроме электромагнитного излучения, потенциальную угрозу представляет бесконтактное электромагнитное воздействие на кабельную систему. Безусловно, в случае использования проводных соединений типа коаксиальных кабелей или витых пар, называемых часто медными кабелями, возможно и непосредственное физическое подключение к кабельной системе. Если пароли для входа в сеть стали известны или подобраны, становится возможным несанкционированный вход в сеть с файл-

сервера или с одной из рабочих станций. Наконец возможна утечка информации по каналам, находящимся вне сети:

– хранилище носителей информации;

– элементы строительных конструкций и окна помещений, которые образуют каналы утечки конфиденциальной информации за счёт так называемого микрофонного эффекта;

– телефонные, радио-, а также иные проводные и беспроводные каналы (в том числе каналы мобильной связи).

Любые дополнительные соединения с другими сегментами или подключение к Интернет порождают новые проблемы. Атаки на локальную сеть через подключение к Интернету для того, чтобы получить доступ к конфиденциальной информации, в последнее время получили широкое распространение, что связано с недостатками встроенной системы защиты информации в протоколах TCP/IP. Сетевые атаки через Интернет могут быть классифицированы следующим образом:

– Сниффер пакетов (sniffer – в данном случае в смысле фильтрация) – прикладная программа, которая использует сетевую карту, работающую в режиме promiscuous (не делающий различия) mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки).

– IP-спуфинг (spoof – обман, мистификация) – происходит, когда хакер, находящийся внутри корпорации или вне её, выдает себя за санкционированного пользователя.

– Отказ в обслуживании (Denial of Service – DoS). Атака DoS делает сеть недоступной для обычного использования за счёт превышения допустимых пределов функционирования сети, операционной системы или приложения.

– Парольные атаки – попытка подбора пароля легального пользователя для входа в сеть.

– Атаки типа Man-in-the-Middle – непосредственный доступ к пакетам, передаваемым по сети.

– Атаки на уровне приложений.

– Сетевая разведка – сбор информации о сети с помощью общедоступных данных и приложений.

– Злоупотребление доверием внутри сети.

– Несанкционированный доступ (НСД), который не может считаться отдельным типом атаки, так как большинство сетевых атак проводятся ради получения несанкционированного доступа.

– Вирусы и приложения типа "троянский конь".

Решения проблем, описанных в курсовом проекте

В этом пункте формируются ответы на поднятые в предыдущем пункте проблемы, помимо этого необходимо дать предложения по поводу того как следует разрешить данные вопросы. Смело рассказать о своих расчётах (для тем по сертификации, обустройству помещений и т.д.), высказать предложения и рекомендации, описать мотивы и показать методы.

Пример

Система предотвращения утечки конфиденциальной информации может включать в себя три основные составляющие.

- Работа с персоналом;

- Основным источником утечки информации является персонал. Человеческий фактор способен свести на нет любые самые изощрённые механизмы безопасности. Основные принципы и правила управления персоналом

определены в международном стандарте ISO/IEC 17799:2000. Соблюдение этих правил позволяет существенно снизить влияние человеческого фактора, избежать характерных ошибок и предотвратить утечку информации;

- Политика безопасности.

Политика безопасности организации – совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.

Основные направления разработки политики безопасности:

– классификация данных по необходимой степени защищённости;

– определение субъекта и размера ущерба, наносимого фирме в информационном аспекте;

– вычисление рисков и определение схемы уменьшения их до приемлемой величины.

- Сервисы безопасности.

Сервисы безопасности используются для ограничения доступа к информации, протоколирования фактов осуществления доступа и контроля информационных потоков. Они позволяют обеспечить предупреждение, предотвращение, обнаружение и реагирование на инциденты, связанные с утечкой информации. К числу сервисов безопасности относятся: сервисы аутентификации, управления доступом, шифрования, и аудита безопасности.

Любой руководитель заинтересован в предотвращении утечки конфиденциальной информации. Прежде чем предпринимать меры по защите конфиденциальной информации, следует определить её ценность и постараться, чтобы затраты на обеспечение её конфиденциальности не превосходили её реальную

стоимость. К основным способам предотвращения потери ценной информации относятся:

–организационные;

–правовые;

–технические.

Основные организационные мероприятия по обеспечению предотвращения утечки информации можно условно разделить на два вида:

–определение концепции кадровой политики и критериев подбора персонала; подбор служащих, текущая работа с постоянными сотрудниками, и их социальная защита;

–реализация мер по определению степени конфиденциальных сведений и обеспечение разграничения доступа: классификация документов по степени важности и конфиденциальности, определение режима их хранения, допуска к ним, учёта.

Организационные меры и мероприятия связаны с управлением предприятием и относятся к таким действиям, которые сводят к минимуму информационную уязвимость предприятия. К компетенции администрации предприятия относится создание оптимальных условий, обеспечивающих безопасность предприятия.

Меры по созданию оптимального режима, обеспечивающие безопасность предприятия, включают следующие действия:

1. организацию пропускного режима на предприятие;
2. организацию соответствующего режима конфиденциальности в соответствии с законодательством; регистрацию сотрудников, включая посетителей, имеющих доступ к конфиденциальной информации;
3. разграничение документации по степени конфиденциальности и разграничение доступа к информации;
4. регулярные профилактические работы с работниками предприятия;

С этой целью на предприятии желательно создать специальную аналитическую группу информационной безопасности, которая будет:

– заниматься определением ценности имеющейся информации;

– изучать клиентов фирмы;

– определять потенциальных конкурентов;

– осуществлять контроль за рекламой, деловыми контактами, следить за конкуренцией и т.п.

Что касается правового аспекта предотвращения потери ценной информации, следует опираться на нормы действующего законодательства и договорные отношения.

Важной основой правовой защиты коммерческой информации является заключение коммерческих договоров и соглашений, включающих вопросы обеспечения конфиденциальности. Технические средства защиты информации даже при их высокой стоимости не гарантируют полную защиту информации без реализации перечисленных выше мер. К техническим средствам защиты информации относятся разнообразные механические, электромеханические, электронные и другие устройства и системы, которые в совокупности с другими средствами способствуют защите информации предприятия.

Технические средства позволяют автоматизировать охрану помещений и снизить возможность утечки информации по другим каналам.

При подборе технических средств защиты следует исходить из разумных соображений и возможностей предпринимателя. Прежде всего, необходимо предусмотреть:

–физическую изоляцию территорий, зданий, помещений;

–оборудование окон решётками, установку специальных дверей;

–оснащение их датчиками систем охранной сигнализации;

–выделение специализированных помещений для техники;

–защиту носителей информации и аппаратуры от похищения;

–регламентацию технологических процессов;

–разработку инструкций для персонала;

–применение специальных технических средств, исключающих прослушивание и перехват информации;

контроль и проверку средств защиты.

Заключение

При написании заключения КП важно не только его содержание, но и вывод о проделанной работе. Для того, чтобы данный раздел получился полным и информативным, необходимо его структурировать, соблюдая следующий порядок:

- Нужно ответить на вопрос: «Были ли достигнуты цели и выполнены задачи, поставленные во введении, в ходе исследования?».

- Нужно написать общий вывод по каждой главе основной части проекта. Для этого нужно еще раз прочесть все выводы, представленные в основном разделе, обобщить их и правильно структурировать.

- В заключительном разделе нужно писать вывод не только по теории, но и по практической части исследования. Здесь можно представить результаты расчётов и рассказать об используемых в ходе выполнения работы методах.

- Автор должен рассказать о своем отношении к теме, обосновать её актуальность, пояснить, с какими трудностями он столкнулся в ходе работы над темой. Результат этого пункта должен быть интересным и познавательным.

Проверяющий должен убедиться, что студент подошел к выполнению исследования с интересом и энтузиазмом.

Обычно этот раздел следует начинать с фраз:

- Результаты проведённой работы показали, что…;
- В заключении, нужно отметить, что…;
- Выполнив курсовой проект, я пришел к выводу, что….

После того, как труд над заключительным разделом закончен, необходимо еще раз его прочитать, чтобы исключить все подробные определения. Они могут быть представлены в основном разделе, а информация, представленная в заключении, должна быть краткой и ясно. Объем «Заключения» не долен превышать двух-трех страниц.

Пример

ЗАКЛЮЧЕНИЕ

Подходя к вопросу сертификации, заказчик должен:

1. Знать законодательство, регулирующее вопросы сертификации.
2. Определиться с тем, какую сертификацию ему нужно провести для устройства.
3. Собрать, подготовить и подать все необходимые документы.
4. Подготовить материальные средства на получение сертификатов.

В данном курсовом проекте рассмотрен процесс сертификации и роль ФСБ РФ в нём. Подробно рассмотрены вопросы Сертификация СЗИ-ГТ, Организационная структура сертификации СЗИ-ГТ, Порядок проведения сертификации и инспекционного

контроля, а также Требования к нормативным и методическим документам по сертификации СЗИ-ГТ.

В первой части работы раскрывается актуальность сертификации по требованиям ФСБ РФ в наше время, подробно излагаются нормативные требования. Во второй части работы представлена модель предприятия, использующего в качестве объекта сертификации МЭ и VPN-шлюз. Произведены обоснованная подборка устройств, расчёт их стоимости, а также рассмотрены варианты получения сертификатов на их использование, в зависимости от обрабатываемой информации.

Список использованных источников

В ***списке используемых источников***, студент должен перечислить все источники, которые он использовал при написании КП. Предпочтительно алфавитное перечисление источников, но допустимо представление по мере появления текстовых отсылок. Если используются в качестве источников сайты, то их тоже необходимо включить в этот список и дать ссылку на этот сайт.

Пример

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. «Семь безопасных информационных технологий» - Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. – М.: ДМК Пресс, 2017. – 224 с.: ил.
2. Доктрина информационной безопасности РФ. Утверждена Указом Президента РФ от 5 декабря 2016 г. N 646 10.
3. Закон РФ от 21 июля 1993 г. N 5485-I "О государственной тайне"

4. Постановление Правительства РФ от 26 июня 1995 г. N 608 "О сертификации средств защиты информации"
5. Приказ ФСБ РФ от 13 ноября 1999 г. N 564 "Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о её знаках соответствия"
6. КоАП РФ, Статья 13.6.

Приложение

В приложении размещает различные графические, табличные и другие материалы, на которые ссылается студент в ходе написания курсового проекта.

ПРИЛОЖЕНИЕ А

Рекомендуемый перечень тем, к рассмотрению в практической работе и в курсовом проекте.

1. Особенности обеспечения информационной безопасности микропроцессорных систем управления;
2. Сертификация средств защиты информации по требованиям ФСБ;
3. Особенности обеспечения информационной безопасности защищённых помещений;
4. Особенности утечки информации по ПЭМИН;
5. Особенности обеспечения информационной безопасности объектов вычислительной техники;
6. Особенности утечки информации по закрытому каналу связи (Intranet);
7. Сертификация средств защиты информации по требованиям ФСТЭК;
8. Утечки информации по виброакустическому каналу;
9. Особенности утечки информации по открытому каналу Ethernet;
10. Особенности обеспечения информационной безопасности на транспортных средствах;
11. Особенности обеспечения информационной безопасности телекоммуникационных сетей с использованием мобильной связи;
12. Особенности обеспечения информационной безопасности с использованием автоматической идентификации объектов при помощи технологии RFID

ПРИЛОЖЕНИЕ Б

Перечень основных вопросов к зачету.

1) Основные каналы утечки информации.
2) Возможные каналы утечки на объекте информатизации.
3) Особенности утечки информации.
4) Характеристика технических каналов утечки информации.
5) Уязвимости основных структурно-функциональных элементов распределенных автоматизированных систем.
6) Виды мер противодействия угрозам безопасности.
7) Основные положения нормативно-методических документов ФСТЭК РФ.
8) Правовые основания контроля.
9) Взломы по политическим мотивам.
10) Основные методы защиты информации от утечки по техническим каналам.
11) Некоторые аспекты использования криптографических средств.
12) Системы оценки защищённости.
13) Исследование компьютерной техники и носителей информации.
14) Алгоритм расследования инцидентов.
15) Организация и проведение поисковых работ.
16) Методика принятия управленческого решения на организацию защиты от утечки информации по техническим каналам.
17) Технические средства защиты и организация основных видов работ по защите информации.
18) Технические средства, применяемые при ведении поиска закладочных устройств.
19) Автоматизированные программно-аппаратные комплексы радиомониторинга.
20) Мошенничество с использованием сети Интернет.
21) Обнаружение и устранение уязвимостей, возможности сканеров безопасности.

ПРИЛОЖЕНИЕ В

Перечень основных вопросов к экзамену.

1. Определение объекта информатизации.
2. Цели создания системы обеспечения информационной безопасности.
3. Особенности технических каналов утечки.
4. Правовые основы обеспечения защиты информации.
5. Государственная система защиты информации.
6. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты информации.
7. Сертификация по требованиям ФСТЭК.
8. Сертификация по требованиям ФСБ.
9. Существующие средства защиты информации от несанкционированного доступа.
10. Возможности применения штатных средств защиты информации от несанкционированного доступа.
11. Возможности применения дополнительных средств защиты информации от несанкционированного доступа.
12. Классификация уязвимостей по уровню в инфраструктуре автоматизированной системы сетей.
13. Классификация атак на объекте информатизации.
14. Классификация компьютерных атак по целям.
15. Классификация компьютерных атак по местонахождению.
16. Атака SYNflood.
17. Атака «ARP-Spoofing».
18. Источники возникновения уязвимостей.
19. Основные защитные механизмы межсетевых экранов.
20. Анализ содержимого почтового и WEB трафика.
21. Виртуальные частные сети (их виды, решения на базе ОС Windows2003).
22. Аудит информационной безопасности (перечислить методы аудита).
23. Мониторинг событий безопасности.

ПРИЛОЖЕНИЕ Г
Примеры титульных листов для практической работы и курсового проекта.

Пример 1. Титульный лист практической работы.

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский университет транспорта (МИИТ)"

Институт транспортной техники и систем управления

Практическая работа на тему:

«Особенности утечки информации по техническим каналам»

По дисциплине:

«Обеспечение информационной безопасности, проектирования, создание, модернизации объектов информации на базе компьютерных систем в защищённом исполнении»

Выполнил: Студент группы ТКИ-511
Кудряшов К. А.

Проверил:

К.т.н. Привалов Александр Андреевич

Москва 2018

Пример 2. Титульный лист курсового проекта.

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский университет транспорта (МИИТ)"

Институт транспортной техники и систем управления

Курсовой проект на тему:

«Особенности утечки информации по техническим каналам»

по дисциплине:

«Обеспечение информационной безопасности, проектирования, создание, модернизации объектов информации на базе компьютерных систем в защищённом исполнении»

Выполнил: Студент группы ТКИ-511
Иванов В.В.

Проверил:

К.т.н. Привалов Александр Андреевич

Москва 2018

ПРИЛОЖЕНИЕ Д
Пример оформления содержания курсового проекта и практической работы.

Пример 1. Содержание курсового проекта.

Содержание:

Пример 2. Содержание практической работы.

Содержание:

ПРИЛОЖЕНИЕ Е

Рекомендуемый образец заявки на сертификацию средства защиты информации или на продление срока действия сертификата соответствия

Федеральная служба по техническому и
экспортному контролю

ЗАЯВКА

на_____

(сертификацию средства защиты информации, продление срока действия сертификата соответствия)

Наименование средства защиты информации: _____

Назначение средства защиты информации: _____

степень секретности защищаемой информации, категория объекта информатизации, тип и класс защищённости информационной (автоматизированной) системы

Заявитель: _____

организационно-правовая форма и наименование

Адрес местонахождения _____

заявителя: _____

Почтовый адрес заявителя: _____

Лицензии ФСТЭК России, имеющиеся у заявителя: _____

номера и даты выдачи лицензий

Ф.И.О. руководителя заявителя: _____

Ф.И.О. лица, ответственного за сертификацию средства защиты информации: _____

Контактный телефон (телефоны) заявителя: _____

Адрес электронной почты заявителя: _____

Разработчик (разработчики) средства защиты информации (при наличии разработчика средства защиты информации): _____

наименование, адрес местонахождения

Лицензии ФСТЭК России, имеющиеся у разработчика (разработчиков) средства _____

защиты информации:

номера и даты выдачи лицензий

Правообладатель (правообладатели) средства защиты информации (при наличии правообладателя (правообладателей) средства защиты информации):

наименование лица (лиц), обладающего (обладающих) исключительными правами на средство защиты информации, адрес его (их) местонахождения

Испытательная лаборатория:

наименование, адрес местонахождения

Тип средства защиты информации:

наименование типа (наименования типов) средства защиты информации

Требования по

безопасности информации:	
	наименования документов, на соответствие которым планируется проводить сертификацию средства защиты информации
Схема сертификации средства защиты информации:	
Заявляемый срок действия сертификата соответствия	
Место проведения сертификационных испытаний:	
	адрес места (адреса мест) проведения сертификационных испытаний, наименование лица, на материально-технической базе которого планируется проводить сертификационные испытания средства защиты информации
Приложение	1. Документы, прилагаемые к заявке 2. Опись прилагаемых к заявке документов

Должность руководителя заявителя (лица, которое в силу закона или учредительных документов выступает от его имени)

М.П. (при наличии)

подпись

инициалы, фамилия

"__" _____ 20__ г.

Должность руководителя испытательной лаборатории (при наличии)

М.П. (при наличии)

подпись

инициалы, фамилия

"__" _____ 20__ г.

Учебно-методическое издание

Привалов Александр Андреевич

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПРОЕКТИРОВАНИЯ, СОЗДАНИЯ, МОДЕРНИЗАЦИИ ОБЪЕКТОВ ИНФОРМАЦИИ НА БАЗЕ КОМПЬЮТЕРНЫХ СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

Учебно-методическое пособие
к курсовому проекту

Тираж 50 экз.
Изд.№ 130-18

Москва, Копировальный центр PrintSide