МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ / О.В. Юсупова
"_____" _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.04.02 «Методы и средства защиты от вредоносного программного обеспечения»

Код и направление подготовки (специальность)	38.03.04 Государственное и муниципальное управление
Направленность (профиль)	Модератор государственных и муниципальных услуг
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2022
Институт / факультет	Институт инженерно-экономического и гуманитарного образования
Выпускающая кафедра	кафедра "Экономика и управление организацией"
Кафедра-разработчик	кафедра "Экономика и управление организацией"
Объем дисциплины, ч. / з.е.	144 / 4
Форма контроля (промежуточная аттестация)	Экзамен

Самара 2022

Б1.В.ДВ.04.02 «Методы и средства защиты от вредоносного программного обеспечения»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **38.03.04 Государственное и муниципальное управление**, утвержденного приказом Министерства образования и науки РФ от № 1016 от 13.08.2020 и соответствующего учебного плана.

Разработчик РПД:

_____	Т.Н Обущенко
(должность, степень, ученое звание)	(ФИО)
Заведующий кафедрой	А.В. Васильчиков, доктор экономических наук, доцент
	(ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета факультета / института (или учебно-методической комиссии)	П.Г Лабзина, кандидат педагогических наук, доцент
	(ФИО, степень, ученое звание)
Руководитель образовательной программы	А.В. Васильчиков, доктор экономических наук, доцент
	(ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы 4
2. Место дисциплины (модуля) в структуре образовательной программы 4
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 5
4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий 6
4.1 Содержание лекционных занятий 6
4.2 Содержание лабораторных занятий 8
4.3 Содержание практических занятий 10
4.4. Содержание самостоятельной работы 10
5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю) 11
6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения 11
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем 12
8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю) 12
9. Методические материалы 12
10. Фонд оценочных средств по дисциплине (модулю) 14

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Общепрофессиональные компетенции			
	ОПК-5 Способен использовать в профессиональной деятельности информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применять технологии электронного правительства и предоставления государственных (муниципальных) услуг;	ОПК-5.1 Знает современные информационно-коммуникационные технологии, государственные и муниципальные информационные системы	Знать современные информационно-коммуникационные технологии, государственные и муниципальные информационные системы
		ОПК-5.2 Использует современные программные средства при решении профессиональных задач	Уметь применять современные программные средства при решении профессиональных задач
	ОПК-8 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-8.1 Использует терминологию цифрового государственного управления в профессиональной деятельности	Знать терминологию цифрового государственного управления в профессиональной деятельности
		ОПК-8.2 Выполняет трудовые действия с использованием информационных технологий при решении задач профессиональной деятельности	Уметь решать задачи профессиональной деятельности с использованием информационных технологий
		ОПК-8.3 Выделяет смысловые конструкции для понимания научных текстов по профилю профессиональной деятельности и объясняет принципы работы описываемых информационных технологий	Владеть смысловыми конструкциями для понимания научных текстов по профилю профессиональной деятельности

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **часть, формируемая участниками образовательных отношений**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины

ОПК-5	Введение в информационные технологии; Документирование управленческой деятельности; Защита данных и обеспечение конфиденциальности в области государственных и муниципальных услуг ; Корпоративная культура; Организационная культура; Основы делопроизводства; Основы математического моделирования социально-экономических процессов; Прикладная информатика в области государственных и муниципальных услуг ; Проектные риски и оценка проектов; Производственная практика: проектно-технологическая практика; Управление государственными и муниципальными заказами	Информационная безопасность в государственной и муниципальной службе; Подготовка к процедуре защиты и защита выпускной квалификационной работы; Производственная практика: преддипломная практика	
ОПК-8	Введение в информационные технологии; Защита данных и обеспечение конфиденциальности в области государственных и муниципальных услуг ; Основы математического моделирования социально-экономических процессов; Прикладная информатика в области государственных и муниципальных услуг ; Производственная практика: проектно-технологическая практика	Информационная безопасность в государственной и муниципальной службе; Подготовка к процедуре защиты и защита выпускной квалификационной работы; Производственная практика: преддипломная практика	

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

Вид учебной работы	Всего часов / часов в электронной форме	8 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	64	64
Лабораторные работы	32	32
Лекции	32	32
Внеаудиторная контактная работа, КСР	4	4
Самостоятельная работа (всего), в том числе:	40	40
подготовка к лабораторным работам	20	20
составление конспектов	20	20

Контроль	36	36
Итого: час	144	144
Итого: з.е.	4	4

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

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Вредоносное ПО. Классификация, структура, принцип действия, каналы распространения	8	0	0	20	28
2	Защита информационных систем от вредоносного программного обеспечения.	24	32	0	20	76
	КСР	0	0	0	0	4
	Контроль	0	0	0	0	36
	Итого	32	32	0	40	144

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	**Содержание лекции** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
8 семестр				
1	Вредоносное ПО. Классификация, структура, принцип действия, каналы распространения	Тема 1.1.	Вредоносное программное обеспечение. Компьютерные вирусы.	2
2	Вредоносное ПО. Классификация, структура, принцип действия, каналы распространения	Тема 1.2.	Каналы проникновения вредоносного программного обеспечения. Компьютерные преступления.	2
3	Вредоносное ПО. Классификация, структура, принцип действия, каналы распространения	Тема 1.1. (продолжение)	Вредоносное программное обеспечение. Компьютерные вирусы.	2

4	Вредоносное ПО. Классификация, структура, принцип действия, каналы распространения	Тема 1.2. (продолжение)	Каналы проникновения вредоносного программного обеспечения. Компьютерные преступления.	2
5	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.1.	Принцип борьбы с вредоносным программным обеспечением.	2
6	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.3.	Средства защиты от НСД.	2
7	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.5.	Алгоритм поиска вредоносного программного обеспечения в зараженной ИС. Уязвимость программного обеспечения.	2
8	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.6.	Взлом программного обеспечения. Защита от взлома. Тестирование безопасности программного обеспечения.	2
9	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.1. (продолжение)	Принцип борьбы с вредоносным программным обеспечением.	2
10	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.1. (продолжение)	Аппаратные средства защиты.	2
11	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.2.	Программные средства защиты.	2
12	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.2. (продолжение)	Антивирусные средства.	2

13	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.3. (продолжение)	Средства анализа трафика.	2
14	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.3. (продолжение)	Средства предотвращения утечки информации.	2
15	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.4.	Средства мониторинга и анализа процессов.	2
16	Защита информационных систем от вредоносного программного обеспечения.	Тема 2.4.(продолжение)	Средства преодоления защиты.	2
			Итого за семестр:	**32**
			Итого:	**32**

4.2 Содержание лабораторных занятий

№ занятия	**Наименование раздела**	**Тема лабораторного занятия**	**Содержание лабораторного занятия** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов / часов в электронной форме**
8 семестр				
1	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №1.	Исследование привязывающего shell-кода.	2
2	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №3.	Исследования уязвимости переполнения стека.	2
3	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №2.	Исследование уязвимости переполнения кучи.	2

4	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №4.	Перехват системных вызовов при помощи загружаемых модулей ядра.	2
5	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №5	Основы работы с пакетом Metasploit Framework.	2
6	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №6	Написание отчета по ЛР	2
7	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №1. (продолжение)	Исследование привязывающего shell-кода.	2
8	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №2. (продолжение)	Исследование уязвимости переполнения кучи.	2
9	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №3. (продолжение)	Исследования уязвимости переполнения стека.	2
10	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №4. (продолжение)	Перехват системных вызовов при помощи загружаемых модулей ядра.	2
11	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №5 (продолжение)	Основы работы с пакетом Metasploit Framework.	2
12	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №5 (продолжение)	Основы работы с пакетом Metasploit Framework.	2

13	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №6. (продолжение)	Написание отчета по ЛР	2
14	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №6. (продолжение)	Написание отчета по ЛР	2
15	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №6. (продолжение)	Написание отчета по ЛР	2
16	Защита информационных систем от вредоносного программного обеспечения.	Лабораторная работа №6. (продолжение)	Написание отчета по ЛР	2
			Итого за семестр:	**32**
			Итого:	**32**

4.3 Содержание практических занятий

Учебные занятия не реализуются.

4.4. Содержание самостоятельной работы

Наименование раздела	**Вид самостоятельной работы**	**Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов**
8 семестр			
Вредоносное ПО. Классификация, структура, принцип действия, каналы распространения	Самостоятельное изучение вопросов и конспектирование литературы	Вредоносное ПО. Классификация, структура, принцип действия, каналы распространения.	20
Защита информационных систем от вредоносного программного обеспечения.	Подготовка к ЛЗ Самостоятельное изучение вопросов и конспектирование литературы	Защита информационных систем от вредоносного программного обеспечения.	20
		Итого за семестр:	**40**
		Итого:	**40**

5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		
1	Запечников , С.В. Криптографические методы защиты информации : учеб. пособие для академ.бакалавриата / С. В. Запечников,О. В. Казарин, А. А. Тарасов.- М., Юрайт, 2015.- 309 с.	Электронный ресурс
2	Мельников, В.П. Информационная безопасность : учеб. / В.П.Мельников,А.И.Куприянов,Т.Ю.Васильева;ред.В.П.Мельников.- М., RuScience, 2017.- 354 с.	Электронный ресурс
3	Мухаев, Р.Т. Система государственного и муниципального управления : учеб. / Р. Т. Мухаев .- 2-е изд., перераб. и доп..- М., Юнити-Дана, 2014.- 688 с.	Электронный ресурс
4	Шубинский, И.Б. Надежные отказоустойчивые информационные системы : методы синтеза / И. Б. Шубинский.- Ульяновск, Журн."Надежность", 2016Обл.тип. "Печатный двор".- 544 с.	Электронный ресурс
Дополнительная литература		
5	Выпускная квалификационная работа: по направлению 38.03.04 «Государственное и муниципальное управление» : метод.указания / Самар.гос.техн.ун-т, Экономика и управление организацией; сост.: Г. П. Гагаринская, Ю. И. Мещерякова, Н. А. Серов.- Самара, 2015.- 57 с..- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||elib||2200	Электронный ресурс
6	Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации; **Издательский Дом МИСиС**, 2018.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||98199	Электронный ресурс
7	Рой, О.М. Основы государственного и муниципального управления : учеб. пособие / О. М. Рой .- 5-е изд..- М., Питер , 2015.- 415 с.	Электронный ресурс
8	Яшин, В.Н. Информатика: программные средства персонального компьютера : учеб. пособие / В. Н. Яшин.- М., Инфра-М, 2014.- 236 с.	Электронный ресурс

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	Microsoft Windows XP Professional операционная система	Microsoft (Зарубежный)	Лицензионное

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	Консультатнт плюс	http://www.consultant.ru/	Ресурсы открытого доступа
2	Библиотека Гумер	http://www.gumer.info/	Ресурсы открытого доступа
3	Сервер органов государственной власти "Официальная Россия"	http://www.gov.ru/	Ресурсы открытого доступа
4	Экономика. Социология. Менеджмент	http://ecsocman.hse.ru/	Ресурсы открытого доступа
5	Библиотека учебно-методической литературы системы "Единое окно"	http://window.edu.ru/	Ресурсы открытого доступа
6	Научная сеть	http://nature.web.ru/	Ресурсы открытого доступа
7	Русская виртуальная библиотека	http://www.rvb.ru/	Ресурсы открытого доступа
8	Корпоративный менеджмент	http://www.cfin.ru/	Ресурсы открытого доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук), программное обеспечение: MS Excel, MS Word;

аудитория, оснащенная учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя.

Лабораторные занятия

- аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук), программное обеспечение: MS Excel, MS Word;

- аудитория, оснащенная учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя.

Самостоятельная работа

рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде;
ресурсы информационно-вычислительных центров университета;

материально-техническое обеспечение НТБ СамГТУ;

ресурсы УИТ СамГТУ.

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при работе на лабораторном занятии

Проведение лабораторной работы делится на две условные части: теоретическую и практическую.

Необходимыми структурными элементами занятия являются проведение лабораторной работы, проверка усвоенного материала, включающая обсуждение теоретических основ выполняемой работы.

Перед лабораторной работой, как правило, проводится технико-теоретический инструктаж по использованию необходимого оборудования. Преподаватель корректирует деятельность обучающегося в процессе выполнения работы (при необходимости). После завершения лабораторной работы подводятся итоги, обсуждаются результаты деятельности.

Возможны следующие формы организации лабораторных работ: фронтальная, групповая и индивидуальная. При фронтальной форме выполняется одна и та же работа (при этом возможны различные варианты заданий). При групповой форме работа выполняется группой (командой). При индивидуальной форме обучающимися выполняются индивидуальные работы.

По каждой лабораторной работе имеются методические указания по их выполнению, включающие необходимый теоретический и практический материал, содержащие элементы и последовательную инструкцию по проведению выбранной работы, индивидуальные варианты заданий, требования и форму отчётности по данной работе.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала

изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
Б1.В.ДВ.04.02 «Методы и средства защиты от вредоносного программного обеспечения»

Фонд оценочных средств
по дисциплине
Б1.В.ДВ.04.02 «Методы и средства защиты от вредоносного программного обеспечения»

Код и направление подготовки (специальность)	38.03.04 Государственное и муниципальное управление
Направленность (профиль)	Модератор государственных и муниципальных услуг
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2022
Институт / факультет	Институт инженерно-экономического и гуманитарного образования
Выпускающая кафедра	кафедра "Экономика и управление организацией"
Кафедра-разработчик	кафедра "Экономика и управление организацией"
Объем дисциплины, ч. / з.е.	144 / 4
Форма контроля (промежуточная аттестация)	Экзамен

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Общепрофессиональные компетенции			
	ОПК-5 Способен использовать в профессиональной деятельности информационно-коммуникационные технологии, государственные и муниципальные информационные системы; применять технологии электронного правительства и предоставления государственных (муниципальных) услуг;	ОПК-5.1 Знает современные информационно-коммуникационные технологии, государственные и муниципальные информационные системы	Знать современные информационно-коммуникационные технологии, государственные и муниципальные информационные системы
		ОПК-5.2 Использует современные программные средства при решении профессиональных задач	Уметь применять современные программные средства при решении профессиональных задач
	ОПК-8 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-8.1 Использует терминологию цифрового государственного управления в профессиональной деятельности	Знать терминологию цифрового государственного управления в профессиональной деятельности
		ОПК-8.2 Выполняет трудовые действия с использованием информационных технологий при решении задач профессиональной деятельности	Уметь решать задачи профессиональной деятельности с использованием информационных технологий
		ОПК-8.3 Выделяет смысловые конструкции для понимания научных текстов по профилю профессиональной деятельности и объясняет принципы работы описываемых информационных технологий	Владеть смысловыми конструкциями для понимания научных текстов по профилю профессиональной деятельности

Матрица соответствия оценочных средств запланированным результатам обучения

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Вредоносное ПО. Классификация, структура, принцип действия, каналы распространения				
ОПК-5.1 Знает современные информационно-коммуникационные технологии, государственные и муниципальные информационные системы	**Знать** современные информационно-коммуникационные технологии, государственные и муниципальные информационные системы	подготовка к экзамену	Нет	Да
		отчет по лабораторным работам	Да	Нет
		Составление конспектов	Да	Нет

ОПК-5.2 Использует современные программные средства при решении профессиональных задач	**Уметь** применять современные программные средства при решении профессиональных задач	подготовка к экзамену	Нет	Да
ОПК-8.1 Использует терминологию цифрового государственного управления в профессиональной деятельности	**Знать** терминологию цифрового государственного управления в профессиональной деятельности	Составление конспектов	Да	Нет
		отчет по лабораторным работам	Да	Нет
		подготовка к экзамену	Нет	Да
ОПК-8.2 Выполняет трудовые действия с использованием информационных технологий при решении задач профессиональной деятельности	**Уметь** решать задачи профессиональной деятельности с использованием информационных технологий	подготовка к экзамену	Нет	Да
		отчет по лабораторным работам	Да	Нет
ОПК-8.3 Выделяет смысловые конструкции для понимания научных текстов по профилю профессиональной деятельности и объясняет принципы работы описываемых информационных технологий	**Владеть** смысловыми конструкциями для понимания научных текстов по профилю профессиональной деятельности	отчет по лабораторным работам	Да	Нет
		подготовка к экзамену	Нет	Да
Защита информационных систем от вредоносного программного обеспечения.				
ОПК-5.1 Знает современные информационно-коммуникационные технологии, государственные и муниципальные информационные системы	**Знать** современные информационно-коммуникационные технологии, государственные и муниципальные информационные системы	подготовка к экзамену	Нет	Да
		отчет по лабораторным работам	Да	Нет
		Составление конспектов	Да	Нет
ОПК-5.2 Использует современные программные средства при решении профессиональных задач	**Уметь** применять современные программные средства при решении профессиональных задач	подготовка к экзамену	Нет	Да
ОПК-8.1 Использует терминологию цифрового государственного управления в профессиональной деятельности	**Знать** терминологию цифрового государственного управления в профессиональной деятельности	подготовка к экзамену	Нет	Да
		отчет по лабораторным работам	Да	Нет
		Составление конспектов	Да	Нет

ОПК-8.2 Выполняет трудовые действия с использованием информационных технологий при решении задач профессиональной деятельности	**Уметь** решать задачи профессиональной деятельности с использованием информационных технологий	подготовка к экзамену	Нет	Да
		отчет по лабораторным работам	Да	Нет
ОПК-8.3 Выделяет смысловые конструкции для понимания научных текстов по профилю профессиональной деятельности и объясняет принципы работы описываемых информационных технологий	**Владеть** смысловыми конструкциями для понимания научных текстов по профилю профессиональной деятельности	отчет по лабораторным работам	Да	Нет
		подготовка к экзамену	Нет	Да

1.1. Примерный перечень вопросов для подготовки к промежуточной аттестации (экзамен)

1. Вредоносное программное обеспечение.
2. Типы ВПО.
3. Компьютерный вирус.
4. Компьютерный червь.
5. Троянская программа.
6. Вредоносная утилита.
7. Каналы проникновение ВПО.
8. Ущерб ВПО.
9. Понятие киберпреступности. Виды киберпреступностей.
10. Понятие киберпреуступника. Классификация киберпреступников.
11. Понятие кибербезопасности. Принцип действия кибербезопасности. Виды мер кибербезопасности.
12. Защита от ВПО. Применение защиты в ИС. Виды средств защиты.
13. Аппаратные средства защиты.
14. Программные средства защиты.
15. Понятие антивируса. Цели и задачи антивируса. Структура антивируса. Принцип работы.
16. Методы обнаружения и устранения вредоносного ПО.
17. Организационные средства защиты.
18. Понятие и принцип политики безопасности. Построение антивирусной защиты.
19. Анализ рисков. Этапы проведения анализа рисков.
20. Планирование мер по обеспечению ИБ.
21. Правовые средства и методы защиты от ВПО.
22. Понятие защиты от ВПО в ПО. Понятие дефекта. Типы дефектов. Причины дефектов. Устранение дефектов.
23. Понятие защиты от ВПО в ПО.
24. Понятие уязвимостей. Причины появления уязвимостей. Защита от уязвимостей.
25. Типы уязвимостей. Источники появления уязвимостей. Устранение уязвимостей.
26. Протоколирование уязвимостей. Политика разглашения информации об уязвимостях. Классификации уязвимостей.
27. Понятие и принцип взлома ПО. Виды взлома ПО.
28. Понятие технических методов защиты ПО. Виды технических методов защиты ПО.
29. Понятие организационных методов защиты ПО. Виды организационных методов защиты ПО.
30. Оценка эффективности систем защиты программного обеспечения.
31. Анализ средств преодоления систем защиты программного обеспечения.
32. Испытания программных средств на наличие вредоносного ПО (ГОСТ Р 51188).
33. Особенности тестирования безопасности ПО.
34. Статический анализ исходного кода
35. Динамический анализ исходного кода
36. Выявление вредоносного кода в ПО.
37. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации.
38. Сертификационные испытания программных средств.

39. Сравнение моделей угроз лицензионного и пиратского ПО.
40. Аттестация программного обеспечения на отсутствие недекларированных возможностей.

1.2. Вопросы к отчету по лабораторным работам

1. Исследование привязывающего shell-кода.
2. Исследование уязвимости переполнения кучи.
3. Исследования уязвимости переполнения стека.
4. Перехват системных вызовов при помощи загружаемых модулей ядра.
5. Основы работы с пакетом Metasploit Framework.

1.3. Вопросы для самостоятельного изучения

1. Потенциально-нежелательные программы.
2. Каналы проникновение ВПО в операционную систему (на ЭВМ).
3. Ущерб ВПО (основной и второстепенный).
4. Признаки присутствия ВПО в ИС. Виды проявлений.
5. Определение хакеров. Виды хакеров. Понятие анонимуса, хактивизма и манифеста хакера.
6. Принцип действия кибербезопасности.
7. Виды мер кибербезопасности.
8. Принцип построение защиты информационной системы на основе программных средств защиты.
9. Цели и задачи антивируса. Структура антивируса.
10. Принцип работы и функционал антивируса.
11. Методы обнаружения и устранения вредоносного ПО в Windows-подобных ОС.
12. Методы обнаружения и устранения вредоносного ПО в Linux-подобных ОС.
13. Принцип построение защиты информационной системы на основе организационных средств.
14. Виды организационных средств защиты.
15. Построение антивирусной защиты.
16. Законы, регламентирующие информационную безопасность и защиту от ВПО.
17. Построение антивирусной защиты.
18. Компьютерная криминалистика. Принципы работы.
19. Определение шелл-кода. Типы шелл-кода.
20. Понятие «Кучи». Принцип организации и защиты от переполнения кучи.
21. Понятие «Стэк». Принцип организации и защиты от переполнения стэка.
22. Понятие «Форматированные строки». Принцип организации и защиты от уязвимостей форматных строк.

1-й этап процедуры оценивания: **оценивание уровня достижения каждого из-запланированных результатов обучения – дескрипторов (знаний, умений, владений) в соответствии со шкалами и критериями, установленными картами компетенций ОПОП. Экспертной оценке преподавателя подлежит сформированность отдельных дескрипторов, для оценивания которых предназначена данная оценочная процедура текущего контроля и промежуточной аттестации согласно матрице соответствия оценочных средств результатам обучения.**

2-й этап процедуры оценивания: **интегральная оценка достижения обучающимся запланированных результатов обучения по итогам отдельных видов текущего**

контроля и промежуточной аттестации.

Учебная дисциплина, как правило, формирует несколько компетенций, процедура оценивания реализуется поэтапно:

1-й этап процедуры оценивания: оценивание уровня достижения каждого из запланированных результатов обучения – дескрипторов (знаний, умений, владений) в соответствии со шкалами и критериями, установленными картами компетенций ОПОП. Экспертной оценке преподавателя подлежит сформированность отдельных дескрипторов, для оценивания которых предназначена данная оценочная процедура текущего контроля и промежуточной аттестации согласно матрице соответствия оценочных средств результатам обучения.

2-й этап процедуры оценивания: интегральная оценка достижения обучающимся запланированных результатов обучения по итогам отдельных видов текущего контроля и промежуточной аттестации.