

МИНОБРНАУКИ РОССИИ



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

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

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Безопасность операционных систем

Рабочая программа дисциплины

Составитель:

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

Ответственный редактор

Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО

Протокол заседания кафедры
комплексной защиты информации

№ 10 от 20.05.2021 г. _____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с индикаторами достижения компетенций

1.3. Место дисциплины в структуре образовательной программы

2. Структура дисциплины

3. Содержание дисциплины

4. Образовательные технологии

5. Оценка планируемых результатов обучения

5.1. Система оценивания

5.2. Критерии выставления оценок

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

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

7. Материально-техническое обеспечение дисциплины

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

9. Методические материалы

9.1. Планы практических занятий

Приложения

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

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 защищенности информационных систем.

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

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
УК-2 Способен определять круг задач в рамках поставленной цели и выбрать оптимальные способы их решения, исходя из действующих правовых норм, имеющих ресурсы и ограничений	УК-2.1 Способен применять соответствующий математический аппарат для решения профессиональных задач	Уметь: решать типовые криптографические задачи защиты информации;
	УК-2.2 Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения	Владеть: навыками использования положений стандартов в области защиты ресурсов ОС при разработке, настройке и эксплуатации
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 защищенности ОС
	ОПК-9.3 Владеет методами и средствами криптографической и технической защиты информации	Владеть: навыками поиска нужной информации в нормативных базах 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.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплин: «Теория вероятностей и математическая статистика», «Дискретная математика», «Технология и методы программирования», «Информационные технологии».

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин: «Безопасность критически важных систем», «Оценка безопасности программного обеспечения автоматизированных систем».

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 учетными записями, идентификация и аутентификация в ОС	Управление учетными 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 надежный 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 Active Directory может содержать строки ACE, назначенные отдельным атрибутам). Регистрация событий и журналы безопасности.
5	Работа с терминалом	Эффективная профессиональная работа в Linux немислима 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 потребуются 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 репозиториями createrepo, работа с утилитами для цифровой подписи пакетов
2	Система подгружаемых модулей аутентификации PAM (Pluggable Authentication Modules)	Назначение, состав и возможности PAM. API, использующие PAM. Написание собственных модулей на bash
3	Углубленное 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 SE-Linux: <ul style="list-style-type: none"> • 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 Изучение материалов лекций
2	Место сервисов безопасности в ОС	Лекция 2.1 Лекция 2.2 Практическое занятие 1. Самостоятельная работа	Традиционная с использованием презентаций 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 Практическое занятие 2. Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания в виртуальной машине CentOS 7. Специализированное ПО – Oracle VM VirtualBox Изучение материалов лекций
4	Управление доступом к объектам файловой системы	Лекция 4.1 Лекция 4.2 Лекция 4.3 Практическое занятие 3. Самостоятельная работа	Традиционная с использованием презентаций 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 Практическое занятие 4. Самостоятельная работа	Традиционная с использованием презентаций 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.	<i>Пакетный менеджер yum</i>	<i>Лекция 1.1 Лекция 1.2 Практическое занятие 1 Самостоятельная работа</i>	<i>Традиционная с использованием презентаций Выполнение задания в виртуальной машине CentOS 7. Изучение материалов лекций</i>
2	<i>Система подгружаемых модулей аутентификации PAM (Pluggable Authentication Modules)</i>	<i>Лекция 2.1 Лекция 2.2 Практическое занятие 2 Самостоятельная работа</i>	<i>Традиционная с использованием презентаций Выполнение задания в виртуальной машине CentOS 7. Изучение материалов лекций</i>
3	<i>Углубленное изучение системы мандатного управления доступом SELinux (Security Enhanced Linux)</i>	<i>Лекция 3.1 Лекция 3.2 Практическое занятие 3. Самостоятельная работа</i>	<i>Традиционная с использованием презентаций Выполнение задания в виртуальной машине CentOS 7. Изучение материалов лекций</i>
4	<i>Работа со справочной системой Linux. Конвейеры. Обработка текстовых файлов</i>	<i>Лекция 4.1 Лекция 4.2 Практическое занятие 4. Самостоятельная работа</i>	<i>Традиционная с использованием презентаций Выполнение задания в виртуальной машине CentOS 7. Изучение материалов лекций</i>

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
– опрос (темы 1-5)	5 баллов	30 баллов
– лабораторные задания (темы 1-3)	6 баллов	6 баллов
– лабораторные задания (темы 4-5)	7 баллов	24 балла
– опрос (темы 1-4)	5 баллов	30 баллов
– лабораторные задания (темы 1-2)	6 баллов	6 баллов
– лабораторные задания (темы 3-4)	7 баллов	24 балла
Промежуточная аттестация		40 баллов
Зачет с оценкой		
Итого за дисциплину экзамен		100 баллов

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

<i>№ п/п</i>	<i>Контролируемые разделы дисциплины</i>	<i>Код контролируемой компетенции</i>	<i>Наименование оценочного средства</i>
1.	Темы 1 – 6	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1	Опрос
2.	Практические занятия 1 – 4 (5 семестр)	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1	План практического занятия
3	Практические занятия 1 – 4 (6 семестр)	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1	План практического занятия

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/ А,В	«отлично»/ «зачтено (отлично)»/ «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>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.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ С	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>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.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,Е	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	<p>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.</p> <p>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.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		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 выставляется 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 дисциплине¹

Примерные контрольные вопросы для экзамена - проверка сформированности компетенций

Контрольные вопросы	Реализуемые компетенции
1. Тактика действия злоумышленника и обманные системы защиты.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
2. Основные разработчики пакетов для квантовых вычислений.	ОПК-9.1; ОПК-9.2; ОПК-9.3
3. Проблема защиты программного обеспечения автоматизированных систем	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
4. Защита программного обеспечения как система научных дисциплин	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
5. Угрозы безопасности программного обеспечения	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
6. Технологическая и эксплуатационная безопасность программного обеспечения	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1

¹ Приводятся примеры оценочных средств в соответствии со структурой дисциплины и системой контроля: варианты тестов, тематика письменных работ, примеры экзаменационных билетов, типовые задачи, кейсы и т.п. Оценочными средствами должны быть обеспечены все формы текущего контроля и промежуточной аттестации. Они должны быть ориентированы не только на проверку сформированности знаний, но также умений и владений.

7. Защита от НСД в современных ОС.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
8. Администрирование ОС.	ОПК-9.1; ОПК-9.2; ОПК-9.3
9. Аудит безопасности.	ОПК-9.1; ОПК-9.2; ОПК-9.3;
10. Защита от НСД в современных ОС.	ОПК-9.1; ОПК-9.2; ОПК-9.3;
11. Порядок проведения аттестации объектов информатизации. Содержание заявок.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
12. Угрозы безопасности программного обеспечения.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
13. Технологическая и эксплуатационная безопасность программного обеспечения.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
14. Модели угроз безопасности программного обеспечения.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
15. Основные принципы обеспечения безопасности программного обеспечения.	УК-2,2, УК-2.1
16. Методы анализа безопасности программного обеспечения.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
17. Методы защиты программ от компьютерных вирусов.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
18. Аутентификация и идентификация. Протокол LDAP.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
19. Системы аудита.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
20. Штатные средства защиты ОС Linux.	ОПК-9.1; ОПК-9.2; ОПК-9.3
21. Понятие кольца защиты ОС.	ОПК-9.1; ОПК-9.2; ОПК-9.3
22. Механизмы доменной защиты.	ОПК-9.1; ОПК-9.2; ОПК-9.3
23. Архитектура ОС.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
24. Доверенная загрузка и контроль BIOS.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
25. Примеры операционных систем в защищенном исполнении.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
26. Мониторинг процессов ОС.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
27. Электронные ключи. Принципы работы.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
28. Идентификация и аутентификация в домене Active Directory.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
29. Протокол LDAP.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
30. Принципы работы Kerberos,	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
31. Мультидоменный гипервизор.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1

32. ОС 2000. Особенности работы планировщика и принципов защиты.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
33. ОС «Феникс». Особенности доменной защиты.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
34. UAC – Контроль учетных записей в ОС Windows.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
35. Методы перехвата информации и технология противодействия ССИВ.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
36. Основные разработчики пакетов для квантовых вычислений.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
37. Проблема защиты программного обеспечения автоматизированных систем.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
38. Защита программного обеспечения как система научных дисциплин.	ОПК-9.1; ОПК-9.2; ОПК-9.3
39. Угрозы безопасности программного обеспечения.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
40. Технологическая и эксплуатационная безопасность программного обеспечения.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
41. Модели угроз безопасности программного обеспечения.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
42. Основные принципы обеспечения безопасности программного обеспечения.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
43. Методы анализа безопасности программного обеспечения.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1
44. Перспективные направления развития высокоскоростных сетей и их защиты.	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1

Примерные задания для тестирования- проверка сформированности компетенций УК-2, ОПК-9

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» (с изм. и доп., посл. от 01.05.2019). [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» (с изм. и доп., посл. от 31.12.2017). [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» (с изм. и доп., посл. от 23.06.2016). [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» (с изм. и доп., посл. от 28.11.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_40241/, свободный. – Загл. с экрана.

Литература Основная

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/452368>
 2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/454453>
 3. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449285>
 4. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451231>
 5. *Комплексная защита информации в корпоративных системах* : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/546679>
 6. *Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства* [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: <http://znanium.com/catalog/product/408107>
- 6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».
1. Официальный сайт компании Microsoft [Электронный ресурс] : Режим доступа: <http://www.microsoft.com/>, свободный. – Загл. с экрана.
 2. Центр разработки Microsoft [Электронный ресурс] : Режим доступа: <http://www.msdn.microsoft.com/>, свободный. – Загл. с экрана.

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 установлены 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 практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. 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	Свободное ПО, Режим доступа: https://www.vmware.com/products/ Демо-версия Открытое ПО Режим доступа: https://www.centos.org/download/ Инсталляционный дистрибутив Linux

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

Перечень БД и ИСС

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

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, регулируемые эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы²

9.1. Планы практических лабораторных занятий - проверка сформированности компетенций УК-2, ОПК-9

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, 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 подго-

² Методические материалы по дисциплине могут входить в состав рабочей программы, либо разрабатываться отдельным документом.

товки 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

Практическое задание 1(4ч.). Основные сервисы безопасности ОС - проверка сформированности компетенций УК-2, ОПК-9

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.

Список литературы:

Приведён в п. 6 данной РПД

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.

Практическое задание 2(6 ч.). Идентификация и аутентификация в ОС - проверка сформированности компетенций УК-2, ОПК-9

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.

Список литературы:

Приведён в п. 6 данной РПД

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.

Практическое задание 3(4 ч.). Регистрация событий и анализ журналов безопасности - проверка сформированности компетенций УК-2, ОПК-9

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.

Список литературы:

Приведён в п. 6 данной РПД

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.

Практическое задание 4(6 ч.). Работа с командной строкой Linux - проверка сформированности компетенций УК-2, ОПК-9

Цель работы: получение практических навыков в эксплуатации современных ОС.

Указания по выполнению задания: обратить внимание на требование комплексного подхода для защиты СВТ.

Выполнение задания:

В ходе практической работы студенты на практике знакомятся с командной строкой Linux.

Список литературы:

Приведён в п. 6 данной РПД

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.

6 семестр

Практическое задание 1(6 ч.). Управление пакетами - проверка сформированности компетенций УК-2, ОПК-9

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 репозиториями 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

Список литературы:
Приведён в п. 6 данной РПД

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.

Практическое задание 2 Изучение PAM - проверка сформированности компетенций УК-2, ОПК-9

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

Список литературы:
Приведён в п. 6 данной РПД

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.

Практическое задание 3 Изучение SELinux - проверка сформированности компетенций УК-2, ОПК-9

Цель:

систему мандатного управления доступом **SELinux** (Security Enhanced Linux).

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 | grep selinux
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
```

Список литературы:

Приведён в п. 6 данной РПД

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.

Практическое задание 4 .Работа со справочной системой Linux.Конвейеры. Обработка текстовых файлов - проверка сформированности компетенций УК-2, ОПК-9

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.

Список литературы:

Приведён в п. 6 данной РПД

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 ДИСЦИПЛИНЫ

Дисциплина «Безопасность операционных систем автоматизированных систем» реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки – Безопасность автоматизированных систем) кафедрой комплексной защиты информации.

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.

Дисциплина направлена на формирование следующих компетенций:

- УК-2 – Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- УК-2.1 – Способен применять соответствующий математический аппарат для решения профессиональных задач
- УК-2.2 - Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения
- 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
- ОПК-9.2 – Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации
- ОПК-9.3 - Владеет методами и средствами криптографической и технической защиты информации

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.

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.

Владеть профессиональной терминологией, навыками настройки и эксплуатации встроенных средств защиты информации ОС; навыками эксплуатации и тестирования программно-аппаратных, криптографических и технических средств защиты информации.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоёмкость освоения дисциплины составляет в 5 семестре 3 зачётные единицы, в 6 семестре – 2 зачетные единицы.

УТВЕРЖДЕНО
Протокол заседания кафедры
№ _____ от _____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины Безопасность операционных систем
(название дисциплины)
по направлению подготовки Информационная безопасность
на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1.;
1.2.;
...
1.9.

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1.;
2.2.;
...
2.9.

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1.;
3.2.;
...
3.9.

Составитель
дата

подпись

расшифровка подписи