Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый проректор

_____ Т.Р. Змызгова

«31» августа 2022 г.

Рабочая программа учебной дисциплины
ОБНАРУЖЕНИЕ И ПРЕДУПРЕЖДЕНИЕ КОМПЬЮТЕРНЫХ АТАК В ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

образовательной программы высшего образования
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Специализация:
Специализация №5 «Безопасность открытых информационных систем»

Форма обучения: **очная**

Курган 2022

Рабочая программа дисциплины «Обнаружение и предупреждение компьютерных атак в открытых информационных системах» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Безопасность открытых информационных систем), утвержденным:
- для очной формы обучения «30» августа 2022 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «29» августа 2022 года, протокол № 1.

Заведующий кафедрой «Безопасность информационных и автоматизированных систем» Д.И. Дик

Согласовано:

Заведующий кафедрой «Безопасность информационных и автоматизированных систем» Д.И. Дик

Специалист по учебно-методической работе учебно-методического отдела Г.В. Казанкова

Начальник управления образовательной деятельности П.В. Григорьев

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 5 зачетных единицы трудоемкости (180 академических часа)

Вид учебной работы	На всю дисциплину	Семестр
		8
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**96**	**96**
Лекции	32	32
Лабораторные работы	32	32
Практические работы	32	32
Самостоятельная работа, всего часов в том числе:	**84**	**84**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (самостоятельное изучение тем (разделов) дисциплины)	66	66
Вид промежуточной аттестации	**Зачет с оценкой**	**Зачет с оценкой**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**180**	**180**

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Обнаружение и предупреждение компьютерных атак в открытых информационных системах» является дисциплиной по выбору Блока 1 и относится к части, формируемой участниками образовательных отношений.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

– Безопасность сетей ЭВМ;
– Безопасность операционных систем;
– Безопасность систем баз данных;
– Управление информационной безопасностью.

Дисциплина «Обнаружение и предупреждение компьютерных атак в открытых информационных системах» является одной из заключительных дисциплин подготовки специалистов, изучается в последнем семестре, поэтому знания, умения и навыки, полученные в ходе изучения дисциплины необходимы для прохождения производственной практики и успешного написания выпускной квалификационной работы.

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины является формирование знаний и умений в области противодействия компьютерной преступности, решения задач в области в области установки, настройки и эксплуатации систем обнаружения компьютерных атак.

Задачами дисциплины являются:

– ознакомление с теоретическими принципами построения систем обнаружения компьютерных атак;
– формирование умений по проектирования базы правил для обнаружения и предупреждения компьютерных атак;
– приобретение обучающимися навыков настройки и эксплуатации систем обнаружения компьютерных атак.

Компетенции, формируемые в результате освоения дисциплины:

– способен формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-13);
– способен обеспечивать работоспособность систем защиты информации открытых информационных систем при возникновении нештатных ситуаций (ПК-15);

В результате изучения дисциплины обучающийся должен:

знать:

– принципы построения систем обнаружения и предупреждения компьютерных атак (ПК-15);

– принципы безопасной разработки программных средств (ПК-13);

– способы управления рисками кибербезопасности (ПК-13);

уметь:

– применять средства обнаружения и предупреждения компьютерных атак (для ПК-15);

– проектировать правила для обнаружения и предупреждения компьютерных атак (для ПК-15);

владеть:

– навыками настройки и эксплуатации систем обнаружения компьютерных атак. (для ПК-15).

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Учебно-тематический план

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Лабораторные работы	Практические работы
Рубеж 1	1	Тренды кибербезопасности	3	–	–
	2	Система управления кибербезопасностью современной цифровой организации	3	–	2
	3	Управление данными кибербезопасности.	4	8	–
	4	Центр мониторинга и реагирования на инциденты информационной безопасности.	6	8	12
		1-ый рубежный контроль (Тестирование)			2
Рубеж 2	5	Управление угрозами и уязвимостями кибербезопасности	3	–	8
	6	Практики безопасной разработки и DevSecOps	4	16	4
	7	Управление рисками кибербезопасности.	3	–	2
	8	Системы противодействия мошенничеству.	6	–	–
		2-ый рубежный контроль (Тестирование)			2
		Всего:	**32**	**32**	**32**

4.2 Содержание лекционных занятий

Тема №1. Тренды кибербезопасности.

Актуальность обеспечения кибербезопасности. Статистика, тенденции и эволюция киберугроз. Атака как сервис. Модель Kill chain. Современные парадигмы кибербезопасности

Тема №2. Система управления кибербезопасностью современной цифровой организации.

Типовые угрозы и нарушители кибербезопасности. Управление рисками и требованиями. Система управления кибербезопасностью организации. Нормативная база. Процессы. Персонал. Технологии и средства защиты информации. Оценка системы кибербезопасности.

Тема №3. Управление данными кибербезопасности.

Данные в кибербезопасности. Управление жизненным циклом данных. Работа с данными. Безопасность данных.

Тема №4. Центр мониторинга и реагирования на инциденты информационной безопасности.

Назначение SOC (Security Operation Center). Модель Cyber Kill-Chain как подход к реагированию на инциденты. Функции и процессы SOC. Технологии SOC. Команда SOC.

Тема №5. Управление угрозами и уязвимостями кибербезопасности.

Базовые понятия и определения. Аналитика киберугроз (Cyber Threat Intelligence). Управление знаниями о киберугрозах. Управление уязвимостями, Подразделение CTI.

Тема №6. Практики безопасной разработки и DevSecOps.

Введение в Application Security и DevSecOps. Практики и инструменты Application Security. Применения Application Security в бизнесе. SSDLC процессы в крупной компании. Культура Application Security.

Тема №7. Управление рисками кибербезопасности.

Цели и задачи управления риском кибербезопасности. Система управления риском кибербезопасности. Управление рисками в инфраструктуре. Управление рисками в процессах. Управление рисками в соответствии с ISO 27005.

Тема №8. Системы противодействия мошенничеству.

Кибермошенничество в РФ и мире. Инструменты выявления мошеннических операций. Типология антифрод-решений. Подходы к оценке риска операций в системах фрод-мониторинга. Типовые схемы приложений антифрод-системы, ее внутренняя структура. Архитектура антифрод-решения. Аналитические инструменты. Риск-ориентированнѧ аутентификация. Оценка качества.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование лабораторной работы	Норматив времени, час.
3	Управление данными кибербезопасности.	Анализ журналов для выявления вторжений и атак	4
		Обнаружение вторжений в журналах аудита системных вызовов	4
4	Центр мониторинга и реагирования на инциденты информационной безопасности.	Платформа с открытым исходным кодом для анализа угроз и обмена информацией MISP	4
		Написание правил для системы обнаружения вторжений	4
6	Практики безопасной разработки и DevSecOps	Сканирование конечных точек на наличие IOC	4

		Статический анализ кода	4
		Фаззинг тестирование	4
		Сканирование веб-приложений на уязвимости	4
		Итого:	**32**

4.4 Практические работы

Номер темы	Наименование темы	Наименование практической работы	Норматив времени, час.
2	Система управления кибербезопасностью современной цифровой организации	Классификация шаблонов компьютерных атак CAPEC	2
4	Центр мониторинга и реагирования на инциденты информационной безопасности.	Стандарт описания, хранения и обмена сигналами тревоги между разнородными средствами защиты Common Event Expression (CEE)	4
		Унифицированный формат описания правил детектирования для SIEM систем Sigma.	4
		Формат обмена данными MISP	4
	1-ый рубежный контроль	***Тестирование***	***2***
5	Управление угрозами и уязвимостями кибербезопасности	Структурированные информационные сообщения об угрозах (Structured Threat Information eXpression, STIX)	4
		Правила описания вредоносных программ YARA.	4
6	Практики безопасной разработки и DevSecOps	Открытый язык описания и оценки уязвимостей OVAL	4
7	Управление рисками кибербезопасности.	Фреймворк быстрой оценки рисков (Rapid RiskAssessment, RRA)	2
	2-ой рубежный контроль	***Тестирование***	***2***
		Итого:	**32**

5 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Лекционный курс базируется на пассивном методе обучения, реализующем традиционную объяснительно-иллюстративную образовательную технологию, в рамках которой обучающиеся выступают в роли слушателей, воспринимающих учебный материал и участвующих в дискуссиях и экспресс-опросах.

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности

те, которые направлены на качественное выполнение соответствующей лабораторной или практической работы.

Залогом качественного выполнения лабораторных и практических работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Преподавателем запланировано применение на лабораторных и практических работах разбор конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных и практических работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным и практическим работам, рубежным контролям и зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела:	**30**
Тренды кибербезопасности	3
Система управления кибербезопасностью современной цифровой организации	4
Управление данными кибербезопасности.	3
Центр мониторинга и реагирования на инциденты информационной безопасности.	4
Управление угрозами и уязвимостями кибербезопасности	4
Практики безопасной разработки и DevSecOps	4
Управление рисками кибербезопасности.	4
Системы противодействия мошенничеству	4
Подготовка к лабораторным работам (по 2 часа на каждую работу)	16
Подготовка к практическим работам (по 2 часа на каждую работу)	16
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4
Подготовка к зачету	18
Всего:	**84**

6 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1 Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ (для очной формы обучения)

2. Отчеты обучающихся по лабораторным и практическим работам.

3. Банк тестовых заданий к рубежным контролям № 1, № 2 (для очной формы обучения).

4. Вопросы к дифференциальному зачету.

6.2 Система балльно-рейтинговой оценки работы обучающихся по дисциплине (для очной формы обучения)

<table>
<tr><td>№</td><td>Наименование</td><td colspan="7">Содержание</td></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения обучающихся на первом учебном занятии)</td><td colspan="7">Распределение баллов</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение лабораторных работ</td><td>Выполнение практических работ</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Дифференциальный зачет</td></tr>
<tr><td>Балльная оценка:</td><td>$1_б$ х 16 =$16_б$</td><td>$2_б$ х 8 = $16_б$</td><td>$2_б$ х 8 = $16_б$</td><td>11</td><td>11</td><td>30</td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачете</td><td colspan="7">60 и менее баллов – неудовлетворительно; не зачтено;
61…73 – удовлетворительно; зачтено;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета по дисциплине, возможность получения бонусных баллов</td><td colspan="7">Для допуска к промежуточной аттестации (дифференциальному зачету) обучающийся должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные и практические работы.
Для получения за дифференциальный зачет «автоматически» оценки «удовлетворительно» обучающемуся необходимо набрать не менее 68 баллов.
По согласованию с преподавателем обучающемуся, набравшему 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на лабораторных работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена «автоматически» оценка «хорошо» или «отлично».</td></tr>
</table>

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (дифференциальному зачету) набрана сумма менее 50 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных лабораторных и практических работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной лабораторной или практической работы (при невозможности дополнительного проведения лабораторной работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 4 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3 Процедура оценивания результатов освоения дисциплины

Мероприятия текущего контроля проводятся на аудиторных занятиях в соответствии с расписанием.

Основной вид текущего контроля результатов освоения дисциплины - защита отчетов по выполненным лабораторным и практическим работам.

В процессе защиты отчетов оценивается уровень понимания обучающимися методики проведения работы, полнота и качество выполнения заданий, а также обоснованность выводов, сделанных обучающимся по результатам выполнения заданий.

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает с обучающимися основной материал соответствующих разделов дисциплины. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 11 вопросов. На каждое тестирование при рубежном контроле обучающемуся отводится 2 академических часа.

Баллы обучающемуся выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании.

Зачет проводится в форме устного ответа на 2 вопроса. Билет состоит из 2 вопросов. Перечень вопросов преподаватель выдает заранее. Время, отводимое обучающемуся на подготовку вопросов, составляет 1 академический час. Каждый вопрос оценивается в 15 баллов.

Результаты текущего контроля успеваемости и зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку обучающегося.

6.4 Примеры оценочных средств для рубежных контролей и зачета

Примерные тестовые задания для рубежного контроля №1

1) Какие стадии кибератаки рассматриваются в модели Kill Chain? Выберите все правильные ответы.

а) разведка
б) расшифровка
в) мониторинг
г) реализация
д) управление
е) прослушивание
ж) запуск
и) анализ

2) Какой тип источников данных относится к слабоструктурированным? Выберите все правильные ответы.

а) базы данных
б) потоковые данные (json-сообщения)
в) XML-файлы
г) ETL Выгрузки

3) Какую модель рекомендуется использовать при реагировании на инциденты кибербезопасности?

а) ITIL
б) COBIT
в) Cyber Kill-Chain
г) TIP

Примерные тестовые задания для рубежного контроля №2

1) Какая из перечисленных моделей применяется для описания хакерских группировок?

а) Kill Chain
б) MITRE ATT&CK
в) Diamond Model
г) OWASP Top 10

2) Какие утверждения, касающиеся Secure Software Development Lifecycle (SSDLC), являются верными? Выберите все правильные ответы.

а) SSDLC включает SDLC
б) SSDLC включает Application Security

в) процесс SSDLC включает шаги: формирование требований, проектирование, разработка и тестирование, ввод в эксплуатацию, сопровождение, внесение изменений или вывод из эксплуатации (в случае завершения цикла)
г) пионером в создании подхода SSDLC выступила компания Apple

3) К какой группе рисков относятся риски кибербезопасности?
а) рыночные
б) ликвидности
в) операционные
г) кредитные
д) нет верного ответа.

Примерный перечень вопросов к зачету

1. Тренды кибербезопасности.
2. Модель Kill chain
3. Типовые угрозы и нарушители кибербезопасности
4. Управление рисками и требованиями.
5. Система управления кибербезопасностью организауции. Нормативная база. Процессы. Персонал.
6. Оценка системы кибербезопасности.
7. Данные в кибербезопасности. Управление жизненным циклом данных.
8. Работа с данными. Безопасность данных.
9. Назначение SOC (Security Operation Center).
10. Модель Cyber Kill-Chain как подход к реагированию на инциденты.
11. Функции и процессы SOC.
12. Технологии SOC.
13. Команда SOC.
14. Аналитика киберугроз (Cyber Threat Intelligence).
15. Управление знаниями о киберугрозах.
16. Управление уязвимостями,
17. Подразделение CTI.
18. Application Security и DevSecOps.
19. Практики и инструменты Application Security.
20. Применения Application Security в бизнесе.
21. SSDLC процессы в крупной компании.
22. Цели и задачи управления риском кибербезопасности.
23. Система управления риском кибербезопасности.
24. Управление рисками в инфраструктуре.
25. Управление рисками в процессах.
26. Управление рисками в соответствии с ISO 27005.
27. Инструменты выявления мошеннических операций.
28. Типология антифрод-решений.
29. Подходы к оценке риска операций в системах фрод-мониторинга.

30. Типовые схемы приложений антифрод-системы, ее внутренняя структура.

31. Архитектура антифрод-решения.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Жукова, М. Н. Управление информационной безопасностью [Электронный ресурс]. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. – Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. – 100 с. – Доступ ЭБС «Znanium»

2. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса [Электронный ресурс] : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Вып. 3. – Москва : Горячая линия, – Телеком, 2013. – 170 с. – Доступ ЭБС «Консультант студента».

7.2 Дополнительная учебная литература

1. Rehman, R. Cybersecurity Arm Wrestling Winning the perpetual fight against crime by building a modern Security Operations Center (SOC) [Electronic resourse] / Rafeeq U. Rehman. – 124 p. – Access mode: https://rafeeqrehman.com/wp-content/uploads/2021/05/soc_book_20210404_first_edition.pdf, free.

2. Managing Security Risks Inherent in the Use of Thirdparty Components / SAFECode. – [?] : SAFECode, 2017. – 32 p. – Access mode: https://safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf, free.

3. Microsoft Security Development Lifecycle SDL Process Guidance Version 5.2 / Microsoft. – May 23, 2012. – 169 p. – Access mode: https://www.microsoft.com/en-us/download/details.aspx?id=29884, free.

7.3 Методическая литература

1. Методические указания по выполнению лабораторных работ по дисциплине «Обнаружение и предупреждение компьютерных атак в открытых информационных системах».

2. Методические указания по выполнению практических работ по дисциплине «Обнаружение и предупреждение компьютерных атак в открытых информационных системах».

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Сайт дистанционного обучения в НОУ (Национальный Открытый Университет) «ИНТУИТ» содержит бесплатные курсы, программы повышения квалификации и профессиональной переподготовки, интересные доклады и другую полезную информацию http://www.intuit.ru.
2. Федеральный портал «Российское образование» http://www.edu.ru/
3. Портал «Информационно-коммуникационные технологии в образовании» http://www.ict.edu.ru.
4. Федеральный портал ЭБС «Лань» - https://e.lanbook.com/;
5. ЭБС «Znanium» - https://znanium.com/;
6. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
7. Электронная библиотека КГУ - http://dspace.kgsu.ru/xmlui/

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Инструментальная платформа для низкоуровневой аналитики и мониторинга операционной системы «osquery» (лицензия на свободное ПО: GNU General Public License v3 и Apache License Version 2.0).

Система реагирования на инциденты, ориентированная на удаленную оперативную криминалистику «GRR Rapid Response» (лицензия на свободное ПО: Apache License Version 2.0).

Платформа с открытым исходным кодом для анализа угроз и обмена информацией MISP (лицензия на свободное ПО: GNU Affero General Public License v3.0).

Сканер Web приложений на уязвимости OWASP Zed Attack Proxy (ZAP) (лицензия на свободное ПО: Apache License Version 2.0).

Фреймворк для фаззинга «American Fuzzy Lop plus plus» (AFL++) (лицензия на свободное ПО: Apache License Version 2.0).

Ориентированная на безопасность платформа статического анализа для Android и Java приложений «Mariana Trench» (лицензия на свободное ПО: MIT license).

Система обнаружения и предотвращения вторжений Suricata (лицензия на свободное ПО: GNU General Public License v2.0).

При чтении лекций используются слайдовые презентации.

Минимальные требования к программному обеспечению компьютера, используемого при показе слайдовых презентаций: офисный пакет LibreOffice (лицензия Mozilla Public License Version 2.0).

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает в себя учебные лаборатории и классы, оснащенные современными компьютерами (все – в стандартной комплектации для лабораторных работ и самостоятельной работы), объединенными локальными вычислительными сетями с выходом в Интернет, мультимедийное оборудование (переносной персональный компьютер, мультимедийный проектор, мультимедийный экран).

11. ДЛЯ ОБУЧАЮЩИХСЯ С ИСПОЛЬЗОВАНИЕМ ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения ведущего преподавателя и доводится до обучающихся.

Аннотация
рабочей программы учебной дисциплины
«Обнаружение и предупреждение компьютерных атак в открытых информационных системах»
образовательной программы высшего образования – программы специалитета
10.05.03 – Информационная безопасность автоматизированных систем

Специализация №5 «Безопасность открытых информационных систем»

Формы обучения: **очная**

Трудоемкость дисциплины: 5 ЗЕ (180 академических часа)
Семестры: 8-й
Форма промежуточной аттестации: зачет с оценкой

Содержание дисциплины

Тренды кибербезопасности. Система управления кибербезопасностью современной цифровой организации. Управление данными кибербезопасности. Центр мониторинга и реагирования на инциденты информационной безопасности. Управление угрозами и уязвимостями кибербезопасности. Практики безопасной разработки и DevSecOps. Управление рисками кибербезопасности. Системы противодействия мошенничеству.