ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Обеспечение безопасности корпоративной информации

Код модуля
1155579(0)

Модуль
ИТ-инновации в бизнесе

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Ермаков Дмитрий Германович	кандидат физико-математических наук, без ученого звания	Доцент	анализа систем и принятия решений

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Ермаков Дмитрий Германович, Доцент, анализа систем и принятия решений**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Обеспечение безопасности корпоративной информации

1.	**Объем дисциплины в зачетных единицах**	3	
2.	**Виды аудиторных занятий**	Лекции Лабораторные занятия	
3.	**Промежуточная аттестация**	Экзамен	
4.	**Текущая аттестация**	Контрольная работа	2
		Коллоквиум	1
		Домашняя работа	2

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Обеспечение безопасности корпоративной информации

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**
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 П-1 - Обосновать выбор технических и программных средств защиты персональных данных и данных организации при работе с	Домашняя работа № 1 Домашняя работа № 2 Коллоквиум Контрольная работа № 1 Контрольная работа № 2 Лабораторные занятия Лекции Экзамен

	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	

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 – 0.2		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Коллоквиум	1,8	*50*
Домашняя работа 1	1,9	*50*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 1		
Промежуточная аттестация по лекциям – нет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – не предусмотрено**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрено		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– не предусмотрено		
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 –0.8		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Контрольная работа 1	1,2	20
Контрольная работа 2	1,4	20
Домашняя работа 2	1,5	20
Выполнение и защита лабораторных работ	1,8	40
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -0.6		
Промежуточная аттестация по лабораторным занятиям –Экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – 0.4**		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
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. Лабораторные занятия

Примерный перечень тем

1. Активный и пассивный сбор информации
2. Атаки на электронную почту
3. Перехват траффика и MITM атаки
4. Подбор паролей
5. Атаки на доменную инфраструктуру
6. OSINT
7. Социальная инженерия
8. Атаки на WiFi
9. Компьютерная криминалистика и расследования инцидентов

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. Контрольная работа № 1

Примерный перечень тем

1. Активный и пассивный сбор информации
2. Атаки на электронную почту
3. Перехват трафика и MITM атаки

Примерные задания

Задание “Активный и пассивный сбор информации”

Выполнить сбор информации используя инструменты сканирования сети, DNS энумерации, поиска сетевых уязвимостей для выбранного вами домена

Задание “Атаки на электронную почту”

Проанализировать выбранный вами домен на наличие уязвимостей спуфинга адресов используя сервис emailrep.io. Реализовать отправку с поддельного адреса на данном домене себе на электронную почту. Проанализировать SMTP-заголовки и указать что в них указывает на подделку адреса отправителя

Задание “Перехват траффика”

Используя вирт. машину с Kali Linux и Windows выполнить ARP-спуфинг используя инструмент Ettercap. Отобразить результат выполнения в виде скриншота ARP-таблицы на атакованном хосте до и после атаки

LMS-платформа − не предусмотрена

5.2.2. Контрольная работа № 2

Примерный перечень тем

1. Подбор паролей
2. Атаки на доменную инфраструктуру

Примерные задания

Задание “Подбор паролей”

Выполнить восстановление паролей с виртуальной машины Windows используя mimikatz и Lazagne

Задание “Атаки на доменную инфраструктуру”

Используя предоставленный дамп реестра и NTDS файл с контроллера домена осуществить извлечение NTLM-хэшей с помощью пакета Impacket. Проанализировать хэши на утечку любым способом

LMS-платформа − не предусмотрена

5.2.3. Коллоквиум

Примерный перечень тем

1. OSINT
2. Атаки на WiFi

Примерные задания

Задание “OSINT”

Собрать информацию о себе, используя фреймворк OSINT-san и SpiderFoot. Оформить в виде отчета

Задание “Атаки на WiFi”

Осуществить анализ уязвимых сетей в кампусах УрФУ, используя возможности портала 3wifi.com

LMS-платформа − не предусмотрена

5.2.4. Домашняя работа № 1

Примерный перечень тем

1. OSINT и социальная инженерия

Примерные задания

Задание “OSINT и социальная инженерия”

Выполнить OSINT в отношении любой организации. Разработать план реализации атаки с использованием социальной инженерии

LMS-платформа − не предусмотрена

5.2.5. Домашняя работа № 2

Примерный перечень тем

1. Компьютерная криминалистика и расследований инцидентов

Примерные задания

Задание “Компьютерная криминалистика”

Используя предоставленные файлы журналов и реестра выполнить восстановление хода атаки с указанием:

1) Построить схему компрометации серверов с учетом времени и использованных учеток

2) Определить как именно злоумышленники проникли за периметр сети

3) Как именно происходило горизонтальное перемещение, какая учетка скомпрометирована где в ней размешались вредоносные программы и хактулы

4) Выполнить поведенческий анализ вредоноса в песочнице, описать как работает и классифицировать

5) Поскольку хост входа был восстановлен из бэкапа – определить куда еще мог попытаться зайти и с какой учеткой злоумышленник когда изучал его логи и реестр (потенциально скомпрометированные хосты не представленные в выборке)

LMS-платформа − не предусмотрена

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

5.3.1. Экзамен

Список примерных вопросов

1. Что из нижеперечисленного не относится к Human-Based социальной инженерии

2. Что из нижеперечисленного не относится к Tech-Based социальной инженерии

3. Какой из нижеперечисленных инструментов и ресурсов предназначен для сбора данных о используемых на домене электронных почтах

4. Какой из нижеперечисленных инструментов и ресурсов предназначен для пассивного (то есть без взаимодействия атакующего) сбора информации о используемых в организации IP-адресах

5. Какой из нижеперечисленных инструментов и ресурсов предназначен для активного сетевого сканирования

6. Какая из перечисленных ниже команд Nmap позволяет получить информацию о операционной системе целевого хоста с использование протокола SMB

7. Какая из перечисленных ниже команд Nmap позволяет получить информацию о пользователях целевого хоста с использование протокола SMB

8. Какая из перечисленных ниже команд Nmap позволяет получить информацию о общих ресурсах целевого хоста с использование протокола SMB

9. Процедура аутентификации

10. В каком разделе реестра представлена информация о сохраненных с помощью оболочки MS Windows Explorer

11. В каком разделе реестра представлена информация выполненных с помощью пункта меню "Выполнить" в MS Windows командах

12. В каком разделе реестра представлена информация о истории поиска (подсказках) в MS Windows Explorer

13. Какие их используемых методов своего закрепления в системе может использовать злоумышленник в ОС Windows …

14. Какой из указанных ниже источников цифровых следов позволяет увидеть не только факт запуска исполняемых файлов но и их историю, а не только время последнего успешного запуска

15. Какая утилита из указанных ниже позволяет восстановить кэш сеансов удаленного рабочего стола пользователя

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.