Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Томский государственный университет систем управления
и радиоэлектроники»

Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

И.А. Рахманенко

Управление средствами защиты информации

Методические указания
по выполнению курсовой работы
для студентов специальностей 10.03.01, 10.05.02, 10.05.03

Томск 2019

Введение

Методические указания предназначены для студентов специальностей 10.03.01, 10.05.02, 10.05.03, выполняющих курсовую работу по дисциплине «Управление средствами защиты информации».

1. Общие требования к курсовым работам

Курсовая работа - это самостоятельная научно-методическая работа студента, выполняемая под непосредственным руководством преподавателя по специальной дисциплине. Главной своей целью преследуемой при выполнении курсовой работы является развитие у студентов навыков самостоятельной исследовательской работы.

Выполнение курсовой работы должно способствовать углубленному знаний полученных из лекционного курса и лабораторных работ предыдущего семестра и приобретению навыков самостоятельной работы.

Темы курсовых работ рекомендуются кафедрой и приведены ниже. Студент в праве взять другую тему, которая должна соответствовать дисциплине управление средствами защиты информации. Тема курсовой работы должна быть согласована с преподавателем и одобрена им. Рекомендуется выбор тема курсовой работы проводить с расчетом на использования результатов курсовой работы при написании дипломной работы.

Студент совместно с руководителем составляют техническое задание, в котором формулируется круг вопросов подлежащих изучению, и ставятся задачи, которые должны быть решены в ходе выполнения курсовой работы. На этом же этапе составляется минимальный список необходимой литературы, программного и программного-аппаратного обеспечения и других материалов (руководства к программным и программно-аппаратным продуктам, список сайтов фирм производителей, форумы технической поддержки).

Структура курсовой работы должна способствовать раскрытию избранной темы и отдельных ее вопросов. В ней основная часть содержит только главы (в основном три) без их разбивки на параграфы (подразделы). Все части курсовой работы должны быть изложены в строгой логической последовательности и взаимосвязи. Содержание работы следует иллюстрировать схемами, таблицами, диаграммами, графиками, фотографиями, рисунками и т. д. Графическому материалу по тексту необходимо давать пояснения.

Курсовая работа проверяется руководителем работы, который выставляет оценку на титульном листе работы. При оценке работы учитываются содержание работы, ее актуаль-

ность, степень самостоятельности, оригинальность выводов и предложений, качество используемого материала, а также уровень грамотности (общий и специальный).

2. Тематика курсовых работ

Основной темой курсовых работ по дисциплине “Управление средствами защиты информации” является тема **“Администрирование и управление СЗИ от НСД Secret Net”**. Совместно с руководителем возможен выбор другой темы курсовой работы, однако необходимым является условие применения в рамках курсовой работы средства защиты от несанкционированного доступа в локальной сети с применением выданных преподавателем виртуальных машин. Кроме того, при выполнении курсовой работы необходимо учитывать требования, определенные в задании по варианту.

3. Структура курсовой работы

Курсовая работа должна содержать техническое задание, утвержденное руководителем.

Структура пояснительной записки должна состоит из введения, теоретической части, основной части, заключения.

Во введении описывается проблематика задачи, которая должна быть решена в ходе выполнения работ, актуальность данного вопроса.

В теоретической части дается обзор круга проблем связанных с задачей курсовой работы. Рассматриваются методы, используемые при решении проблем. Предлагается метод решения проблемы сформулированной в техническом задании. Приводится обоснование выбора метода.

В основной части подробно описывается ход выполнения работы. Приводятся все расчеты, схемы, алгоритмы, которые были выполнены и использовались в данном проекте. Окончательный результат работы должен быть сформулирован в основной части в полной мере и должен логически вытекать из поставленной в технической части задачи и описанного хода выполнения работы.

В заключении констатируется результат, полученный в ходе выполнения курсовой работы и полно сформулированного в основной части. Указываются области

применения полученных решений и прогнозируются перспективы развития данной тематики.

4. Исходные данные для курсовой работы

Исходными данными для курсовой работы являются средства защиты информации от несанкционированного доступа отечественных и зарубежных производителей; техническая документация, руководства для программистов и разработчиков предоставляемые производителями программных и программно-аппаратных средств защиты информации. Теоретические знания и практические навыки, полученные и усвоенными студентами по таким дисциплинам как безопасность операционных систем, программно-аппаратные средства защиты информации, управление средствами защиты информации. Результаты научных исследований проводимых сотрудниками кафедры и опубликованных в научной печати. Также исходными данными для выполнения курсовых работ могут являться результаты курсовых и дипломных работ выполненных в предшествующие годы студентами кафедры.

При подготовке курсовой работы необходимо использовать ОС ТУСУР 01-2013: “Работы студенческие по направлениям подготовки и специальностям технического профиля. Общие требования и правила оформления”. Кроме того, рекомендуется активное использование документации и поисковых систем с целью решения задач, появляющихся в ходе выполнения курсовой работы.

Рассмотрим задание, которое необходимо выполнить в рамках выполнения курсовой работы:

1. В соответствии с вариантом, определить информацию, обрабатываемую в автоматизированных системах организации. Конкретизировать область деятельности организации. Определить угрозы, а также информацию, нуждающуюся в защите, круг лиц, имеющих право на работу с этой информацией.
2. Определить нормативные документы, регулирующие обработку и защиту информации определенной категории. Зафиксировать требования по защите информации в соответствии с данными нормативными документами.
3. Объединить виртуальные машины (серверную и клиентскую) в домен.
4. Скачать демо-версию СЗИ от НСД Secret Net Studio (https://www.securitycode.ru/products/demo-versions/) и требуемую документацию.

5. Произвести установку серверной и клиентских частей Secret Net Studio на виртуальные машины.

6. Произвести установку ПО, использующегося для обработки данных или ведения деятельности согласно индивидуальному заданию.

7. Произвести настройку подсистем Secret Net Studio в соответствии с вариантом (создать каталоги и файлы на виртуальных машинах, которые бы соответствовали данной информации). Сюда входит настройка, а также объяснение причин, в соответствии с которыми были настроены данные подсистемы:

- Политик Secret Net Studio.
- Разграничение доступа к устройствам.
- Задание мандатного или дискреционного метода управления доступом (необходимо определить и пояснить какой метод управления доступом требуется согласно индивидуальному заданию).
- Настройка замкнутой программной среды.
- Настройка контроля целостности данных.
- Настройка затирания данных.
- Настройка контроля печати.

8. Подготовить пояснительную записку, содержащую описание выполненных работ, а также выводы по всей работе.

Следует отметить, что во время выполнения практической части курсовой работы рекомендуется сохранять состояние виртуальных машин, чтобы избежать возможных проблем с потерей работоспособности создаваемых студентом автоматизированных систем.

Список вариантов

1. Дана информационная система обработки персональных данных, касающихся расовой и национальной принадлежности граждан, в объеме менее 100 тыс. субъектов без учета сотрудников. Для системы актуальны угрозы 3-го типа.
2. Дана государственная информационная система регионального уровня, обрабатывающая информацию, не составляющую государственную тайну, разглашение которой может привести к умеренным негативным последствиям в социальной или экономической области деятельности.
3. Удостоверяющий центр.
4. Банковская организация.
5. Дана автоматизированная система управления технологическими процессами (АСУ ТП). В случае нарушения целостности информации, обрабатываемой в данной системе, возможно возникновение чрезвычайной ситуации межрегионального характера.
6. Организация, ведущая деятельность по разработке и продаже программно-аппаратных средств шифрования данных.
7. Интернет-провайдер.
8. Дана автоматизированная система управления технологическими процессами (АСУ ТП). В случае нарушения конфиденциальности информации, обрабатываемой в данной системе, возможны умеренные негативные последствия в экономической области деятельности.
9. Дана государственная информационная система федерального уровня, обрабатывающая информацию, не составляющую государственную тайну, разглашение которой может привести к существенным негативным последствиям.
10. Дана информационная система обработки персональных данных, касающихся расовой и национальной принадлежности граждан, в объеме более 100 тыс. субъектов без учета сотрудников. Для системы актуальны угрозы 3-го типа.
11. Организация, занимающаяся обеспечением электроснабжения, относящаяся к объектам критической информационной инфраструктуры. Нарушение к потере электроэнергии в нескольких районах города федерального значения.
12. Организация, ведущая деятельность по разработке и продаже средств антивирусной защиты.

13. Дана информационная система обработки персональных данных, в объеме более 100 тыс. субъектов без учета сотрудников. Для системы актуальны угрозы 3-го типа.

14. Организация, занимающаяся разработкой систем контроля и управления доступом в помещения и видеонаблюдения, систем пожарной сигнализации.

15. Поликлиника.

16. В организации используется государственная информационная система объектового уровня, обрабатывающая информацию, не составляющую государственную тайну, информация имеет минимальный уровень значимости.

17. В организации используется автоматизированная система управления технологическими процессами (АСУ ТП). В случае нарушения конфиденциальности информации, обрабатываемой в данной системе, возможны умеренные негативные последствия в экономической области деятельности.

18. Оператор услуг платежной инфраструктуры социально значимых платежных систем, относящийся к объектам критической информационной инфраструктуры. Нарушение работоспособности оператора приведет к проблемам с 20 млн. операций в день.

19. Промышленное предприятие, относящееся к объектам критической информационной инфраструктуры. Нарушение работоспособности информационных систем может привести к повышению уровня выбросов вредных загрязняющих веществ на территории г. Томска и Томской области.

20. В организации используется информационная система, обрабатывающая без использования СКЗИ персональные данные субъектов, не являющихся работниками организации, в объеме менее 100 тыс. субъектов. К обрабатываемым персональным данным относят фотографии и отпечатки пальцев пользователей. Для системы актуальны угрозы, связанные с наличием недекларированных возможностей в прикладном программном обеспечении, используемом в информационной системе.