МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Гусев П.Ю.

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Защита в операционных системах»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /Белоножкин В.И./

Заведующий кафедрой
Систем информационной
безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ /Остапенко А.Г./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Формирование и закрепление профессиональных компетенций, направленных на знание и владение методами обеспечения защиты информации в современных операционных системах.

1.2. Задачи освоения дисциплины

- ознакомление с методами, способами, средствами защиты информации в операционных системах;
- формирование умений управления политиками безопасности и администрирования операционных систем;
- приобретение навыков настройки и использования механизмов и средств защиты операционных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита в операционных системах» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Защита в операционных системах» направлен на формирование следующих компетенций:

ОПК-12 - Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-12	Знать методы и механизмы защиты, средства аутентификации, контроля доступа, аудита и восстановления работоспособности в операционных системах
	Уметь настраивать политики безопасности и администрировать операционные системы
	Владеть навыками использования средств управления доступом, аудита, восстановления работоспособности прикладного и системного программного обеспечения

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Защита в операционных системах» составляет 4 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего	Семестры

	часов	7
Аудиторные занятия (всего)	54	54
В том числе:		
Лекции	18	18
Практические занятия (ПЗ)	36	36
Самостоятельная работа	90	90
Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость: академические часы зач.ед.	 144 4	 144 4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
1	Структура, механизмы и компоненты подсистем безопасности ОС	Характеристика подсистем безопасности ОС. Механизмы аутентификациии, контроля доступа, аудита, поддержания работоспособности. Основные типы средств, реализующих защитные механизмы.	4	8	20	32
2	Реализация механизмов и компонентов защиты ОС семейства Windows	Политики безопасности Windows. Механизмы и службы безопасности. Active Directory. Шифрованная файловая система. Виртуализация. Аудит. Поддержание работоспособности и восстановление..	4	10	20	34
3	Реализация механизмов и компонентов защиты ОС семейства Linux	Основные механизмы и средства защиты ОС Linux. Проекты расширений безопасности Linux. Средства обеспечения безопасности сетей под управлением Linux.	4	8	20	32
4	Реализация механизмов и компонентов защиты других типов ОС	Механизмы и инструменты защиты сертифицированных в России релизов ОС. Механизмы и средства защиты ОС компании Apple. Механизмы и средства защиты ОС семейства ОС Android.	6	10	30	46
		Итого	**18**	**36**	**90**	**144**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-12	Знать методы и механизмы защиты, средства аутентификации, контроля доступа, аудита и восстановления работоспособности в операционных системах	Ответ на вопрос преподавателя, выполнение теста	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь настраивать политики безопасности и администрировать операционные системы	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками использования средств управления доступом, аудита, восстановления работоспособности прикладного и системного программного обеспечения	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 7 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-12	Знать методы и	Тест	Выполнение	Выполнение	Выполнение	В тесте

	механизмы защиты, средства аутентификации, контроля доступа, аудита и восстановления работоспособности в операционных системах		теста на 90-100%	теста на 80-90%	теста на 70-80%	менее 70% правильных ответов
	Уметь настраивать политики безопасности и администрировать операционные системы	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть навыками использования средств управления доступом, аудита, восстановления работоспособности прикладного и системного программного обеспечения	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2. Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Степень защищенности ОС определяется:

а) количеством блокируемых угроз безопасности;

б) наличием или отсутствием уязвимостей;

в) уровнем риска.

2. В защищенной ОС базовые средства защиты располагаются в:

а) прикладных программах;

б) ядре;

в) системных службах.

3. К функциям подсистемы безопасности ОС относятся:

а) управление доступом к объектам;

б) выполнение файловых операций;

в) маршрутизация сетевых пакетов.

4. Разграничение доступа на основе мандатного принципа контроля использует механизм:

а) ролей;
б) меток безопасности;
в) набора правил.
5. Авторизация в ОС осуществляет:
а) опознавание пользователя
б) запрет действий пользователя
в) привязку процессов к пользователю
6. К объектам групповой политики относятся:
а) домен
б) локальная сеть
в) кластер
7. К видам политик безопасности ОС семейства Windows относится
а) политика объектов;
б) политика учетных записей;
в) сетевая политика.
8. Защиту от вредоносного сетевого трафика обеспечивает:
а) межсетевой экран;
б) сетевая карта сервера;
в) контроллер домена.
9. Обеспечение работоспособности ОС – это:
а) оптимизация нагрузки;
б) поддержание доступности и целостности;
в) защита системных настроек.
10. К функциям аудита безопасности в ОС относятся:
а) мониторинг несанкционированного доступа;
б) контроль полномочий пользователей;
в) фиксация настроек ОС.

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Типовая структура подсистемы безопасности ОС включает в себя:
а) средства аутентификации;
б) сетевые драйверы;
в) модуль ввода-вывода.
2. К основным действиям по управлению процессами ОС относятся:
а) визуализация выполнения процесса на дисплее;
б) сопровождение выполнения каждого процесса записью в журнале;
в) создание и удаление процессов.
3. Открытие файла – это:
а) запись на носитель;
б) обнуление признаков защиты;
в) считывание заголовка и одного или нескольких смежных блоков в оперативную память.
4. В процессе аутентификации ОС проверяет:
а) полномочия пользователя

б) наличие учетной записи пользователя

в) совпадения атрибутов, предъявляемых пользователем и сохраненных в системе.

5. Пароли в ОС Linux хранятся:

а) в реестре;

б) в файле;

в) в специальной базе данных

6. В состав элементов механизма авторизации ОС Windows входит:

а) логин пользователя

б) привилегия

в) маркер доступа

7. К оснасткам безопасности ОС Windows относится:

а) диспетчер устройств;

б) центр поддержки;

в) администрирование.

8. Настройки межсетевого экрана регулируют:

а) входящий трафик;

б) отображение графики на экране;

в) количество запускаемых приложений.

9. К средствам восстановления ОС после сбоя относятся:

а) утилиты сканирование и дефрагментация дисков;

б) загрузка в безопасном режиме работы;

в) средства устранения “зависаний” программ.

10. В журнал безопасности ОС записываются:

а) данные сеанса работы пользователей;

б) события нарушения политик безопасности;

в) запуск системных служб.

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Настройка параметров ОС при установке включает:

а) максимальное количество хранимых файлов;

б) период обновления системы;

в) пароль учетной записи администратора.

2. Автоматическая установка обновлений ОС:

а) оперативно закрывает выявленные уязвимости;

б) снижает стабильность работы;

в) исключает контроль пользователя.

3. Повышение уровня требований к паролям пользователей:

а) затрудняет работу на компьютере

б) повышает защищенность учетных записей

в) успокаивает администратора безопасности

4. Использование системных привилегий:

а) дает приоритет в использовании дискового пространства;

б) позволяет копировать файлы любой длины;

в) позволяет управлять доступом к классам операций.

5. Коммуникация между процессами организуется:

а) по электронной почте

б) с помощью файловых операций

в) с помощью передачи сообщений или общей области памяти

6. Для авторизации действий пользователя в ОС:

а) запускается специальная программа:

б) используется его идентификатор;

в) проверяется системный журнал.

7. Структура прав доступа к файлам в ОС Linux:

а) владелец – группа владельца – все остальные;

б) администратор – остальные пользователи;

в) root — владелец – остальные пользователи.

8. Отличным правом доступа к файлам в ОС Windows от Linux является:

а) чтение;

б) запись;

в) изменение

9. Настройка средств аудита включает в себя:

а) выбор вида событий регистрации;

б) выбор фиксируемых пользователей;

в) выбор места размещения журнала.

10. Регламент резервирования ОС устанавливает:

а) количество сохраняемых файлов;

б) ответственного пользователя;

в) периодичность проведения операции резервирования.

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Классификация угроз безопасности ОС.
2. Требования безопасности ОС.
3. Понятие защищенной ОС.
6. Содержание системного подхода к обеспечению безопасности ОС.
7. Подходы к оценке эффективности реализации защиты ОС.
8. Способы аутентификации пользователей ОС.
9. Средства и методы повышения надежности аутентификации в ОС.
10. Механизмы управления доступом в ОС.
11. Методы, права доступа и привилегии субъектов по отношению к объектам ОС.
12. Встроенные средства защиты файлов в ОС.
13. Реализация дискреционного и мандатного принципов в защищенных ОС.
14. Задачи аудита в ОС.
15. Методы и средства реализации аудита в современных ОС.
16. Подходы к организации восстановления работоспособности в современных ОС.

7.2.5 Примерный перечень вопросов для подготовки к экзамену

Не предусмотрено учебным планом.

7.2.6 Методика выставления оценки при проведении промежуточной аттестации

Зачет проводится по тест-билетам, каждый из которых содержит 5 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, верное решение адачи оценивается в 5 баллов. Максимальное количество набранных баллов – 10.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 2 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 2 до 4 баллов.

3. Оценка «Хорошо» ставится в случае, если студент набрал от 5 до 7 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 8 до 10 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Структура, механизмы и компоненты подсистем безопасности ОС	ОПК-12	Тест, контрольное задание, защита реферата
2	Реализация механизмов и компонентов защиты ОС семейства Windows	ОПК-12	Тест
3	Реализация механизмов и компонентов защиты ОС семейства Linux	ОПК-12	Тест, защита реферата
4	Реализация механизмов и компонентов защиты других типов ОС	ОПК-12	Тест

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении

промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8. УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1. Перечень учебной литературы, необходимой для освоения дисциплины

1. Проскурин В.Г. Защита в операционных системах. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 192 с.

2. Буренин П.В., Девянин П.Н., Лебеденко Е.В., Проскурин В.Г., Цибуля А.Н. Безопасность операционной системы специального назначения Astra Linux Special Edition.

3. Линн С. Администрирование Microsoft Windows Server 2012. — СПб.: Питер, 2014. -304 с.

4. Хакер Р. Active Directory глазами хакера. — СПб.: БХВ-Петербург, 2021. -176 с.

5. Гончарук С.В. Администрирование ОС Linux. - М.: Национальный открытый университет «ИНТУИТ», 2016. -165 с.

6. Зобнин Е. Е. Android глазами хакера. — СПб.: БХВ-Петербург, 2021. — 272 с.

8.2. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

- ЕИОС ВГТУ http://eios.vorstu.ru/;
– ЭБС «Консультант студента» http://www.studentlibrary.ru/;
– Портал «Anti-Malware» https://www.anti-malware.ru;
– портал «Information Security» https://www.itsec.ru;
– электронный журнал «Information Security» http://lib.itsec.ru/imag/;
– операционные системы Windows, Linux, Android.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Аудитория с компьютерными рабочими местами, локальная сеть, презентационное оборудование.

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

По дисциплине «Защита в операционных системах» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков настройки и администрирования средств защиты ОС. Занятия проводятся путем решения конкретных задач в аудитории.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.