КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

2025

Рабочая программа по дисциплине «Программно-аппаратные средства защиты Информации» по специальности 10.05.01 Компьютерная безопасность, специализации «Разработка защищенного программного обеспечения», составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «26» ноября 2020 г. № 1459, профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 533н, профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. №525н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины

Цели определены государственным образовательным стандартом высшего образования и соотнесены с общими целями ООП ВО по специальности подготовки «Компьютерная безопасность», в рамках которой преподается дисциплина.

Целью преподавания и изучения дисциплины «Программно-аппаратные средства защиты информации» является формирование у бакалавров знаний о работе программноаппаратных комплексов защиты информации(КЗИ), умений по настройке и обслуживанию таких комплексов, навыков по развёртыванию и внедрению комплексов в информационные системы.

Основные задачи освоения дисциплины:

− Работа с программно апаратными комплексами защиты информации;

В результате освоения дисциплины студент должен:

Знать:

− принципы работы программно-аппаратных КЗИ,

− основные компоненты и их назначение;

− базовые конфигурации программных компонентов и стандартные настройки аппаратных частей КЗИ

Уметь:

− настраивать программные конфигурации КЗИ;

− обслуживать аппаратные компоненты КЗИ;

− собирать и анализировать данные, предоставляемые КЗИ о работе информационной системы;

− собирать и анализировать данные, предоставляемые КЗИ о угрозах и уязвимостях информационной системы;

− собирать и анализировать данные, предоставляемые КЗИ о работе пользователей в информационных системах. Иметь навыки (приобрести опыт):

− в решении типовых задач информационной безопасности на программноаппаратных КСЗ.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратные средства защиты информации» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» основной образовательной программы – программы специалитета по специальности 10.05.01 Компьютерная безопасность специализация «Разработка защищенного программного обеспечения».

Код компетенции	Предшествующие дисциплины (модули), практики	Изучаемые в текущем семестре дисциплины (модули), практики	Последующие дисциплины (модули), практики
ОПК-13	-	Программно-аппаратные средства защиты информации	-

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование у обучающихся компетенций.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	ОПК-13.1 Применяет знания основных уязвимостей программного обеспечения при разработке компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах	Знает основные программные компоненты КЗИ и их назначение, принципы работы аппаратных компонентов КЗИ, особенности реализации формирования политики информационной безопасности в КЗИ, принципы реализации защиты от основных угроз безопасности информации в КЗИ Умеет настраивать основные компоненты программно-аппаратных КЗИ, проводить плановые мероприятия по обслуживанию аппаратных компонент КЗИ, выполнять настройку политики информационной безопасности в КЗИ в соответствии с регламентирующими документами, разрабатывать инструкции по работе с пользователей информационной системы по работе с компонентами КЗИ, их касающихся, собирать и анализировать данные, предоставляемые КЗИ о угрозах и уязвимостях информационной системы.
	ОПК-13.3. Демонстрирует умение проводить анализ безопасности компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах	Имеет навыки в решении типовых задач информационной безопасности на программно-аппаратных КСЗ, Имеет практический опыт оценки качества работы различных примеров аппаратных средств защиты информации и выбора подходящего средства для решения задач информационной безопасности

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

очная форма обучения

Вид учебной деятельности		ак.часов	
		Всего	По семестрам
			4
1. Контактная работа обучающихся с преподавателем:		69	69
Аудиторные занятия, часов всего, в том числе:		68	68
• занятия лекционного типа		34	34
• занятия семинарского типа:		-	-
практические занятия		-	-
лабораторные занятия		34	34
в том числе занятия в форме практической подготовки		-	-
Консультации		0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий		0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		39	39
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		19	19
- выполнение домашних заданий по практическим занятиям		10	10
- подготовка к текущему контролю		10	10
Промежуточная аттестация: зачет		-	-
ИТОГО:	часов	108	108
общая трудоемкость	зач. ед.	3	3

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

5.1. Содержание дисциплины

Тема 1. Введение. Общие вопросы ОБИ и дисциплины ПАСЗИ.

Связь дисциплины с другими дисциплинами учебного плана. Взаимосвязь понятий: защищенность, уязвимость, угроза, нарушитель, атака, ущерб, риск.

Виды программно-аппаратных (программно-технических) средств защиты информации. Отличия их от технических средств защиты информации. Каналы утечки компьютерной информации: защищаемые элементы; источники угроз; основные каналы утечки информации и средства их образования.

Тема 2. Защита от РПВ (ПМВ).

Понятие РПВ. Виды РПВ. Программные закладки (ПЗ): понятие ПЗ; виды ПЗ; модели работы (воздействия на компьютерные системы) ПЗ на компьютеры; защита от программных закладок (поиск недокументированных (недекларированных) возможностей); понятие изолированной программной среды и изолированного компьютера; контроль отсутствия НДВ. Защита от троянов и вредоносных утилит: утилиты скрытого администрирования

(backdoor), exploit'ы, rootkit'ы и просто трояны; кейлоггеры; руткиты (руткиты уровня пользователя, руткиты уровня ядра). Защита от троянов и руткитов. Защита от вирусов: понятие вируса; классификация вирусов; файловые вирусы; макровирусы; сетевые вирусы (черви); почтовые вирусы; загрузочные вирусы; методы защиты вирусов от обнаружения; вредоносные утилиты, специальные упаковщики и парольные взломщики; антивирусное ПО; методы защиты от вирусов и ПЗ; белый и черный ящики (Blacklisting и Whitelisting). Вредоносные программы для мобильных устройств. Внедрение вредоносного ПО через автозагрузку (реестр и Планировщик Windows): как устроен реестр; ключи автозагрузки; описание (определение) возможностей разных вариантов автозапуска программ; планировщик заданий в Windows.

Тема 3. Защита данных.

Направления и методы защиты данных: - контроль доступа к локальным портам, внешним носителям и принтерам; - разграничение доступа к ресурсам ПК; - антивирусная защита; - защита данных от утечки (DLP); - резервное копирование и восстановление (данных и разделов) - шифрование данных: - использование RAIDмассивов (RAID 1 - зеркало); - архивирование с паролем (WinRar); - устранение потенциальных опасностей хищения данных: - отслеживание временных файлов; - контроль записи на переносные носители; - отключение службы «Сервер»; - отключение удаленного доступа (RDP или терминальный сервер); - устранение потенциальных опасностей потери данных: - стабильное электропитание; - резервное копирование; - завершение транзакции записи «нового» перед удалением «старого» (чтобы не потерять «старое»); - контроль целостности программ и данных; - гарантированное уничтожение (затирание) данных. Программные средства резервного копирования (Acronis Backup). Программные средства восстановления: - данных - EasyRecovery - RStudio - GetDataBack - разделов - Acronis Partition Expert (в составе Acronis Disk Director) Программные средства защиты данных от утечки: - статистика состояния проблемы утечек информации; - задачи системы защиты от утечек данных; - классификация внутренних нарушителей; - использование DLP-систем для предотвращения утечки дан-ных: - принципы работы DLP; - основные функции DLP; - состав DLP и их виды:

- хостовые DLP; - шлюзовые DLP; - универсализация систем DLP; - примеры систем DLP; Средства шфрования данных: - EFS (можно зашифровывать отдельные папки) - BitLocker + TPM (зашифровывает весь раздел) Средства гарантированного уничтожения (затирания) данных: - Требования стандартов и руководящих документов к гарантированному уничтожению информации - Удаление информации - Виды остаточной информации - Восстановление удаленной информации - Виды гарантированного уничтожения - Достоинства и недостатки аппаратного и программного способов гарантированного уничтожения информации - Аппаратные средства уничтожения информации - Средства, использующие физический принцип воздействия магнитным полем - Средства,

использующие механический принцип воздействия - Программное гарантированное уничтожение информации - Наиболее известные алгоритмы затирания информации - Особенности гарантированного уничтожения информации с различных носителей - Сертифицированные программные средства удаления и затирания информации - Программа Terrier 3.0 - СЗИ Secret Net - СЗИ Dallas Lock 8.0 - СЗИ Страж NT - Бесплатные программные средства удаления и затирания информации - Программа Eraser - Программа CCleaner - Mem Reduct - Сравнение программных средств гарантированного уничтожения информации

Программные средства контроля целостности программ и данных.

Тема 4. Защита программ.

Направления защиты программ. Классификация средств атаки на средства защиты ПО. Классификация методов защиты ПО: - методы защиты от НСД к ПО: - защита с помощью регистрационных кодов; - защита на основе ключевого файла; - защита методом online регистрации; - защита на основе аппаратных (электронных) ключей; - защита с помощью протекторов («навесная» защита); - защита с помощью криптографических методов: - использование шифрования; - использование стеганографии (сокрытие информации в файлах с другой информацией); - методы защиты от НСК (ПО на носителе или самого носителя) - методы, затрудняющие считывание копируемой информации с материального носителя (стандартными методами копирования): - нестандартная разбивка (форматирование) носителя; - нанесение на поверхность носителя специальных меток; - преднамеренная порча (искажение) оглавления защищаемого носителя; - методы, препятствующие использованию скопированной информации; - привязка защищаемого ПО к уникальным характеристикам компьютера или носителя; - скрытое хранение данных или ПО (стеганография) или шифрование данных или ПО; - методы защиты от несанкционированного исследования, анализа и восстановления алгоритмов: 1) структурные методы защиты от анализа (усложнения анализа) а) искусственное усложнение (запутывание) (англ. obfuscation, обфускация) алгоритмов обработки данных б) искусственное усложнение структуры програм-мы 2) затруднение дизассемблирования (статического анализа программ) а) использование самогенерирующих кодов б) динамическое изменение (мутация) кода про-граммы в) архивация кода программы г) шифрование кода программы 3) обнаружение и затруднение отладки (динамического анализа программ) а) выявление факта выполнения программы под отладчиком б) затруднение отладки - навязывание отладчику ложных точек останова - засорение консоли отладчика - использование своего отладчика для работы защищаемого ПО - использование (провоцирование) известных программных ошибок конкретных отладчиков 4) эмуляция процессоров и операционных систем 5) нестандартные методы работы с аппаратным обеспечением 6) нестандартные обращения к функциям ОС Построение технической защиты ПО от несанкционированного

копирования (НСК): а) Структура системы технической защиты от НСК. б) Подсистема внедрения управляющих механизмов . в) Подсистема противодействия нейтрализации защитных механизмов . г) Блок ответной реакции д) Блок сравнения характеристик среды. е) Блок установки характеристик среды Защита программ от НСД и НСК с помощью регистрационных кодов: - требования к защите ПО от НСК и классификация методов защиты; - методы проверки регистрационных кодов: - «черный» ящик; - решение сложной математической задачи ; - табличные методы; - достоинства и недостатки защиты ПО от НСК . Защита программ от НСД и НСК с помощью навесных защит (протекторов): - какую защиту обеспечивают протекторы; - как работают протекторы; - сценарии атаки (- действия взломщика этой защиты); - защита от взлома протектора; - примеры протекторов : - ASProtect - Armadillo - VMProtect - Themida/WinLicense - HASP Envelope - StarForce - недостатки защиты с помощью протекторов . Защита ПО от НСД и НСК с помощью электронных ключей: - виды электронных ключей; - состав ключа; - Аппаратная част ь - блок логики, - блок памяти) - Программная часть - драйвер - модуль, встраиваемый в защищаемое ПО - варианты реализации электронных ключей : - Ключи с неизвестны м алгоритмом - Ключи с известным алгоритмом - Ключи с программируемым алгоритмом - Ключи с таймером - Сетевые ключи - приемы защиты ключей от взлома - достоинства и недостатки использования ключей для защиты ПО; - производители электронных ключей : - ЗАО «Аладдин Р . Д . » - Rainbow security (WibuKey) - ЗАО "Актив-софт" (Guardant) «МультиСофт» (Rockey, раньше Feitian Rockey) - «Компания "Эримекс"» (Sentinel (HASP) HL).

Тема 5. Программные и программнотехнические средства обеспечения безопасности (не относящиеся к защите программ и данных).

Электронный замок (аппаратный модуль доверенной загрузки) «Соболь». Средства безопасной аутентификации типа RuToken. СЗИ SecretNet (SecretNet Studio) и Страж. Программные средства генерации паролей. Программные средства анализа защищенности сети (Ревизор).

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самос-тоятельная работа	
1	Тема 1. Введение. Общие вопросы ОБИ и дисциплины ПАСЗИ	6	6/6	6	ОПК-13, ОПК-13.1, ОПК-13.3
2	Тема 2 Защита от РПВ (ПМВ).	6	6/6	8	ОПК-13, ОПК-13.1, ОПК-13.3
3	Тема 3. Защита данных.	6	6/6	8	ОПК-13, ОПК-13.1, ОПК-13.3
4	Тема 4. Защита программ..	8	8/8	8	ОПК-13, ОПК-13.1, ОПК-13.3
5	Тема 5. Программные и программнотехнические средства обеспечения безопасности (не относящиеся к защите программ и данных).	8	8/8	9	ОПК-13, ОПК-13.1, ОПК-13.3
	Всего	**34**	**34/34**	**39**	

6. Практические занятия

Практические занятия не предусмотрены.

7. Лабораторные работы

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
1.	Тема 1. Введение. Общие вопросы ОБИ и дисциплины ПАСЗИ	Виды программно-аппаратных (программно-технических) средств защиты. Виды РПВ. Модели работы (воздействия на компьютерные системы) ПЗ на компьютеры	6
2.	Тема 2 Защита от РПВ (ПМВ).	Трояны и руткиты; защита от троянов и руткитов Вредоносные программы для мобильных устройств; белый и черный ящики (Blacklisting и Whitelisting);	6

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
		внедрение вредоносного ПО через автозагрузку (реестр и Планировщик Windows) Изучение возможностей и настроек про-грамм семейства Acronis для резервного ко-пирования.	
3.	Тема 3. Защита данных.	Восстановление данных с помощью про-граммно-аппаратных средств Работа с программами семейства Acronis (восстановление разделов). Работа с программно-аппаратным средством «ФИКС 2.0.1».	6
4.	Тема 4. Защита программ..	Изучение защиты программ от изучения статическим методом. Построение технической защиты ПО от несанкционированного копирования (НСК). Защита программ от НСД и НСК с помощью регистрационных кодов. Защита программ от НСД и НСК с помощью навесных защит (протекторов).	8
5.	Тема 5. Программные и программнотехнические средства обеспечения безопасности (не относящиеся к защите программ и данных).	Электронный замок (аппаратный модуль доверенной загрузки) «Соболь». Средства безопасной аутентификации типа RuToken. СЗИ SecretNet (SecretNet Studio) и Страж. Программные средства анализа защищенности сети (Ревизор).	8
	Всего		**34**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Программно-аппаратные средства защиты Информации» направлена на:

– освоение нормативных правовых актов и учебной литературы, необходимых для освоения дисциплины;

– самостоятельный поиск информации в Интернете и других источниках;

– выполнение домашних заданий по практическим занятиям;

– подготовку к зачету.

Краткие рекомендации по выполнению самостоятельной работы:

Успешное усвоение дисциплины предполагает большой, упорный, серьезный, систематический труд студентов. Важнейшая его составная часть – выполнение разных видов самостоятельной работы.

1. **Составление тематического конспекта** на основе изученной

основной и дополнительной учебной литературы. В тематическом конспекте за основу берется содержание темы, вопросы для обсуждения.

Этапы работы.

1.1 Конспектирование делается только после того, как прочитан или усвоен материал для конспектирования.

1.2. Необходимо мысленно или письменно составить план конспекта. По этому плану и будет строиться конспект далее.

1.3. Составление самого конспекта. Можно сказать, что конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, содержащимися в материалах для конспекта, а также собственными мыслями и положениями составителя конспекта.

Писать конспект рекомендуется четко и разборчиво. В конспекте можно выделять места текста в зависимости от их значимости. Для этого применяются различного размера буквы, подчеркивания, замечания на полях.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

1. Взаимосвязь понятий: защищенность, уязвимость, угроза, нарушитель, атака, ущерб, риск.
2. Виды программно-аппаратных (программно-технических) средств защиты информации. Отличия их от технических средств защиты информации.
3. Каналы утечки компьютерной информации: защищаемые элементы; источники угроз; основные каналы утечки информации и средства их образования
4. 4. Понятие РПВ. Виды РПВ.
5. Программные закладки (ПЗ): понятие ПЗ; виды ПЗ;
6. модели работы (воздействия на компьютерные системы) ПЗ на компьютеры;
7. защита от программных закладок (поиск недокументированных (недекларированных) возможностей);
8. понятие изолированной программной среды и изолированного компьютера; контроль отсутствия НДВ.
9. Защита от троянов и вредоносных утилит: утилиты скрытого администрирования (backdoor), exploit’ы, rootkit’ы и просто трояны;
10. кейлоггеры; руткиты (руткиты уровня пользователя, руткиты уровня ядра).
11. Защита от троянов и руткитов.
12. Защита от вирусов: понятие вируса; классификация вирусов; файловые вирусы; макро-вирусы; сетевые вирусы (черви); почтовые вирусы; загрузочные вирусы;
13. 13. методы защиты вирусов от обнаружения;

14. вредоносные утилиты, специальные упаковщики и парольные взломщики;

15. антивирусное ПО;

16. методы защиты от вирусов и ПЗ

17. белый и черный ящики (Blacklisting и Whitelisting).

18. Вредоносные программы для мобильных устройств.

19. Внедрение вредоносного ПО через автозагрузку (реестр и Планировщик Windows): как устроен реестр; ключи автозагрузки; описание (определение) возможностей разных вариантов автозапуска программ; планировщик заданий в Windows.

20. 20. Направления и методы защиты данных.

21. Программные средства резервного копирования (Acronis Backup).

22. Программные средства восстановления: - данных - EasyRecovery - RStudio - GetDataBack - разделов - Acronis Partition Expert (в составе Acronis Disk Director)

23. Программные средства защиты данных от утечки: - статистика состояния проблемы утечек информации; - задачи системы защиты от утечек данных;

24. - классификация внутренних нарушителей; - использование DLP-систем для предотвращения утечки дан-ных:

25. - принципы работы DLP; - основные функции DLP;

26. - состав DLP и их виды: - хостовые DLP; - шлюзовые DLP;

27. - универсализация систем DLP; - примеры систем DLP;

28. Средства шфрования данных

29. Средства гарантированного уничтожения (затирания) данных: - Требования стандартов и руководящих документов к гарантированному уничтожению информации - Удаление информации - Виды остаточной информации - Восстановление удаленной информации

30. - Виды гарантированного уничтожения - Достоинства и недостатки аппаратного и программного способов гарантированного уничтожения информации

31. - Аппаратные средства уничтожения информации

32. - Средства, использующие физический принцип воздействия магнитным полем **О**

33. - Средства, использующие механический принцип воздействия

34. - Программное гарантированное уничтожение информации

35. - Наиболее известные алгоритмы затирания информации

36. - Особенности гарантированного уничтожения информации с различных носителей

37. - Сертифицированные программные средства удаления и затирания информации

38. - СЗИ Secret Net

39. СЗИ Страж NT – **О**

40. Бесплатные программные средства удаления и затирания информации
41. Сравнение программных средств гарантированного уничтожения информации
42. Программные средства контроля целостности программ и данных
43. Направления защиты программ.
44. Классификация средств атаки на средства защиты ПО.
45. Классификация методов защиты ПО
46. методы защиты от несанкционированного исследования, анализа и восстановления алгоритмов:
47. структурные методы защиты от анализа (усложнения анализа)
48. затруднение дизассемблирования (статического анализа программ)
49. обнаружение и затруднение отладки (динамического анализа программ
50. эмуляция процессоров и операционных систем
51. нестандартные методы работы с аппаратным обеспечением
52. нестандартные обращения к функциям ОС
53. Построение технической защиты ПО от несанкционированного копирования (НСК
54. Защита программ от НСД и НСК с помощью регистрационных кодов
55. Защита программ от НСД и НСК с помощью навесных защит (протекторов)
56. Защита ПО от НСД и НСК с помощью электронных ключей виды электронных ключей; - состав ключа;
57. - варианты реализации электронных ключей : - Ключи с неизвестны м алгоритмом - Ключи с известным алгоритмом - Ключи с программируемым алгоритмом Сетевые ключи - приемы защиты ключей от взлома - достоинства и недостатки использования ключей для защиты ПО
58. 58. Электронный замок (аппаратный модуль доверенной загрузки) «Соболь»
59. Средства безопасной аутентификации типа RuToken
60. СЗИ SecretNet (SecretNet Studio) и Страж
61. Программные средства генерации паролей

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии с оценочными материалами.

11. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. –

URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 14.02.2025). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный..

2. Щерба, Е. В. Противодействие сетевым атакам в локальных сетях : учебное пособие : [16+] / Е. В. Щерба, М. В. Щерба, А. А. Магазев ; ред. О. В. Маер ; Омский государственный технический университет. – Омск : Омский государственный технический университет (ОмГТУ), 2021. – 119 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 14.02.2025). – Библиогр. в кн. – ISBN 978-5-8149-3250-1. – Текст : электронный. 3. Ларионова, С. Л. Информационная безопасность дистанционного банковского обслуживания : учебное пособие : [16+] / С. Л. Ларионова ; Финансовый университет при Правительстве Российской Федерации. – Москва : Прометей, 2022. – 296 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=701063 (дата обращения: 14.02.2025). – Библиогр. в кн. – ISBN 978-5-00172-343-1. – Текст : электронный.

Дополнительная литература:

1. Жмуров, Д. Б. Программно-аппаратные средства защиты информации : учебное пособие / Д. Б. Жмуров, С. В. Жуков. — Самара : Самарский университет, 2022. — 80 с. — ISBN 978-5-7883-1799-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/336515 — Режим доступа: для авториз. пользователей.

2. Булычёв, Г. Г. Программно-аппаратные средства защиты информации : учебно-методическое пособие / Г. Г. Булычёв. — Москва : РТУ МИРЭА, 2022 — Часть 1 — 2022. — 203 с. — ISBN 978-5-73391652-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/310781 — Режим доступа: для авториз. пользователей.

3. Булычёв, Г. Г. Программно-аппаратные средства защиты информации : учебно-методическое пособие / Г. Г. Булычёв. — Москва : РТУ МИРЭА, 2022 — Часть 2 — 2022. — 177 с. — ISBN 978-5-73391653-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/310784. — Режим доступа: для авториз.

пользователей.

1. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электроннобиблиотечная система. — URL: https://e.lanbook.com/book/237770 (дата обращения: 29.06.2023). — Режим доступа: для авториз. пользователей.

Электронные библиотечные системы (ЭБС) и электронные образовательные ресурсы

1. Электронно-библиотечная система ZNANIUM https:// www.znanium.com
2. Универсальная справочно-информационная полнотекстовая база данных периодических изданий «East View» (ИВИС) https://dlib.eastview.com/
3. Электронно-библиотечная система «BOOK.ru» www.book.ru
4. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru/
5. ЭБС «Национальный цифровой ресурс «Руконт» https://lib.rucont.ru/search
6. Образовательная платформа ЮРАЙТ http://www.urait.ru

Электронный каталог Университета – Автоматизированная информационная библиотечная система (АИБС «МегаПро»)

12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

Лицензионное программное обеспечение, в том числе отечественного производства:

– DsktpEdu ALNG LicSARk OLV F1 1Y Acdmc Ent (MS Windows) (подписка на ПО).

Свободно распространяемое программное обеспечение, в том числе отечественного производства:

– 7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО).

– FastStone Image Viewer (программа для просмотра изображений в Microsoft Windows (лицензия бесплатного программного обеспечения)).

– Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения)).

– Indigo (система программ для создания и проведения компьютерного тестирования знаний).

– Google Crome, ЯндексБраузер (браузер).

– Adobe Acrobat Reader DC (• ПО для просмотра, печати и

комментирования документов в формате PDF)

– Visual Studio Code (интегрированная среда разработки программного обеспечения)

Профессиональные базы данных не используются.

Информационные справочные системы:

– СПС КонсультантПлюс. Компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной

13. Материально–техническое обеспечение дисциплины

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий, а именно для проведения занятий лекционного типа, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) - 1

Учебная аудитория для проведения лабораторных занятий. Лаборатория программно-аппаратных средств защиты информации

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения: персональный компьютер с подключением к сети «Интернет» - 15, сетевое оборудование; антивирусная программа; аппаратные средства аутентификации пользователя, средства анализа программных реализаций; программы поиска и уничтожения остаточной информации,; программы доверенной загрузки; программы защиты информации, включающими в том числе средства криптографической защиты информации

Учебная аудитория для проведения лабораторных занятий. Аудитория информационных технологий

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения:

персональный компьютер с подключением к сети «Интернет» - 15, сетевое оборудование.

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет»

и обеспечением доступа в электронную информационно-образовательную среду института.

Рабочие места обучающихся.

Технические средства обучения: персональный компьютер - 13.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы, в который внесены изменения

(измененное содержание раздела)

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____