ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

C=RU, S=Ставропольский край, L=г. Ставрополь, T=проректор по учебной работе, OU=ректорат, O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ ""СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ""", СНИЛС=15230589951, ИНН=263411176761, E=s.a.maksimovich@stgau.ru, G=Светлана Александровна, SN=Максимович, CN=Максимович Светлана Александровна

УТВЕРЖДАЮ

Директор/Декан
факультета цифровых технологий
Шлаев Дмитрий Валерьевич

_____

_____

«___» _____ 20___ г.

Рабочая программа дисциплины

Б1.В.ДВ.02.01 Обнаружение и анализ вредоносного программного обеспечения

09.04.03 Прикладная информатика

Искусственный интеллект в кибербезопасности

магистр

очная

Ставрополь, 2026

1. Цель дисциплины

Целью освоения дисциплины «Обнаружение и анализ вредоносного программного обеспечения» является формирование у обучающихся знаний, умений и навыков в области выявления, классификации и анализа вредоносного программного обеспечения, изучения методов его распространения, принципов работы средств антивирусной защиты и технологий противодействия вредоносным программам в информационных системах.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций ОП ВО и овладение следующими результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения по дисциплине
ПК-3 Способен применять методы машинного обучения и искусственного интеллекта для решения задач кибербезопасности	ПК-3.1 Проводит анализ безопасности компьютерных систем с использованием методов машинного обучения для выявления уязвимостей и оценки рисков	**знает** методы машинного обучения для анализа безопасности компьютерных систем, выявления уязвимостей и оценки рисков **умеет** применять методы машинного обучения для выявления уязвимостей и оценки рисков безопасности **владеет навыками** навыками анализа безопасности компьютерных систем с применением методов машинного обучения
ПК-3 Способен применять методы машинного обучения и искусственного интеллекта для решения задач кибербезопасности	ПК-3.2 Применяет методы инструментального мониторинга защищённости, включая алгоритмы ИИ для обнаружения и классификации аномалий и атак	**знает** методы инструментального мониторинга защищенности и алгоритмы ИИ для обнаружения аномалий и атак **умеет** использовать инструменты мониторинга и алгоритмы ИИ для обнаружения и классификации аномалий и атак **владеет навыками** навыками инструментального мониторинга защищенности и анализа аномалий с применением ИИ
ПК-4 Способен администрировать средства защиты информации и обеспечивать безопасность информационных систем	ПК-4.1 Администрирует средства защиты информации прикладного и системного программного обеспечения (ОС, СУБД, приложения), настраивая политики безопасности и контролируя их соблюдение	**знает** средства защиты информации, политики безопасности и методы противодействия вредоносному программному обеспечению **умеет** настраивать средства защиты информации и контролировать выполнение политик безопасности **владеет навыками** навыками администрирования средств защиты информации и противодействия вредоносному ПО
ПК-5 Способен проводить	ПК-5.1 Проводит инструментальный	**знает**

инструментальный анализ защищённости, тестирование на проникновение и расследование компьютерных инцидентов	анализ защищённости и тестирование на проникновение информационных систем	методы инструментального анализа защищенности и тестирования информационных систем на наличие угроз **умеет** проводить инструментальный анализ защищенности информационных систем и выявлять признаки вредоносного ПО **владеет навыками** навыками применения инструментов анализа защищенности и тестирования информационных систем
ПК-5 Способен проводить инструментальный анализ защищённости, тестирование на проникновение и расследование компьютерных инцидентов	ПК-5.2 Проводит экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов, анализируя цифровые следы и составляя заключения	**знает** методы анализа цифровых следов, расследования компьютерных инцидентов и подготовки экспертных заключений **умеет** анализировать цифровые следы вредоносного ПО и готовить заключения по результатам расследования инцидентов **владеет навыками** навыками экспертизы цифровых следов и документирования результатов анализа вредоносного ПО

3. Место дисциплины в структуре образовательной программы

Дисциплина «Обнаружение и анализ вредоносного программного обеспечения» является дисциплиной части, формируемой участниками образовательных отношений программы.

Изучение дисциплины осуществляется в 4семестре(-ах).

Для освоения дисциплины «Обнаружение и анализ вредоносного программного обеспечения» студенты используют знания, умения и навыки, сформированные в процессе изучения дисциплин:

Ознакомительная практика

Технологии программирования

Теория информационных процессов и системАдминистрирование безопасных информационных систем

Ознакомительная практика

Технологии программирования

Теория информационных процессов и системАдминистрирование защищенных сетей

Ознакомительная практика

Технологии программирования

Теория информационных процессов и системУправление информационной безопасностью

Ознакомительная практика

Технологии программирования

Теория информационных процессов и системПрикладные системы искусственного интеллекта

Ознакомительная практика

Технологии программирования

Теория информационных процессов и системНаучно-исследовательская работа

Ознакомительная практика

Технологии программирования

Теория информационных процессов и системСовременные интеллектуальные системы и технологии

Ознакомительная практика

Технологии программирования

Теория информационных процессов и системБезопасность облачных технологий

Ознакомительная практика
Технологии программирования
Теория информационных процессов и системПроектирование автономных ИИ-агентов
Ознакомительная практика
Технологии программирования
Теория информационных процессов и системТехнологии расследования компьютерных преступлений и инцидентов
Ознакомительная практика
Технологии программирования
Теория информационных процессов и системТехнологии разработки защищенного ПО
Ознакомительная практика
Технологии программирования
Теория информационных процессов и системАтаки на системы искусственного интеллекта
Ознакомительная практика
Технологии программирования
Теория информационных процессов и системМашинное обучение в кибербезопасности
Освоение дисциплины «Обнаружение и анализ вредоносного программного обеспечения» является необходимой основой для последующего изучения следующих дисциплин:

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины «Обнаружение и анализ вредоносного программного обеспечения» в соответствии с рабочим учебным планом и ее распределение по видам работ представлены ниже.

Семестр	Трудоемкость час/з.е.	Контактная работа с преподавателем, час			Самостоятельная работа, час	Контроль, час	Форма промежуточной аттестации (форма контроля)
		лекции	практические занятия	лабораторные занятия			
4	108/3	12	24		72		За
в т.ч. часов: в интерактивной форме		4	6				
практической подготовки		12	24		72		

Семестр	Трудоемкость час/з.е.	Внеаудиторная контактная работа с преподавателем, час/чел					
		Курсовая работа	Курсовой проект	Зачет	Дифференцированный зачет	Консультации перед экзаменом	Экзамен
4	108/3			0.12			

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

№	Наименование раздела/темы	Семестр	Количество часов					Формы текущего контроля успеваемости и промежуточной аттестации	Оценочное средство проверки результатов достижения индикаторов компетенций	Код индикаторов достижения компетенций
			всего	Лекции	Семинарские занятия		Самостоятельная работа			
					Практические	Лабораторные				

1.	1 раздел. 1									
1.1.	Программно-аппаратная защита ин-формации, основные понятия, определения, возможности использования.	4	16	4	12		18		Устный опрос	ПК-3.1, ПК-3.2, ПК-4.1, ПК-5.1, ПК-5.2
1.2.	КТ 1	4	2		2			КТ 1	Тест	ПК-3.1, ПК-3.2, ПК-4.1, ПК-5.1, ПК-5.2
1.3.	Методы и средства программно-аппаратных средства защиты ин-формации.	4	16	8	8		54		Устный опрос	ПК-3.1, ПК-3.2, ПК-4.1, ПК-5.1, ПК-5.2
1.4.	КТ 2	4	2		2			КТ 2	Тест	ПК-3.1, ПК-3.2, ПК-4.1, ПК-5.1, ПК-5.2
	Промежуточная аттестация	За								
	Итого		108	12	24		72			
	Итого		108	12	24		72			

5.1. Лекционный курс с указанием видов интерактивной формы проведения занятий

Тема лекции (и/или наименование раздел) (вид интерактивной формы проведения занятий)/ (практическая подготовка)	Содержание темы (и/или раздела)	Всего, часов / часов интерактивных занятий/ практическая подготовка
Программно-аппаратная защита ин-формации, основные понятия, определения, возможности использования.	Введение. Предмет и задачи программно-аппаратной за-щиты информации. Основные понятия.	2/2
Программно-аппаратная защита ин-формации, основные понятия, определения, возможности использования.	Классификация разрушающих программных средств (РПС)	2/-
Методы и средства программно-аппаратных средства защиты ин-формации.	Классификация средств защиты от РПС.	2/-
Методы и средства программно-аппаратных средства защиты ин-формации.	Практические рекомендации по защите от РПС	2/-
Методы и средства программно-аппаратных средства защиты ин-формации.	Программно-аппаратные средства безопасности ИС	2/-

Методы и средства программно-аппаратных средства защиты ин-формации.	Основные программно-технические меры	2/2
Итого		12

5.2.1. Семинарские (практические) занятия с указанием видов проведения занятий в интерактивной форме

Наименование раздела дисциплины	Формы проведения и темы занятий (вид интерактивной формы проведения занятий)/(практическая подготовка)	Всего, часов / часов интерактивных занятий/ практическая подготовка	
		вид	часы
Программно-аппаратная защита ин-формации, основные понятия, определения, возможности использования.	Программные и программно-аппаратные методы и средства за-щиты информации	Пр	6/2/6
Программно-аппаратная защита ин-формации, основные понятия, определения, возможности использования.	Антивирусные программы	Пр	6/-/6
КТ 1	КТ 1	Пр	2/-/2
Методы и средства программно-аппаратных средства защиты ин -формации.	Анализ защищенности корпоративных систем	Пр	4/-/4
Методы и средства программно-аппаратных средства защиты ин -формации.	Построение крипто-графической системы с конфигурацией ключе-вой пары.	Пр	4/2/4
КТ 2	КТ 2	Пр	2/2/2
Итого			

5.3. Курсовой проект (работа) учебным планом не предусмотрен

5.4. Самостоятельная работа обучающегося

Темы и/или виды самостоятельной работы	Часы

Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала и подготовка к лабораторной работе	24
Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала	6
Контрольная работа (аудиторная) Аутентификация, идентификация в программно-аппаратной защите информации	6
Подготовка к зачету	6

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Учебно-методическое обеспечение для самостоятельной работы обучающегося по дисциплине «Обнаружение и анализ вредоносного программного обеспечения» размещено в электронной информационно-образовательной сре-де Университета и доступно для обучающегося через его личный кабинет на сайте Университета. Учебно-методическое обеспечение включает:

1. Рабочую программу дисциплины «Обнаружение и анализ вредоносного программного обеспечения».

2.Методические рекомендации для организации самостоятельной работы обучающегося по дисциплине «Обнаружение и анализ вредоносного программного обеспечения».

3. Методические рекомендации по выполнению письменных работ () (при наличии).

4. Методические рекомендации по выполнению контрольной работы студентами заочной формы обучения (при наличии)

5. Методические указания по выполнению курсовой работы (проекта) (при наличии).

Для успешного освоения дисциплины, необходимо самостоятельно детально изучить представленные темы по рекомендуемым источникам информации:

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)		
		основная (из п.8 РПД)	дополнительная (из п.8 РПД)	метод. лит. (из п.8 РПД)
1	Программно-аппаратная защита информации, основные понятия, определения, возможности использования.. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1		
2	Программно-аппаратная защита информации, основные понятия, определения, возможности использования.. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1		
3	Программно-аппаратная защита информации, основные понятия, определения, возможности использования.. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1		
4	Методы и средства программно-аппаратных средства защиты информации.. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1		
5	Методы и средства программно-аппаратных средства защиты информации.. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1		
6	Методы и средства программно-аппаратных средства защиты информации.. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1		

7	Методы и средства программно-аппаратных средства защиты информации.. Изучение пройденного материала	Л1.1		
8	Методы и средства программно-аппаратных средства защиты информации.. Контрольная работа (аудиторная) Аутентификация, идентификация в программно-аппаратной защите информации	Л1.1		
9	Методы и средства программно-аппаратных средства защиты информации.. Подготовка к зачету	Л1.1		

7. Фонд оценочных средств (оценочных материалов) для проведения промежуточной аттестации обучающихся по дисциплине «Обнаружение и анализ вредоносного программного обеспечения»

7.1. Перечень индикаторов компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Индикатор компетенции (код и содержание)	Дисциплины/элементы программы (практики, ГИА), участвующие в формировании индикатора компетен-ции	

7.2. Критерии и шкалы оценивания уровня усвоения индикатора компетенций, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Оценка знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций по дисциплине «Обнаружение и анализ вредоносного программного обеспечения» проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение семестра с целью определения уровня усвоения обучающимися знаний, формирования умений и навыков, своевременного выявления преподавателем недостатков в подготовке обучающихся и принятия необходимых мер по её корректировке, а также для совершенствования методики обучения, организации учебной работы и оказания индивидуальной помощи обучающемуся.

Промежуточная аттестация по дисциплине «Обнаружение и анализ вредоносного программного обеспечения» проводится в виде Зачет.

За знания, умения и навыки, приобретенные студентами в период их обучения, выставляются оценки «ЗАЧТЕНО», «НЕ ЗАЧТЕНО». (или «ОТЛИЧНО», «ХОРОШО», «УДОВЛЕТВОРИТЕЛЬНО», «НЕУДОВЛЕТВОРИТЕЛЬНО» для дифференцированного зачета/экзамена)

Для оценивания знаний, умений, навыков и (или) опыта деятельности в университете применяется балльно-рейтинговая система оценки качества освоения образовательной программы. Оценка проводится при проведении текущего контроля успеваемости и промежуточных аттестаций обучающихся. Рейтинговая оценка знаний является интегрированным показателем качества теоретиче-ских и практических знаний и навыков студентов по дисциплине.

Состав балльно-рейтинговой оценки студентов очной формы обучения

Для студентов очной формы обучения знания по осваиваемым компетенциям формируются на лекционных и практических занятиях, а также в процессе самостоятельной подготовки.

В соответствии с балльно-рейтинговой системой оценки, принятой в Университете студентам начисляются баллы по следующим видам работ:

№ контрольной точки	Оценочное средство результатов индикаторов достижения компетенций	Максимальное количество баллов

4 семестр		
КТ 1	Тест	15
КТ 2	Тест	15
Сумма баллов по итогам текущего контроля		**30**
Посещение лекционных занятий		20
Посещение практических/лабораторных занятий		20
Результативность работы на практических/лабораторных занятиях		30
Итого		100

№ контрольной точки	Оценочное средство результатов индикаторов достижений компетенций	Максимальное количество баллов	Критерии оценки знаний студентов
4 семестр			
КТ 1	Тест	15	15 баллов выставляется обучающемуся, если тестовые задания выполнены на 85 % и выше; 12–14 баллов выставляется обучающемуся, если тестовые задания выполнены на 70–84 %; 9–11 баллов выставляется обучающемуся, если тестовые задания выполнены на 55–69 %; 6–8 баллов выставляется обучающемуся, если тестовые задания выполнены на 44–54 %; 0–5 баллов выставляется обучающемуся, если тестовые задания выполнены на 43 % и менее.
КТ 2	Тест	15	15 баллов выставляется обучающемуся, если тестовые задания выполнены на 85 % и выше; 12–14 баллов выставляется обучающемуся, если тестовые задания выполнены на 70–84 %; 9–11 баллов выставляется обучающемуся, если тестовые задания выполнены на 55–69 %; 6–8 баллов выставляется обучающемуся, если тестовые задания выполнены на 44–54 %; 0–5 баллов выставляется обучающемуся, если тестовые задания выполнены на 43 % и менее.

Критерии и шкалы оценивания результатов обучения на промежуточной аттестации

При проведении итоговой аттестации «зачет» («дифференцированный зачет», «экзамен») преподавателю с согласия студента разрешается выставлять оценки («отлично», «хорошо», «удовлетворительно», «зачет») по результатам набранных баллов в ходе текущего контроля успеваемости в семестре по выше приведенной шкале.

В случае отказа – студент сдает зачет (дифференцированный зачет, экзамен) по приведенным выше вопросам и заданиям. Итоговая успеваемость (зачет, дифференцированный зачет, экзамен) не может оцениваться ниже суммы баллов, которую студент набрал по итогам текущей и промежуточной успеваемости.

При сдаче (зачета, дифференцированного зачета, экзамена) к заработанным в течение семестра студентом баллам прибавляются баллы, полученные на (зачете, дифференцированном зачете, экзамене) и сумма баллов переводится в оценку.

Критерии и шкалы оценивания ответа на зачете

По дисциплине «Обнаружение и анализ вредоносного программного обеспечения» к зачету допускаются студенты, выполнившие и сдавшие практические работы по дисциплине, имеющие ежемесячную аттестацию и без привязке к набранным баллам. Студентам, набравшим более 65 баллов, зачет выставляется по результатам текущей успеваемости, студенты, не набравшие 65 баллов, сдают зачет по вопросам, предусмотренным РПД. Максимальная сумма баллов по промежуточной аттестации (зачету) устанавливается в 15 баллов

Вопрос билета	Количество баллов
Теоретический вопрос	до 5
Задания на проверку умений	до 5
Задания на проверку навыков	до 5

Теоретический вопрос

5 баллов выставляется студенту, полностью освоившему материал дисциплины или курса в соответствии с учебной программой, включая вопросы рассматриваемые в рекомендованной программой дополнительной справочно-нормативной и научно-технической литературы, свободно владеющему основными понятиями дисциплины. Требуется полное понимание и четкость изложения ответов по экзаменационному заданию (билету) и дополнительным вопросам, заданных экзаменатором. Дополнительные вопросы, как правило, должны относиться к материалу дисциплины или курса, не отраженному в основном экзаменационном задании (билете) и выявляют полноту знаний студента по дисциплине.

4 балла заслуживает студент, ответивший полностью и без ошибок на вопросы экзаменационного задания и показавший знания основных понятий дисциплины в соответствии с обязательной программой курса и рекомендованной основной литературой.

3 балла дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Студент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции.

2 балла дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

1 балл дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

0 баллов - при полном отсутствии ответа, имеющего отношение к вопросу.

Задания на проверку умений и навыков

5 баллов Задания выполнены в обозначенный преподавателем срок, письменный отчет без замечаний. Работа выполнена в полном объеме с соблюдением необходимой последовательности.

4 балла Задания выполнены в обозначенный преподавателем срок, письменный отчет с небольшими недочетами.

2 баллов Задания выполнены с задержкой, письменный отчет с недочетами. Работа выполнена не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы.

1 баллов Задания выполнены частично, с большим количеством вычислительных ошибок, объем выполненной части работы не позволяет сделать правильных выводов.

0 баллов Задания выполнены, письменный отчет не представлен или работа выполнена не полностью, и объем выполненной части работы не позволяет сделать правильных выводов.

7.3. Примерные оценочные материалы для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Обнаружение и анализ вредоносного программного обеспечения»

1. Понятие вредоносного программного обеспечения и его основные признаки.
2. Классификация вредоносного программного обеспечения.
3. Основные способы распространения вредоносных программ.
4. Методы обнаружения вредоносного программного обеспечения.
5. Сигнатурный и поведенческий анализ вредоносного ПО.
6. Статический анализ вредоносного программного обеспечения.
7. Динамический анализ вредоносного программного обеспечения.
8. Инструменты анализа вредоносного программного обеспечения.
9. Анализ цифровых следов вредоносного ПО.
10. Выявление уязвимостей и оценка рисков информационной безопасности.
11. Применение методов машинного обучения для обнаружения вредоносного ПО.
12. Использование алгоритмов искусственного интеллекта для классификации аномалий и атак.
13. Настройка средств защиты информации для противодействия вредоносному ПО.
14. Документирование результатов анализа вредоносного программного обеспечения.
15. Подготовка заключения по результатам расследования компьютерного инцидента.
1. Вредоносное программное обеспечение: понятие, виды и признаки.
2. Современные угрозы, связанные с распространением вредоносного ПО.
3. Методы обнаружения вредоносных программ.
4. Сигнатурный анализ вредоносного программного обеспечения.
5. Поведенческий анализ вредоносного программного обеспечения.
6. Статический и динамический анализ вредоносного ПО.
7. Инструментальные средства анализа вредоносных программ.
8. Анализ цифровых следов при расследовании компьютерных инцидентов.
9. Применение машинного обучения для выявления вредоносного ПО.
10. Использование искусственного интеллекта для классификации аномалий и атак.
11. Антивирусные технологии и средства защиты информации.
12. Политики безопасности при противодействии вредоносному программному обеспечению.
13. Оценка рисков при обнаружении вредоносного ПО.
14. Документирование результатов анализа вредоносных программ.
15. Перспективы развития технологий обнаружения и анализа вредоносного программного обеспечения.

Примерные вопросы для устного опроса:

1. Что понимается под вредоносным программным обеспечением?
2. Какие основные виды вредоносного программного обеспечения существуют?
3. Какие признаки могут указывать на заражение системы вредоносным ПО?

4. Какие способы распространения вредоносных программ наиболее распространены?
5. В чем заключается сигнатурный анализ вредоносного ПО?
6. В чем заключается поведенческий анализ вредоносного ПО?
7. Чем статический анализ отличается от динамического анализа?
8. Какие инструменты используются для анализа вредоносных программ?
9. Как выявляются цифровые следы вредоносного ПО?
10. Как машинное обучение применяется для обнаружения вредоносного программного обеспечения?
11. Как искусственный интеллект используется для классификации аномалий и атак?
12. Как оформляются результаты анализа вредоносного программного обеспечения?

Примерные тестовые задания:

1. Вредоносное программное обеспечение предназначено для:
а) нарушения работы системы, кражи данных или несанкционированного воздействия;
б) повышения производительности компьютера;
в) автоматического обновления учебных материалов;
г) создания резервных копий.
Правильный ответ: а.

2. Сигнатурный анализ основан на:
а) сравнении объекта с известными признаками вредоносного кода;
б) случайном удалении файлов;
в) отключении сетевого соединения;
г) изменении пароля пользователя.
Правильный ответ: а.

3. Динамический анализ вредоносного ПО предполагает:
а) наблюдение за поведением программы при выполнении;
б) изучение только названия файла;
в) проверку цвета интерфейса;
г) удаление операционной системы.
Правильный ответ: а.

4. Машинное обучение при анализе вредоносного ПО используется для:
а) выявления закономерностей, аномалий и классификации объектов;
б) замены всех средств защиты;
в) отключения журналов событий;
г) удаления сетевых настроек.
Правильный ответ: а.

5. Результаты анализа вредоносного ПО должны быть:
а) документированы и представлены в виде отчета или заключения;
б) удалены без проверки;
в) скрыты от ответственных специалистов;
г) заменены устным сообщением без фиксации.
Правильный ответ: а.

Примерные практические задания:

1. Определить признаки возможного заражения информационной системы вредоносным ПО.
2. Составить классификацию вредоносного программного обеспечения.
3. Описать порядок проведения статического анализа подозрительного файла.
4. Описать порядок проведения динамического анализа подозрительного файла.
5. Сравнить сигнатурный и поведенческий методы обнаружения вредоносного ПО.

6. Проанализировать цифровые следы компьютерного инцидента.
7. Предложить меры защиты от распространения вредоносного программного обеспечения.
8. Подготовить краткое заключение по результатам анализа вредоносного ПО.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

основная

Л1.1 Хорев П. Б. Программно-аппаратная защита информации [Электронный ресурс]:учеб. пособие; ВО - Бакалавриат, Магистратура. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 327 с. – Режим доступа: http://znanium.com/catalog/document?id=397282

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

№	Наименование ресурса сети «Интернет»	Электронный адрес ресурса
1	Баранова Е. К. Информационная безопасность и защита информации : учебное пособие. ЭБС Znanium.	https://znanium.ru/catalog/document?id=435080
2	Информационная безопасность компьютерных систем и сетей : учебное пособие. ЭБС Лань.	https://e.lanbook.com/book/211997

10. Методические указания для обучающихся по освоению дисциплины

Основа освоения дисциплины – лекция, целью которой является целостное и логичное рассмотрение основного материала курса. Вместе с тем значимость лекции определяется тем, что она не только способствует выработке логического мышления, но и способствует развитию интереса к пониманию современной действительности.

Задача студентов в процессе умелой и целеустремленной работы на лекциях – внимательно слушать преподавателя, следить за его мыслью, предлагаемой системой логических посылок, доказательств и выводов, фиксировать (записывать) основные идеи, важнейшие характеристики понятий, теорий, наиболее существенные факты. Лекция задает направление, содержание и эффективность других форм учебного процесса, нацеливает студентов на самостоятельную работу и определяет основные ее направления (подготовку к практическим занятиям, выполнение творческих заданий, рефератов, решение контекстных задач).

Записывание лекции – творческий процесс. Запись лекции крайне важна. Это позволяет надолго сохранить основные положения лекции; способствует поддержанию внимания; способствует лучшему запоминания материала. Важно уметь оформить конспект так, чтобы важные моменты были выделены графически, а главную информацию следует выделять в самостоятельные абзацы, фиксируя ее более крупными буквами или цветными маркерами. Конспект должен иметь поля для заметок. Это могут быть библиографические ссылки и, наконец, собственные комментарии. Для быстрой записи теста можно придумать условные знаки, при этом таких знаков не должно быть более 10–15. Условные обозначения придумывают для часто встречающихся слов (существует, который, каждый, точка зрения, на основании и т.п.).

Перед каждой лекцией необходимо внимательно прочитать материал предыдущей лекции. В рабочей тетради графически выделить: тему лекции, основные теоретические положения. Подготовленный студент легко следит за мыслью преподавателя, что позволяет быстрее запоминать новые понятия, сущность которых выявляется в контексте лекции. Повторение материала облегчает в дальнейшем подготовку к экзамену. Затем надо ознакомиться с материалом темы по учебнику, внести нужные уточнения и дополнения в лекционный материал. После усвоения каждой темы рекомендуется проверять свои знания, отвечая на контрольные вопросы по теме.

Лабораторные занятия

Целью лабораторных занятий является закрепление, расширение, углубление теоретических

знаний, полученных на лекциях и в ходе самостоятельной работы, развитие познавательных способностей.

Являясь частью образовательного процесса, лабораторные занятия преследует ряд основополагающих задач:

- работа с источниками, которая идет на уровнях индивидуальной самостоятельной работы и в ходе коллективного обсуждения;

- формирование умений и навыков индивидуальной и коллективной работы, позволяющих эффективно использовать основные методы исследования, грамотно выстраивать его основные технологические этапы (знакомство с темой и имеющейся по ней информацией, определение основной проблемы, первичный анализ, определение подходов и ключевых узлов механизма ее развития, публичное обсуждение, предварительные выводы);

- анализ поставленных проблем, умение обсуждать тему, высказывать свое мнение, отстаивать свою позицию, слушать и оценивать различные точки зрения, конструктивно полемизировать, учиться думать, говорить, слушать, понимать, находить точки соприкосновения разных позиций, их разумного сочетания;

- формирование установок на творчество;

- диалог, внутренний и внешний; поиск и разрешение проблемы в рамках имеющейся о ней информации;

- поиск рационального зерна в самых противоречивых позициях и подходах к проблеме;

- открытость новому и принципиальную возможность изменить свою позицию и вытекающие из нее решения, в случае получения новой информации и связанных с ней обстоятельств сознательный отход от подготовленного к семинару текста во время своего, построенного на тезисном изложении фактов и мыслей, когда конспект привлекается лишь в том случае, когда надо привести какие-то факты.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства и информационных справочных систем (при необходимости).

11.1 Перечень лицензионного программного обеспечения

1. Kaspersky Endpoint Security 12.11 - Антивирус
2. Microsoft Windows Server STDCORE AllLngLicense/Software AssurancePack Academic OLV 16Licenses LevelE AdditionalProduct CoreLic 1Year - Серверная операционная система

11.3 Перечень программного обеспечения отечественного производства

1. Kaspersky Endpoint Security 12.11 - Антивирус

При осуществлении образовательного процесса студентами и преподавателем используются следующие информационно справочные системы: СПС «Консультант плюс», СПС «Гарант».

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование специальных помещений и помещений для самостоятельной работы	Номер аудитории	Оснащенность специальных помещений и помещений для самостоятельной работы

1	Учебная аудитория для проведения занятий всех типов (в т.ч. лекционного, семинарского, практической подготовки обучающихся), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Э-160	Специализированная мебель на 180 посадочных мест, персональный компьютер – 1 шт., проектор Panasonic EX620 X6A – 1 шт., интерактивная доска SMART Board 690 – 1 шт., трибуна для лектора – 1 шт., микрофон – 1 шт., мониторы - 3 шт., плазменная панель - 1 шт., учебно-наглядные пособия в виде презентаций, информационные плакаты, подключение к сети «Интернет», выход в корпоративную сеть университета.
		423/НК	Оснащение: специализированная мебель на 56 посадочных мест, стол преподавателя – 1 шт., Sharp 70" Информационный ЖК-дисплей – 1 шт., магнитно-маркерная доска – 1 шт., учебно-наглядные пособия в виде тематических презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета.
2	Помещение для самостоятельной работы обучающихся, подтверждающее наличие материально-технического обеспечения, с перечнем основного оборудования		

13. Особенности реализации дисциплины лиц с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники и учебные пособия, иная учебная литература, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

а) для слабовидящих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- задания для выполнения, а также инструкция о порядке проведения промежуточной аттестации оформляются увеличенным шрифтом;
- задания для выполнения на промежуточной аттестации зачитываются ассистентом;
- письменные задания выполняются на бумаге, надиктовываются ассистенту;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- студенту для выполнения задания при необходимости предоставляется увеличивающее устройство;

в) для глухих и слабослышащих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- промежуточная аттестация проводится в письменной форме;
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости поступающим предоставляется звукоусиливающая аппаратура индивидуального пользования;
- по желанию студента промежуточная аттестация может проводиться в письменной форме;

д) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента промежуточная аттестация проводится в устной форме.

Рабочая программа дисциплины «Обнаружение и анализ вредоносного программного обеспечения» составлена на основе Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 916).

Автор (ы)

_____ доцент , к.т.н. Трошков А.М.

Рецензенты

_____ доцент , к.т.н. Рачков В.Е.

Рабочая программа дисциплины «Обнаружение и анализ вредоносного программного обеспечения» рассмотрена на заседании Кафедра информационных систем протокол № 9 от 07.04.2026 г. и признана соответствующей требованиям ФГОС ВО и учебного плана по направлению подготовки 09.04.03 Прикладная информатика

Заведующий кафедрой _____ Хабаров Алексей Николаевич

Рабочая программа дисциплины «Обнаружение и анализ вредоносного программного обеспечения» рассмотрена на заседании учебно-методической комиссии Факультет цифровых технологий протокол № 2 от 08.04.2026 г. и признана соответствующей требованиям ФГОС ВО и учебного плана по направлению подготовки 09.04.03 Прикладная информатика

Руководитель ОП _____