МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

«СОГЛАСОВАНО»
Руководитель ОП
Подпись Дремлюга Р.И.

«УТВЕРЖДАЮ»
И.о. директора департамента
Боршевников А.Е.
«27» сентября 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Расследование инцидентов кибербезопасности
Направление подготовки - 09.04.01 Информатика и вычислительная техника
(Кибербезопасность)

Форма подготовки очная

курс 2 семестр 3
лекции 00 час.
практические занятия 54 час.
лабораторные работы 00 час.
в том числе с использованием МАО практические занятия 54 час.
всего часов аудиторной нагрузки 54 час.
самостоятельная работа 90 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 3 семестр

Рабочая программа дисциплины разработана в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 918 (с изменениями и дополнениями)

Рабочая программа обсуждена на заседании департамента информационной безопасности протокол № 1 от 27 сентября 2021 г.

И.о директора департамента информационной безопасности Боршевников А.Е.

Составитель (ли): Антонова А.А.

Владивосток
2021

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

I. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является изучение студентами основных теоретических вопросов касающихся инцидентов кибербезопасности подразделяются и эффективного управления инцендентами, поскольку даже случайные киберинциденты могут повлечь за собой разрушительные последствия.

Задачи:

- управление инцидентами кибербезопасности;
- изучение фаз подготовки к отражению инцидента кибербезопасности, сдерживания и устранения инцидента и его последствий;
- восстановление работоспособности затронутых инцидентом информационных систем, а также анализ причин произошедшего и принятие корректирующих мер.

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы, характеризуют формирование следующих компетенций:

Профессиональные компетенции выпускников и индикаторы их достижения:

Тип задач	Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
производственно-технологический	ПК-2 Способен проводить анализ безопасности компьютерных систем	ПК-2.2 Оценивает риски, связанные с осуществлением угроз безопасности в отношении компьютерных систем, и механизмы безопасности компьютерной системы в точки зрения их адекватности существующим рискам
	ПК-3 Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-3.2 Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов
	ПК-4 Способен управлять рисками информационных технологий и кибербезопасностью	ПК-4.2 Формирует и декомпозирует цели управления информационной безопасностью

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ПК-2.2 Оценивает риски, связанные с осуществлением угроз безопасности в отношении компьютерных систем, и механизмы безопасности компьютерной системы в точки зрения их адекватности существующим рискам	Знает основные методы оценки рисков связанных с осуществлением угроз безопасности в отношении компьютерных систем.
	Умеет применять на практике навыки оценки рисков связанных с угрозами безопасности в отношении компьютерных систем
	Владеет навыками применения механизмов безопасности компьютерной системы с точки зрения их адекватности существующим рискам
ПК-3.2 Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов	Знает виды компьютерных преступлений.
	Умеет выбирать методы для эффективного прогнозирования
	Владеет приемами и инструментами прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов.
ПК-4.2 Формирует и декомпозирует цели управления информационной безопасностью	Знает способы формирования целей управления информационной безопасностью.
	Умеет оценивать трудоемкость управления информационной безопасностью.
	Владеет навыками формирования и декомпозиции целей управления информационной безопасностью.

II. ТРУДОЁМКОСТЬ ДИСЦИПЛИНЫ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ

Общая трудоемкость дисциплины составляет 4 зачётных единицы (144 академических часа).

Видами учебных занятий и работы обучающегося по дисциплине могут являться:

Обозначение	Виды учебных занятий и работы обучающегося
Пр	Практические занятия
СР	Самостоятельная работа обучающегося в период теоретического обучения
Контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

Структура дисциплины:

Форма обучения – очная.

№	Наименование раздела дисциплины	Семестр	Количество часов по видам учебных занятий и работы обучающегося						Формы текущего контроля успеваемости и промежуточной аттестации
			Лек	Лаб	Пр	ОК	СР	Контроль	
1	Раздел 1.	3			20				УО-1, ПР-7; ПР-9;

2	Раздел 2.	3			34				УО-1, ПР-7; ПР-9;
	Итого:				54		54	36	экзамен

III. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Не предусмотрены

IV. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические работы (54 час.)

Раздел 1.

Практическое занятие № 1. (6 час)

1. Источники событий ИБ.
2. Системы управления событиями ИБ.
3. Системы управления информацией о безопасности и событиями ИБ.
4. Cyber Threat Hunting (поиск киберугроз).
5. Cyber Threat Intelligence (кибербразведка).
6. Индикаторы компрометации (IoCs).

Практическое занятие № 2. (8 час)

1. Подготовка
2. Детектирование
3. Анализ
4. Сдерживание/локализация
5. Устранение
6. Восстановление
7. Пост-инцидентные действия

Практическое занятие № 3. - Центры SOC (Security Operations Center) (6 час)

1. Задачи SOC.
2. Технологии SOC-Центров.
3. Процессы SOC-Центров.
4. Сотрудники SOC-Центров.

Раздел 2.

Практическое занятие № 4. «SIEM - Security Information and Event Managemen.» (**8 час.)**

1. Получение журналов с разнообразных средств защиты.
2. Нормализация полученных данных.
3. Таксономия нормализованных данных.
4. Корреляция классифицированных событий.

5. Создание инцидента, предоставление инструментов для проведения расследования.
6. Хранение информации о событиях и инцидентах в течение длительного времени.
7. Быстрый поиск по хранящимся в SIEM данным.

Практическое занятие № 5. «Cyber Threat Intelligence» **(6 час.)**

1. TI-фиды набор индикаторов компрометации (Indicators of Compromise (IoC)).
2. Индикатор компрометации.
3. Cyber Threat Hunting (поиск киберугроз) .
4. Cyber Threat Intelligence (кибербразведка).

Практическое занятие № 6. «Индикаторы компрометации (IoCs)» **(8 час.)**

1. Статические объекты.
2. Динамические объекты.

Практическое занятие № 7. «Стандарты и протоколы для получения данных кибербразведки.» (**6 час.)**

1. STIX/TAXII
2. OpenIOC
3. CybOX.

Практическое занятие №8. «Технологии SOC-Центров.» **(6 час.)**

1. SIEM - Security Information and Event Management, системы управления информацией о безопасности и событиями информационной безопасности;
2. IRP - Incident Response Platform, платформы реагирования на инциденты информационной безопасности;
3. SOAR - Security Orchestration, Automation and Response, системы управления, автоматизации и реагирования на инциденты;
4. SGRC - Security Governance, Risk-management and Compliance, системы управления информационной безопасностью, рисками и соответствия законодательству.

V. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

План-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию.

Примерная дата проведения	Наименование контрольного мероприятия	Форма контроля	Нормы времени на выполнение
1-7 недели	Работа с конспектом	Просмотр и проверка выполнения самостоятельной работы преподавателем, обсуждение результатов выполненной работы на занятии	18 часов
8-13недели	Работа с конспектом, работа с литературой, подготовка к проектной работе	Устный опрос, собеседование с группой.	18 часов
14-18 недели	Подготовка проектов	Презентация проектов	18 часов
Итого			54 часов

Учебно-методическое обеспечение самостоятельной работы студента по дисциплине «Расследование киберинцидентов» предусматривает:

- поиск дополнительной литературы, к которой студенты могут приобщаться при возникновении особой заинтересованности в конкретной теме;
- определение перечня контрольных вопросов, позволяющих студентам самостоятельно проверить качество полученных знаний;
- организацию консультаций преподавателя со студентами для разъяснения вопросов, вызывающих у студентов затруднения при самостоятельном освоении учебного материала.

Дополнительными формами самостоятельной работы являются групповые и индивидуальные задания, выступающие продолжением аудиторных занятий и направленные на овладение практическими навыками по основным разделам дисциплины.

Материалы для организации самостоятельной работы студентов

Самостоятельная работа студентов состоит из подготовки к практическим занятиям, работы над рекомендованной литературой, написания докладов по теме занятия, подготовки презентаций, решения творческих задач, подготовка проектов.

При организации самостоятельной работы преподаватель должен учитывать уровень подготовки каждого студента и предвидеть трудности, которые могут возникнуть при выполнении самостоятельной работы. Преподаватель дает каждому студенту индивидуальные и дифференцированные задания. Некоторые из них могут осуществляться в

группе (например, подготовка доклада и презентации по одной теме могут делать несколько студентов с разделением своих обязанностей – один готовит научно-теоретическую часть, а второй проводит анализ практики).

Методические рекомендации для написания конспектов

Конспекты, написанные от руки, предоставляются преподавателю для оценки (зачёт/незачёт). Учитывая, что в большинстве случаев тексты первоисточников весьма объёмные, для конспектирования можно выбрать только страницы, разделы или главы (30-50 стр. печатного текста). Объём законспектированного текста в тетради определяется самим студентом.

Методические указания к самостоятельному выполнению проектного задания

Выполнение проектного задания (ТЗ) в рамках дисциплины является обязательным и предполагает индивидуальную или групповую работу.

Этапы работы над творческим заданием:

1. Определение темы проекта. На этом этапе следует определить, будет ли выполняться проект индивидуально или в группе.

2. Формулировка проблемы, постановка цели и задач.

3. Организация деятельности. Если проект выполняется в группе, следует организовать рабочую группу, определить роли каждого участника рабочей группы, спланировать совместную или индивидуальную деятельность по решению задач проекта.

4. Активная и самостоятельная работа над проектом; консультации преподавателя; оформление полученных результатов.

5. Подготовка к защите проекта.

Проект считается выполненным полностью в случае

1. Предоставления полного объема учебных материалов по заранее утвержденной теме, полностью раскрывающих заявленную тему;

2. Предоставления материалов на электронном носителе и в печатном виде;

3. Соответствия представленных материалов требованиям по оформлению;

4. Наличия в материалах проекта описания методики использования ЦОР;

5. Успешной презентации и защиты проекта

Методические рекомендации для подготовки презентаций

Общие требования к презентации:

- презентация не должна быть меньше 10 слайдов;
- первый лист – это титульный лист, на котором обязательно должны быть представлены: название проекта; фамилия, имя, отчество автора;

- следующим слайдом должно быть содержание, где представлены основные этапы (моменты) презентации; желательно, чтобы из содержания по гиперссылке можно перейти на необходимую страницу и вернуться вновь на содержание;
- дизайн-эргономические требования: сочетаемость цветов, ограниченное количество объектов на слайде, цвет текста;
- последними слайдами презентации должны быть глоссарий и список литературы.

Презентация должна отражать тематику реализуемого проекта.

VI. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

Для текущей аттестации при изучении дисциплины «Расследование киберинцидентов» используются следующие оценочные средства:

1) Устный опрос (УО):

Собеседование (консультация с преподавателем) (УО-1)

2) Письменные работы (ПР):

Конспект (ПР-7)

№ п/п	Контролируемые разделы / темы дисциплины	Код и наименование индикатора достижения	Результаты обучения	Оценочные средства	
				текущий контроль	промежуточная аттестация
	Раздел 1. Раздел 2.	ПК-2.2 Оценивает риски, связанные с осуществлением угроз безопасности в отношении компьютерных систем, и механизмы безопасности компьютерной системы в точки зрения их адекватности существующим рискам	Знает	УО-1	Вопросы к экзамену 1-4,
			Умеет	ПР-7	
			Владеет		

		ПК-3.2 Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов	Знает.	УО-1	Вопросы к экзамену 5-8
			Умеет.	ПР-7	
			Владеет	УО-1	
		ПК-4.2 Формирует и декомпозирует цели управления информационной безопасностью	Знает	УО-1	Вопросы к экзамену 9-10
			Умеет	ПР-7	
			Владеет	ПР-7	

VII. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(печатные и электронные издания)

1. Data Mining for Service [Electronic resource] / Katsutoshi Yada. — Springer Berlin Heidelberg, 2014. — 291 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:857706&theme=FEFU
2. Principles of Big Data [Electronic resource] / Jules J. Berman. — Morgan Kaufmann, 2013. — 288 с. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:809472&theme=FEFU
3. Воронова Л.И. Big Data. Методы и средства анализа [Электронный ресурс] : учебное пособие / Л.И. Воронова, В.И. Воронов. — Электрон. текстовые данные. — М. : Московский технический университет связи

и информатики, 2016. — 33 c. — 2227-8397. — Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=IPRbooks:IPRbooks-61463&theme=FEFU

Дополнительная литература

(печатные и электронные издания)

1. Апокин, И.А. Развитие вычислительной техники и систем на ее основе /И. А. Апокин // Новости искусственного интеллекта. -2004. - №1. – Режим доступа: http://www.computer-museum.ru/galglory/apokin.htm
2. Апокин, И. А. Развитие вычислительных машин /И. А. Апокин, Л. Е. Майстров. - М., Наука, 2004. – Режим доступа: http://bookre.org/reader?file=474073
3. Бахвалов, Н. С. Численные методы [Электронный ресурс] / Н. С. Бахвалов, Н. П.Жидков, Г. М. Кобельков. - 7-е изд. (эл.). - М. : БИНОМ. Лаборатория знаний, 2012. - 636 с. : ил. - (Классический университетский учебник). - http://storage.library.opu.ua/online/books/kaf_is/bahvalov_.pdf
4. Быченков, Ю. В. Итерационные методы решения седловых задач [Электронный ресурс] / Ю. В. Быченков, Е. В. Чижонков. - М . : БИНОМ. Лаборатория знаний, 2010. - 349 с.
5. Воеводин В.В., Воеводин Вл. В. Параллельные вычисления // БХВ-Петербург, СПб., 2002, 609 с. Компьютеры в Европе. Прошлое, настоящее и будущее. В кн.: Труды международного симпозиума по истории создания первых ЭВМ и вкладу европейцев в развитие компьютерных технологий. – Киев, 1998. Режим доступа: http://rutracker.org/forum/viewtopic.php?t=2465944
6. Ершов, А. Компьютеризация школы и математическое образование /А. Ершов // "Программирование". – 2002. - № 1. (см. также "Информатика и образование", № 5-6, 1992).
7. Ершов, А. П. Информатика: предмет и понятие /А. Ершов // Кибернетика. Становление информатики. - М.: Наука, 2006.
8. Ершов, А. П. Становление программирования в СССР /А.П. Ершов, М. Р. Шура-Бура // Кибернетика. -2006. - № 6.
9. К 100-летию со дня рождения С.А. Лебедева. Информационные технологии и вычислительные системы. - № 3. - 2002. Режим доступа:
10. Левин, В.И. Носители информации в цифровом веке / Под общ. ред. Д.Г. Красковского. - М.: КомпьютерПресс, 2000. Режим доступа: http://www.slideshare.net/liliya_m/c-13358003

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. «ИТ-образование в Рунете». Образовательные ресурсы Рунета: http://ifets.ieee.org/russian/depository/resourse.htm
2. «Российский общеобразовательный портал»: http://www.school.edu.ru/
3. «Издание литературы в электронном виде»: http://www.magister.msk.ru/library/library.htm
4. Annual Reviiew: http://www.annualreviews.org/ebvc
5. Scopus - мультидисциплинарная реферативная база данных: http://www.scopus.com/
6. Единая коллекция образовательных ресурсов: http://school-collection.edu.ru/catalog/
7. Информационные ресурсы Российской Библиотечной Ассоциации (РБА): http://www.rba.ru/
8. Каталог электронных ресурсов научной библиотеки ДВФУ: http://www.dvfu.ru/web/library/elib
9. Коллекция журналов издательства Elsevier на портале ScienceDirect: http://www.sciencedirect.com/.
10. Научная электронная библиотека (НЭБ): http://www.elibrary.ru/
11. Портал «Гуманитарное образование» http://www.humanities.edu.ru/index.html
12. Российская государственная библиотека (электронный каталог): http://www.rsl.ru/
13. Университетская информационная система Россия (УИС Россия): http://uisrussia.msu.ru
14. Электронная библиотечная система «Айбукс»: http://ibooks.ru/
15. Электронная библиотечная система «Университетская библиотека»: www.biblioclub.ru.
16. Электронная библиотечная система издательства «Лань»: http://e.lanbook.com/

Перечень информационных технологий и программного обеспечения

При осуществлении образовательного процесса студентами и профессорско-преподавательским составом используется следующее программное обеспечение: Microsoft Office (Access, Excel, PowerPoint, Word и т. д), Open Office, Skype, программное обеспечение электронного ресурса сайта ДВФУ, включая ЭБС ДВФУ.

VIII.МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Работа с теоретическими материалами. Изучение дисциплины следует начинать с проработки тематического плана лекций, уделяя особое внимание структуре и содержанию темы и основных понятий. Изучение «сложных» тем следует начинать с составления логической схемы основных понятий, категорий, связей между ними. Целесообразно прибегнуть к классификации материала, в частности при изучении тем, в которых присутствует большое количество незнакомых понятий, категорий, теорий, концепций, либо насыщенных информацией типологического характера. Студенты должны составлять конспекты лекций, систематически готовиться к практическим занятиям, вести глоссарий и быть готовы ответить на контрольные вопросы в ходе лекций и аудиторных занятий. Успешное освоение программы курса предполагает прочтение ряда оригинальных работ и выполнение практических заданий.

Подготовка и выполнение практических заданий. По каждой теме дисциплины предлагаются вопросы и практические задания. Перед выполнением заданий изучите теорию вопроса, предполагаемого к исследованию. Самостоятельная работа студентов заключается:

- в подготовке к практическим занятиям в форме консультаций и дискуссий;
- в выполнении индивидуальных и групповых заданий,
- в подготовке к защите курсовой работы,
- в подготовке к итоговому собеседованию.

Цель практических (семинарских) занятий – научить студентов самостоятельно анализировать учебную и научную литературу и вырабатывать у них опыт самостоятельного мышления по проблемам курса, а также выработать навыки практического применения теоретических знаний. Как правило, семинары проводятся в виде практик-консультаций с элементами дискуссии. При этой форме работы отдельным студентам могут поручаться сообщения по тому или иному вопросу, а также ставя дополнительные вопросы, как всей аудитории, так и определенным участникам обсуждения.

Самостоятельная работа студентов, предусмотренная учебным планом, соответствует более глубокому усвоению изучаемого курса, формирует навыки исследовательской работы и ориентирует на умение применять теоретические знания на практике.

Материалом для подготовки могут стать конспекты лекций, профессиональная литература, учебно-методическое обеспечение дисциплины.

Методические рекомендации для написания конспектов

Конспекты, написанные от руки, предоставляются преподавателю для оценки (зачёт/незачёт). Учитывая, что в большинстве случаев тексты первоисточников весьма объёмные, для конспектирования можно выбрать только страницы, разделы или главы (30-50 стр. печатного текста). Объём законспектированного текста в тетради определяется самим студентом.

Методические указания к выполнению проектного задания

Выполнение проектного задания в рамках дисциплины является обязательным и предполагает индивидуальную или групповую работу.

Проект – совокупность мероприятий, направленных на достижение определённой и четко структурированной цели в конкретные сроки с привлечением оптимальных средств и ресурсов.

Проект представляет собой конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.

Технология разработки проектов включает в себя следующие этапы:

разработка замысла проекта в соответствии с требованиями программы по следующей структуре:

- аудитория проекта (т.е. характеристика проблем целевой группы и лиц, непосредственно получающих пользу от проекта);
- цели и задачи проекта;
- содержание проекта;
- организация-исполнитель (или форма реализации проекта);
- планируемые результаты и критерии эффективности.

Проект считается выполненным полностью в случае

1. Предоставления полного объема учебных материалов по заранее утвержденной теме, полностью раскрывающих заявленную тему;

2. Предоставления материалов на электронном носителе и в печатном виде;

3. Соответствия представленных материалов требованиям по оформлению;

4. Наличия в материалах проекта описания методики использования ЦОР;

5. Успешной презентации и защиты проекта

Проект считается выполненным полностью в случае

1. Предоставления полного объема учебных материалов по заранее утвержденной теме, полностью раскрывающих заявленную тему;

2. Предоставления материалов на электронном носителе и в печатном виде;

3. Соответствия представленных материалов требованиям по оформлению;

4. Наличия в материалах проекта описания методики использования ЦОР;

5. Успешной презентации и защиты проекта

IX. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные занятия по дисциплине проводятся в помещениях, оснащенных соответствующим оборудованием и программным обеспечением.

Перечень материально-технического и программного обеспечения дисциплины приведен в таблице.

Материально-техническое и программное обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Мультимедийная аудитория: G467	Проектор DLP, 3000 ANSI Lm, WXGA 1280x800, 2000:1 EW330U Mitsubishi,; Моноблок HP ProOne 440 G3 23.8" All-in-One, диагональ экрана 23.8", разрешение экрана 1920x1080, Bluetooth, Wi-Fi, операционная система: Windows 10 Enterprise, оптический привод DVD, процессор: Intel Core i5-7500T, размер оперативной памяти: 8 ГБ, видеопроцессор: Intel HD Graphics 630, объем жесткого диска: 1Tb. Беспроводные ЛВС для обучающихся обеспечены системой на базе точек доступа 802.11a/b/g/n 2x2 MIMO(2SS). AfterEffects	Techdesigner, MAX8, VVVV, Adobe Photoshop, Adobe Premier, Adobe
Мультимедийная аудитория: G469	Проектор DLP, 4000 ANSI Lm, 1920x1080, 2000:1 FD630u Mitsubishi; Проектор DLP, 2800 ANSI Lm, 1920x1080, 2000:1 GT1080 Optoma; Проектор DLP, 3000 ANSI Lm, WXGA	Techdesigner, MAX8, VVVV, Adobe Photoshop, Adobe Premier, Adobe

	1280x800, 2000:1 EW330U Mitsubishi; Беспроводные ЛВС для обучающихся обеспечены системой на базе точек доступа 802.11a/b/g/n 2x2 MIMO(2SS). Специализированное оборудование: Платформа Adruino UNO, Бесконтактный сенсорный Microsoft Kinnect 2.0, Аудио система Dialog 2.0, MIDI контроллер Playtron, Одноплатный компьютер Raspberry PI	

Рабочие места для людей с ограниченными возможностями здоровья оснащены дисплеями и принтерами Брайля; оборудованы: портативными устройствами для чтения плоскопечатных текстов, сканирующими и читающими машинами, видеоувеличителем с возможностью регуляции цветовых спектров; увеличивающими электронными лупами и ультразвуковыми маркировщиками.

В целях обеспечения специальных условий обучения инвалидов и лиц с ограниченными возможностями здоровья в ДВФУ все здания оборудованы пандусами, лифтами, подъемниками, специализированными местами, оснащенными туалетными комнатами, табличками информационно-навигационной поддержки.

X. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценочных средств

Для дисциплины «Расследование киберинцидентов» используются следующие оценочные средства:

1. Устный опрос (УО-1),
2. Конспект (ПР-7),
3. Проект (ПР-9).

	Наименование оценочного средства	**Краткая характеристика оценочного средства**	**Представление оценочного средства в фонде**
УО-1	Устный опрос	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения	Литература для конспектирования

ПР-9	Проект	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе	Задания для проекта

Текущая аттестация студентов

Текущая аттестация студентов по дисциплине «Расследование киберинцидентов» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация по дисциплине «Расследование киберинцидентов» проводится в форме контрольных мероприятий (устного опроса, выступления с проектом, тестирования, конспекта первоисточника) по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

− учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

− степень усвоения теоретических знаний;

− уровень овладения практическими умениями и навыками по всем видам учебной работы;

− результаты самостоятельной работы.

Каждому объекту оценивания присваивается конкретный балл. Составляется календарный план контрольных мероприятий по дисциплине и внесения данных в АРС. По окончании семестра студент набирает определенное количество баллов, которые переводятся в пятибалльную систему оценки.

Критерии оценки устного опроса:

Результат работы студента в ходе устного ответа в виде собеседования с преподавателем оценивается по следующим критериям: полнота раскрытия вопросов; степень самостоятельности выполнения задания; и его презентация; исполнение сроков предоставления выполненных заданий; способность отвечать на вопросы преподавателя и студентов в ходе устного опроса по заданной тематике.

✓ 100-86 баллов выставляется, если студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Продемонстрировано знание и владение

навыком самостоятельной исследовательской работы по теме вопроса. Фактических ошибок, связанных с пониманием проблемы, нет

- ✓ 85-76 баллов работа студента характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет.
- ✓ 75-61 баллов проведен достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимание базовых основ и теоретического обоснования выбранной темы. Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в смысле или содержании проблемы
- ✓ 60-50 баллов если работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы, то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок смыслового содержание раскрываемой проблемы.

Критерии оценки конспекта:

- ✓ 100-85 баллов - выставляется студенту, если студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент знает и владеет навыком самостоятельной исследовательской работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно
- ✓ 85-76 баллов - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы
- ✓ 75-61 балл – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы.

Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы

- ✓ 60-50 баллов – если работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы, то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценки студента по выполнению проекта

Баллы	**Оценка** (стандартная)	**Требования к сформированным компетенциям**
100-86	*«отлично» («зачтено»)*	Оценка **«отлично»** («зачтено») выставляется студенту, если он разработал и реализовал проект в соответствии со всеми требованиями (проблема; цель, задачи и целевая аудитория проекта; методы и средства реализации проекта; анализ проекта и рекомендации). Проект может быть рекомендован для дальнейшего использования.
85-76	*«хорошо» («зачтено»)*	Оценка **«хорошо»** («зачтено») выставляется студенту, если он разработал проект в соответствии с основными требованиями, но допустил некоторые ошибки в его подготовке и реализации (например, неправильно выбрал методы и средства для его реализации; не учёл особенности целевой аудитории и т.п.). Проект нуждается в корректировке.
75-61	*«удовлетворительно» («зачтено»)*	Оценка **«удовлетворительно»** («зачтено») выставляется студенту, если он разработал проект, но проект не соответствует предъявляемым требованиям.
60-50	*«неудовлетворительно» («не зачтено»)*	Оценка **«неудовлетворительно»** («не зачтено») выставляется студенту, если он не разработал проект.

Критерии оценки презентации проекта

Оценка	**50-60 баллов (неудовлетворительно)**	**61-75 баллов (удовлетворительно)**	**76-85 баллов (хорошо)**	**86-100 баллов (отлично)**
Критерии	**Содержание критериев**			

Раскрытие Проблемы	Проблема не раскрыта. Отсутствуют выводы	Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы	Проблема раскрыта. Проведен анализ проблемы без привлечения дополнительной литературы. Не все выводы сделаны и/или обоснованы	Проблема раскрыта полностью. Проведен анализ проблемы с привлечением дополнительной литературы. Выводы обоснованы
Представление	Представляемая информация логически не связана. Не использованы профессиональные термины	Представляемая информация не систематизирована и/или не последовательна. Использовано 1-2 профессиональных термина	Представляемая информация не систематизирована и последовательна. Использовано более 2 профессиональных терминов	Представляемая информация систематизирована, последовательна и логически связана. Использовано более 5 профессиональных терминов
Оформление	Не использованы технологии Power Point. Больше 4 ошибок в представляемой информации	Использованы технологии Power Point частично. 3-4 ошибки в представляемой информации	Использованы технологии Power Point. Не более 2 ошибок в представляемой информации	Широко использованы технологии (Power Point и др.). Отсутствуют ошибки в представляемой информации
Ответы на вопросы	Нет ответов на вопросы	Только ответы на элементарные вопросы	Ответы на вопросы полные и/или частично полные	Ответы на вопросы полные, с привидением примеров и/или пояснений

Оценочные средства для промежуточной аттестации

Промежуточная аттестация студентов по дисциплине «Расследование инцидентов кибербезопасности» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Согласно учебному плану видом промежуточной аттестации по дисциплине «Расследование инцидентов кибербезопасности» предусмотрен экзамен, который выставляется по результатам работы в семестре.

Оценочные средства для промежуточной аттестации

Вопросы к экзамену

1. Правила корреляции в системах SIEM
2. Правила автоматического реагирования, локализации, восстановления информационных систем при помощи SOAR и IRP решений
3. Сигнатуры, т.е. правила, по которым угроза должна быть обнаружена
4. Технологии SOC-Центров
5. Процессы SOC-Центров

6. Пост-инцидентные действия
7. Стандарты и протоколы для получения данных кибербразведки
8. Источники получения данных кибербразведки
9. Индикаторы компрометации (IoCs)
10. Виды кибербразведки

Критерии выставления оценки студенту на экзамене по дисциплине «Расследование киберинцидентов»

К экзамену допускаются обучающиеся, выполнившие программу обучения по дисциплине, прошедшие все этапы текущей аттестации.

Оценка «отлично» (зачтено) - ставится студенту, если он продемонстрировал сформированность всех вышеперечисленных навыков компетенции (85-100 баллов).

Оценка «хорошо» (зачтено) – если сформированы большинство знаний, умений и навыков, но допускается не более 1 недостаточно освоенного навыка компетенции (65 – 84 балла).

Оценка «удовлетворительно» (зачтено) – если сформированы большинство навыков, но допускается не более 2 недостаточно освоенных навыков компетенции (45 – 64 балла).

Оценка «неудовлетворительно» (не зачтено) выставляется, если практические задания выполнены студентом не в полном объеме, и часть навыков компетенции не сформированы (менее 45 баллов).