Приложение к РПД

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущей и промежуточной аттестации

по учебной дисциплине(модулю)

«Программно-аппаратные средства обеспечения информационной безопасности телекоммуникационных сетей»

для направления подготовки/специальности
11.03.02 - Инфокоммуникационные технологии и системы связи

Направленность программы: Мобильная связь и интернет вещей

1. Описание показателей (дескрипторов) и критериев оценивания компетенций на различных этапах их формирования

Контроль качества освоения дисциплины(модуля) включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Компетенции	Показатели* (дескрипторы)	Критерии в соответствии с уровнем освоения ОП			Оценочное средство (технология)
		пороговый (удовлетворительно) 55-69 баллов	стандартный (хорошо) 70-84 балла	эталонный (отлично) 85-100 баллов	
ПК-5	Знать	Частично знает архитектуру и общие принципы функционирования, аппаратных, программных и программно-аппаратных средств администрируемой сети	Знает архитектуру и общие принципы функционирования, аппаратных, программных и программно-аппаратных средств администрируемой сети	В совершенстве знает архитектуруи общие принципы функционирования, аппаратных, программныхи программно-аппаратных средств администрируемой сети	тестирование
	Уметь	Частично умеет использовать современные стандарты при администрировании устройств и программного обеспечения; применять штатные и внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры	Умеет использовать современные стандарты при администрировании устройств и программного обеспечения; применять штатные и внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры	В совершенстве умеет использовать современные стандарты при администрировании устройств и программного обеспечения; применять штатные и внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры	Лабораторные работы
	Владеть	Частично владеет навыками диагностики отказов и ошибок сетевых устройств и программного обеспечения;	Владеет навыками диагностики отказов и ошибок сетевых устройств и программного обеспечения;	В совершенстве владеет навыками диагностики отказов и ошибок сетевых устройств и программного обеспечения;	Проект

ПК-7	Знать	Частично знает основы инфокоммуникационных технологий и способы поиска информации по продажам инфокоммуникационных систем и/или их составляющих	Знает основы инфокоммуникационных технологий и способы поиска информации по продажам инфокоммуникационных систем и/или их составляющих	В совершенстве знает основы инфокоммуникационных технологий и способы поиска информации по продажам инфокоммуникационных систем и/или их составляющих	тестирование
	Уметь	Частично умеет применять системы управления взаимоотношениями с клиентами при подготовке аналитических отчетов по продажам инфокоммуникационных систем и/или их составляющих	умеет применять системы управления взаимоотношениями с клиентами при подготовке аналитических отчетов по продажам инфокоммуникационных систем и/или их составляющих	В совершенстве умеет применять системы управления взаимоотношениями с клиентами при подготовке аналитических отчетов по продажам инфокоммуникационных систем и/или их составляющих	Лабораторные работы
	Владеть	Частично владеет навыками сбора, аналитического и численного исследования информации по продажам инфокоммуникационных систем и/или их Составляющих	Владеет навыками сбора, аналитического и численного исследования информации по продажам инфокоммуникационных систем и/или их Составляющих	В совершенстве владеет навыками сбора, аналитического и численного исследования информации по продажам инфокоммуникационных систем и/или их Составляющих	Проект
ПК-10	Знать	Частично знает общие принципы функционирования и архитектуру аппаратных, программных и программно - аппаратных средств	Знает общие принципы функционирования и архитектуру аппаратных, программных и программно - аппаратных средств	В совершенстве знает общие принципы функционирования и архитектуру аппаратных, программных и программно - аппаратных средств	тестирование
	Уметь	Частично умеет подключать и настраивать современные средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов); работать с контрольно-измерительными аппаратными и программными средствами;	Умеет подключать и настраивать современные средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов); работать с контрольно-измерительными аппаратными и программными средствами;	В совершенстве умеет подключать и настраивать современные средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов); работать с контрольно-измерительными аппаратными и программными средствами;	Лабораторные работы

	Владеть	Частично ладеет навыками установки дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация;	Владеет навыками установки дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация;	В совершенстве владеет навыками установки дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация;	Проект
ПК-12	Знать	Частично знает принципы работы, технические характеристики, конструктивные особенности элементов оптических и медножильных линий связи	Знает принципы работы, технические характеристики, конструктивные особенности элементов оптических и медножильных линий связи	В совершенстве знает принципы работы, технические характеристики, конструктивные особенности элементов оптических и медножильных линий связи	тестирование
	Уметь	Частично умеет устранять технические проблемы на участке сети доступа, не требующие проведения аварийно восстановительных работ	Умеет устранять технические проблемы на участке сети доступа, не требующие проведения аварийно восстановительных работ	В совершенстве умеет устранять технические проблемы на участке сети доступа, не требующие проведения аварийно восстановительных работ	Лабораторные работы
	Владеть	Частично владеет методами изменения настроек оборудования клиента дистанционно с применением средств дистанционного доступа или путем инструктирования клиента	Владеет методами изменения настроек оборудования клиента дистанционно с применением средств дистанционного доступа или путем инструктирования клиента	В совершенстве владеет методами изменения настроек оборудования клиента дистанционно с применением средств дистанционного доступа или путем инструктирования клиента	Проект

2. Описание критериев и шкал оценивания результатов обучения по дисциплине (модулю)

2.1.Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением семинаров, оцениванием контрольных заданий, проверкой конспектов лекций, выполнением индивидуальных и творческих заданий, периодическим опросом обучающихся на занятиях. Контролируемые разделы (темы) дисциплины(модуля), компетенции и оценочные средства представлены в таблице.

№ п/п	Контролируемые разделы (темы) дисциплины*(модуля)	Код контролируемой компетенции и/или индикаторы компетенции	Наименование оценочного средства**
1	Разграничение доступа к ресурсам	ПК-5, ПК-7, ПК-10, ПК-12	Лабораторные работы, тестирование, проект
2	Средства для сбора записей	ПК-5, ПК-7, ПК-10, ПК-12	Лабораторные работы, тестирование, проект
3	Журналирование событий, журнал безопасности.	ПК-5, ПК-7, ПК-10, ПК-12	Лабораторные работы, тестирование, проект
4	Правовые вопросы применимости применения ЭЦП и СКЗИ в России	ПК-5, ПК-7, ПК-10, ПК-12	Лабораторные работы, тестирование, проект

Критерии и шкала оценивания тестирования

Оценка	*Критерий оценки*
«зачтено»	*Выполнение более 60% тестовых заданий*
«не зачтено»	*Выполнение менее 60% тестовых заданий*

Критерии оценивания проекта

Оценка	*Критерии*	*Расшифровка уровня критерия*
«зачтено»	*Актуальность*	*Очень современная тема. Отклик на событие. Новые программы и устройства.*
		Продвинутая тема, интересная многим
		Углублённое изучение программного материала.
		Проработка и иллюстрирование тем базового курса
	Осведомлённость	*Изучено очень много источников. Освоены новые разделы темы. Осведомлённость на уровне эксперта*
		Изучено достаточно много источников
		Изучено не очень много источников. Проект на уровне изученного примера рассмотренного на занятиях.
		Материал недостаточно освоен, скопирован, есть ошибки, используются термины без объяснения.
	Научность	*Проведено научное исследование темы. Выдвинуты новые идеи, рацпредложения. Проведён анализ. Разработан новый материал.*
		Проект практико-ориентированный. Разработаны дидактические материалы.
		Проект реферативный

	Значимость	*Разработаны документы готовые к последующему использованию. Разработан справочник, мастер-класс, инструкция доступная любому.*
		Собраны материалы, которые после изучения и доработки можно применить. Можно читать как интересную статью.
		Тема раскрыта недостаточно. Изложен материал по учебной теме, имеет значимость только для самого исполнителя.
	Презентабельность (публичное представление)	*Оформление в соответствии с требованиями. Полный пакет документов: отчет о работе в текстовом виде + разработанные документы+ презентация для выступления. Оригинальная презентация. Яркое выступление*
		Недостатки в оформлении
		Неполный пакет документов
		Слабое оформление
	Оригинальность	*Индивидуальное отношение авторов проекта к процессу проектирования и результату своей деятельности. Дополнительные средства оформления. Оценивается оригинальность раскрываемой работой темы, глубина идеи работы, образность, индивидуальность творческого мышления, оригинальность используемых средств*
	Качество	*оценивается художественный уровень произведения, дизайн элементов оформления, гармоничное цветовое сочетание, качество композиционного решения, наличие перспективы*
	Скорость выполнения	*2- досрочно, 1 –сдан в срок, 0 – сроки сдачи нарушены*
«не зачтено»	*Выполнение менее 60% оцениваемых критериев*	

Критерии оценивания лабораторных работ

Оценка	Критерий оценки
«зачтено»	1) студент выполнил экспериментальную часть работы; 2) студент представил отчёт по проделанной работе; 3) содержание отчёта соответствует правилам обработки экспериментальных результатов, студент в состоянии сформулировать эти правила (по дополнительным вопросам преподавателя); 4) Студент защитил теоретическую часть работы в устной беседе с преподавателем по вопросам, содержащимся в методических указаниях к каждой работе
«не зачтено»	Студент не выполнил один из пунктов , приведенных выше.

2.2.Критерии и шкалы оценивания результатов обучения при проведении промежуточной аттестации

. Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Для оценивания результатов обучения при проведении промежуточной аттестации используется четырехбалльная шкала: «Отлично», «Хорошо», «Удовлетворительно», «Неудовлетворительно».

Шкала оценивания	*Критерии*	*Уровень освоения компетенций*
Отлично	*наличие глубоких и исчерпывающих знаний в объеме пройденного программного материала, правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы*	*Эталонный*
Хорошо	*наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильные действия по применению знаний на практике, четкое изложение материала*	*Стандартный*
Удовлетвори-тельно	*наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополни- тельных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике*	*Пороговый*
Не-удовлетворительно	*наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.*	*Компетенции не сформированы*

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1. Оценочные средства текущего контроля успеваемости

3.1.1 Перечень тем проектов

1. Расширение системы обеспечения безопасности семейства ОС Windows за счет применения программно-аппаратных средств защиты информации
2. Организация безопасной удаленной деятельности сотрудника с мобильного устройства с применением программных и программно-аппаратных средств защиты информации
3. Аутентификация пользователей при локальном и удаленном доступе в компьютерных системах
4. Установка и настройка ПО ZoneMimder для систем видеонаблюдения на СХД с использованием RAID 60
5. Изучение антивирусных программных продуктов и внедрение их в компьютерные классы СОШ
6. Организация защиты данных с использованием средств безопасности ОС Windows и программных средств защиты информации «Rohos»

7. Организация аутентификации пользователей с использованием usb – устройств Миграция серверов с ПО Орион

8. Про для организации СКУД на виртуальные сервера Организации системы обнаружения атак и предотвращения утечки информации в беспроводных сетях

9. Проектирование системы программно-аппаратной защиты информации в образовательном агентстве ООО «Личная стратегия»

10. Технология антивирусной защиты информации и сравнительный анализ антивирусных программ

11. Разработка проекта комплексной защиты информации медицинского центра «Салютем»

12. Изучение сканеров уязвимости компьютерных систем и их сравнительный анализ Инструментальные средства анализа рисков информационной безопасности

13. Изучение системы мониторинга информационной инфраструктуры Zabbix и её внедрение в компьютерных классах АГТУ

14. Технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности

15. Обзор и сравнение средств обеспечения резервного копирования в информационных системах

16. Изучение средств уничтожения остаточной информации в запоминающих устройствах и их сравнительный анализ Изучение и внедрение

17. Kaspersky Security Center в компьютерные классы ЗабГУ

18. Настройка операционной системы Astra Linux по требованиям безопасности информации

19. Организация защиты рабочего места генерального директора ООО «Личная стратегия» от действий инсайдеров

3.1.2. Пример теста по теме «Администрирования средств защиты информации в компьютерных сетях»

Вариант 0

1 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» устанавливается _____ (сколько?) классов защищённости государственной информационной системы.

а) 1; б) 2; в) 3; г) 4

2 Согласно Постановлению Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» устанавливается ___ (сколько?) уровней защищённости информационной системы персональных данных.

а) 1; б) 2; в) 3; г) 4.

3 Согласно Постановлению Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» уровень защищенности информационной системы зависит от

а) типа актуальных угроз;

б) масштаба системы;

в) категории персональных данных;

г) типа актуальных угроз и масштаба системы;

д) масштаба системы и категории персональных данных;

е) типа актуальных угроз и категории персональных данных.

4 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» класс защищенности информационной системы зависит от

а) уровня значимости информации;

б) масштаба системы;

в) уровня значимости информации и масштаба системы;

г) уровня значимости информации и категории персональных данных.

5 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» устанавливается ___ (сколько?) степеней возможного ущерба.
а) 1; б) 2; в) 3; г) 4.

6 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» информация имеет высокий уровень значимости (УЗ 1), если
а) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба

б) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;

в) для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

7. Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» информация имеет средний уровень значимости (УЗ 2), если
а) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба;

б) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;

в) для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

8. Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» информация имеет низкий уровень значимости (УЗ 3), если а) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба;

б) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;

в) для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба

9 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» при обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством

Российской Федерации виды информации ограниченного доступа) уровень значимости информации (УЗ)
а) определятся отдельно для каждого вида информации;
в) является единым для всех

10 определены низкие степени ущерба. 2 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» информация имеет средний уровень значимости (УЗ 2), если
а) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба;
б) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;
в) для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

11. Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» информация имеет низкий уровень значимости (УЗ 3), если а) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба;
б) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;
в) для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

12 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» при обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации (УЗ)
а) определятся отдельно для каждого вида информации;
в) является единым для всех.

13 Какое из перечисленных средств защиты информации не обеспечивает защиту от несанкционированного доступа
а) Secret Net Studio; б) Dallas Lock; в) Dr. Web.

3.1.3. Темы лабораторных занятий

Лабораторная работа №1. Антивирусное программное обеспечение

1. Какие типы вирусных угроз Вы знаете?

2. Какие антивирусные пакеты Вы знаете? Какие типы защит обеспечивает современный антивирусный пакет?

3. Что такое база сигнатур и зачем требуется еѐ обновление?

4. Зачем может потребоваться загрузка антивирусного пакета с помощью LiveCD?

Лабораторная работа №2. Технология виртуализации. Изучение виртуальной машины как средства защиты данных.

1. Что такое «песочница» и в чем преимущества ее использования?
2. Приводит ли использование виртуальной машины к потере производительности?
3. Какие операционные системы могут быть установлены в качестве гостевых?
4. Как использование виртуальной машины может повысить безопасность компьютера?

Лабораторная работа №3 Изучение функциональных возможностей программы-анализатора сетевого трафика Wireshark.

1. Какие фильтры можно использовать в Wireshark для выделения пакетов определенного протокола (например, TCP)?
2. Каким образом можно настроить захват трафика только между двумя конкретными IP-адресами?
3. Опишите процесс анализа содержимого пакетов HTTP-запросов и ответов.
4. Какие преимущества имеет Wireshark перед другими анализаторами сетевых пакетов?

Лабораторная работа №4Изучение функциональных возможностей межсетевого экрана Netfilter.

1. Объясните различия между цепочками INPUT, OUTPUT и FORWARD в таблице фильтрации iptables.
2. Как правильно заблокировать доступ к определенному порту или протоколу с помощью правил iptables?
3. В каких случаях целесообразно использовать NAT в межсетевом экране Netfilter?
4. Как добавить правило, которое разрешает исходящие соединения, но блокирует входящие, кроме уже установленных сессий?

Лабораторная работа №5 Изучение функциональных возможностей системы обнаружения вторжений Snort

1. Что такое сигнатуры в Snort и как они используются для выявления подозрительной активности?
2. Опишите процесс настройки Snort для мониторинга конкретного интерфейса сети.
3. Какие существуют режимы работы Snort (sniffer, packet logger, intrusion detection) и какие задачи они решают?
4. Как настроить Snort для отправки уведомлений о найденных угрозах через электронную почту?

3.2. Оценочные средства промежуточной аттестации

В данном разделе представляются теоретические вопросы (для оценки знаний), типовые контрольные задания (для оценки умений), типовые практические задания (для оценки навыков и (или) опыта деятельности).

Например:

Перечень теоретических вопросов (для оценки знаний):

Вопрос 1

1.Что такое исходные данные для проектирования подсистем средств обеспечения защиты информации?

2. Какие методы используются для подготовки исходных данных?

3. Какие требования должны быть учтены при подготовке исходных данных?
4. Какие документы необходимо составить при подготовке исходных данных?
5. Какие риски могут возникнуть при неправильной подготовке исходных данных?
6. Какие средства обеспечения защиты информации могут быть использованы?
7. Какие факторы необходимо учитывать при выборе средств обеспечения защиты информации?
8. Какие методы используются для экономического обоснования проектных решений?
9. Какие данные необходимо учесть при проведении технико-экономического обоснования?
10. Какие методы используются для анализа эффективности проектных решений?
11. Какие риски могут возникнуть при неправильном технико-экономическом обосновании проектных решений?
12. Какие документы необходимо составить при технико-экономическом обосновании проектных решений?
13. Какие методы используются для оценки стоимости проектных решений?
14. Какие факторы необходимо учесть при проведении экономического обоснования проектных решений?
15. Какие преимущества и недостатки могут быть у различных проектных решений?
16. Какие методы используются для оценки эффективности средств обеспечения защиты информации?
17. Какие методы используются для оценки рисков при выборе средств обеспечения защиты информации?
18. Какие факторы необходимо учесть при проведении анализа эффективности средств обеспечения защиты информации?
19. Какие методы используются для оценки стоимости средств обеспечения защиты информации?
20. Какие преимущества и недостатки могут быть у различных средств обеспечения защиты информации?
21. Какие требования должны быть учтены при выборе средств обеспечения защиты информации?
22. Какие методы используются для анализа эффективности проектных решений в условиях ограниченного бюджета?
23. Какие факторы необходимо учесть при проведении анализа эффективности проектных решений в условиях ограниченного бюджета?
24. Какие методы используются для оценки стоимости проектных решений в условиях ограниченного бюджета?
25. Какие преимущества и недостатки могут быть у различных проектных решений в условиях ограниченного бюджета?

Вопрос 2

1. Что такое администрирование средств защиты информации?
2. Какие основные задачи выполняет администратор средств защиты информации?
3. Какие типы угроз информационной безопасности могут возникнуть в компьютерных системах и сетях?
4. Что такое аутентификация и почему она важна для обеспечения безопасности?
5. Какие методы аутентификации можно использовать?
6. Что такое авторизация и как она связана с аутентификацией?
7. Какие методы авторизации можно использовать?
8. Что такое шифрование и как оно помогает защитить информацию?
9. Какие алгоритмы шифрования широко используются в сетях?
10. Что такое брандмауэр и как он обеспечивает безопасность сети?
11. Какие типы брандмауэров существуют?
12. Какие функции выполняет брандмауэр?
13. Какие методы обнаружения вторжений (IDS) существуют?
14. Как IDS помогает обнаружить и предотвратить атаки на сеть?

15. Что такое вирус и какие методы защиты от них существуют? 16. Какие типы вредоносных программ существуют?
17. Какие методы обнаружения и удаления вредоносных программ существуют?
18. Что такое антивирусное программное обеспечение и как оно работает?
19. Какие методы обнаружения и предотвращения DDoS-атак существуют?
20. Что такое VPN и как оно помогает обеспечить безопасность соединения?
21. Какие типы VPN-соединений существуют?
22. Какие методы защиты от перехвата данных существуют?
23. Что такое аудит безопасности и почему он важен?
24. Какие инструменты аудита безопасности можно использовать?
25. Что такое политика безопасности и как она помогает обеспечить безопасность информации?
26. Какие основные элементы политики безопасности существуют?
27. Какие методы резервного копирования данных существуют?
28. Что такое фильтрация содержимого и как она помогает обеспечить безопасность информации?
29. Какие методы фильтрации содержимого существуют?
30. Что такое многофакторная аутентификация и как она помогает обеспечить безопасность?
31. Какие методы многофакторной аутентификации существуют?
32. Что такое управление доступом и как оно помогает обеспечить безопасность?
33. Какие методы управления доступом существуют?
34. Что такое протоколы безопасности и как они помогают обеспечить безопасность сети?
35. Какие протоколы безопасности широко используются в компьютерных системах и сетях?
36. Что такое физическая безопасность и почему она важна?
37. Какие методы физической безопасности существуют?
38. Что такое угрозы внутреннего происхождения и как их предотвратить?
39. Какие методы обнаружения и предотвращения угроз внутреннего происхождения существуют?
40. Что такое защита от вредоносных программ на уровне операционной системы?
41. Какие методы защиты от вредоносных программ на уровне операционной системы существуют?
42. Что такое защита от сетевых атак на уровне операционной системы?
43. Какие методы защиты от сетевых атак на уровне операционной системы существуют?
44. Что такое защита от физических угроз на уровне операционной системы?
45. Какие методы защиты от физических угроз на уровне операционной системы существуют?
46. Что такое защита от угроз внутреннего происхождения на уровне операционной системы?
47. Какие методы защиты от угроз внутреннего происхождения на уровне операционной системы существуют?
48. Что такое защита от вредоносных программ на уровне сети?
49. Какие методы защиты от вредоносных программ на уровне сети существуют
50. Что такое защита от сетевых атак на уровне сети?

Перечень типовых задач (для оценки умений):

Анализ уязвимостей

- **Задача**: Провести анализ известных уязвимостей в конкретном программном обеспечении (например, веб-сервере Apache или маршрутизаторе Cisco). Определить возможные способы эксплуатации этих уязвимостей и предложить меры по их устранению.
- **Цель**: Оценка способности студента выявлять слабые места в ПО и предлагать решения.

2. Настройка межсетевого экрана

- **Задача**: Настроить межсетевой экран (например, pfSense или iptables) таким образом, чтобы обеспечить защиту от определенных типов атак (DDoS, SQL-инъекции, спуфинг).
- **Цель**: Проверка знаний принципов работы и настроек межсетевых экранов.

3. Криптографическая защита данных

- **Задача**: Реализовать шифрование передаваемых данных с использованием симметричного алгоритма (AES) и асимметричного (RSA). Сравнить производительность обоих методов.
- **Цель**: Определение уровня понимания криптографии и её практического применения.

4. Разработка политики безопасности

- **Задача**: Разработать политику безопасности для организации, включая правила доступа к данным, использование паролей, шифрования и другие меры защиты.
- **Цель**: Оценка способностей к стратегическому планированию и созданию комплексной системы безопасности.

5. Мониторинг и обнаружение вторжений

- **Задача**: Настроить систему обнаружения вторжений (IDS/IPS), такую как Snort, для отслеживания подозрительных действий в сети. Предложить методы улучшения её эффективности.
- **Цель**: Тестирование знаний в области обнаружения аномалий и реакции на инциденты.

6. Создание VPN-соединения

- **Задача**: Создать защищенное VPN-соединение между двумя удаленными офисами с использованием OpenVPN или аналогичного программного обеспечения. Обеспечить аутентификацию пользователей и шифрование трафика.
- **Цель**: Демонстрация практических навыков по настройке виртуальных частных сетей.

7. Защита беспроводных сетей

- **Задача**: Проанализировать существующие механизмы защиты беспроводных сетей (WEP, WPA, WPA2) и предложить рекомендации по улучшению безопасности корпоративной Wi-Fi сети.
- **Цель**: Изучение современных стандартов безопасности и их применимости в реальных условиях.

8. Реализация аутентификации и авторизации

- **Задача**: Реализовать двухфакторную аутентификацию для доступа к критически важным ресурсам. Описать плюсы и минусы различных подходов (SMS, аппаратные токены, биометрия).
- **Цель**: Понимание механизмов аутентификации и их интеграции в системы безопасности.

9. Оценка рисков и управление ими

- **Задача**: Выполнить оценку рисков для конкретной инфраструктуры и разработать план управления этими рисками. Включить такие элементы, как резервное копирование, мониторинг и аудит.
- **Цель**: Анализ возможных угроз и разработка мер реагирования.

10. Моделирование атаки и её предотвращение

- **Задача**: Смоделировать сценарий атаки типа MITM (человек посередине) и предложить способы её предотвращения.
- **Цель**: Практическое применение знаний о методах защиты от распространенных атак.

Перечень типовых практических заданий (для оценки навыков и (или) опыта деятельности):

1. Установка и настройка межсетевого экрана (Firewall)

- **Задание:** Установите и настройте межсетевой экран (например, pfSense или iptables) для защиты локальной сети от внешних угроз. Включите правила для блокировки нежелательного трафика и разрешения безопасного обмена данными.
- **Ожидаемый результат:** Полностью настроенный межсетевой экран с правилами, обеспечивающими безопасность сети.

---

2. Настройка VPN-сервера

- **Задание:** Настройте сервер VPN (например, OpenVPN или WireGuard) для обеспечения безопасной передачи данных между удалёнными пользователями и локальной сетью.

- **Ожидаемый результат:** Рабочая конфигурация VPN-сервера с корректной настройкой аутентификации и шифрования.

---

3. Шифрование данных в сети

- **Задание:** Реализуйте симметричное и асимметричное шифрование для защиты передаваемых данных между двумя узлами сети. Используйте стандартные алгоритмы, такие как AES и RSA.
- **Ожидаемый результат:** Функционирующая система шифрования данных с демонстрацией процесса обмена ключами и расшифровки сообщений.

---

4. Разработка политики безопасности

- **Задание:** Разработайте и внедрите политику безопасности для небольшой компании, включающую правила доступа к данным, управление учетными записями, использование паролей и шифрование данных.
- **Ожидаемый результат:** Документированная политика безопасности с рекомендациями по её реализации.

---

5. Мониторинг и анализ сетевого трафика

- **Задание:** Используя инструмент захвата пакетов (например, Wireshark), проанализируйте трафик в сети и выявите потенциальные угрозы или нарушения безопасности.
- **Ожидаемый результат:** Отчет с результатами анализа, включающий выявление аномального поведения и предложения по усилению безопасности.

---

6. Обнаружение и реагирование на вторжения

- **Задание:** Настройте систему обнаружения вторжений (IDS) на основе Snort или Suricata. Убедитесь, что она способна детектировать известные типы атак (например, DDoS, SQL-инъекции).
- **Ожидаемый результат:** Настроенная IDS с корректными сигнатурами и возможностью отправки предупреждений о попытках взлома.

---

7. Тестирование на проникновение (Penetration Testing)

- **Задание:** Проведите тестирование на проникновение в сеть с целью выявления слабых мест и потенциальных уязвимостей. Используйте инструменты вроде Nmap, Metasploit и Burp Suite.
- **Ожидаемый результат:** Подробный отчет с описанием выявленных уязвимостей и предложениями по их устранению.

---

8. Защита беспроводных сетей

- **Задание:** Настройте защищенную беспроводную сеть с использованием протоколов WPA2/WPA3. Проверьте устойчивость сети к известным атакам (например, brute force).
- **Ожидаемый результат:** Конфигурация беспроводной сети с высоким уровнем безопасности и отчёт о проведённых тестах на стойкость.

---

9. Управление правами доступа

- **Задание:** Организуйте контроль прав доступа к файлам и каталогам в операционной системе Linux. Настройте права доступа для разных групп пользователей, обеспечивая минимально необходимые привилегии.
- **Ожидаемый результат:** Правильно настроенные права доступа, исключающие несанкционированный доступ к конфиденциальным данным.

---

10. Создание системы резервного копирования

- **Задание:** Спроектируйте и реализуйте систему резервного копирования для критичных данных компании. Рассмотрите варианты онлайн и оффлайн бэкапов, автоматизацию процессов.
- **Ожидаемый результат:** Работающая система автоматического резервного копирования с расписаниями и проверкой целостности копий

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

4.1. Описание процедур проведения текущего контроля успеваемости студентов

В таблице представлено описание процедур проведения контрольно-оценочных мероприятий текущего контроля успеваемости студентов, в соответствии с рабочей программой дисциплины(модуля), и процедур оценивания результатов обучения с помощью спланированных оценочных средств.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Проект	Проект защищается на практическом занятии. Задание выдается не позже чем за три недели до защиты. Защита проекта должна быть выполнены в установленный преподавателем срок и в соответствии с требованиями к оформлению (текстовой и графической частей). Выполненные задания в назначенный срок сдаются на проверку
Лабораторная работа	Лабораторная работа выполняется на занятие в лабораториях. Измерения проводит группа студентов количеством 3-5 человек. Расчет результатов экспериментов производится каждым студентом индивидуально. Отчет по лабораторной работе оценивается преподавателем. Преподаватель так же оценивает ответы на теоретические вопросы к лабораторным работам. Теоретическая часть лабораторных работ описывается в методическом указании к лабораторным работам.
Компьютерное тестирование	Компьютерное тестирование проводится по результатам освоения разделов дисциплины во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте время выполнения.

4.2. Описание процедур проведения промежуточной аттестации

Экзамен

При определении уровня достижений обучающих на экзамене обращается особое внимание на следующее:

- дан полный, развернутый ответ на поставленный вопрос;

- показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные признаки, причинно-следственные связи;
- знание об объекте демонстрируются на фоне понимания его в системе данной дисциплины(модуля) и междисциплинарных связей;
- ответ формулируется в терминах дисциплины(модуля), изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающегося;
- теоретические постулаты подтверждаются примерами из практики.

Вопросы к экзамену

1. Подсистема управления доступом. Особенности реализации в различных ОС.
2. Подсистема регистрации и учёта событий. Особенности реализации в различных ОС.
3. Криптографическая подсистема. Особенности реализации в различных ОС.
4. Подсистема обеспечения целостности. Особенности реализации в различных ОС.
5. Контрольная сумма CRC.
6. Межсетевые экраны. Определение, назначение, классификация.
7. Архитектура систем активного аудита.
8. Обзор инструментальных средств анализа защищённости АС.
9. Средства защиты информации активного сетевого оборудования.
10. Генерация случайных чисел в ОС Linux.
11. Атака на переполнение буфера.
12. Принципы построения систем обнаружения вторжений.
13. Сигнатурный анализ как антивирусная техника.
14. Эвристические антивирусные техники.
15. Статические и динамические антивирусные техники.
16. Полиморфизм компьютерных вирусов.
17. Методы защиты от атаки на переполнение буфера.
18. Виртуальные частные сети.
19. Дискреционный контроль доступа.
20. Сравнительный анализ средств защиты информации различных операционных систем.