ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Расследование инцидентов в области информационной безопасности

Код модуля	Модуль
1156876(1)	Защита информации в объектах критической информационной инфраструктуры (КИИ)

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Агафонов Алексей Владимирович	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
2	Князева Наталия Сергеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Расследование инцидентов в области информационной безопасности

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

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Расследование инцидентов в области информационной безопасности

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**
ОПК-6 -Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации,	З-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа З-2 - Изложить содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю) по защите информации П-1 - Осуществлять обоснованный выбор	Домашняя работа Зачет Контрольная работа Лабораторные занятия Лекции

Федеральной службы по техническому и экспортному контролю	нормативной базы в области защиты информации ограниченного доступа У-1 - Систематизировать и классифицировать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах	
ОПК-15 -Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием	З-1 - Описывать особенности инструментального мониторинга качества обслуживания в телекоммуникационных системах и сетях П-1 - Проводить инструментальный мониторинг качества обслуживания от несанкционированного доступа У-1 - Анализировать защищенность информации от несанкционированного доступа в телекоммуникационных системах и сетях	Домашняя работа Зачет Контрольная работа Лабораторные занятия Лекции
ОПК-20 -Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям	З-1 - Определять и объяснять существующие виды уязвимостей П-1 - Оформлять отчеты по выявленным уязвимостям У-1 - Обосновывать методику выявления уязвимостей в защищенных сетевых ресурсах	Домашняя работа Зачет Контрольная работа Лабораторные занятия Лекции

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
контрольная работа	10,3	*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 – 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 –0.5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	10,15	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -1		
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, 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. Анализ событий аудита ОС MS Windows
2. Исследование процессов в ОС Linux
3. Наблюдение и аудит в ОС Linux
4. Анализ и восстановление данных файловой системы NTFS
5. Восстановление данных программными средствами ОС Linux
6. Создание и регистрация индикаторов
7. Сбор данных компьютерного инцидента

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

Примерный перечень тем

1. Получение доступа к информации
2. Аудит событий безопасности
Примерные задания
1. Программа dd способна извлечь:
Ответ:
(1) данные, которых файловая система не может видеть
(2) перезаписанные данные
(3) удаленные данные

2. Программу dd целесообразно применять для:
Ответ:
(1) побитного копирования данных с созданием зеркального образа данных на другом жестком диске или разделе диска
(2) побитного копирования данных с созданием одного большого файла
(3) создания логических копий файловых систем

3. Программа dd:
Ответ:
(1) напрямую обращается к носителю
(2) обращается к носителю без посредничества файловой системы
(3) обращается к носителю средствами файловой системы

4. После устранения непосредственной опасности ИС необходимо:
Ответ:
(1) контратаковать систему нарушителей
(2) обратиться в полицию за квалифицированной помощью
(3) сделать копии всех важных данных для просмотра в автономном режиме в соответствии с догматами надлежащего судебного анализа

5. dd - это:
Ответ:
(1) средство восстановления дисков и файлов
(2) средство тиражирования дисков и файлов
(3) средство необратимого удаления данных

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем
1. Реагирование и ликвидация последствий компьютерных инцидентов
Примерные задания
1. На предложенной виртуальной машине под управлением ОС Linux найти процесс, открывший самое большое количество файлов, и перечислить эти файлы.

2. На предложенной виртуальной машине под управлением ОС MS Windows найти процесс, открывший самое большое количество файлов, и перечислить эти файлы.

3. На предложенной системе найти все открытые сокеты (сетевые и UNIX).

4. Определить имя удаленного файла и его каталог размещения с использованием i-node.

5. Найти остаточную информацию больших файлов в файловой системе NTFS.

6. Клонировать флэш-носитель информации средствами WinHex.

7. Оформите отчет по домашней работе

LMS-платформа − не предусмотрена

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

5.3.1. Зачет

Список примерных вопросов

1. 1. Журнал событий безопасности 2. Системный монитор 3. Средства наблюдения за процессами 4. Способы автоматического запуска и остановки программ 5. Сокрытие процессов 6. Аудит событий и его безопасность 7. . Устройство файловой системы NTFS 8. Архитектура файловых систем ext*fs 9. Алгоритмы логического удаления и восстановления файлов 10. Нормативное регулирование деятельности центров ГосСОПКА 11. Поиск данных на NTFS-разделах по контексту и временным отметкам 12. Реагирование на компьютерный инцидент 13. Технические параметры компьютерного инцидента 14. Временные отметки файлов 15. Подключение и взаимодействие с НКЦКИ

LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	**Контрольно-оценочные мероприятия**
Профессиональное воспитание	целенаправленная работа с информацией для использования в практических целях	Технология самостоятельной работы	ОПК-6	З-1	Домашняя работа Зачет Контрольная работа Лабораторные занятия
			ОПК-15	З-1	