МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Гусев П.Ю.

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Разработка и эксплуатация автоматизированных систем в защищенном исполнении»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /Разинкин К.А./

Заведующий кафедрой Систем информационной безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ / Остапенко А.Г./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цель дисциплины сформировать у студентов, будущих специалистов систему знаний и умений в области разработки и эксплуатации автоматизированных систем, реализующих информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

1.2. Задачи освоения дисциплины

рассмотрение теоретических основ автоматизированных (информационных) систем в защищенном исполнении;

усвоение порядка установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях при эксплуатации автоматизированных (информационных) систем в защищенном исполнении;

изучение основных методов организации и проведения технического обслуживания автоматизированных (информационных) систем в защищенном исполнении

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» направлен на формирование следующих компетенций:

ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-14 - Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-6	знать методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации
	уметь проектировать защищенные

	автоматизированные системы с учетом действующих нормативных и методических документов
ОПК-14	знать критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем
	обнаруживать и устранять нарушения правил разграничения доступа в автоматизированных системах; определять источники и причины возникновения инцидентов безопасности в автоматизированных системах контролировать события безопасности и действия пользователей автоматизированных систем; контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем; документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» составляет 7 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		10
Аудиторные занятия (всего)	108	108
В том числе:		
Лекции	36	36
Лабораторные работы (ЛР)	72	72
Самостоятельная работа	108	108
Курсовой проект	+	+
Часы на контроль	36	36
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 252 7	 252 7

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Разработка защищенных автоматизированных (информационных) систем	Основы информационных систем как объекта защиты. Жизненный цикл автоматизированных систем. Угрозы безопасности информации в автоматизированных системах. Основные меры защиты информации в автоматизированных системах. Содержание и порядок эксплуатации АС в защищенном исполнении. Защита информации в распределенных автоматизированных системах. Особенности разработки информационных систем персональных данных.	18	36	54	108
2	Эксплуатация защищенных автоматизированных систем	Особенности эксплуатации автоматизированных систем в защищенном исполнении. Администрирование автоматизированных систем. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении. Защита от несанкционированного доступа к информации. СЗИ от НСД. Эксплуатация средств защиты информации в компьютерных сетях. Документация на защищаемую автоматизированную систему.	18	36	54	108
		Итого	**36**	**72**	**108**	**216**

5.2 Перечень лабораторных работ

1. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании).
2. Разработка технического задания на проектирование автоматизированной системы.
3. Категорирование информационных ресурсов.
4. Анализ угроз безопасности информации.
5. Построение модели угроз
6. Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.
7. Установка и настройка СЗИ от НСД
8. Защита входа в систему (идентификация и аутентификация пользователей)
9. Разграничение доступа к устройствам
10. Управление доступом
11. Использование принтеров для печати конфиденциальных документов. Контроль печати
12. Настройка системы для задач аудита
13. Настройка контроля целостности и замкнутой программной среды
14. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовых проектов в 10 семестрах для очной формы обучения.

Примерная тематика курсового проекта .

1. Разработка предложений по защите конфиденциальной речевой информации от съѐма с волоконно-оптических линий связи.
2. Разработка программно-аппаратного комплекса по изучению характеристик и методов маскирования речевых сигналов.
3. Разработка предложений по выбору технических средств системы контроля и управления доступом для защиты информации предприятия.
4. Разработка предложений по инженерно-технической защите информации предприятия с распределенной территориальной структурой.
5. Разработка предложений по защите данных в PLC-сетях.
6. Разработка метода защиты графических изображений от встраивания вредоносной информации стеганографическими средствами.
7. Разработка методики защиты персональных данных на предприятии и ее реализация.
8. Разработка методики анализа защищенности СУБД систем электронного документооборота от SQL-инъекций.
9. Разработка демонстрационной модели волоконного акустооптического технического канала утечки информации.
10. Разработка анализатора настроек безопасности узлов локальной сети.
11. Разработка метода низкоуровневого контроля целостности системных файлов.
12. Разработка способа защиты информации для доступа в компьютерную систему от утечки по оптическому каналу.
13. Построение системы контроля физического доступа посторонних лиц с помощью средств охранного телевидения.
14. Разработка модуля обнаружения вредоносного программного обеспечения в сетевом трафике по сигнатурам.
15. Разработка способа обнаружения и противодействия атакам типа ARP-spoofing.
16. Разработка предложений по использованию протоколов обеспечения анонимности абонентов связи в компьютерных сетях.
17. Разработка модели резервного комплекса для управления банком в кризисных ситуациях.
18. Разработка утилиты обфускации программ, написанных на скриптовых языках.

19. Разработка метода и программного средства деобфускации обфусцированных программ.

20. Разработка предложений по защите корпоративной сети на основе межсетевого экранирования.

21. Разработка предложений по проведению аудита информационной безопасности информационно-вычислительных систем организаций финансово-кредитной сферы.

22. Разработка предложений по защите мультимедийной продукции от несанкционированного копирования.

23. Разработка модуля оценки соответствия балансировщика нагрузки BIG-IP требованиям безопасности.

24. Разработка механизмов защиты информационного портала для органов государственной власти.

25. Автоматизация исследований защищенности объекта информатизации от утечки по каналам акустоэлектрических преобразователей.

26. Организация спецпроверок защищаемого помещения с использованием нелинейных радиолокаторов.

27. Разработка предложений по организации защиты конфиденциальных переговоров в необорудованном помещении.

28. Анализ способов оценки защищенности автоматизированных систем в соответствии с документами ФСТЭК России.

29. Сравнительный анализ протоколов, используемых для построения защищенных (частных) виртуальных сетей (VPN).

30. Моделирование защищенных (частных) виртуальных сетей с помощью программы Cisco Packet Tracer.

31. Сравнительный анализ систем обнаружения и предотвращения компьютерных атак.

32. Моделирование процессов межсетевого экранирования локальной вычислительной сети с помощью программы Cisco Packet Tracer.

33. Оценка защищенности межсетевых экранов в соответствии с документами ФСТЭК России.

34. Анализ угроз атак на клиентов в автоматизированных системах и методов противодействия им.

35. Моделирование процессов защиты в локальной вычислительной сети организации с внешним доступом в сеть Интернет.

36. Разработка предложений по противодействию деструктивным информационным воздействиям в социальных сетях.

37. Разработка предложений по контент-анализу данных социальных сетей.

38. Разработка многополосной шкалы для анализа тональности текстов в задачах информационной безопасности. Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-6	знать методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации	знание методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь проектировать защищенные автоматизированные системы с учетом действующих нормативных и методических документов	умение проектировать защищенные автоматизированные системы с учетом действующих нормативных и методических документов	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-14	знать критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем	знание критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь обнаруживать и устранять нарушения правил разграничения доступа в автоматизированных системах; определять источники и причины возникновения инцидентов безопасности в автоматизированных системах контролировать события безопасности и действия пользователей автоматизированных систем; контролировать эффективность принятых мер по	умение обнаруживать и устранять нарушения правил разграничения доступа в автоматизированных системах; определять источники и причины возникновения инцидентов безопасности в автоматизированных системах контролировать события безопасности и действия пользователей автоматизированных систем; контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем; документировать процедуры и результаты	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	реализации политик безопасности информации автоматизированных систем; документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы	контроля функционирования системы защиты информации автоматизированной системы		

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 10 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-6	знать методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь проектировать защищенные автоматизированные системы с учетом действующих нормативных и методических документов	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-14	знать критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	обнаруживать и устранять нарушения правил разграничения	Решение стандартных практических задач	Задачи решены в полном объеме и получены	Продемонстрирован верный ход решения всех,	Продемонстрирован верный ход решения в большинстве	Задачи не решены

	доступа в автоматизированных системах; определять источники и причины возникновения инцидентов безопасности в автоматизированных системах контролировать события безопасности и действия пользователей автоматизированных систем; контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем; документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы		верные ответы	но не получен верный ответ во всех задачах	задач	

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. На какой стадии создания системы защиты информации АС создается частное техническое задание на СЗИ?

стадия классификации АС
предпроектная стадия +
стадия проектирования
стадия ввода в действие

2. На какой стадии создания системы защиты информации АС определяется перечень сведений конфиденциального характера, подлежащих защите от утечки по техническим каналам?

стадия классификации АС
предпроектная стадия +
стадия проектирования
стадия ввода в действие

3. На какой стадии создания системы защиты информации АС опреде-

ляется класс защищенности АС?

стадия классификации АС
предпроектная стадия +
стадия проектирования
стадия ввода в действие

4.На какой стадии создания системы защиты информации АС выполняется разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями?

стадия классификации АС
предпроектная стадия
стадия проектирования +
стадия ввода в действие

5.На какой стадии создания системы защиты информации АС производится закупка сертифицированных технических, программных и программно-технических средств защиты информации и их установка?

стадия классификации АС
предпроектная стадия
стадия проектирования +
стадия ввода в действие

6.На какой стадии создания системы защиты информации АС происходит организация охраны и физической защиты помещений объекта информатизации?

стадия классификации АС
предпроектная стадия
стадия проектирования +
стадия ввода в действие

7.На какой стадии создания системы защиты информации АС происходит опытная эксплуатация средств защиты информации?

стадия классификации АС
предпроектная стадия
стадия проектирования
стадия ввода в действие +

8.На какой стадии создания системы защиты информации АС происходит аттестация объекта информатизации по требованиям безопасности информации?

стадия классификации АС
предпроектная стадия
стадия проектирования
стадия ввода в действие +

9.На какой стадии создания системы защиты информации на АС проводятся приемо-сдаточные испытания средств защиты информации?

стадия классификации АС

предпроектная стадия

стадия проектирования

стадия ввода в действие +

10. В случае формирования конфиденциальных документов с помощью информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть:

учтены в специальных журналах

отформатированы после обработки

открыты на запись

закрыты на запись +

11. При использовании Flash-Bios в автоматизированных рабочих местах на базе автономных ПЭВМ необходимо обеспечить:

форматирование Flash-Bios после обработки

открытие Flash-Bios на запись

доступность информации, записанной на Flash-Bios

целостность информации, записанной на Flash-Bios +

12. В случае обеспечения безопасности в локальных вычислительных сетях средства защиты должны использоваться:

во всех узлах сети, где обрабатывается конфиденциальная информация

во всех узлах сети, независимо от того, обрабатывают они конфиденциальную информацию или нет +

на серверах сети

на пользовательских ЭВМ

13. Выберите правильное утверждение. Состав пользователей ЛВС ...

должен быть неизменным

должен утверждаться администратором безопасности ЛВС

должен утверждаться руководителем организации +

может изменяться, а все изменения регистрироваться +

14.Каждый пользователь ЛВС должен иметь:

свой съемный накопитель информации

права доступа, позволяющие настраивать антивирусную защиту

права доступа, позволяющие настраивать свое рабочее место

уникальный идентификатор и пароль +

15. При построении сети и конфигурировании коммуникационного оборудования рекомендуется учитывать:

количество пользователей сети

разделение трафика по производственной основе +

расположение межсетевых экранов

разделение трафика по видам деятельности предприятия +

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Выберите правильную последовательность уровней защиты информационной системы:

Пользовательский -Сетевой -Локальный -Технологический -Физический

Пользовательский -Технологический -Физический-Сетевой -Локальный

Локальный -Технологический -Физический -Пользовательский -Сетевой

2. Для чего создаются информационные системы?

получения определенных информационных услуг

обработки информации

все ответы правильные

3. Какие трудности возникают в информационных системах при конфиденциальности?

сведения о технических каналах утечки информации являются закрытыми

на пути пользовательской криптографии стоят многочисленные технические проблемы

все ответы правильные

4. Основными источниками внутренних отказов информационных систем являются:

ошибки при конфигурировании системы

отказы программного или аппаратного обеспечения

выход системы из штатного режима эксплуатации

5. Наиболее распространены угрозы информационной безопасности корпоративной

информационной системы:

Покупка нелицензионного ПО

Ошибки эксплуатации и неумышленного изменения режима работы системы

Сознательного внедрения сетевых вирусов

6. Утечкой информации в информационной системе называется ситуация, характеризуемая:

Потерей данных в системе

1580436089

32

Изменением формы информации

Изменением содержания информации

7. Угроза информационной системе (компьютерной сети) – это:

Вероятное событие

Детерминированное (всегда определенное) событие

Событие, происходящее периодически

8. Политика безопасности в информационной системе (сети) – это комплекс:

Руководств, требований обеспечения необходимого уровня безопасности

Инструкций, алгоритмов поведения пользователя в сети

Нормы информационного права, соблюдаемые в сети

9. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она:

с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с

другой — ее наличие и функционирование не создает информационных угроз для элементов самой

системы и внешней среды

с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с

другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой

информации

способна противостоять только информационным угрозам, как внешним так и внутренним

способна противостоять только внешним информационным угрозам

10. Документ, определивший важнейшие сервисы безопасности и предложивший метод

классификации информационных систем по требованиям безопасности:

рекомендации X.800

Оранжевая книга

Закон «Об информации, информационных технологиях и о защите информации»

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)

1. Рассмотреть компоненты информационной системы: база данных (БД); схема базы данных; система управления базой данных (СУБД); приложения; пользователи; технические средства.
2. Найти информацию, характеризующую назначение и область применения заданного вида информационных систем.
3. Определить, к какому классу относится заданный вид информационных систем (по характеру использования информации, по сфере применения, по способу организации, по уровню и масштабу решаемых задач).
4. Составить общее описание заданного вида информационных систем.
5. Найти описание нескольких (не менее двух) современных информационных систем, относящихся к заданному виду.

6. Сформулировать краткое описание назначения и функциональных возможностей каждой из информационных систем по отдельности. Указать на характеристики и свойства, которые являются общими для всех рассматриваемых ИС.
7. Составить таблицу отличий между информационными системами. Указать на их индивидуальные особенности, различающиеся количественные и качественные характеристики.
8. Разработать пример возможного применения одной из информационных систем в деятельности некоторого объекта автоматизации (предприятия или организации). Вид деятельности объекта автоматизации выбирается самостоятельно.
9. Составить документ-обоснование для внедрения информационной системы. Описать, чего позволит достичь внедрение информационной системы с точки зрения повышения эффективности работы объекта автоматизации (организации, предприятия).

2.Для создания пояснительной записки использовать MS Word, а для создания схем и диаграмм рекомендуется использовать MS Visio.

1. Ознакомиться с примером технического задания для разработки какой-либо автоматизированной системы (АС), изучить основные типовые его разделы, ГОСТ 34.602-89
2. Необходимо для себя ответить на следующие вопросы: 1). на основании каких документов разрабатывается методическое и информационное обеспечение системы (нормативные и другие документы); 2). перечень исходных данных: - какие массивы данных используются и в каких форматах; - на каких носителях эти данные будут поставляться в систему; 3). перечень выходных данных: - какие массивы данных будут являться результатом работы ПС; - какие документы будут представлены пользователю и в каком виде (указывается вид носителя) и с какой периодичностью; - какие требования по целостности данных и их защите должны быть выполнены в проектируемой системе.
3. Используя пример и ГОСТ в пояснительной записке технического задания сформировать и описать раздел «Характеристика объекта управления»
4. Сформировать и описать раздел «Назначение АС»
5. Сформировать и описать раздел «Основные требования к АС»
6. Сформировать и описать раздел «Технико-экономические показатели АС»
7. Сформировать и описать раздел «Состав, содержание и организация работ по созданию АС»
8. Сформировать и описать раздел «Порядок приемки АС»

Результаты зафиксировать в отчете.

3. **Изучите предложенную классификацию мировых информационных ресурсов:**

Государственные (национальные) информационные ресурсы Государственные информационные ресурсы - информационные ресурсы, полученные и оплаченные из федерального бюджета.	1)федеральные ресурсы; 2) информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов РФ: • библиотечная сеть России; • архивный фонд Российской Федерации; • государственная система статистики; • государственная система научно-технической информации 3) информационные ресурсы субъектов РФ.
Информационные ресурсы организаций и предприятий Информационные ресурсы предприятий – информационные ресурсы, созданные или накопленные в организациях и на предприятиях.	• центры-генераторы; • центры распределения; • информационные агентства; • базы данных.
Персональные информационные ресурсы Персональные информационные ресурсы – информационные ресурсы, созданные и управляемые каким-либо человеком и содержащие данные, относящиеся к его личной деятельности.	

Определите вид следующих информационных ресурсов в соответствии с данной классификацией:

1. http://portal.gersen.ru
2. http://school-coUection.edu.ru
3. http://fcior.edu.ru
4. http://e-lib.gasu.ru
5. http://books.ifmo.ru
6. http://window.edu.ru
7. http://ivanurgant.com/
8. http://www.schwarzenegger.com/
9. http://zim-angel.ucoz.ru/
10. http://www.educom.ru/ru/works/

Задание №2

Раскройте суть основных параметров информационного ресурса:

№	Параметр информационного ресурса	Характеристика параметра
1.	Содержание	
2.	Охват	
3.	Время получения	
4.	Источник	
5.	Качество информации	
6.	Соответствие потребностям	
7.	Способ фиксации	
8.	Язык	
9.	Стоимость	

Задание №3

Создайте презентацию «Параметры информационных ресурсов» и представьте результаты работы преподавателю.

Результаты зафиксировать в отчете.

4.Задание Анализ угроз безопасности информации

Задание (оформить в виде отчета):

В соответствии с:

1. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.
2. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.
3. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России.
4. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России.
5. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России.

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы

Приоритет	**Виды угроз**	**Субъекты угроз**			
		Стихия	**Нарушитель**	**Злоумышленник**	
				На территории	**Вне территории**
1	Травмы и гибель людей	+	+	+	+
2	Повреждение оборудования, техники	+	+	+	+
3	Повреждение систем жизнеобеспечения	+	+	+	+
4	Несанкционированное изменение технологического процесса		+	+	
5	Использование нерегламентированных технических и программных средств		+	+	
6	Дезорганизация функционирования предприятия	+		+	
7	Хищение материальных ценностей			+	
8	Уничтожение или перехват данных путем хищения носителей информации			+	
9	Устное разглашение конфиденциальной информации		+		
10	Несанкционированный съем информации			+	+
11	Нарушение правил эксплуатации средств защиты		+	+	

Результаты зафиксировать в отчете.

5. Построение модели угроз

1. Получить у преподавателя описание ИС (Приложение).
2. Для данной ИС построить модель угроз и уязвимостей:

выделить угрозы, применимые к рассматриваемой ИС;
выделить уязвимости, через которые могут быть реализованы угрозы;
определить угрозы, которые могут воздействовать на каждый из ресурсов в рамках ИС, и обосновать причины наличия этих угроз;
определить уязвимости, через которые могут быть реализованы указанные угрозы.

Содержание отчета

1. Формулировка задачи.
2. Описание построенной модели угроз и уязвимостей.

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для решения прикладных задач

1. Общие вопросы технической защиты информации. Понятие информация, конфиденциальная информация, злоумышленник.
2. Цели защиты информации
3. Разделение мер защиты информации *по* способам осуществления. Опишите каждую из перечисленных Вами мер.
4. Базовые организационные меры *по* защите информации
5. Техническая защита информацию. Объекты технической защиты информации
6. Основные принципы, которым должна удовлетворять система защиты информации с позиции системного подхода.
7. Концептуальные основы защиты информации
8. Доктрина информационной безопасности
9. Законодательные и иные правовые акты в области технической защиты информации
10. Государственные органы в области защиты информации
11. ФСТЭК России
12. Основные задачи ФСТЭК России
13. Общий порядок лицензирования
14. Лицензирование деятельности в области технической защиты информации
15. Контроль за соблюдением лицензионных требований и условий
16. Общий порядок сертификации средств защиты информации
17. Функции федерального органа по сертификации
18. Процедура сертификации
19. Основные схемы проведения сертификации средств защиты информации

20. Порядок сертификации во ФСТЭК России
21. Заключение договора с испытательной лабораторией
22. Аттестация объектов информатизации
23. Структура системы аттестации
24. Функции ФСТЭК в рамках системы аттестации
25. Документы и данные, которые предоставляет заявитель органу по аттестации для проведения испытаний
26. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации
27. Протокол аттестационных испытаний
28. Аттестат соответствия
29. Структура, источники сигнала технического канала утечки информации
30. Классификация технических каналов утечки информации (ТКУИ).
31. Классификация акустических каналов УИ.
32. Показатели и свойства акустических волн. Достоинства и недостатки акустических каналов.
33. Прямой акустический и акустовибрационный КУИ.
34. Структура прямого акустического и акустовибрационного каналов. ФЭ в прямом акустическом канале. Используемые технические средства. Средства противодействия перехвату по каналам.
35. Акустоэлектрический и акусторадиоэлектронный КУИ.
36. Структура каналов. ФЭ в каналах. Используемые технические средства. Средства противодействия перехвату по каналам.
37. Акустопараметрический и акустооптический КУИ.
38. Структура каналов. ФЭ в каналах. Используемые технические средства. Средства противодействия перехвату по каналам.
39. Анализ образования каналов утечки информации на примерах бытовой техники, оргтехники и систем жизнеобеспечения.
40. Изучение технических средств обнаружения и подавления утечки информации по параметрическому каналу
41. Изучение технических средств обнаружения утечки информации по акустооптическому каналу.
42. Классификация электрических каналов УИ.
43. Классификация электрических каналов утечки информации. Причины возникновения утечки информации по электрическим каналам.
44. Канал утечки информации по телефонной линии.
45. Контактные способы подключения. Бесконтактные способы подключения.
46. Способы перехвата речевой информации из телефонной линии. Предотвращение утечки информации по телефонной линии. Методы выявления утечки информации по телефонной линии.
47. Каналы утечки информации по цепям электропитания и заземления.
48. Предотвращение утечки информации по цепям электропитания и заземления. Средства контроля цепей для предотвращения утечки информации.

49. Изучение принципа работы скремблеров.

50. Изучение принципа работы устройств выявления утечки информации по телефонной линии.

51. Классификация оптических КУИ.

52. Визуально-оптический канал. Фототелеканалы. Канал инфракрасного излучения. Волоконнооптический канал. Системы обнаружения оптических устройств.

53. Классификация электромагнитных КУИ.

54. Назначение ЭМВ. Достоинства перехвата по радиоканалу. Классификация радиоканалов утечки информации.

55. Способы перехвата сигналов. Защита от перехвата.

56. Перехват сигналов связных радиостанций. Перехват радиотелефонных сигналов. Радиомаяки. Радиозакладки. Методы и средства предотвращения утечки информации по радиотехническим каналам. Методы и средства контроля утечки информации по радиоканалам.

57. Источники электромагнитных излучений и наводок.

58. Причины появления и разновидности электромагнитных излучений и наводок. Источники электромагнитных излучений. Классификация источников электромагнитных излучений и наводок.

59. Использование различных эффектов.

60. Использование эффектов паразитных связей. Использование эффектов электромагнитных наводок.

Использование эффектов для образования случайных антенн.

61. Методы защиты информации от утечки через ПЭМИН.

62. Группы технических методов защиты информации от утечки через ПЭМИН. Методы пассивной защиты. Методы активной защиты. Методы и средства контроля ПЭМИН.

63. Изучение принципов действия радиозакладных устройств

64. Сокращения и основные термины. Общие вопросы организации и обеспечения информационной безопасности в техническом аспекте ее защиты.

65. Организационные вопросы обеспечения информационной безопасности

66. Структура технического канала утечки информации

67. Классификация технических каналов утечки информации. Информационный сигнал и его характеристики

68. Понятие информационного сигнала. Аналоговый и цифровой сигналы

69. Модуляция сигналов.

70. Опасные сигналы и их источники

71. Основные показатели технического канала утечки информации

72. Технические каналы утечки акустической информации

73. Основные понятия в области акустики.

74. Классификация акустических каналов утечки информации

75. Средства акустической разведки. Радиозакладки

76. Защита акустической (речевой) информации

77. Звукоизоляция. Зашумление. Средства создания акустических помех

78. Требования и рекомендации по защите речевой информации. Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях

79. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения кинофильмов. Защита информации при проведении звукозаписи

80. Побочные электромагнитные излучения и наводки

81. Виды паразитной связи. Средства перехвата радиосигналов

82. Упрощенная схема комплекса для перехвата радиосигналов

83. Средства предотвращения утечки информации через ПЭМИН

84. Методы защиты информации в отходах производства

85. Средства инженерной защиты

86. Ограждения территории. Ограждения зданий и помещений. Металлические шкафы, сейфы и хранилища

87. Средства систем контроля и управления доступом

88. Средства технической охраны объектов

89. Средства телевизионной охраны. Средства освещения

90. Средства противодействия наблюдению.

91. Структурное скрытие объектов радиолокационного наблюдения

92. Средства противодействия подслушиванию

93. Средства предотвращения утечки информации с помощью закладных подслушивающих устройств

94. Индикаторы электромагнитных излучений. Радиочастотометры. Автоматизированные поисковые комплексы

95. Досмотровая техника. Металлодетекторы. Эндоскоп

96. Генераторы помех. Рентгеновские комплексы

97. Методы поиска электронных устройств перехвата информации

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Разработка защищенных автоматизированных (информационных) систем	ОПК-6, ОПК-14	Тест, защита лабораторных работ, требования к курсовому проекту
2	Эксплуатация защищенных автоматизированных систем	ОПК-6, ОПК-14	Тест, защита лабораторных работ, требования к курсовому проекту

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

1.Белоножкин В.И. Автоматизированные защищенные системы [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (1.38 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.

2.Павлов, В.А. Основы построения и эксплуатации защищенных телекоммуникационных систем [Электронный ресурс] : учеб. пособие. - Электрон.дан(1 файл). - Воронеж : ВГТУ, 2004. - 1 дискета. - 30.00.

3.Методические указания к практическим занятиям по дисциплинам «Методы проектирования защищенных распределенных систем» «Разработка и эксплуатация защищенных автоматизированных систем», для студентов

специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: А. Г. Остапенко, М. В. Бурса. - Электрон. текстовые, граф. дан. (348 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

4.Методические указания к самостоятельным работам по дисциплинам «Методы проектирования защищенных распределенных информационных систем», «Разработка и эксплуатация защищенных автоматизированных систем» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: А. Г. Остапенко, Д. А. Никулин. - Электрон. текстовые, граф. дан. 400 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

Дополнительная литература

1.Комплексное обеспечение информационной безопасности автоматизированных систем : учебное пособие / составители М. А. Лапина [и др.]. — Ставрополь : СКФУ, 2016. — 242 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155111.

2. Заляжных, В. А. Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем : учебно-методическое пособие / В. А. Заляжных, А. В. Гирик. — Санкт-Петербург : НИУ ИТМО, 2014. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/71193.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

1. https://www.virtualbox.org/ - Виртуальная машина
2.http://www.edu.ru/
3. http://window.edu.ru/window/library
4.http://www.intuit.ru/catalog/
5.http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
6.https://cchgeu.ru/education/cafedras/kafsib/?docs
7.http://www.eios.vorstu.ru
8. http://e.lanbook.com/ (ЭБС Лань)
9. http://IPRbookshop.ru/ (ЭБС IPRbooks)
10. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
11.Информационный портал по безопасности www.SecurityLab.ru.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специфического материально-технического обеспечения не требуется.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к	Готовиться к промежуточной аттестации следует систематически, в

промежуточной аттестации	течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.