МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГАОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2026

Безопасность операционных систем и программного обеспечения
Рабочая программа дисциплины

Составитель:
Кандидат технических наук, доцент, доцент кафедры КЗИ А.С. Моляков

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 5 от 25.12.2025

Оглавление

1 Пояснительная записка 4
1.1 Цель и задачи дисциплины 4
1.2 Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине: 4
1.3 Место дисциплины в структуре образовательной программы 5
2 Структура дисциплины 5
3 Содержание дисциплины 5
4 Образовательные технологии 7
5 Оценка планируемых результатов обучения 8
5.1 Система оценивания 8
5.2 Критерии выставления оценки по дисциплине 8
5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине 9
6 Учебно-методическое и информационное обеспечение дисциплины 11
6.1 Список источников и литературы 11
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет» 13
6.3 Профессиональные базы данных и информационно-справочные системы 14
7 Материально-техническое обеспечение дисциплины 14
8 Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья 15
9 Методические материалы 16
9.1 Планы лабораторных занятий 16
Приложение 1. Аннотация рабочей программы дисциплины 18

1 Пояснительная записка

1.1 Цель и задачи дисциплины

Цель дисциплины: приобретение знаний о базовых методах и способах защиты программного обеспечения (ПО) автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа, научить студентов использовать для решения профессиональных задач современные средства программно-аппаратной защиты информации ОС.

Задачи дисциплины: приобретение знаний о базовых методах и способах защиты ПО автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа, формирование у студентов представлений о механизмах защиты ОС, выработка умений настраивать функций безопасности ОС.

1.2 Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-3 Способен администрировать подсистемы информационной безопасности объекта защиты	*ПК-3.1 Знает требования к встроенным средствам защиты информации программного обеспечения*	*Знать: архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; протоколы локальной и сетевой аутентификации*
	ПК-3.2 Умеет анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации	*Уметь: осуществлять настройку политики учётных записей, выполнять администрирование учётных записей пользователей на платформах Windows и Linux, идентифицировать слабые места и уязвимости подсистемы идентификации и аутентификации; разрабатывать матрицу разграничения доступа, реализовывать дискреционное разграничение доступа к объектам файловой системы и системного реестра.*
	ПК-3.3 Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования	*Владеть: навыками администрирования подсистем безопасности, настройки системы, политик безопасности, управления учетными записями*

ПК-6 *Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации*	*ПК-6.1* *Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик*	*Знать основные принципы оценки работоспособности и тестирования* *оборудования обработки и передачи данных, критерии и меры надёжности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.* *Уметь составлять и реализовывать планы тестирующих мероприятий,*
	ПК-6.2 *Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик*	*Уметь: составлять и реализовывать планы тестирующих мероприятий, моделировать и оценивать эффективность применяемых средств защиты*
	ПК-6.3 *Владеет навыками определения уровня защищённости и доверия средств защиты информации*	*Владеть: навыками эксплуатации и тестирования программно-аппаратных защиты информации, определение профиля защиты.*

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность операционных систем и программного обеспечения» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

2 Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 зачётные единицы, 108 часов

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
6	Лекции	**26**
6	Лабораторные работы	**32**
	Всего:	**58**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _50_ академических часов.

3 Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Введение в теорию**	Проблема защиты программного обеспечения автоматизи-

	и практику защиты программного обеспечения и Общая архитектура ОС	рованных систем. Объекты защиты. Системное и общесистемное программное обеспечение. Специальное программное обеспечение. Прикладное программное обеспечение. Языки, системы и оболочки программирования, инструментальные средства автоматизации программирования. Защита программного обеспечения как система научных дисциплин. Угрозы безопасности программного обеспечения. Принятая аксиоматика и терминология. Жизненный цикл программного обеспечения автоматизированных систем. Технологическая и эксплуатационная безопасность программного обеспечения. Модели угроз безопасности программного обеспечения и ОС. Основные принципы обеспечения безопасности программного обеспечения и ОС.
2	**Место сервисов безопасности в ОС**	Базовые научные положения и основания теории защиты программ. Понятие Сервиса безопасности.
3	**Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения и Управление учётными записями ОС**	Модели и методы разработки безопасного ПО, принципы верификации. Управление учётными записями и механизмы аутентификации в ОС. Идентификация и аутентификация в домене Active Directory. Процедуры идентичны простой локальной идентификации и аутентификации, но в данном случае, при регистрации в домене, обмен данными между рабочей станцией и сервером происходит по протоколу Kerberos v5 rev6 (более надёжный за счёт обоюдной аутентификации, более быстрое соединение и др.).
4	**Средства и системы защиты программного обеспечения. Управление доступом к объектам файловой системы. Управление доступом к объектам файловой системы**	Система контроля доступа состоит из участника безопасности (пользователи, группы пользователей, службы, компьютеры), маркера доступа, объектов доступа, дескрипторов безопасности и алгоритма проверки прав. Дескрипторы безопасности – это список запретов и разрешений (Discretionary Access Control List, DACL), установленных для данного объекта, список назначений аудита (System Access Control List, SACL) и назначение прав для каждого конкретного SID (Access Control Entry, ACE, при этом список назначений аудита объекта Active Directory может содержать строки ACE, назначенные отдельным атрибутам). Регистрация событий и журналы безопасности.
5	**Отечественные нормативные акты. Работа с терминалом устройств**	Федеральный закон «Об информации, информационных технологиях и о защите информации». ГОСТ Р ИСО/МЭК 12207-2010. ГОСТ Р ИСО/МЭК 15408-2002. ГОСТ Р МЭК 61508-2007. Руководящий документ ФСТЭК России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей. Эффективная профессиональная работа в `Linux` немыслима без использования командной строки. Пользователям, привыкшим работать в системах с графическим интерфейсом, работа с командной строкой может показаться неудобной: то, что можно сделать одним перетаскиванием мышью в командной строке потребует ввода с клавиатуры несколь-

		ких слов: команды с аргументами. В командных оболочках, используемых в Linux, есть масса способов экономии усилий (нажатий на клавиши) при выполнении наиболее распространённых действий: Преимущества командной строки становятся особенно очевидны, когда требуется выполнять однотипные операции над множеством объектов. В системе с графическим интерфейсом потребуется столько перетаскиваний мышью, сколько есть объектов, в командной строке будет достаточно одной команды.

4 Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	*Введение в теорию и практику защиты программного обеспечения и Общая архитектура ОС*	*Лекция 1* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Изучение материалов лекций*
2	*Место сервисов безопасности в ОС.*	*Лекция 2.1* *Лекция 2.2* *Лабораторное занятие 1.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Выполнение задания в виртуальной машине CentOS 7.* *Изучение материалов лекций*
3	*Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения и Управление учетными записями ОС*	*Лекция 3.1* *Лекция 3.2* *Лабораторное занятие 2.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Выполнение задания в виртуальной машине CentOS 7.* *Изучение материалов лекций*
4	*Средства и системы защиты программного обеспечения. Управление доступом к объектам файловой системы*	*Лекция 4.1* *Лекция 4.2* *Лекция 4.3* *Лабораторное занятие 3.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Выполнение задания в виртуальной машине CentOS 7.* *Изучение материалов лекций*
5	*Отечественные нормативные акты. Работа с терминалом устройств*	*Лекция 5.1* *Лекция 5.2* *Лабораторное занятие 4.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Выполнение задания в виртуальной машине CentOS 7.* *Изучение материалов лекций*

5 Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос (темы 1)* *– Лабораторное задание (темы 2)* *– Лабораторное задание (темы 3-5)*	 *5 баллов* *6 баллов* *7 баллов*	 *30 баллов* *6 баллов* *24 балла*
Промежуточная аттестация – *зачёт*		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетвори-тельно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Примерные контрольные вопросы для зачёта

Контрольные вопросы	Реализуемые компетенции
1. Наиболее вероятный объект воздействия в АС? Дайте определения «защищенности ПО АС» и «уровня безопасности ПО». Технологическая и эксплуатационная безопасность ПО.	ПК-3, ПК-6
2. Объекты защиты. Системное и общесистемное ПО. ПО промежуточного слоя. Специальное и прикладное ПО. Языки, системы и оболочки программирования. Защита программного обеспечения как система научных дисциплин.	ПК-3, ПК-6
3. Угрозы и модели угроз безопасности ПО. Основные принципы обеспечения безопасности программного обеспечения.	ПК-3, ПК-6
4. Модели вычислений: Машина Тьюринга, машина Поста, RAM-машина, РАСП-машина и их разновидности. Схемы. Булевы схемы. Процессоры и сети процессоров.	ПК-3, ПК-6
5. Символ О-большое и Омега-большое. Вычислимые функции и разрешимые предикаты. Сложность и классы вычислений. Односторонние функции и функции с секретом. Псевдослучайные генераторы.	ПК-3, ПК-6
6. Криптосистемы с секретным и открытым ключом. Схемы электронной подписи. Схемы хеширования. Схемы построения псевдослучайных генераторов. Схемы вероятностного шифрования. Конфиденциальные вычисления.	ПК-3, ПК-6

7. Методы анализа безопасности программного обеспечения. Контрольно-испытательные методы анализа безопасности программного обеспечения. Логико-аналитические методы контроля безопасности программ. Сравнение логико-аналитических и контрольно-испытательных методов анализа безопасности программ.	ПК-3, ПК-6
8. Методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами ПССИВ. Способы внедрения ПССИВ посредством инструментальных средств. Возможные методы защиты программ от потенциально опасных инструментальных средств.	ПК-3, ПК-6
9. Методы идентификации программ и их характеристик. Идентификация программ по внутренним характеристикам. Способы оценки подобия целевой и исследуемой программ с точки зрения наличия программных дефектов.	ПК-3, ПК-6
10. Методы защиты программ от компьютерных вирусов. Общая характеристика и классификация компьютерных вирусов. Общая характеристика средств нейтрализации компьютерных вирусов. Классификация методов защиты от компьютерных вирусов.	ПК-3, ПК-6
11. Методы защиты программ от исследования. Классификация средств исследования программ. Способы защиты программ от исследования. Способы встраивания защитных механизмов в программное обеспечение. Обфускация программ.	ПК-3, ПК-6
12. Методы и средства обеспечения целостности и достоверности используемого программного кода.	ПК-3
13. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком. Манипуляции с кодом программы. Методы противодействия динамическим способам снятия защиты программ от копирования.	ПК-3, ПК-6
14. Создание защищенных операционных систем.	ПК-3, ПК-6
15. Методы аутентификации и идентификации в современных ОС.	ПК-6
16. Особенности создания защищенных ОС с учетом современных технологий виртуализации.	ПК-6.
17. Средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность.	ПК-6.
18. Обобщенные способы анализа программных средств на предмет наличия (отсутствия) недекларированных возможностей.	ПК-6.
19. Построение программно-аппаратных комплексов для контроля технологической безопасности программ.	ПК-6
20. Средства и комплексы защиты программ от компьютерных вирусов.	ПК-6
21. Обфускаторы программ.	ПК-3
22. Средства обеспечения целостности и достоверности используемого программного кода.	ПК-3
23. Основные разработчики пакетов для квантовых вычислений.	ПК-6
24. Проблема защиты программного обеспечения автоматизированных систем.	ПК-6
25. Защита программного обеспечения как система научных дисциплин.	ПК-3, ПК-6
26. Угрозы безопасности программного обеспечения.	ПК-3
27. Технологическая и эксплуатационная безопасность программного обеспечения.	ПК-3, ПК-6
28. Модели угроз безопасности программного обеспечения.	ПК-6

29. Основные принципы обеспечения безопасности программного обеспечения.	ПК-6
30. Методы анализа безопасности программного обеспечения.	ПК-6
31. Методы защиты программ от компьютерных вирусов.	ПК-6
32. Аутентификация и идентификация. Протокол LDAP.	ПК-3
33. Системы аудиты.	ПК-3, ПК-6
34. Штатные средства защиты ОС Linux.	ПК-3
35. Понятие кольца защиты ОС.	ПК-3, ПК-6
36. Механизмы доменной защиты.	ПК-3, ПК-6
37. Архитектура ОС.	ПК-3, ПК-6
38. Доверенная загрузка и контроль BIOS.	ПК-3, ПК-6
39. Примеры операционных систем в защищенном исполнении.	ПК-3, ПК-6
40. Мониторинг процессов ОС.	ПК-3, ПК-6
41. Электронные ключи. Принципы работы.	ПК-3, ПК-6
42. Защита байт-кодов в виртуальной среде.	ПК-3, ПК-6
43. Отладчики системного уровня.	ПК-3, ПК-6
44. Сигнатурный анализ. Принципы детектирования.	ПК-3, ПК-6
45. Эвристический анализ.	ПК-3, ПК-6
46. Контроль выполнений контекстно-зависимых операций в средах виртуализации.	ПК-3, ПК-6

Примерные задания для тестирования

1. Что такое X-Force:

а) Глобальная система IBM сбора, обработки и реагирования на инциденты ИБ.

б) Сайт компании IBM.

в) Название ПО.

2. Эвристика – это:

а) мера кривизны пространства.

б) совокупность приёмов и методов, облегчающих и упрощающих решение познавательных, конструктивных, практических задач.

в) раздел математики.

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

Основные

1. *Базовая модель угроз безопасности* персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/files/492/---15--2008-/887/---15--2008-.pdf, свободный. – Загл. с экрана.

2. *ГОСТ Р 50922-2006*. Защита информации. Основные термины и определения. [Электронный ресурс] / Режим доступа : https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=0&month=3&year=2024&search=50922&id=129024, свободный. – Загл. с экрана

3. *Методика определения актуальных угроз безопасности* персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] / ФСТЭК

России. – Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g, свободный. – Загл. с экрана.

4. *Методические рекомендации по разработке* нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. Утверждены руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432 [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://www.consultant.ru/document/cons_doc_LAW_185051/, свободный. – Загл. с экрана.

5. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-3, свободный. – Загл. с экрана.

6. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-2, свободный. – Загл. с экрана.

7. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.

Дополнительные

8. *Руководящий докумен*т. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-1, свободный. – Загл. с экрана.

9. Руководящий документ ФСТЭК России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей. [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-4-iyunya-1999-g-n-114.

10. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ . [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

11. Приказ ФСБ России от 27.12.2011 N 796 (ред. от 13.04.2022) "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра" [Электронный ресурс]. – Режим доступа : https://www.consultant.ru/document/cons_doc_LAW_126209/, свободный в комм. версии. – Загл. с экрана.

12. Приказ ФСТЭК России от 29.04.2021 г. № 77 [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77, свободный. – Загл. с экрана.

Литература
Основная

1. Окороков, В. А. Безопасность операционных систем / В. А. Окороков. — Санкт-Петербург : Лань, 2024. — 228 с. — ISBN 978-5-507-48297-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/367472. — Режим доступа: для авториз. пользователей.

2. Зубарев, И. В. Методы обоснования основных требований к вычислительным системам : учебное пособие / И. В. Зубарев, С. А. Красников, К. В. Гусев. — Москва : РТУ МИРЭА, 2024. — 152 с. — ISBN 978-5-7339-2275-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/448802. — Режим доступа: для авториз. пользователей.

3. Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. – 6-е изд., стер. – СПб.: Лань, 2025. – 124 с. – ISBN 978-5-507-52899-8. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/462293. – Режим доступа: для авториз. пользователей.

Дополнительная

4. Флоу, С. Занимайся хакингом как невидимка. Искусство взлома облачных инфраструктур : руководство / С. Флоу ; перевод с английского В. С. Яценкова. – М.: ДМК Пресс, 2023. – 272 с. – ISBN 978-5-97060-977-4. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/314924

5. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. – 5-е изд., стер. – СПб.: Лань, 2023. – 96 с. – ISBN 978-5-507-45868-4. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/288974

6. Музипов, Х. Н. Программно-технические комплексы автоматизированных систем управления : учебное пособие для вузов / Х. Н. Музипов. – 2-е изд., стер. – СПб.: Лань, 2022. – 164 с. – ISBN 978-5-507-44103-7. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/215717. – Режим доступа: для авториз. пользователей.

7. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. – 3-е изд., стер. – СПб.: Лань, 2024. – 324 с. – ISBN 978-5-507-49077-6. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/370967. – Режим доступа: для авториз. пользователей.

8. 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 : электронно-библиотечная система. – URL: https://e.lanbook.com/book/237770

9. Ларина, Т. Б. Администрирование операционных систем. Управление системой : учебное пособие / Т. Б. Ларина. – М.: РУТ (МИИТ), 2020. – 71 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/175980. – Режим доступа: для авториз. пользователей.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7 Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должны быть установлено следующее ПО:

№ п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для лабораторных занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента с выходом в интернет. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Microsoft Share Point 2010	Microsoft	лицензионное
4	Microsoft Office 2013	Microsoft	лицензионное
5	Windows 10 Pro	Microsoft	лицензионное
6	Kaspersky Endpoint Security	Kaspersky	Лицензионное
7	Vmware Player 15.5 + Гостевая ОС CentOS 7	VMWare	Режим доступа: https://www.vmware.com/products/ Демоверсия Режим доступа: https://www.centos.org/download/ Инсталляционный дистрибутив Linux Открытое ПО

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

8 Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

• для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

• для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

• для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

• для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.

• для глухих и слабослышащих: в печатной форме, в форме электронного документа.

• для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

• для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;

• для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;

• для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9 Методические материалы

9.1 Планы лабораторных занятий

Темы учебной дисциплины предусматривают проведение лабораторных работ, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для лабораторных работ, выдаваемые преподавателем на каждом занятии, задания на самостоятельную подготовку, перечень вопросов для подготовки к экзамену и контрольные домашние задания для самостоятельной работы студентов.

Целью лабораторных работ является закрепление теоретического материала и приобретение практических навыков использования методов применения пакетов компьютерной математики в профессиональной деятельности, применять навыки для принятия наиболее эффективных решений в условиях быстро меняющейся реальности, для быстрой адаптации к изменяющимся условиям деятельности.

Лабораторное занятие 1(8 ч.). Основные сервисы безопасности ОС
Цель работы: получение практических навыков в эксплуатации штатных средств защиты ОС.
Указания по выполнению задания: обратить внимание на свойства защищенности программ на этапах производства, поставки и эксплуатации программных комплексов.
Выполнение задания:
В ходе практической работы студенты на практике знакомятся с сервисами безопасности, предоставляемые ОС Windows и Linux. Обучаются настраивать профили защиты, добавлять и блокировать учетные записи.

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

Лабораторное занятие 2(8 ч.). Идентификация и аутентификация в ОС
Цель работы: получение практических навыков в эксплуатации подсистем разграничения доступа в современных ОС.
Указания по выполнению задания: обратить внимание на оценку криптостойкости функций хеширования паролей.
Выполнение задания:
В ходе практической работы студенты на практике знакомятся с механизмами идентификации и аутентификации ОС Windows и Linux.

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

Лабораторное занятие 3(8 ч.). Регистрация событий и анализ журналов безопасности
Цель работы: получение практических навыков в исследовании несанкционированного доступа и своевременного предупреждения.

Указания по выполнению задания: обратить внимание на режимы записи информации в журналах безопасности ОС Linux и Windows.
Выполнение задания:
В ходе практической работы имитируется процесс, осуществляющий несанкционированный доступ к ресурсам ОС. Задача студентам, как будущим администраторам СЗИ, своевременно анализировать и выявлять подобные угрозы.

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

Лабораторное занятие 4(8 ч.). Работа с командной строкой Linux
Цель работы: получение практических навыков в эксплуатации современных ОС.
Указания по выполнению задания: обратить внимание на требование комплексного похода для защиты СВТ.
Выполнение задания:
В ходе практической работы студенты на практике знакомятся с командной строкой Linux.

Материально-техническое обеспечение практического занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины: приобретение знаний о базовых методах и способах защиты программного обеспечения (ПО) автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа, научить студентов использовать для решения профессиональных задач современные средства программно-аппаратной защиты информации ОС.

Задачи: приобретение знаний о базовых методах и способах защиты ПО автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа, формирование у студентов представлений о механизмах защиты ОС, выработка умений настраивать функций безопасности ОС.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

Знать: архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; протоколы локальной и сетевой аутентификации; Знать основные принципы оценки работоспособности и тестирования оборудования обработки и передачи данных, критерии и меры надёжности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.

Уметь: осуществлять настройку политики учётных записей, выполнять администрирование учётных записей пользователей на платформах Windows и Linux, идентифицировать слабые места и уязвимости подсистемы идентификации и аутентификации; разрабатывать матрицу разграничения доступа, реализовывать дискреционное разграничение доступа к объектам файловой системы и системного реестр; составлять и реализовывать планы тестирующих мероприятий, моделировать и оценивать эффективность применяемых средств защиты.

Владеть: навыками администрирования подсистем безопасности, настройки системы, политик безопасности, управления учётными записями; навыками эксплуатации и тестирования программно-аппаратных средств защиты информации, определения профиля защиты информации.