

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ**

Методы обнаружения и противодействия компьютерным атакам

Код модуля
1156875(1)

Модуль
Методы и системы обнаружения компьютерных
атак

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	Пономарева Ольга Алексеевна		старший преподаватель	УНЦ ИБ
3	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Согласовано:

Управление образовательных программ

Т.Г. Комарова

Авторы:

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Методы обнаружения и противодействия компьютерным атакам

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 Методы обнаружения и противодействия компьютерным атакам

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-13 -Способен оценивать технические возможности, анализировать угрозы и выработать рекомендации по построению элементов информационно-телекоммуникационной и инфраструктуры с учетом обеспечения требований информационной безопасности	З-1 - Распознавать угрозы информационно-телекоммуникационной структуры З-2 - Объяснять модели угроз и оценивать их риски в информационно-телекоммуникационных инфраструктурах П-1 - Разрабатывать рекомендации по обеспечению информационной безопасности на элементном уровне информационно-телекоммуникационной инфраструктуры У-1 - Оценивать технические возможности обеспечения информационной безопасности	Домашняя работа Зачет Контрольная работа Лабораторные занятия Лекции

	У-2 - Анализировать возможные угрозы в информационно-телекоммуникационных инфраструктурах	
--	---	--

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
<i>контрольная работа</i>	8,4	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
<i>домашняя работа</i>	8,15	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. Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования
2. Копирование содержимого оперативной памяти СВТ и получение данных операционных систем

3. Копирование протоколов (журналов) регистрации
 4. Копирование сетевого трафика
 5. Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление
 6. Программный инструментарий эксперта-криминалиста
 7. Механизмы компьютерного следообразования
- 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. Обработки технических данных в рамках реагирования на инциденты ИБ.
2. Программный инструментарий эксперта-криминалиста.

Примерные задания

Контрольная работа проводится для определения теоретической подготовки студентов по темам контрольных работ.

Тестовые задания не предполагается размечать в открытом доступе.

LMS-платформа – не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Изучить методы сбора технических данных с компонентов информационной инфраструктуры на инциденты ИБ
2. Изучить методы криминалистического копирования энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования

Примерные задания

Домашняя работа направлена на практическое применение методов, их апробирование в ограниченных условиях. По результатам проведения исследования составить отчет.

LMS-платформа – не предусмотрена

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

5.3.1. Зачет

Список примерных вопросов

1. Понятие инцидентов ИБ.
2. Нормативная база в сфере управления инцидентами ИБ.
3. Система управления инцидентами ИБ.
4. Обработка событий и инцидентов ИБ.
5. Реагирование на инциденты ИБ.
6. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ.
7. Сбор технических данных с компонентов информационной инфраструктуры.
8. Поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформление.
- 9.

Распространение (передача) выделенной и оформленной содержательной (семантической) информации. 10. Обеспечение наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры. 11. Сбор и фиксация информации об инцидентах ИБ. 12. Проверка целостности (неизменности) собранных данных, маркирование носителей собранных данных. 13. Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования. 14. Копирование содержимого оперативной памяти СВТ и получение данных операционных систем. 15. Копирование протоколов (журналов) регистрации. 16. Копирование сетевого трафика. 17. Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление. 18. Структура протокола обработки технических данных. 19. Технические средства и инструменты для сбора и обработки технических данных

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	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-13	3-2	Домашняя работа Зачет Контрольная работа Лабораторные занятия Лекции