ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Информационная безопасность

Код модуля	Модуль
1163449(1)	Информационная безопасность

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Ронкин Михаил Владимирович	кандидат технических наук, без ученого звания	Доцент	информационных технологий и систем управления
2	Чернышов Юрий Юрьевич	кандидат физико-математических наук, без ученого звания	Доцент	информационных технологий и систем управления

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Ронкин Михаил Владимирович**, **Доцент**, **информационных технологий и систем управления**
- **Чернышов Юрий Юрьевич**, **Доцент**, **информационных технологий и систем управления**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Информационная безопасность

1.	**Объем дисциплины в зачетных единицах**	3	
2.	**Виды аудиторных занятий**	Лекции Практические/семинарские занятия	
3.	**Промежуточная аттестация**	Зачет	
4.	**Текущая аттестация**	Домашняя работа	1
		Программный продукт	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Информационная безопасность

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	**Планируемые результаты обучения (индикаторы)**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
ПК-4 -Способен управлять процессами развертывания и введения в эксплуатацию информационно-коммуникационных систем	З-1 - Определять специфику функционирования программного обеспечения, принципы организации, состав и схемы работы операционных систем, основы архитектурной и системотехнической организации вычислительных сетей П-1 - Иметь практический опыт управления процессами настройки, развертывания и введения в эксплуатацию информационно-коммуникационных систем У-1 - Анализировать работу с программно-аппаратными	Домашняя работа Зачет Лекции Практические/семинарские занятия Программный продукт

	средствами сопровождения и развертывания программного обеспечения в создаваемых вычислительных и информационных системах и сетевых структурах с учетом требований организации	
УК-7 -Способен обрабатывать, анализировать, передавать данные и информацию с использованием цифровых средств для эффективного решения поставленных задач с учетом требований информационной безопасности	З-1 - Сделать обзор угроз информационной безопасности, основных принципов организации безопасной работы в информационных системах и в сети интернет З-2 - Описать способы и средства защиты персональных данных и данных в организации в соответствии с действующим законодательством З-3 - Сделать обзор современных цифровых средств и технологий, используемых для обработки, анализа и передачи данных при решении поставленных задач П-1 - Обосновать выбор технических и программных средств защиты персональных данных и данных организации при работе с информационными системами на основе анализа потенциальных и реальных угроз безопасности информации П-2 - Решать поставленные задачи, используя эффективные цифровые средства и средства информационной безопасности У-1 - Определять основные угрозы безопасности при использовании информационных технологий и выбирать оптимальные способы и средства защиты персональных данных и данных организации от мошенников и вредоносного ПО У-2 - Выбирать современные цифровые средства и технологии для обработки,	Домашняя работа Зачет Лекции Практические/семинарские занятия Программный продукт

	анализа и передачи данных с учетом поставленных задач	

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	3,7	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.5		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
программный продукт	3,14	100
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрено		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -не предусмотрено		
Промежуточная аттестация по лабораторным занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено**		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	**Сроки – семестр,**	**Максимальная оценка в баллах**

	учебная неделя	
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		
Промежуточная аттестация по онлайн-занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено**		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	**Сроки − семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Практические/семинарские занятия

Примерный перечень тем

1. Обнаружение компьютерных атак. Атаки, связанные с аутентификацией и авторизацией.

2. Обнаружение компьютерных атак. Атаки на клиента.Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак.

3. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА.

4. Обнаружение компьютерных атак. Разглашение информации и логические атаки.

5. Технология межсетевого экранирования. Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.

6. Организация виртуальных частных сетей. Установка и настройка VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP.

7. Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server.

8. Аудит информационной безопасности в компьютерных сетях. Этапы и методы проведения, результаты работ.

Примерные задания

Практическая работа по заданной тематике.

- Обнаружение компьютерных атак.
- Разглашение информации и логические атаки.
- Классификация систем обнаружения атак (СОА).
- Обнаружение атак, связанные с аутентификацией и авторизацией.
- Организация виртуальных частных сетей.
- Установка и настройка VPN. Туннелирование в VPN.
- Защита данных на канальном уровне.
- Организация VPN средствами протокола PPTP.

LMS-платформа − не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Домашняя работа

Примерный перечень тем

1. Настройки и проверка информационной безопасности

Примерные задания

1. Используя тестовую площадку, команда студентов получает доступ к веб-приложению и осуществляет в нем различные действия с правами администратора.

2. Используя тестовую площадку, команда студентов осуществляет поиск уязвимостей и разрабатывает рекомендации по их устранению.

3. Подготовка доклада и презентации о проделанной командной работе с тестовой площадкой.

4. Подготовка доклада и презентации о выявлении и построении схемы информационных потоков защищаемой информации на предлагаемом веб-ресурсе.

LMS-платформа − не предусмотрена

5.2.2. Программный продукт

Примерный перечень тем

1. Практическое применение информационной безопасности

Примерные задания

1. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами сетевых фильтров.

2. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами сетевых фильтров.

3. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами сетевых фильтров.

4. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение извне доступа к ресурсам компьютера за исключением двух доверенных узлов. Реализуйте политику средствами сетевых фильтров.

5. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение доступа к Web-ресурсам определенного узла. Реализуйте политику средствами сетевых фильтров.

6. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только получение доступа к Web-ресурсам двух определенных узлов. Реализуйте политику средствами сетевых фильтров.

7. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами сетевых фильтров.

8. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами протокола IPSec.

9. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами протокола IPSec.

10. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами протокола IPSec.

11.С использованием программы «Брандмауэр Windows» (Windows Firewall) выполнить настройки, запрещающие использование всех портов защищаемого узла за исключением TCP-порта 3389.

12. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами протокола IPSec.

13.Сгенерируйте и получите в виде файла сертификат открытого ключа с использованием образа ОС Windows Server 2003.

14. Настройте Web-сервер для организации защищенного доступа к Web-странице с использованием протокола SSL. Выполнить с использованием образа ОС Windows Server 2003. Файл-сертификат открытого ключа прилагается.

15. Настройте входящее подключение VPN с использованием протокола PPTP. Настроить и установить подключение клиентского узла. Выполнить с использованием образа ОС Windows Server 2003.

16. Осуществите криптографическую защиту сетевого трафика средствами протокола IPSec в ОС Windows. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

17. Осуществите криптографическую защиту сетевого трафика средствами СКЗИ StrongNet. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

18. Организовать защищенный обмен почтовой информацией между двумя пользователями. Шифрование почтовых сообщений выполнить с помощью алгоритма ГОСТ 28147-89, реализуемого средствами СКЗИ КриптоПро CSP. Выполнить с использованием образов ОС Windows Server 2003.

19. Разработайте файл конфигурации и настройте СОА Snort на обнаружение тестирования внутренней структуры сети ICMP-запросами.

20. Разработайте файл конфигурации и настройте СОА Snort на обнаружение ICMPпакетов большой длины.

21. Разработайте файл конфигурации и настройте СОА Snort на обнаружение устанавливаемых из внешней сети TCP-соединений.

22. Установить службу терминального доступа. Выполнить настройки службы MSTS, разрешающие доступ к ресурсам терминального сервера только для учетных записей, зарегистрированных в созданной по умолчанию группе «Remote Desktop Users».

23. Установить службу терминального доступа. Выполнить настройки протокола RDP, запрещающие использование ресурсов рабочей станции, включая буфер обмена, принтеры и накопители.

24.Выявите сетевые узлы в локальном сетевом сегменте с использованием: утилиты fping; утилиты ping и широковещательной ICMP-посылки; утилиты icmpush (тип ICMPпакетов13 и 17); утилиты ping и многоадресной рассылки; утилиты arping; утилиты hping3 и методов TCP- и UDP-разведки; утилиты Ethereal и метода прослушивания сети.

25.С помощью утилиты nmap проведите сканирование портов сетевого узла. Сформируйте списки открытых TCP- и UDP-портов, идентифицируйте версии ОС и запущенных сервисов. По результатам сделайте вывод о возможности обнаружения открытых портов и идентификации типа и версии ОС, а также сетевых сервисов.

26. С помощью программы NetCrunch, постройте карту сети компьютерного класса.

LMS-платформа − не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Зачет

Список примерных вопросов

1. Атаки на протоколы и службы Интернет. Методы и средства защиты.

2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.

3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.

4. Создание защищенных сегментов сетей с использованием межсетевых экранов.

5. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows.

6. Защита рабочих станций с использованием персональных сетевых фильтров.

7. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.

8. Электронные сертификаты. Понятие инфраструктуры открытых ключей.

9. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.

10. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.

11. Преимущества технологии терминального доступа. Обеспечение безопасности.

12. Назначение систем обнаружения атак. Классификация систем обнаружения атак.

13. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.

14. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.

15. Аудит безопасности компьютерных систем. Цели, стандарты, подходы.

16. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки. Применение инструментальных средств аудита безопасности компьютерных систем.

17. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности. Методика проведения инструментальных проверок.

18. Классификация средств и информационных ресурсов в соответствии со стандартом ISO-17799.

19. Назначение и основные функции программных комплексов «Гриф-специалист» и «Кондор-специалист». Построение модели защиты компьютерной системы с использованием комплексной экспертной системы «АванГард».

20. Виды требований безопасности согласно ГОСТ Р ИСО/МЭК 15408-1-2002. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

21. Назначение систем обнаружения атак. Классификация систем обнаружения атак. Использование системы обнаружения атак «Snort».

LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.