МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
«Информационные технологии»
_____ / Д.Г.Демидов /
«15» февраля 2024г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность операционных систем Windows»

Направление подготовки
10.03.01 «Информационная безопасность»

Профиль/специализация
«Безопасность компьютерных систем»

Квалификация
Бакалавр

Формы обучения
Очная

Москва, 2024 г.

Разработчик(и):

Должность, звание / _____/

Согласовано:
Заведующий кафедрой «Информационная безопасность»  /И.В.Калуцкий/

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Безопасность операционных систем Windows» следует отнести:

- обучение студентов принципам построения операционных систем (ОС) Windows;
- обучение принципам построения защиты информации в ОС Windows и анализа надежности защиты ОС Windows.

К **основным задачам** освоения дисциплины «Безопасность операционных систем Windows» следует отнести:

- знание принципов функционирования ОС Windows;
- знание принципов построения подсистем защиты в ОС Windows;
- знание средств и методов несанкционированного доступа (НСД) к ресурсам ОС Windows .

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ИОПК-1.1.1. Знает формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; ИОПК-1.1.2. Умеет применять формальные модели для разработки политик безопасности, политик управления доступом; ИОПК-1.1.3. Владеет навыками создания формальных моделей управления доступом

2 Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность операционных систем Windows» относится к числу учебных дисциплин обязательной части (Б1.1) основной образовательной программы (Б1.1.21).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационно-коммуникационных технологий».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лабораторные занятия – 72 часа, самостоятельная работа - 72 часа, форма контроля – экзамен, курсовой проект) в 3 семестре.

Структура и содержание дисциплины «Безопасность операционных систем Windows» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость (по очной форме обучения)

№ п/п	Вид учебной работы	Количество часов	Семестры	
			3	
1	**Аудиторные занятия**	**72**	72	
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	72	
2	**Самостоятельная работа**	72	72	
	В том числе:			
2.1	…			
3	**Промежуточная аттестация**			
	Экзамен, курсовой проект			
	Итого:	**144**	144	

Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1.	Тема 1. Понятие операционная система, классификация операционных систем. Семейство операционных систем Windows. Устройство ОС Windows. Требования регуляторов Российской Федерации по обеспечению безопасности информации: ФСТЭК России, ФСБ России, Минобороны России	28			14		14
2.	Тема 2. Процессы, потоки, работы, задания. Управление памятью. Файловая система. Система ввода-вывода. Основные системные процессы ОС Windows	28			14		14

3.	Тема 3. Угрозы безопасности информации. БДУ ФСТЭК России. Уязвимости ОС. ОС отечественного производства. Производители ОС российского производства. ОС российского и зарубежного производства в отечественных реестрах.	28			14		14
4.	Тема 4. Базовый (out of box) уровень безопасности ОС Windows. Меры по повышению уровня безопасности ОС Windows	28			14		14
5.	Тема 5. Требования безопасности информации к операционным системам ФСТЭК России	32			16		16
6.	Тема 6. Управление пользователями и группами. Файловая система NTFS. Разграничение доступа с помощью механизмов NTFS.						
7.	Тема 7. Реализация встроенных механизмов защиты информации Microsoft Windows на автономном рабочем месте, в одноранговой сети, в сети Active Directory						
8.	Тема 8. Применение Group Policy ОС Windows						
9.	Тема 9. Технологии для работы ОС Windows в сети, мониторинга и аудита, резервного копирования						
10.	Тема 10. Наложенные средства защиты информации,						

	применяемые для ОС Windows						
Итого		**144**			**72**		**72**

3.2 Содержание дисциплины

1. **Содержание дисциплины**

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1.	Понятие операционная система, классификация операционных систем. Семейство операционных систем Windows. Устройство ОС Windows. Требования регуляторов Российской Федерации по обеспечению безопасности информации: ФСТЭК России, ФСБ России, Минобороны России	Понятие операционная система, классификация операционных систем. Архитектура многозадачной сетевой операционной системы. Семейство операционных систем Windows. Требования регуляторов Российской Федерации по обеспечению безопасности информации: ФСТЭК России, ФСБ России, Минобороны России. Профили защиты операционных систем, задания по безопасности. Требования безопасности информации к операционным системам ФСТЭК России. Подсистемы системы защиты информации от НСД в соответствии с «РД. АС. Защита от НСД. Классификация АС и требования по ЗИ» (от 30 марта 1992 года).
2.	Процессы, потоки, работы, задания. Управление памятью. Файловая система. Система ввода-вывода. Основные системные процессы ОС Windows	Процессы, потоки, работы, задания. Основные системные процессы ОС Windows. Семейство утилит Sysinternals Suite. Диспетчер задач (Task Manager). Утилита Sysinternals Process Explorer и Process Monitor. Управление памятью. Файловая система. Система ввода-вывода.
3.	Угрозы безопасности информации. БДУ ФСТЭК России. Уязвимости ОС. ОС отечественного производства. Производители ОС российского производства. ОС российского и зарубежного производства в отечественных реестрах.	Угрозы безопасности информации. БДУ ФСТЭК России. Уязвимости ОС. Понятие сертифицированных и лицензированных ОС. ОС российского производства, производители ОС российского производства. ОС российского и зарубежного производства в реестре российского программного обеспечения, едином реестре российских программ для электронных вычислительных машин и баз данных, реестр средств защиты информации ФСТЭК России и ФСБ России. Уровни конфиденциальности информации, обрабатываемой в ОС.
4.	Базовый (out of box) уровень безопасности ОС Windows. Меры по повышению уровня безопасности ОС Windows	Базовый (out of box) уровень безопасности ОС Windows. Меры по повышению уровня безопасности ОС Windows. Подходы к повышению уровня безопасности ОС Windows (чек-листы безопасности ОС Windows).

5.	Требования безопасности информации к операционным системам ФСТЭК России	Требования безопасности информации к операционным системам ФСТЭК России: типы и классы. Рассмотрение профилей защиты и примеров заданий по безопасности ОС различных типов и классов.
6.	Управление пользователями и группами. Файловая система NTFS. Разграничение доступа с помощью механизмов NTFS.	Пользователи и их виды. Группы пользователей. Учётные записи пользователей и работа с ними. Управление пользователями на автономном рабочем месте, в домене Active Directory. Файловая система NTFS. Файлы и папки. Разграничение доступа с помощью механизмов NTFS, настройка ACL прав доступа пользователей в NTFS.
7.	Реализация встроенных механизмов защиты информации Microsoft Windows на автономном рабочем месте, в одноранговой сети, в сети Active Directory	Криптографическая защита пользовательских данных средствами шифрующей файловой системы EFS. Технология BitLocker и BitLocker To Go. Технология DirectAccess. Технология Network Access Control. Создание замкнутой программной среды с помощью функции AppLocker.
8.	Применение Group Policy ОС Windows	Применение Group Policy ОС Windows для защиты информации на автономном рабочем месте и в сети Active Directory. Технологии безопасного удалённого доступа к корпоративным ресурсам (применение встроенного функционала операционных систем).
9.	Технологии для работы ОС Windows в сети, мониторинга и аудита, резервного копирования	Установка и настройку служб и компонентов DNS, DHCP, Windows Backup Services, Windows Deployment Services
10.	Наложенные средства защиты информации, применяемые для ОС Windows	Классификация, виды наложенных средств защиты информации, применяемые для ОС Windows

1. **Тематика семинарских/практических и лабораторных занятий**

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

№ п/п	Наименование лабораторной работы	Объем, час.
1.	Выполнение лабораторной работы № 1 по теме 1	6
2.	Выполнение лабораторной работы № 2 по теме 2	6
3.	Выполнение лабораторной работы № 3 по теме 3	6
4.	Выполнение лабораторной работы № 4 по теме 4	8

5.	Выполнение лабораторной работы № 5 по теме 5	8
6.	Выполнение лабораторной работы № 6 по теме 6	8
7.	Выполнение лабораторной работы № 7 по теме 7	8
8.	Выполнение лабораторной работы № 8 по теме 8	8
9.	Выполнение лабораторной работы № 9 по теме 9	8
10.	Выполнение лабораторной работы № 10 по теме 10	6
Итого		72

2. Тематика и содержание курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом запланировано, тема курсовой работы: «Освоение встроенных механизмов защиты информации в ОС Windows». В ходе выполнения курсовой работы учащиеся должны выполнить:
установку Microsoft Windows Server;
выполнить настройку Microsoft Windows Server для повышения начального уровня информационной безопасности;
установку и настройку служб домена Windows – AD DS;
развёртывание ОС АРМ (пользовательская ОС Windows, не серверная) по сети с помощью Windows Deployment Services (WDS), Microsoft Deployment Toolkit;
выполнить настройку ОС АРМ - Microsoft Windows (пользователя) для повышения начального уровня информационной безопасности;
создание и применение параметров безопасности по сети с помощью механизма Group Policy (GP);
настройку роли «файл-сервер», настройку ACL прав доступа пользователей в NTFS;
установку и управление в сети домена Microsoft Windows серверных и клиентских СрЗИ;
установку и настройку Windows Backup Services.

4 Учебно-методическое и информационное обеспечение

1. Нормативные документы и ГОСТы

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность».

4.2 Основная литература

1. Астапчук, В. А. Корпоративные информационные системы: требования при проектировании : учебное пособие для вузов / В. А. Астапчук, П. В. Терещенко. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 113 с. — (Высшее образование). — ISBN 978-5-534-08546-4. — Текст : электронный //

Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/514213 (дата обращения: 24.09.2023).
2. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512144 (дата обращения: 24.09.2023).

4.3 Дополнительная литература

1. Староверова, Н. А. Операционные системы : учебник для спо / Н. А. Староверова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 412 с. — ISBN 978-5-8114-8984-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/186048 (дата обращения: 24.09.2023). — Режим доступа: для авториз. пользователей.
2. Малахов, С. В. Операционные системы и оболочки / С. В. Малахов. — Санкт-Петербург : Лань, 2023. — 120 с. — ISBN 978-5-507-45325-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/302681 (дата обращения: 24.09.2023). — Режим доступа: для авториз. пользователей.

4.4 Электронные образовательные ресурсы

1. ЭОР «Безопасность операционных систем Linux» [Электронный ресурс] — URL: https://online.mospolytech.ru/course/view.php?id=9267 (дата обращения: 01.10.2023).

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Microsoft Windows

4.6 Современные профессиональные базы данных и информационные справочные системы

1. Федеральная государственная информационная система - Национальная электронная библиотека (НЭБ) https://нэб.рф

5. Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

6. Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

7. Фонд оценочных средств

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- компьютерное тестирование;
- экзамен.

Образцы тестовых заданий, экзаменационных билетов, приведены в приложении.

7.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

7.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК-1.2	Способен администрировать средства защиты информации в компьютерных системах и сетях

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

7.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

Показатель	Критерии оценивания			
	2	3	4	5
ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах				
ИОПК-1.1.1. Знает формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний,	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины

ИОПК-1.1.2. Умеет применять формальные модели для разработки политик безопасности, политик управления доступом; ИОПК-1.1.3. Владеет навыками создания формальных моделей управления доступом	указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	«Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	«Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств

Оценочные средства для текущей аттестации

Компьютерное тестирование.

По каждой теме предлагается 10 вопросов по каждой теме. Освоение темы зависит от результата написания теста: 9-10 баллов - тема считается освоенной на продвинутом уровне; 6-8 баллов - тема считается освоенной на базовом уровне; 0-5 баллов – тема считается не освоенной.

Оценочные средства для промежуточной аттестации

Экзамен.

Список вопросов для экзамена по дисциплине

1. Понятие операционная система, классификация операционных систем.
2. Архитектура многозадачной сетевой операционной системы.
3. Защищённые файловые системы.
4. Понятие политики разграничения доступа в компьютерных системах.
5. Одноуровневая и многоуровневая модели разграничения доступа, их достоинства и недостатки.
6. Реализация технологии разграничения доступа в операционных системах.
7. Идентификация, аутентификация. Факторы аутентификации.
8. Загрузчики операционных систем. Обеспечение защиты от НСД при загрузке системы.
9. Понятие сертифицированных и лицензированных операционных систем.
10. Операционные системы семейства Microsoft Windows. Особенности реализации механизмов защиты информации.
11. Криптографическая защита пользовательских данных средствами шифрующей файловой системы EFS.
12. Технология BitLocker и BitLocker To Go.
13. Технология DirectAccess.
14. Технология Network Access Control.
15. Создание замкнутой программной среды с помощью функции AppLocker.
16. Реализация встроенных механизмов защиты информации Microsoft Windows на автономном рабочем месте, в одноранговой сети.
17. Защита информации в Active Directory.
18. Пользователи и их виды. Группы пользователей. Учётные записи пользователей и работа с ними.
19. Применение Group Policy операционных систем Windows для защиты информации.
20. Технологии безопасного удалённого доступа к корпоративным ресурсам (применение встроенного функционала операционных систем).
21. Операционная система Astra Linux. Особенности реализации механизмов защиты информации.
22. Механизм избирательного управления доступом Astra Linux.
23. Механизм PAM как реализация функции идентификации и аутентификации пользователей в Astra Linux. Средства поддержки двухфакторной аутентификации.
24. Домен Astra Linux Directory. Технологии защиты информации в домене Astra Linux.
25. Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками (МРОСЛ ДП-модель) Astra Linux Special Edition.

26. Основные положения руководящих документов (РД) ФСТЭК России (Гостехкомиссии) по защите информации.
27. РД. АС. Защита от НСД. Классификация АС и требования по ЗИ (от 30 марта 1992 года).
28. РД. Защита от НСД. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля НДВ (от 4 июня 1999 года).
29. РД. СВТ. Защита от НСД к информации. Показатели защищённости от НСД к информации (от 30 марта 1992 года).
30. Средства защиты информации, устанавливаемые на операционные системы. Классификация. Решаемые задачи.
31. Системы защиты информации. Метод определения состава и оценки эффективности системы защиты информации.
32. Угрозы безопасности информации.
33. Уязвимости операционных систем.

Пример билета.

1. Алгоритмы и механизмы синхронизации.
2. Разграничение доступа в ОС.