ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Спецкурс 2

Код модуля
1163600(1)

Модуль
Спецкурс 2

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Карпушин Андрей Валерьевич	без ученой степени, без ученого звания	Старший преподаватель	интеллектуальных информационных технологий
2	Поршнев Сергей Владимирович	доктор технических наук, профессор	Профессор	Учебно-научный центр ”Информационная безопасность”

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Карпушин Андрей Валерьевич, Старший преподаватель, интеллектуальных информационных технологий**
- **Поршнев Сергей Владимирович, Профессор, Учебно-научный центр "Информационная безопасность"**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Спецкурс 2

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

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Спецкурс 2

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-1 -Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства З-2 - Описать психологические аспекты информационной безопасности в современном обществе З-3 - Сделать обзор основных методов обеспечения информационной безопасности П-1 - Иметь практический опыт выбора базовых методов	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен

	выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности У-1 - Определять оптимальные методы обеспечения информационной безопасности	
ПК-2 -Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	З-1 - Изложить состав, классификацию, особенности функционирования программных средств системного и прикладного назначений П-1 - Иметь навыки использования системного программного обеспечения для решения задач профессиональной деятельности П-2 - Иметь навыки использования прикладного программного обеспечения для решения задач профессиональной деятельности У-1 - Рационально использовать функциональные возможности программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен
ПК-3 -Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	З-1 - Изложить состав и содержание Российских и международных нормативных правовых актов, нормативных и методических документов, межгосударственных и международных стандартов, регламентирующих деятельность по защите информации З-2 - Изложить методологию управления информационной безопасностью, основанную на	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен

	нормативных и методических документах П-1 - Осуществлять обоснованный выбор методов поиска и анализа нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации П-2 - Разрабатывать проекты нормативно-правовых актов и организационно-распорядительных документов, регламентирующих деятельность по защите информации У-1 - Применять действующую нормативную базу, нормативные правовые акты, нормативные и методические документы для принятия правовых и организационных мер по защите информации	
ПК-9 -Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	З-1 - Описать основные методы администрирования и контроля функционирования средств и систем защиты информации телекоммуникационных систем З-2 - Описать основные методы инструментального мониторинга и аудита защищенности телекоммуникационных систем П-1 - Иметь практический опыт выбора средств контроля функционирования средств и систем управления информационной безопасностью телекоммуникационных систем У-1 - Администрировать средства и системы защиты информации телекоммуникационных систем	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен

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	5,10	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – экзамен **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**
домашняя работа	5,6	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, 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)		
№	**Содержание уровня**	**Шкала оценивания**

п/п	выполнения критерия оценивания результатов обучения (выполненное оценочное задание)	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. Методы используемые OSINT
2. Whonix^
3. Блок схемы Michael Bazell
4. GEOINT
5. КА, КИ, обнаружение, регистрация, реагирование
6. CyberKillChain
7. MITRE&ATTACK
8. Оркестрация процессов реагирования
9. Методологии DFIR
10. Сбор энергонезависимой информации в ОС Windows
11. Поиск следов компрометации в ОС Windows
12. Поиск следов закрепления в ОС Windows
13. Анализ журналов МЭ, DNS, DHCP

14. Исследование сетевого трафика

Примерные задания

Предоставить конспект с основными тезисами по одной из тем практических занятий. Примерный перечень тем:

- Методы используемые OSINT
- Whonix
- Блок схемы Michael Bazell
- GEOINT
- КА, КИ, обнаружение, регистрация, реагирование
- CyberKillChain
- MITRE&ATTACK
- Оркестрация процессов реагирования
- Методология DFIR
- Сбор энергонезависимой информации в ОС Windows
- Поиск следов компрометации в ОС Windows
- Поиск следов закрепления в ОС Windows
- Анализ журналов МЭ, DNS, DHCP
- Исследование сетевого трафика

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. Заражение вирусом-шифровальщиком

Примерные задания

Для обучающихся будет сформулировано кейс-задание. Задача обучающихся - определить и обосновать необходимые мероприятия для решения смоделированной ситуации. Пример такого задания:

Организация была заражена вирусом-шифровальщиком через атаку на RDP-сервисы. Какие меры вы предпримите для решения данной ситуации? Обоснуйте свое решение.

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Подделка платежных поручений

Примерные задания

Для обучающихся будет сформулировано кейс-задание. Задача обучающихся - определить и обосновать необходимые мероприятия для решения смоделированной ситуации. Пример такого задания:

Произошла атака на организацию с целью заражения вредоносным ПО семейства BuhTrap. Какие меры вы предпримите для решения данной ситуации? Обоснуйте свое решение.

LMS-платформа − не предусмотрена

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

5.3.1. Экзамен

Список примерных вопросов

1. Методы используемые OSINT
2. Приватность и анонимность - Windows или Linux. Оценка защищенности и приватности данных JC
3. Whonix^: принципы работы, настройка параметров конфигурации, слабые места
4. Настройка рабочего места: ОС, Хост, сеть, VPN
5. Блок схемы Michael Bazell
6. Использование поисковых систем (ClearNet)
7. Поиск в DarkNet
8. Сбор информации о ФЛ
9. Сбор информации о ЮЛ
10. CounterOSINT - ФЛ
11. CounterOSINT - ЮЛ
12. Методы поиска по изображению
13. Open - source инструменты OSINT
14. GEOINT: Принципы поиска и определения координат объекта по изображению
15. КА, КИ, обнаружение, регистрация, реагирование
16. CyberKillChain
17. MITRE&ATTACK
18. PoP (Pyramid of Pain)
19. Threat Hunting
20. Процесс обнаружения инцидента. Сбор данных об инфраструктуре (SIEM, XDR, EDR, NDR, NTA, NGFW, Sysmon).
21. Процесс обнаружения инцидента. Агрегация данный и формирование инцидентов
22. Оркестрация процессов реагирования (IRP/SOAR)
23. Момент инцидента и первые действия (проверка на ЛПС, приоритезация, сбор информации, эскалация)
24. Реагирование средствами AD
25. Реагирование средствами сетевого оборудования
26. Реагирование средствами XDR
27. Физическое реагирование
28. Ликвидация последствий (восстановление)
29. Нарушение политик информационной безопасности
30. Методологии DFIR
31. Сбор энергонезависимой информации в ОС Windows
32. Сбор энергонезависимой информации в ОС Linux
33. Поиск следов компрометации в ОС Windows

34. Поиск следов запуска программного обеспечения в ОС Windows
35. Поиск следов закрепления в ОС Windows
36. Поиск следов горизонтального продвижения в ОС Windows
37. Поиск следов компрометации в ОС Linux
38. Поиск следов закрепления в ОС Linux
39. Поиск следов горизонтального продвижения в ОС Linux
40. Методология сетевого криминалистического анализа
41. Средства сбора и анализа журналов (ELK-стэк) для сетевого криминалистического анализа
42. Анализ журналов МЭ, DNS, DHCP
43. Исследование сетевого трафика

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	профориентационная деятельность	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-2	У-1	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен