ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Вычислительные системы и информационная безопасность»

Методические указания

к курсовому проекту
по дисциплине

«Проектирование комплексной системы защиты информации»

Автор
Цветкова О.Л.

Ростов-на-Дону, 2017

Аннотация

Методические указания предназначены для студентов очной формы обучения направления 10.03.01.

Автор

доцент, к.т.н.,
доцент кафедры «Вычислительные системы и информационная безопасность»
Цветкова О.Л.

Оглавление

ВВЕДЕНИЕ

В настоящее время информация является одним из важнейших факторов эффективного управления деятельностью любого предприятия. Она приобрела ощутимый стоимостный вес, который четко определяется размерами ущерба, с разной степенью вероятности наносимого владельцу информации. Для снижения возможности причинения ущерба информационным ресурсам до приемлемого минимума необходимо серьезно заниматься таким понятием как информационная безопасность.

Многие предприятия в процессе работы обрабатывают большие объемы конфиденциальных сведений, в том числе персональные данные сотрудников, партнеров, клиентов, защита которых обязательна по требованиям законодательства.

Жесткая конкуренция на рынке приводит к тому, что конфиденциальная информация, которой обладает предприятие, может дать значительное конкурентное преимущество.

Комплексная система защиты информации (КСЗИ) позволит обеспечить бесперебойное функционирование сервисов, предотвратить прямые материальные потери от утечки или утраты конфиденциальной информации, а также предотвратить возможный ущерб репутации компании.

Для того чтобы определить целесообразность создания КСЗИ, зону и глубину ее охвата следует провести анализ предприятия, включающий:

— анализ деятельности предприятия;

— выявление конфиденциальной информации и защищаемых ресурсов;

— анализ угроз, уязвимостей и потенциального ущерба от реализации угрозы.

На основе полученной информации о деятельности предприятия и уязвимых местах в действующей системе защиты необходимо сформулировать техническое задание на проектирование КСЗИ.

Исходя из технического задания, следует определить практические меры для его реализации. Совокупность этих мер составит проект внедрения КСЗИ.

1. ТЕМАТИКА КУРСОВОГО ПРОЕКТИРОВАНИЯ

Цель курсового проекта: систематизация и закрепление знаний, полученных при изучении дисциплины, выработка комплексного подхода и развитие навыков к самостоятельной работе при построении комплексных систем защиты информации.

Задачи курсового проектирования:

— изучение особенностей конкретной предметной области, относящихся к теме курсового проекта;

— анализ возможных подходов и методов решения задачи построения комплексной системы защиты информации и обоснование выбранного подхода;

— выработка навыков анализа деятельности и информационных ресурсов предприятия, построения схематических планов предприятия;

— получение практического опыта по формированию требований к комплексной системе защиты информации на основе анализа возможных угроз информационной безопасности и каналов утечки информации.

Основным результатом курсового проектирования является разработанный комплекс мероприятий обеспечения информационной безопасности на объекте защиты предприятия. В качестве объекта защиты может выступать:

— информационная система предприятия (совокупность базы данных предприятия, программы-оболочки, используемой для работы с ней, серверов, на которых расположена база, АРМ пользователей, коммуникационное оборудование, линии связи, дополнительное оборудование (принтеры, сканеры и т.п.).);

— локальная (ЛВС) или корпоративная вычислительная сеть;

— система электронного документооборота.

2. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ПОЯСНИТЕЛЬНОЙ ЗАПИСКИ И ГРАФИЧЕСКОЙ ЧАСТИ КУРСОВОГО ПРОЕКТА

Курсовой проект состоит из следующих документов:

— пояснительная записка (ПЗ);

— графическая часть (плакаты).

Объем **пояснительной записки курсового проекта** определяется трудоемкостью его выполнения (рекомендуется в пределах 30 печатных страниц).

Объем **графической части курсового проекта** 3 листа формата А1. Графическая часть курсового проекта наглядно показывает выполненную работу и помогает кратко изложить ее основные положения.

На плакатную часть графического материала проекта можно вынести:

— основные формулы, полученные в процессе теоретических исследований;

— экспериментально измеренные и теоретически рассчитанные графики и диаграммы;

— рисунки, поясняющие те или иные аспекты функционирования объекта исследований.

Правила обозначения текстовых и графических документов:

YYYY. XXZZFF. RRR W

— **УУУУ** — заглавные буквы, соответствующие наименованию дисциплины (не более четырех) — **МСПС**;

— **XX** — последние цифры номера зачетной книжки студента;

— **ZZFF** — 0000;

— **RRR** — 000.

— **W**:

– курсовой проект (работа) КП(Р);

– пояснительная записка ПЗ;

– ведомость курсового проекта (работы) ВК;

– плакаты Д.

К курсовому проекту составляется **отзыв руководителя**.

Пояснительная записка и графическая часть курсового проекта должны быть оформлены в соответствии с требованиями, приведенными в документе «№ 227 Правила ВКР(НОВЫЕ 2016)».

3. ИНДИВИДУАЛЬНЫЕ ВАРИАНТЫ

1. Администрация района города
2. Отделение полиции
3. Производственное предприятие (завод)
4. Радиостанция
5. Авиакомпания, осуществляющая грузовые перевозки
6. Супермаркет
7. Оптовая база
8. Рекламное агентство
9. Адвокатская контора
10. Книжное издательство (Издательский дом)
11. Агентство недвижимости
12. Агентство дизайна интерьеров
13. Салон красоты
14. Спортивный комплекс (фитнес-клуб, бассейн)
15. Компания занимается оказанием логистических услуг (таксопарк, автотранспортное предприятие)
16. Компания занимается учебной деятельностью (школа, ВУЗ)
17. Компания занимается производством мебели
18. Компания является туроператором
19. Компания занимается оказанием услуг в сфере здравоохранения
20. Компания разрабатывает средства защиты информации
21. Компания занимается изготовлением полиграфической продукции
22. Компания оказывает услуги по инкассации торговых объектов
23. Компания занимается разработкой и сопровождением отраслевого программного обеспечения
24. Компания занимается кинопрокатом фильмов
25. Компания осуществляет подключение к сети Интернет и IP телефонии
26. Компания занимается разработкой и администрированием веб-сайтов
27. Компания занимается бронированием гостиниц по России
28. Компания занимается бронированием и доставкой железнодорожных и авиабилетов
29. Компания занимается локализацией программных продуктов
30. Гостиница
31. Дворец культуры
32. Театр
33. Цирк
34. Ресторан
35. Музей

4. СТРУКТУРА ПОЯСНИТЕЛЬНОЙ ЗАПИСКИ КУРСОВОГО ПРОЕКТА

Титульный лист (оформляется на бланке)
Задание на курсовой проект (оформляется на бланке)
СОДЕРЖАНИЕ
ВВЕДЕНИЕ
1 Анализ объекта защиты
1.1 Анализ деятельности предприятия
1.2 Описание территориального расположения и анализ технической оснащенности предприятия
1.3 Анализ информационных ресурсов и потоков предприятия
2 Анализ уровня информационной безопасности предприятия
2.1 Анализ угроз информационной безопасности и каналов утечки информации
2.2 Построение модели потенциального нарушителя информационной безопасности
2.3 Оценка фактического уровня информационной безопасности предприятия
3 Составление технического задания на разработку комплексной системы защиты информации
3.1 Построение схемы причинно-следственных связей
3.2 Разработка требований к комплексной системе защиты информации
ЗАКЛЮЧЕНИЕ
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ
ВЕДОМОСТЬ КУРСОВОГО ПРОЕКТА (оформляется на бланке)
ПРИЛОЖЕНИЕ (если имеется в наличии)

5. ПОРЯДОК ВЫПОЛНЕНИЯ ПУНКТОВ КУРСОВОГО ПРОЕКТА

Примечание. Для построения всех требуемых схем студенты могут использовать любое подходящее свободно распространяемое программное обеспечение.

1 Анализ объекта защиты

1.1 Анализ деятельности предприятия

1. Сформулируйте цели и задачи предприятия, указанного в индивидуальном задании. Опишите основные показатели деятельности предприятия, характеризующие его масштабы (5—6 показателей), и приведите их числовые значения за какой-то период.

2. Постройте схему иерархической структуры предприятия (штат сотрудников с указанием структуры подчинения).

3. Кратко (2—4 стр.) сформулируйте должностные инструкции сотрудников, составляющих штат предприятия.

4. Постройте схему организационной структуры предприятия (совокупность подразделений (отделов) предприятия). Опишите назначение и функции каждого подразделения.

5. Опишите график работы предприятия и его отдельных подразделений. Сформулируйте правила доступа на предприятие, в отдельные помещения и к оборудованию персонала и посетителей (регулярный, случайный, ограниченный доступ).

1.2 Описание территориального расположения и анализ технической оснащенности предприятия

1. Выполните описание территориального расположения предприятия.

2. Постройте схематический план территории предприятия с указанием расположения всех зданий, подземных сооружений; коммуникаций и мест их выхода за территорию объекта; ограждений по периметру территории объекта; существующих средств защиты.

3. Постройте поэтажные планы с указанием расположения всех помещений, с обозначением дверных и оконных проемов, внутренних и наружных (пожарных) лестниц, толщины материала стен и существующих средств защиты; коммуникаций с обозначением коммуникационных шкафов и других мест санкционированного доступа к каналам связи и жизнеобеспечения.

4. Постройте планы помещений с указанием их функционального назначения; мест размещения оборудования, технических средств (телефонов, персональных ЭВМ, принтеров и т.д.); расположения коммуникаций и мест размещения коммутационного оборудования (коробки, розетки и т.п.); особенностей технологического процесса (для производственных помещений), важных с точки зрения обеспечения безопасности.

5. Составьте технический паспорт предприятия (заполните таблицу табл. 1).

Таблица 1 — Технический паспорт объекта защиты

Этаж (этажей в многоэтажном здании)	
Наличие хранилищ бумажных документов	Количество Расположение
Наличие комнат с неконтролируемым доступом	Количество Расположение

Порядок доступа в помещения	Правила сдачи комнат под охрану, их расположение
Состав технических средств	
Количество и технические характеристики серверов	Тип: — процессора; — материнской платы; — ОС. Объем: — ОЗУ; — жесткого диска.
Количество и характеристики АРМ	Тип: — процессора; — материнской платы; — ОС; — монитора. Объем: — ОЗУ; — жесткого диска.
Количество коммутаторов ЛВС	Пропускная способность Количество портов
Выход в Internet	
Тип подключения	Dial-Up/ADSL/коммутированный канал/Wi-Fi Скорость передачи
Коммуникационное оборудование	Тип Характеристики
Коммуникационное ПО	Шлюз, сетевой экран
Характеристика ПО	
Тип ПО	Перечень ПО Сетевое (да/нет) Количество мест
Дополнительное ПО	
Наименование	Назначение Сетевое (да/нет)
Дополнительное оборудование	
Факсы	Количество
Внутренняя АТС	Количество
Телефоны	Количество

1.3 Анализ информационных ресурсов и потоков предприятия

1. Выполните определение уровней важности конфиденциальной информации на предприятии. Заполните табл. 2.

Таблица 2 — Пример определения уровней важности конфиденциальной информации на предприятии

Уровень важности	Описание
Базовый (Б)	
Средний (С)	
Повышенный (П)	

2. В результате анализа деятельности предприятия, сферы деятельности каждого отдела, и должностных обязанностей сотрудников составьте табл. 3, содержащую список информационных ресурсов предприятия.

Таблица 3 — Информационные ресурсы предприятия

Информационный ресурс	Общедоступная информация / Информация ограниченного доступа	Уровень важности конфиденциальной информации	Сотрудники каких подразделений допущены к информации	В каких помещениях предприятия обрабатывается (хранится) информация	На каких носителях распространяется (хранится) информация

3. Постройте схемы внутренних и внешних информационных потоков, проходящих через отделы предприятия, используя одну из методологий: диаграммы IDEF0, диаграммы потоков данных DFD или язык моделирования UML.

2 Анализ уровня информационной безопасности предприятия

2.1 Анализ угроз информационной безопасности и каналов утечки информации

1. Проведите анализ и составьте перечень возможных угроз информационной безопасности предприятия.

2. Проведите анализ и составьте перечень возможных каналов утечки информации на предприятии.

2.2 Построение модели потенциального нарушителя информационной безопасности

1. Постройте модель потенциального нарушителя информационной безопасности предприятия.

2.3 Оценка фактического уровня информационной безопасности предприятия

1. Выполните оценку фактического уровня информационной безопасности предприятия (опишите реализованную на предприятии систему защиты информации).

2. Сделайте выводы о том, какие угрозы и каналы утечки перекрыты существующей системой безопасности предприятия, а какие нет.

3 Составление технического задания на разработку комплексной системы защиты информации

3.1 Построение схемы причинно-следственных связей

1. Объедините результаты, полученные при анализе возможных угроз, каналов утечки информации, характеристик потенциальных нарушителей и, используя MS Visio, постройте схему причинно-следственных связей, отражающую влияние различных факторов на информационную безопасность предприятия.

3.2 Разработка требований к комплексной системе защиты информации

1. На основе результатов, полученных при выполнении предыдущих пунктов, сформулируйте требования, предъявляемые к проектируемой комплексной системе

защиты информации.

2. Проведите аргументированный выбор состава комплексной системы защиты информации, который обеспечит требуемый уровень информационной безопасности предприятия.

3. Постройте схематические планы предприятия (территории, зданий, помещений) с указанием расположения элементов разрабатываемой системы защиты информации.

6. СОДЕРЖАНИЕ ГРАФИЧЕСКОЙ ЧАСТИ КУРСОВОГО ПРОЕКТА

Возможные варианты содержания графической части курсового проекта:

1. Схема иерархической (и/или организационной) структуры предприятия.
2. Схемы внутренних и внешних информационных потоков, проходящих через отделы предприятия (с указанием уровня важности информации).
3. Перечень возможных угроз информационной безопасности, каналов утечки информации, модель потенциального нарушителя (в виде схем, диаграмм или таблиц).
4. Схема причинно-следственных связей, отражающая влияние различных факторов (угроз, каналов утечки информации, возможных нарушителей) на информационную безопасность предприятия.
5. Схематические планы предприятия (территории, зданий, помещений) с указанием размещения технических средств обработки информации, рабочих мест сотрудников предприятия, линий электроснабжения, связи и т.п. Дополнительно, на этом же плане, необходимо указать направления воздействия угроз безопасности информации.
6. Схематический план размещения средств защиты, составляющих разрабатываемую комплексную систему защиты информации предприятия.

7. ГОСУДАРСТВЕННЫЕ СТАНДАРТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»
2. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
3. Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»
4. ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»
5. ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»
6. ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности»
7. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»
8. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
9. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»
10. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий»
11. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер»
12. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети»
13. ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности»
14. ГОСТ Р ИСО/МЭК 15026-2002 «Информационная технология. Уровни целостности систем и программных средств»
15. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»
16. ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»

17. ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки»
18. ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца»
19. ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица»
20. ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза»
21. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»
22. ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»
23. ГОСТ Р 51725.6-2002 «Каталогизация продукции для федеральных государственных нужд. Сети телекоммуникационные и базы данных. Требования информационной безопасности»
24. ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты»
25. ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения»
26. ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»
27. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»
28. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
29. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хеширования»

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Галатенко В.А. Стандарты информационной безопасности: справ. пособие / В.А. Галатенко. — М.: Интернет-университет информационных технологий, 2006. — 328 с.
2. Грибунин В.Г. Комплексная система защиты информации на предприятии: учебное пособие для вузов / В.Г. Грибунин, В.В. Чудовский. — М.: Издательский центр «Академия», 2009. — 416 с.
3. Попов Л.И., Зубарев А.В. Основные принципы повышения эффективности реализации мероприятий по комплексной защите информации. — М.: «Альтпресс», 2009. — 512 с.
4. Корнеев И.К. Защита информации в офисе: учебник — М.: Изд-во «Проспект», 2008. — 336 с.
5. Мельников. Информационная безопасность и защита информации — М.: Academia, 2007.
6. Шелупанов А.А. Технические средства и методы защиты информации: учебник для вузов. — М.: ООО «Издательство Машиностроение», 2009. — 508 с.
7. Алексеенко В.Н., Соколовский Б.В. Система защиты коммерческих объектов. Технические средства защиты. Практическое пособие для предпринимателей и руководителей служб безопасности. М., 2008.
8. Барсуков В.С. Особенности обеспечения информационной безопасности. — М.: ТЭК, 2006.
9. Герасименко В.А., Малюк А.А. Основы защиты информации М: ООО «Инком-бук», 2005. — 537 с.
10. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: Издательство «ДиаСофт», 2008.
11. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие. — М.: Логос; ПБЮЛ Н.А. Егоров, 2010.
12. Домарев В.В. Защита информации и безопасность компьютерных систем / В.В. Домарев. — К.: Издательство «ДиаСофт»,2009.
13. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. — М.: Горячая линия Телеком, 2009.
14. Камарович В.А. Адаптивная защита сетей в условиях информационного противоборства. К.: Издательство «ДиаСофт», 2008.
15. Каторин Ю.Ф., Куренков Е.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. — СПб.: ООО «Издательство Полигон», 2009.
16. Малюк А.А. Информационная безопасность: концептуальные и методические основы защиты информации. Учеб. пособие для вузов. — М: Горячая линия-Телеком, 2010. — 280 с.
17. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. — М.Ж Горячая линия-Телеком, 2010.
18. Прокофьев И.В. Защита информации в информационных системах. — М.: «Европейский центр по качеству», 2009.