Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.В.05
Методы защиты программного обеспечения
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и вычислительной техники**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **5 ЗЕТ**

Часов по учебному плану 180
в том числе:
аудиторные занятия 80
самостоятельная работа 63
контактная работа во время промежуточной аттестации (ИКР) 0
часов на контроль 34,7

Виды контроля в семестрах:
экзамены 7
курсовые работы 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	15 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Практические	16	16	16	16
Индивидуальные консультации	0,5	0,5	0,5	0,5
Контактная работа на аттестации (в период экз. сессий)	0,3	0,3	0,3	0,3
Контактная работа на аттестации	0,5	0,5	0,5	0,5
Консультации перед экзаменом	1	1	1	1
В том числе в форме практ.подготовки	8		8	
Итого ауд.	80	80	80	80
Контактная работа	82,3	82,3	82,3	82,3
Сам. работа	63	63	63	63
Часы на контроль	34,7	34,7	34,7	34,7
Итого	180	180	180	180

Программу составил(и):
к.ф.-м.н., доцент, Бужан В.В.

Рецензент(ы):
д.т.н, профессор кафедры информационных систем и программирования КубГТУ, Хисамов Ф.Г.;директор АО «ЮГ-СИСТЕМА ПЛЮС», Глебов О.В.

Рабочая программа дисциплины
Методы защиты программного обеспечения

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:
10.03.01 Информационная безопасность
утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры
Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	формирование целостного представления о современных организационных,
1.2	технических, алгоритмических и других методах и средствах защиты
1.3	компьютерной информации, используемых в современных криптосистемах,
1.4	знакомство с законодательством и стандартами в этой области.
Задачи: Сформировать у обучающихся следующие способности – принимать эффективные проектные решения в условиях неопределенности и риска – использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Системы охраны и инженерной защиты информации
2.1.2	Безопасность систем баз данных
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Производственная практика: Преддипломная практика
2.2.3	Комплексная защита объектов информатизации

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
УК-3: Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	
УК-3.1: Определяет свою роль в команде, исходя из стратегии сотрудничества для достижения поставленной цели	
Знать	
Уровень 1	Минимальный необходимый уровень знаний определения своей роли в команде, исходя из стратегии сотрудничества для достижения поставленной цели
Уровень 2	Уровень знаний определения своей роли в команде, исходя из стратегии сотрудничества для достижения поставленной цели в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний определения своей роли в команде, исходя из стратегии сотрудничества для достижения поставленной цели в объёме, соответствующем программе подготовки, без ошибок
УК-3.2: При реализации своей роли в команде учитывает особенности поведения других членов команды	
Уметь	
Уровень 1	Продемонстрированы основные умения учитывать особенности поведения других членов команды, при реализации своей роли в команде, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения учитывать особенности поведения других членов команды, при реализации своей роли в команде, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения учитывать особенности поведения других членов команды, при реализации своей роли в команде, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
УК-3.3: Анализирует возможные последствия личных действий и планирует свои действия для достижения заданного результата	
Владеть	
Уровень 1	Имеется минимальный набор навыков для анализа возможных последствий личных действий и планирования свои действия для достижения заданного результата с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки для анализа возможных последствий личных действий и планирования свои действия для достижения заданного результата с некоторыми недочётами
Уровень 3	Продемонстрированы навыки для анализа возможных последствий личных действий и планирования свои действия для достижения заданного результата без ошибок и недочётов
УК-3.4: Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели	
Уметь	
Уровень 1	Продемонстрированы основные умения осуществлять обмен информацией, знаниями и опытом с членами команды, оценивать идеи других членов команды для достижения поставленной цели, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения осуществлять обмен информацией, знаниями и опытом с членами

	команды, оценивать идеи других членов команды для достижения поставленной цели, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения осуществлять обмен информацией, знаниями и опытом с членами команды, оценивать идеи других членов команды для достижения поставленной цели, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
УК-3.5: Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат	
Знать	
Уровень 1	Минимальный необходимый уровень знаний установленных норм и правил командной работы, несет личную ответственность за общий результат
Уровень 2	Уровень знаний установленных норм и правил командной работы, несет личную ответственность за общий результат в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний установленных норм и правил командной работы, несет личную ответственность за общий результат в объёме, соответствующем программе подготовки, без ошибок

ПК-4: Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении	
ПК-4.1: Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем	
Знать	
Уровень 1	Минимальный необходимый уровень знаний разработки проектных документов на средства защиты информации создаваемых автоматизированных систем
Уровень 2	Уровень знаний разработки проектных документов на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний разработки проектных документов на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
ПК-4.2: Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем	
Уметь	
Уровень 1	Продемонстрированы основные умения подготовки технической и проектной документации по вопросам создания и эксплуатации автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения подготовки технической и проектной документации по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения подготовки технической и проектной документации по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-4.3: Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков проверки программы и алгоритмы на предмет соответствия требованиям защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки проверки программы и алгоритмы на предмет соответствия требованиям защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки проверки программы и алгоритмы на предмет соответствия требованиям защиты информации без ошибок и недочётов
ПК-4.4: Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем
Уровень 2	Уровень знаний Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения проведения сравнительного анализ вариантов конфигураций и состава автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные проведения сравнительного анализ вариантов конфигураций и состава автоматизированных систем, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные проведения сравнительного анализ вариантов конфигураций и состава

	автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем без ошибок и недочётов
ПК-4.5: Предлагает конфигурации и состав автоматизированной системы	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Предлагает конфигурации и состав автоматизированной системы
Уровень 2	Уровень знаний Предлагает конфигурации и состав автоматизированной системы в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Предлагает конфигурации и состав автоматизированной системы в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Предлагает конфигурации и состав автоматизированной системы, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Предлагает конфигурации и состав автоматизированной системы, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Предлагает конфигурации и состав автоматизированной системы, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков предложения конфигурации и состав автоматизированной системы с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки предложения конфигурации и состав автоматизированной системы с некоторыми недочётами
Уровень 3	Продемонстрированы навыки предложения конфигурации и состав автоматизированной системы без ошибок и недочётов

ПК-5: Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла	
ПК-5.1: Проверяет соответствие внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности	
Знать	
Уровень 1	Минимальный необходимый уровень знаний проверки соответствий внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности
Уровень 2	Уровень знаний проверки соответствий внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний проверки соответствий внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности в объёме, соответствующем программе подготовки, без ошибок
ПК-5.2: Восстанавливает работоспособность автоматизированных систем после инцидентов информационной безопасности	
Уметь	
Уровень 1	Продемонстрированы основные умения восстановления работоспособности автоматизированных систем после инцидентов информационной безопасности, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения восстановления работоспособности автоматизированных систем после инцидентов информационной безопасности, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения восстановления работоспособности автоматизированных систем после инцидентов информационной безопасности, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-5.3: Проводит операции вывода защищённых автоматизированных систем из эксплуатации	
Владеть	
Уровень 1	Имеется минимальный набор навыков проведения операции вывода защищённых автоматизированных систем

	из эксплуатации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки проведения операции вывода защищённых автоматизированных систем из эксплуатации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки проведения операции вывода защищённых автоматизированных систем из эксплуатации без ошибок и недочётов

ПК-7: Способен определять уровень защищённости автоматизированных систем	
ПК-7.1: Формулирует целевые показатели функционирования защищенных автоматизированных систем	
Знать	
Уровень 1	Минимальный необходимый уровень знаний формулирований целевых показателей функционирования защищенных автоматизированных систем
Уровень 2	Уровень знаний формулирований целевых показателей функционирования защищенных автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний формулирований целевых показателей функционирования защищенных автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
ПК-7.2: Анализирует уязвимости автоматизированных систем в соответствии с нормативными документами	
Уметь	
Уровень 1	Продемонстрированы основные умения анализирования уязвимости автоматизированных систем в соответствии с нормативными документами, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения анализирования уязвимости автоматизированных систем в соответствии с нормативными документами, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения анализирования уязвимости автоматизированных систем в соответствии с нормативными документами, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-7.3: Формулирует угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы	
Владеть	
Уровень 1	Имеется минимальный набор навыков формулирования угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулирования угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулирования угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы без ошибок и недочётов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Раздел 1. Введение в теорию обеспечения безопасности программного обеспечения					
1.1	Жизненный цикл программного обеспечения компьютерных систем /Лек/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

1.2	Технологическая и эксплуатационная безопасность программ /Лек/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.3	Модель угроз и принципы обеспечения безопасности программного обеспечения /Лаб/	7	8	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.4	Модель угроз и принципы обеспечения безопасности программного обеспечения /Пр/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 2. Раздел 2. Обеспечение технологической безопасности программного обеспечения					
2.1	Формальные методы доказательства правильности программ и их спецификаций /Лек/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
2.2	Методы и средства анализа безопасности программного обеспечения /Лек/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

2.3	Методы обеспечения надежности программ для контроля их технологической безопасности /Лаб/	7	6	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
2.4	Методы создания алгоритмически безопасных процедур /Лек/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
2.5	Методы идентификации программ и их характеристик /Пр/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 3. Раздел 3. Обеспечение эксплуатационной безопасности программного обеспечения					
3.1	Методы и средства защиты программ от компьютерных вирусов /Лек/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
3.2	Методы защиты программного обеспечения от внедрения на этапе его эксплуатации /Лек/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

3.3	Методы выявления программных закладок /Лаб/	7	6	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
3.4	Средства обеспечения целостности и достоверности используемого программного кода /Лаб/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
3.5	Защита программ от несанкционированного копирования /Лаб/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 4. Раздел 4. Правовая и организационная поддержка процессов разработки и применения программного обеспечения					
4.1	Нормативные документы, регламентирующие защищённость программного обеспечения и обрабатываемой информации /Лек/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
4.2	Сертификационные испытания программных средств /Лаб/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

4.3	Безопасность программного обеспечения и человеческий фактор /Пр/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
4.4	Психология программирования /Пр/	7	4	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
4.5	/Ср/	7	63			
	Раздел 5. Промежуточная аттестация					
5.1	/КАЭ/	7	0,3	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
5.2	/Консл/	7	1	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
5.3	/КА/	7	0,5	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

5.4	/ИК/	7	0,5	УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Объект защиты информации.
2. Угрозы безопасности информации в компьютерных системах.
3. Методика оценки возможностей противника.
4. Типовые требования к средствам защиты, предъявляемые пользователем.
5. Количественные характеристики уровня защиты.
6. Правовые методы защиты информации.
7. Организационные методы защиты информации.
8. Криптографические методы защиты информации.
9. Стеганографические методы защиты информации.
10. Инженерно-технические методы защиты информации.
11. Программные методы защиты информации.
12. Федеральный закон “ Об информации, информатизации и защите информации”.
13. Закон Российской Федерации “О государственной тайне”.
14. Особенности юридической защиты коммерческой тайны.
15. Правовая защита интеллектуальной собственности.
16. Оценка надежности шифров перестановки и простой замены. Дешифрование.
17. Частотные характеристики знаков и биграмм открытого текста.
18. Теоретическая и практическая стойкость криптографических алгоритмов.
19. Шифры многоалфавитной замены. Коды.
20. Подстановочные и перестановочные шифры.
21. Блочные шифры.
22. Стандарты шифрования DES и ГОСТ 28147-89.
23. Поточные и дисковые шифраторы.
24. Скремблеры и способы их дешифрования методом “игры в кубики”.
25. Шифры гаммирования. Шифр Виженера. Программный шифр гаммирования RC-4.
26. Сравнительный анализ блочных и поточных шифров.
27. Понятие о криптографическом анализе на примере шифров гаммирования.
28. Асимметричные системы шифрования.
29. Однонаправленные преобразования, система RSA.
30. Открытое распределение ключей.
31. Задача защиты сообщения от искажений.
32. Электронная подпись с помощью однонаправленных преобразований.
33. Электронная подпись по системе RSA и по системе Эль-Гамаля.
34. Задача выбора хеш-функции электронной подписи.
35. Сложность задачи разложения большого целого числа на множители.
36. Сложность задачи дискретного логарифмирования по большому простому модулю.
37. Особенности защиты информации в вычислительной системе.
38. Основные угрозы безопасности вычислительной системы.
39. Наблюдение за каналами связи. Задержка, изменение, подмена сообщений.
40. Перехват побочных излучений. Установка “жучков”.
41. Организация отводов для получения парольной информации и прав доступа.
42. Классификация компьютерных вирусов.
43. Получение конфиденциальных охраняемых сведений из базы данных.
44. Получение полномочий других пользователей и супервизора системы.
45. Анализ программного обеспечения с целью выявления слабых мест в защите.
46. Изменение программного обеспечения (“троянский конь” и т.п.).
47. Методы разграничения доступа. Требования к выбору и использованию паролей.
48. Подтверждение подлинности по модели “рукопожатия”.
49. Методы поддержания целостности информации.
50. Классификация компьютерных вирусов.
51. Антивирусные программы, их достоинства и недостатки.
52. Методы поддержания конфиденциальности информации.

53. Физическая защита вычислительного центра и каналов связи.
54. Методы защиты программного обеспечения от копирования и анализа.
55. Оптимизация взаимодействия пользователей и обслуживающего персонала.
56. Организация работ с конфиденциальными информационными ресурсами.
57. Противодействие наблюдению в оптическом диапазоне.
58. Средства борьбы с закладными подслушивающими устройствами.
59. Защита от злоумышленных действий обслуживающего персонала и пользователей.
60. Методы защиты от побочных электромагнитных излучений и наводок.
61. Противодействие несанкционированному подключению устройств.
62. Защита внутреннего монтажа, средств управления и коммутации.
63. Контроль целостности программной структуры в процессе эксплуатации.
64. Система разграничения доступа к информации.
65. Методы, препятствующие использованию скопированной информации.
66. Защита программных средств от исследования.
67. Большие числа и способы их представления.
68. Криптография с несколькими открытыми ключами.
69. Формальный анализ протоколов проверки подлинности и обмена ключами.
70. Разделение секрета.
71. Совместное использование секрета.
72. Электронные деньги.
73. Шифрование коммуникационных каналов.
74. Алгоритм цифровой подписи ГОСТ.
75. Протокол управления секретными ключами компании IBM.

5.2. Темы письменных работ

1. Мотивы действий компьютерных хакеров.

2. Использование средств активной разведки в компьютерных системах и сетях.

3. Средства атак на пароли в системах аутентификации.

4. Российские стандарты в области средств идентификации и аутентификации.

5. Международные стандарты в области средств идентификации и аутентификации.

6. Методы социальной инженерии в компьютерных системах.

7. Эволюция парольной аутентификации в ОС Unix.

8. Обзор стандартов и руководств по управления паролями.

9. Способы управления выбором паролей.

10. Способы организации словарных атак на пароли.

11. Способы хранения паролей в компьютерных системах.

12. Средства атаки на пароли BIOS.

13. Методы атак на устройства аутентификации.

14. Основные причины успеха компьютерных преступлений.

15. Эволюция методов аутентификации в ОС Windows.

16. Средства аутентификации в компьютерных системах Apple Macintosh.

17. Эволюция алгоритмов симметричной криптографии и атак на них.

18. Методы шифрования на основе условного (депонированного) ключа.

19. Способы усиления парольной аутентификации.

20. Сертифицированные средства шифрования файлов.

21. Сертифицированные средства шифрования дисков.

22. Возможности пользователей по запоминанию сложных паролей.

23. Обзор и сравнительный анализ средств хранения парольных баз данных.

24. Эволюция методов и средств биометрической аутентификации.

25. Атаки на системы биометрической аутентификации.

26. Способы защиты от подбора паролей.

27. Обзор средств «запоминания» паролей в сетевых службах.

28. Особенности биометрической аутентификации.

29. Обзор средств шифрования информации на флэш-дисках.

30. Обзор функций хеширования паролей в ОС и СУБД.

31. Обзор средств генерации паролей.

32. Обзор средств выявления «слабых» паролей.

33. Обзор средств фильтрации паролей.

34. Использование биометрии в идентификационных картах и паспортах.

35. Практическое применение биометрии в России.

36. Другая тема, выбранная студентом и согласованная с преподавателем.

5.3. Фонд оценочных средств

1 Службы безопасности предназначенные для защиты от атак доступа

конфиденциальность, идентифицируемость
целостность, идентифицируемость
доступность , целостность
идентифицируемость, доступность

2 Какое свойство службы безопасности предназначаются для защиты от атак отказа в обслуживании?

конфиденциальность
целостность
доступность
идентифицируемость

3 Для защиты от атак какого типа предназначена служба конфиденциальности?

атаки доступа
атаки модификации
атаки отказа в обслуживании
атаки отказа от обязательств

4 Для защиты от атак какого типа предназначена служба доступности?

атаки доступа
атаки модификации
атаки отказа в обслуживании
атаки отказа от обязательств

5 К механизмам конфиденциальности относятся:

идентификация и аутентификация
шифрование файлов
правильное управление ключами при использовании шифрования

6 Обеспечивает секретность информации, открывает доступ к информации только аутентифицированным пользователям

служба конфиденциальности
служба целостности

служба доступности
служба идентифицируемости

7 Атака доступа направлена на:

нарушение конфиденциальности информации
уничтожение компьютера
уничтожение информации

8 Поддерживает готовность информации к работе, позволяет обращаться к компьютерным системам, хранящимся в этих системах данным и приложениям

служба конфиденциальности
служба целостности
служба доступности
служба идентифицируемости
служба идентифицируемости

9 Для обеспечения конфиденциальности потока данных применяются методы:

физической защиты
скрытия информации
аудита

10 Переключение по отказу:

предотвращает полную потерю информации при случайном или преднамеренном уничтожении файлов
обеспечивает восстановление информации и сохранение производительности
защищает системы, информацию и производственные мощности от стихийных бедствий

11 Выделите верное утверждение в отношении информационной безопасности.

наступление нового этапа развития ИТ приводит к быстрому повышению уровня информационной безопасности
наступление нового этапа развития ИТ приводит к быстрому падению уровня информационной безопасности
уровень информационной безопасности не зависит от этапов развития ИТ

12 Какие меры должен в себя включать комплексный подход к обеспечению информационной безопасности?

Законодательные, административные, процедурные, научно-технические
Социальные, Законодательные, административные, процедурные, моральные
Административные, процедурные, научно-технические, моральные
Процедурные, Социальные, Законодательные, административные
научно-технические, Социальные, Законодательные, административные, процедурные

13К какому уровню обеспечения ИБ относятся действия общего и специального характера, предпринимаемые руководством организации?

законодательный
административный
процедурный
научно-технический

14 К какому уровню обеспечения ИБ относятся конкретные методики, программно-аппаратные, технологические и технические меры?

законодательный
административный
процедурный
научно-технический

15 В организации проводятся проверки «чистый стол», целью которых является выявление нарушений требований по хранению ключевых носителей и конфиденциальных документов. К какому уровню обеспечения ИБ они относятся?

законодательный
административный
процедурный
научно-технический

16 Какой термин определяет защищенность информации, ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений —

производителям, владельцам и пользователям информации и поддерживающей инфраструктуре?
стратегическая безопасность
информационная безопасность
экономическая безопасность
корпоративная безопасность

17 Какой аспект информационной безопасности отражает то, что защищенная информация должна быть доступна только тому, кому она предназначена?

целостность
конфиденциальность
доступность

18 Какой аспект информационной безопасности отражает актуальность и непротиворечивость информации, её защищенность от разрушения и несанкционированного изменения?

целостность
конфиденциальность
доступность

19 Если злоумышленник подменил исходное сообщение, передаваемое по сети Интернет, какое свойство информации он нарушил?

целостность
конфиденциальность
доступность

20 Какой аспект ИБ наиболее актуален для провайдера Интернет-услуг?

целостность
конфиденциальность
доступность

21 Какой аспект ИБ наиболее актуален для фармацевтической компании, занимающейся разработкой новых лекарств?

целостность
конфиденциальность
доступность

22 Какая из нижеперечисленных угроз представляет наибольшую опасность?

вредоносные программы
хакерские атаки
действия инсайдеров
финансовое мошенничество

23 Как называется практически бесполезная информация, рассылаемая абонентам электронной почты?

DoS
Virus
Spam
Worm

24 Что принято считать ресурсом или активом информационной системы?

модель информационной системы
все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет
именованный элемент информационной системы, имеющий (материальную) ценность и подлежащий защите

25 Какие из перечисленных вариантов решений в отношении рисков являются неуместными:

принят, устранен
принят, дезавуирован
дезавуирован, отклонен

26 Какой из перечисленных классов функциональных требований включает требования кодирования информации?

класс приватности (конфиденциальности)”
класс защиты функций безопасности объекта
класс криптографической поддержки (криптографической защиты)

27 Что представляет собой событие – триггер?

событие, повлекшее реализацию или дальнейшее развитие рисков и являющееся идентификатором риска
событие, увеличивающее время отклика web – сервера
это одна из разновидностей атак на сервер

28 Что формируют потенциальные злоумышленные действия по отношению к объектам?

вероятностный набор действий по подавлению угроз
шаблоны мер потенциального противодействия
набор угроз ИБ

29 Что из перечисленного предписывается выполнить при проектировании системы с полным перекрытием?

выверить остаточную стоимость активов
детально прописать пути потенциального проникновения
согласовать порядок применения альтернативных инструментов защиты

30 Может ли анализ угроз каким-то образом помочь при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня?

нет
да
спорно

31 Чем определяется высокая стойкость системы?

уровнем стойкости функции безопасности объекта оценки, на котором она обеспечивает защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителем с высоким потенциалом нападения
уровнем стойкости, при котором обеспечивается защита от целенаправленного нарушения безопасности объекта оценки нарушителем с умеренным потенциалом нападения
уровнем стойкости функции безопасности объекта оценки, на котором обеспечивается адекватная защита от случайного нарушения безопасности ОО нарушителем с низким потенциалом нападения

32 Что обеспечивает базовая стойкость?

защиту от тщательно спланированного и организованного нарушения безопасности объекта оценки нарушителем с высоким потенциалом нападения
защиту от целенаправленного нарушения безопасности объекта оценки нарушителем с умеренным потенциалом нападения
адекватную защиту от случайного нарушения безопасности объекта оценки нарушителем с низким потенциалом нападения

33 Что из перечисленного предписывается выполнить при проектировании системы с полным перекрытием?

выверить остаточную стоимость активов
детально прописать пути потенциального проникновения
согласовать порядок применения альтернативных инструментов защиты

34 Что определяет ресурсы или активы ИС?

модель ИС
все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет
именованный элемент ИС, имеющий (материальную) ценность и подлежащий защите

35 Каковы цели анализа и тестирования прикладных систем в аспектах информационной безопасности?

оперативное внесение изменений в операционные системы
обеспечение целостности программного обеспечения
обеспечение более эффективного использования готовых пакетов программ

36 Окно опасности перестает существовать, когда:

администратор безопасности узнает об угрозе
производитель ПО выпускает заплату
заплата устанавливается в защищаемой ИС

37 Окно опасности появляется, когда:

становится известно о средствах использования уязвимости
появляется возможность использовать уязвимость
устанавливается новое ПО

38 Окно опасности – это:

промежуток времени
часть пространства
плохо закрепленная деталь строительной конструкции

39 Самыми опасными источниками внутренних угроз являются:

некомпетентные руководители
обиженные сотрудники
любопытные администраторы

40 Самыми опасными источниками угроз являются:

внутренние
внешние
пограничные

41 Самыми опасными угрозами являются:

непреднамеренные ошибки штатных сотрудников
вирусные инфекции
атаки хакеров

42 Агрессивное потребление ресурсов является угрозой:

доступности
конфиденциальности
целостности

43 Перехват данных является угрозой:

доступности
конфиденциальности
целостности

44 Дублирование сообщений является угрозой:

доступности
конфиденциальности
целостности

45 Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:

отсутствие целостной концепции безопасности при проектировании базового программного обеспечения
просчеты при реализации базового программного обеспечения
недостаточное тестирование базового программного обеспечения

46 Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:

использование недостаточно апробированных технологий
архитектурные просчеты при построении информационных систем
использование приложений, полученных из ненадежных источников

47 Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:

просчеты при администрировании информационных систем
необходимость постоянной модификации информационных систем
сложность современных информационных систем

48 Выберите вредоносную программу, которая открыла новый этап в развитии данной области:

Melissa
Bubble Boy
ILOVEYOU

49 Для внедрения бомб чаще всего используются ошибки типа:

отсутствие проверок кодов возврата
переполнение буфера
нарушение целостности транзакций

50 Меры информационной безопасности направлены на защиту от:

нанесения неприемлемого ущерба
нанесения любого ущерба
подглядывания в замочную скважину

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых верный(ые). Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Угринович Н. Д.	Информатика. Практикум: Учебное пособие	Москва: КноРус, 2021, URL: https://book.ru/book/940090
Л1.2	Коваленко Ю.И.	Защита информационных технологий: Словарь	Москва: Русайнс, 2020, URL: https://book.ru/book/936189
Л1.3	Дергачев К. В., Титарев Д. В.	Защита информации: лабораторный практикум: Учебное пособие	Москва: Русайнс, 2021, URL: https://book.ru/book/940250
Л1.4	Голицына О. Л., Партыка Т. Л.	Программное обеспечение: Учебное пособие	Москва: Издательство "ФОРУМ", 2019, URL: http://znanium.com/catalog/document?id=359201

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Прохорский Г. В.	Информатика. Практикум: Учебное пособие	Москва: КноРус, 2021, URL: https://book.ru/book/941449
Л2.2	Угринович Н. Д.	Информатика: Учебник	Москва: КноРус, 2020, URL: https://book.ru/book/932057

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	Национальный открытый университет "ИНТУИТ". - Режим доступа: https://www.intuit.ru/studies/courses%20
Э2	Электронно-библиотечная система . - Режим доступа: http://znanium.com/%20
Э3	ЭИОС. - Режим доступа: http://eios.imsit.ru/
Э4	ЭБС Айбукс. - Режим доступа: http://www.ibooks.ru/
Э5	Методы и средства криптографической защиты информации ресурсы. - Режим доступа: http://rpd.eios.imsit.ru:8080/RPD/Index/1636711/%20http://www.book.ru

6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL

6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL
6.3.2. Перечень профессиональных баз данных и информационных справочных систем	
6.3.2.1	Консультант Плюс http://www.consultant.ru
6.3.2.2	Кодекс – Профессиональные справочные системы https://kodeks.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
120	Кабинет технологий и методов программирования	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate Klite Mega Codec Pack УМКК "Объектно-ориентированные технологии» УМКК "Основы алгоритмизации и программирования» Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная панель EliteBoard LR-75UT40i7 - 1 шт., соответствующее программное обеспечение
119	Лаборатория системного и прикладного программирования	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение

		MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Embarcadero RAD Studio XE8 Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express AnyLogic Archimate Klite Mega Codec Pack MS Office Standart 2007 Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.
Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.
Учебный материал по дисциплине «Методы защиты программного обеспечения», разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ. Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).
Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.

Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.
Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Методы защиты программного обеспечения».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.
Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями