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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность
Код и наименование направления подготовки/специальности

«Безопасность автоматизированных систем
(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
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

1.1 Цель и задачи дисциплины

Цель дисциплины: развить у слушателей подход к решению технических задач программно-аппаратной защиты информации.

Задачи: изучение встроенных механизмов безопасности ОС, освоение принципов использования программно-аппаратных средств защиты информации, выработка умений проведения оценки защищённости информационных систем.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4.1 Знает критерии оценки защищённости автоматизированной системы, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Знать: критерии оценки защищённости автоматизированной системы, основные угрозы безопасности информации и модели нарушителя согласно РД ФСТЭК (Гостехкомиссия) и ФСБ
	ОПК-4.4.2 Умеет контролировать уровень защищённости в автоматизированных системах, регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах	Уметь: контролировать уровень защищённости ресурсов ОС, регистрировать и анализировать события в системных журналах ОС Windows и Linux
	ОПК-4.4.3 Владеет навыками проведения аудита защищённости информации в автоматизированных системах	Владеть: навыками проведения аудита защищённости информации в ОС Windows и Linux
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Знать: математические модели кодирования систем информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации в ОС Windows и Linux
	ОПК-9.2 Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации	Уметь: применять теоретические знания при разработке ОРД; применять информационные технологии для поиска и обработки информации; применять математические модели для оценки защищённости ОС
	ОПК-9.3 Владеет методами и средствами	Владеть: навыками поиска нужной информации в нормативных базах

	криптографической и технической защиты информации	и источниках; навыками эксплуатации криптографических протоколов и схем в современных ОС

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность операционных систем» относится к обязательной части блока дисциплин учебного плана.

2 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 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
5	Лекции	**28**
5	Практические занятия	**32**
6	Лекции	**16**
6	Практические занятия	**16**
6	Промежуточная аттестация	**18**
	Всего:	**92**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _70_ академических часов.

3 Содержание дисциплины

5 семестр

№	Наименование раздела дисциплины	Содержание
1	**Общая архитектура ОС**	Проблема защиты программного обеспечения автоматизированных систем. Объекты защиты. Защита программного обеспечения как система научных дисциплин. 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	**Управление учётными записями, идентификация и аутентификация в ОС**	Управление учётными записями и механизмы аутентификации в ОС. Идентификация и аутентификация в домене ActiveDirectory. 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 счет

		обоюдной аутентификации, более быстрое соединение и др.).
4	**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 ActiveDirectory может содержать строки ACE, назначенные отдельным атрибутам).Регистрация событий и журналы безопасности.
5	**Работа с терминалом**	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 нескольких слов: команды с аргументами. Однако в `Linux` этот вид интерфейса всегда был основным, а поэтому и хорошо развитым. В командных оболочках, используемых в `Linux`, есть масса способов экономии усилий (нажатий на клавиши) при выполнении наиболее распространённых действий: автоматическое дополнение длинных названий команд или имён файлов, поиск и повторное выполнение команды, уже когда-то исполнявшейся раньше, подстановка списков имён файлов по некоторому шаблону и многое другое. 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.

6 семестр

№	Наименование раздела дисциплины	Содержание
1	**Пакетный менеджер yum**	Работа с утилитами управления пакетами и репозиториями rpm и yum, работа с утилитами создания новых пакетов rpmbuild и репозиториев createrepo, работа с утилитами для цифровой подписи пакетов
2	**Система подгружаемых модулей аутентификации PAM (Pluggable**	Назначение, состав и возможности **PAM**. API, использующие PAM. Написание собственных модулей habash

	Authentication Modules)	
3	**Углублённое изучение системы мандатного управления доступом SELinux (Security Enhanced Linux)**	• Назначение, состав и возможности SELinux.API, научиться писать программы, использующие SELinux. Написание собственных модулей безопасности. Установка и конфигурирование SELinux: • Конфигурационные файлы: /etc/selinux/config, /etc/selinux/targeted/setrans.conf. • Политика безопасности: /etc/selinux/targeted/policy/policy.29. • Расположение модулей: /etc/selinux/targeted/modules/.
4	**Работа со справочной системой Linux. Конвейеры. Обработка текстовых файлов**	Работа в командной строке происходит в виде интерактивного диалога со специальной программой - командной оболочкой. Конвейеры - мощный инструмент объединения команд. В конвейере стандартный вывод команды подаётся на ввод другой. С помощью конвейеров решается множество задач: поиск/замена строк, сортировка, преобразования строк.

4 Образовательные технологии

5 семестр

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	Общая архитектура ОС	Лекция 1.1 Самостоятельная работа	Традиционная с использованием презентаций Тестирование Изучение материалов лекций
2	Место сервисов безопасности в ОС	Лекция 2.1 Лекция 2.2 Практическая работа 1. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания в виртуальной машине CentOS 7. Специализированное ПО – Oracle VM VirtualBox Изучение материалов лекций
3	Управление учетными записями, идентификация и аутентификация в ОС	Лекция 3.1 Лекция 3.2 Лекция 3.3 Практическая работа 2.	Традиционная с использованием презентаций Тестирование Выполнение задания в виртуальной машине CentOS 7. Специализированное ПО – Oracle VM VirtualBox

		Самостоятельная работа	Изучение материалов лекций
4	Управление доступом к объектам файловой системы	Лекция 4.1 Лекция 4.2 Лекция 4.3 Практическая работа 3. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания в виртуальной машине CentOS 7. Специализированное ПО – Oracle VM VirtualBox Изучение материалов лекций
5	Работа с терминалом	Лекция 5.1 Лекция 5.2 Лекция 5.1 Практическая работа 4. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания в виртуальной машине CentOS 7. Специализированное ПО – Oracle VM VirtualBox Изучение материалов лекций

6 семестр

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	Пакетный менеджер yum	Лекция 1.1 Лекция 1.2 Практическая работа 1 Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания в виртуальной машине CentOS 7. Специализированное ПО – Oracle VM VirtualBox Изучение материалов лекций
2	Система подгружаемых модулей аутентификации PAM (PluggableAuthentication Modules)	Лекция 2.1 Лекция 2.2 Практическая работа 2 Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания в виртуальной машине CentOS 7. Специализированное ПО – Oracle VM VirtualBox Изучение материалов лекций
3	Углубленное изучение системы мандатного управления доступом SELinux (SecurityEnhancedLinux)	Лекция 3.1 Лекция 3.2 Практическая работа 3. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания в виртуальной машине CentOS 7. Специализированное ПО – Oracle VM VirtualBox Изучение материалов лекций

4	Работа со справочной системой Linux. Конвейеры. Обработка текстовых файлов	Лекция 4.1 Лекция 4.2 Практическая работа 4. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания в виртуальной машине CentOS 7. Специализированное ПО – Oracle VM VirtualBox Изучение материалов лекций

5 Оценка планируемых результатов обучения

5.1 Система оценивания

5 семестр

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– тестирование (темы 1-5)* *– лабораторные задания 1-2* *– практические задания 3-4*	 *4 балла* *9 баллов* *11 баллов*	 *20 баллов* *18 баллов* *22 балла*
Промежуточная аттестация - *зачет с оценкой (зачет по билетам)*		*40 баллов*
Итого за семестр		*100 баллов*

6 семестр

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– тестирование (темы 1-5)* *– практические задания 1-2* *– практические задания 3-4*	 *4 балла* *9 баллов* *1 баллов*	 *20 баллов* *18 баллов* *22 балла*
Промежуточная аттестация - *экзамен (экзамен по билетам)*		*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 (EuropeanCreditTransferSystem; 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	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	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. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно/ 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	неудовлет-ворительно/ 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 экзамена

Контрольные вопросы	**Реализуемые компетенции**

1. Тактика действия злоумышленника и обманные системы защиты.	ОПК-9
2. Основные разработчики пакетов для квантовых вычислений.	ОПК-9
3. Проблема защиты программного обеспечения автоматизированных систем	ОПК-9
4. Защита программного обеспечения как система научных дисциплин	ОПК-9
5. Угрозы безопасности программного обеспечения	ОПК-9
6. Технологическая и эксплуатационная безопасность программного обеспечения	ОПК-9
7 Защита от НСД в современных ОС.	ОПК-9
8. Администрирование ОС.	ОПК-9
9. Аудит безопасности.	ОПК-9
10 Защита от НСД в современных ОС.	ОПК-9
11 Порядок проведения аттестации объектов информатизации. Содержание заявок.	ОПК-9; ОПК-4.4
12. Угрозы безопасности программного обеспечения.	ОПК-9; ОПК-4.4
13. Технологическая и эксплуатационная безопасность программного обеспечения.	ОПК-9; ОПК-4.4
14. Модели угроз безопасности программного обеспечения.	ОПК-9; ОПК-4.4
15. Основные принципы обеспечения безопасности программного обеспечения.	ОПК-9; ОПК-4.4
16. Методы анализа безопасности программного обеспечения.	ОПК-9; ОПК-4.4
17. Методы защиты программ от компьютерных вирусов.	ОПК-9; ОПК-4.4
18. Аутентификация и идентификация. Протокол LDAP.	ОПК-9; ОПК-4.4
19. Системы аудиты.	ОПК-9; ОПК-4.4
20. Штатные средства защиты ОС Linux.	ОПК-9
21. Понятие кольца защиты ОС.	ОПК-9
22. Механизмы доменной защиты.	ОПК-9
23. Архитектура ОС.	ОПК-9
24. Доверенная загрузка и контроль BIOS.	ОПК-9
25. Примеры операционных систем в защищенном исполнении.	ОПК-9
26. Мониторинг процессов ОС.	ОПК-9; ОПК-4.4
27. Электронные ключи. Принципы работы.	ОПК-9; ОПК-4.4
28. Идентификация и аутентификация в домене ActiveDirectory.	ОПК-9; ОПК-4.4
29. Протокол LDAP.	ОПК-9; ОПК-4.4
30. Принципы работы Kerberos,	ОПК-9
31. Мультидоменный гипервизор.	ОПК-9; ОПК-4.4
32. ОС 2000. Особенности работы планировщика и принципов защиты.	ОПК-9; ОПК-4.4
33. ОС «Феникс». Особенности доменной защиты.	ОПК-9; ОПК-4.4
34. UAC – Контроль учетных записей в ОС Windows.	ОПК-9
35. Методы перехвата информации и технология противодействия ССИВ.	ОПК-9
36. Основные разработчики пакетов для квантовых вычислений.	ОПК-9; ОПК-4.4
37. Проблема защиты программного обеспечения автоматизированных систем.	ОПК-9; ОПК-4.4
38. Защита программного обеспечения как система научных дисциплин.	ОПК-9
39. Угрозы безопасности программного обеспечения.	ОПК-9; ОПК-4.4
40. Технологическая и эксплуатационная безопасность программного обеспечения.	ОПК-9; ОПК-4.4

41. Модели угроз безопасности программного обеспечения.	ОПК-9; ОПК-4.4
42. Основные принципы обеспечения безопасности программного обеспечения.	ОПК-9; ОПК-4.4
43. Методы анализа безопасности программного обеспечения.	ОПК-9; ОПК-4.4
44. Перспективные направления развития высокоскоростных сетей и их защиты.	ОПК-9; ОПК-4.4

Примерные задания для тестирования

1. Что такое AAA:

а) аутентификация, авторизация, аудит.

б) аудит безопасности.

в) расследование инцидентов ИБ.

2. Winlogon – это:

а) Логотип ОС Windows.

б) Компонент ОС Windows, ответственный за идентификацию/аутентификацию пользователей.

в) Сервис печати.

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

Основные

1. *Федеральный закон* от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Федеральный закон* от 27 июля 2006 г. № 152-ФЗ «О персональных данных». [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *Федеральный закон* от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_112701/, свободный. – Загл. с экрана.
4. *Федеральный закон* от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_40241/, свободный. – Загл. с экрана.
5. Приказ ФСБ России от 27.12.2011 № 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.
6. Выписка из Приказа ФСТЭК России № 76 от 02.06.2020 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к СТЗИ и СОБИТ» [Электронный ресурс] : Режим доступа : https://fstec.ru/files/585/---------2--2020--N-76/1116/---------2--2020--N-76.pdf, свободный. – Загл. с экрана.
7. 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. Лозовецкий, В. В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей : учебное пособие для вузов / В. В. Лозовецкий, Е. Г. Комаров, В. В. Лебедев ; под редакцией В. В. Лозовецкий. — 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 488 с. — ISBN 978-5-507-47615-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/397355. — Режим доступа: для авториз. пользователей.

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 6-е изд., стер. — Санкт-Петербург : 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

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

6. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/288974 — Режим доступа: для авториз. пользователей.

7. Музипов, Х. Н. Программно-технические комплексы автоматизированных систем управления : учебное пособие для вузов / Х. Н. Музипов. — 2-е изд., стер. — Санкт-Петербург : 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.

8. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : 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.

9. 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

10. Минзов, А.С. Информационная безопасность и защита информации : учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. — Дубна : Государственный университет «Дубна», 2020. — 85 с. — ISBN 978-5-89847-608-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154490

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Официальный сайт компании Microsoft [Электронный ресурс] : Режим доступа: http://www.microsoft.com/, свободный. – Загл. с экрана.

Центр разработки Microsoft [Электронный ресурс] : Режим доступа:http://www.msdn.microsoft.com/, свободный. – Загл. с экрана.

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 обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. MicrosoftOffice
3. Kaspersky Endpoint Security

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

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Microsoft Share Point 2010
6. Vmware Player 15.5 + Гостевая ОС CentOS 7

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 практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепле-

ния изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических 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 практических занятий 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.

Тематика практических занятий соответствует программе курса.

5 семестр

Практическая работа 1. (6ч.). 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.

Практическая работа 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.

Практическая работа 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.

Практическая работа 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.

6 семестр

Практическая работа 1. (4 ч.). Управление пакетами

Цель: изучить работу пакетного менеджера yum
Задачи:
работа с утилитами управления пакетами и репозиториями rpm и yum
работа с утилитами создания новых пакетов rpmbuild и репозиториев createrepo
работа с утилитами для цифровой подписи пакетов
Указания для выполнения задания: для выполнения индивидуальных заданий используйте уникальный номер, как комбинацию k01-<номер_группы>-<номер_студента>. Например: студент №1 - k01-361-01 или k01-362-01.
Выполнение задания:
В ходе практической работы студенты на практике знакомятся с пакетным менеджером yum

Практическая работа 2. Изучение PAM (4 ч.)

Цель работы:
Изучить систему подгружаемых модулей аутентификации PAM (Pluggable Authentication Modules).
Задачи:
Изучить назначение, состав и возможности PAM.
Изучить API, научиться писать программы, использующие PAM.
Научиться создавать собственные модули (в будущем).
Расположение файлов:
Конфигурационные файлы: /etc/pam.conf, /etc/pam.d/.
Расположение модулей: /lib64/security/.
Определить, использует ли данная программа систему PAM, или нет.
Изучить содержимое каталогов, в которых хранятся библиотеки и модули:
$ ls -l /lib64/libpam* $ ls -l /lib64/security/
Изучите формат конфигурационных файлов. Определить управляющие группы и флаги.
Выполнение задания:
В ходе практической работы студенты на практике изучают модуль PAM

Практическая работа 3. Изучение SELinux (4 ч.)

Цель:
систему мандатного управления доступом **SELinux** (SecurityEnhancedLinux).
Задачи
Изучить назначение, состав и возможности **SELinux**.
Изучить API, научиться писать программы, использующие **SELinux** (*в будущем*).
Научиться создавать собственные модули безопасности (*в будущем*).
Расположение файлов:
Конфигурационные файлы: /etc/selinux/config, /etc/selinux/targeted/setrans.conf.
Политика безопасности: /etc/selinux/targeted/policy/policy.29.
Расположение модулей: /etc/selinux/targeted/modules/.
Задание
Использование SELinux
Определите, использует ли данная программа систему SELinux, или нет. Например:
$ ldd /bin/ls | grepselinux
libselinux.so.1 => /lib64/libselinux.so.1 (0x00007f13a075c000)
Расположение в файловой системе
Изучите содержимое каталогов, в которых хранятся библиотеки и модули:
$ ls -l /etc/selinux/
$ ls -l /etc/selinux/targeted/

Конфигурационные файлы
Изучите формат конфигурационного файла.
$ vi /etc/selinux/config

Практическая работа 4. Работа со справочной системой Linux.Конвейеры. Обработка текстовых файлов (4 ч.)

Цель: приобрести навыки выполнения команд, редактирования команд, просмотра истории, работы с аргументами команд.
Задачи:
Изучить команды: bash, man, whoami, cal, history, clear, date, echo, sudo, su.

Ход выполнения заданий

1. Команды могут группироваться и объединяться в потоки, а результат их выполнения перенаправляться в файл. Последовательности команд можно объединять в сценарии для повторного использования.
2. Управление командами осуществляется с помощью аргументов. Аргументы отделяются друг от друга пробелом.
3. Необходимо выполнить задания, приведенные в методичке, объяснив каждый шаг конвейера. Вместо знаков вопроса подставьте нужную команду/аргумент. Работа выполняется: на виртуальной машине.
4. Навыки: построение конвейеров из команд, сортировка, фильтрация, поиск.
5. Изучаемые команды: cut, grep, sort, wc, tr, uniq, head, tail, fold, column, less.

Примечание. Используйте команду man, чтобы получить больше информации об используемых командах и их аргументах.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины: научить студентов использовать для решения профессиональных задач современные средства программно-аппаратной защиты информации.

Задачи: формирование у студентов представлений о механизмах защиты ОС, выработка умений настраивать функций безопасности ОС, научить студентов использовать встроенные средства защиты информации ОС.

В результате освоения дисциплины обучающийся должен:

Знать место средств защиты информации в современных ОС, принципы реализации механизмов идентификации и аутентификации субъектов доступа в ОС, принципы разграничения доступа к объектам в ОС, принципы организации регистрации событий безопасности в ОС, критерии оценки защищённости автоматизированной системы, основные угрозы безопасности информации и модели нарушителя согласно РД ФСТЭК (Гостехкомиссия) и ФСБ.

Уметь определять источники и угрозы информационной безопасности в ОС, разрабатывать меры по защите от идентифицированных угроз, выбирать, устанавливать и настраивать средства защиты информации ОС, принимать участие в разработке политики безопасности; составлять и реализовывать планы тестирующих мероприятий, имитировать внешние и внутренние атаки нарушения системы безопасности, контролировать уровень защищенности ресурсов ОС, регистрировать и анализировать события в системных журналах ОС Windows и Linux.

Владеть профессиональной терминологией, навыками настройки и эксплуатации встроенных средствах защиты информации ОС; навыками эксплуатации и тестирования программно-аппаратных, криптографических и технических средств защиты информации, навыками проведения аудита защищенности информации в ОС Windows и Linux.