МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита в операционных системах

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью изучения дисциплины «Защита в операционных системах» является формирование у студентов знаний по основам использования операционных систем в защищенном исполнении, по средствам и методам обеспечения защиты информации в ОС, а также навыков и умения в применении знаний при проведении работ: - по разработке и конфигурированиюпрограммно-аппаратных средств защиты информации; - по установке, наладке, тестированию и обслуживанию системного и прикладного программного обеспечения; - по разработке технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов; - по подготовке аналитических отчетов по результатам проведенного анализаивыработка предложений по устранению выявленных уязвимостей; - по установке, наладке, тестированию и обслуживанию программно-аппаратных средств обеспечения информационной безопасности компьютерных систем.

Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода. Задачи дисциплины – дать знания: -по концепции построения защищенных ОС; -по теоретическим основам защиты информации в ОС; -по возможным угрозам безопасности информации при ее обработке в информационных системах; -по встроенным в ОС средствам защиты информации; -по средствам и методам управления доступом в ОС; -по использованию защищенных ОС в сетях передачи данных.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-6 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

ПК-3 - Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- Нормативные правовые акты и методические документы ФСТЭК и ФСБ России, регламентирующие защиту информации ограниченного доступа в операционных системах.
- Современные тенденции развития криптографических методов и средств, применяемых для защиты информации в операционных системах.
- Принципы администрирования и критерии корректности функционирования компьютерных сетей с точки зрения безопасности.
- Методики мониторинга работоспособности и критерии оценки эффективности средств защиты информации в операционных системах.
- Основные этапы исторического развития России и роль информационных технологий в современном обществе.
- Методики и инструментарий для проверки эффективности систем защиты информации и политик безопасности в различных операционных системах (Windows, Linux).
- Типовые неисправности и уязвимости программно-аппаратных средств защиты информации в операционных системах.
- Принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации.

Уметь:

- Организовывать защиту информации ограниченного доступа при настройке и конфигурировании операционных систем.
- Использовать встроенные криптографические средства (шифрование дисков, EFS, BitLocker) операционных систем для решения профессиональных задач.
- Администрировать сетевые параметры операционных систем и контролировать безопасность сетевых соединений.
- Проводить мониторинг событий безопасности и анализировать журналы аудита операционной системы.
- Анализировать исторические процессы и их влияние на формирование требований к защите информации.
- Определять критерии и осуществлять проверку эффективности реализации политик безопасности в защищенных операционных системах.
- Выполнять работы по восстановлению работоспособности подсистем защиты информации (аутентификации, разграничения доступа) после сбоев.

- Участвовать в разработке архитектуры защиты операционных систем для вновь создаваемых или модернизируемых объектов информатизации.

Владеть:

- Организовывать защиту информации ограниченного доступа при настройке и конфигурировании операционных систем.
- Использовать встроенные криптографические средства (шифрование дисков, EFS, BitLocker) операционных систем для решения профессиональных задач.
- Администрировать сетевые параметры операционных систем и контролировать безопасность сетевых соединений.
- Проводить мониторинг событий безопасности и анализировать журналы аудита операционной системы.
- Анализировать исторические процессы и их влияние на формирование требований к защите информации.
- Определять критерии и осуществлять проверку эффективности реализации политик безопасности в защищенных операционных системах.
- Выполнять работы по восстановлению работоспособности подсистем защиты информации (аутентификации, разграничения доступа) после сбоев.
- Участвовать в разработке архитектуры защиты операционных систем для вновь создаваемых или модернизируемых объектов информатизации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 академических часа(ов).

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

Тип учебных занятий	Количество часов	
	Всего	Семестр №8
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	48	48
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с

педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 100 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Понятие защищенной операционной системы. Рассматриваемые вопросы: - Управление доступом.
2	Угрозы и классификация наиболее распространенных угроз. Рассматриваемые вопросы: - Понятие защищенной ОС. - Подходы к организации защиты. - Этапы построения защиты. - Административные методы защиты. - Субъекты, объекты, методы и права доступа. - Требования к правилам управления доступом. - Мандатное управление доступом.
3	Управление доступом в операционных системах семейства UNIX Рассматриваемые вопросы: - Управление доступом в операционных системах семейства UNIX
4	Субъекты, объекты, методы и права доступа, UID, EUID, GID, EGID. Рассматриваемые вопросы: - Субъекты, объекты, методы и права доступа, UID, EUID, GID, EGID. - Средства динамического изменения полномочий субъектов: SUID/SGID.
5	Управление доступом в операционных системах семейства Windows Рассматриваемые вопросы: - Управление доступом в операционных системах семейства Windows
6	Субъекты, объекты, методы и права доступа, привилегии субъекта. Рассматриваемые вопросы: - Субъекты, объекты, методы и права доступа, привилегии субъекта. - Порядок проверки прав доступа
7	Средства динамического изменения полномочий субъектов. Рассматриваемые вопросы: - Средства динамического изменения полномочий субъектов.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Контроль целостности, контроль учетных записей. - Элементы изолированной программной среды
8	Идентификация, аутентификация и авторизация Рассматриваемые вопросы: - Понятие идентификации, аутентификации и авторизации пользователей. - Средства и методы хранения эталонных копий аутентификационной информации. - Протоколы аутентификационной информации. - Протоколы передачи аутентификационной информации по каналам сети. - Криптографическое обеспечение аутентификации пользователей
9	Аутентификация на основе паролей. Рассматриваемые вопросы: - Средства и методы защиты от компроментации и подбора паролей. - Парольная аутентификаци в UNIX
10	Парольная аутентификация в Windows. Рассматриваемые вопросы: - Средства управления параметрами аутентификации
11	Аутентификация на основе внешних носителей ключа Рассматриваемые вопросы: - Особенности проверки аутентификационной информации для различных типов носителей ключа. - Проблемы рассылки и смены ключей
12	Биометрическая аутентификация Рассматриваемые вопросы: - Общая схема, преимущества, проблемы. - Достоинства и недостатки различных схем биометрической аутентификации
13	Аудит в операционных системах UNIX и WINDOWS Рассматриваемые вопросы: - Необходимость аудита в защищенной системе. - Требования к подсистеме аудита ОС. - Реализация аудита в UNIX и WINDOWS
14	Интеграция защищенных операционных систем в защищенную сеть Рассматриваемые вопросы: - Преимущества доменной архитектуры локальной сети. - Понятие домена. - Сквозная аутентификация. - Проблемы и способы их решения.
15	Централизованное управление политикой безопасности Рассматриваемые вопросы: - Управление политикой безопасности в домене. - Порядок наделения пользователей домена полномочиями на отдельных компьютерах
16	Доменная архитектура WIN-DOWS Рассматриваемые вопросы: - Ее преимущества по сравнению с доменной архитектурой Windows NT. - Идентификация компьютеров в сети. - Средства и методы синхронизации баз данных контроллеров разных доменов. - Аутентификация по Kerberos. - Групповая политика.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Доступ в Unix В результате выполнения работы студент Управление доступом в Unix
2	Доступ ОС Linux В результате работы студент отрабатывает умение по созданию политики безопасности для разграничения доступа ОС Linux
3	Защита современных ОС Windows В результате выполнения работы студент получает навык по настраиванию штатных механизмов защиты в современных ОС Windows
4	Аудит в ОС Windows В результате выполнения лабораторной работы студент получает навык по отрабатыванию задания по безопасности для подсистемы аудита в ОС Windows
5	Удаленная авторизация на серверах по паролю. В результате выполнения работы студент рассматривает удаленную авторизацию на серверах по паролю. Разграничение прав доступа в многопользовательской системе
6	Биометрическая аутентификация В результате выполнения лабораторной работы студент получает навык построения схемы биометрической аутентификации
7	UNIX и WINDOWS В результате выполнения лабораторной работы отрабатывает умение по реализации аудита в UNIX и WINDOWS
8	Внешние сети к внутрисетевым ресурсам В результате выполнения работы студент рассматривает организацию безопасного доступа из внешних сетей к внутрисетевым ресурсам
9	Экранирование приватных вычислительных сетей В результате выполнения лабораторной работы студент изучает экранирование приватных вычислительных сетей.
10	Доменная сеть В результате лабораторной работы студент отрабатывает умение создавать и управлять доменной сетью.
11	Домены в Windows В результате выполнения работы студент получает навык управления доменами в Windows

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к лабораторным работам.
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1. Организация и обобщенный алгоритм защиты информации в ОС Windows 2. Организация и обобщенный алгоритм защиты информации в ОС UNIX 3. Организация и обобщенный алгоритм защиты информации в ОС Linux 4. Обеспечение безопасного доступа к информационным ресурсам в среде Windows 5. Обеспечение безопасного доступа к информационным ресурсам в среде Linux 6. Сравнительный анализ обеспечения ИБ в ОС Window и ОС UNIX 7. Современные средства защиты от вредоносного программного обеспечения операционных систем 8. Защита от сбоев и НСД в современных ОС 9. Методы оценки защищенности ОС 10. Встроенные средства защиты ОС и способы защиты ОС от вирусных атак

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Введение в защиту компьютерной информации Клементьев, К. Е. Учебное пособие Самара : Самарский университет, — 183 с. - ISBN 978-5-7883-1526-3 , 2020	https://reader.lanbook.com/book/189043#2
2	Основы безопасности прикладных информационных технологий и систем «Криулин А. А., Нефедов В. С., Смирнов С. И. Учебное пособие М.: РТУ МИРЭА, — 136 с. , 2020	https://reader.lanbook.com/book/167606#2

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Microsoft Internet Explorer (или другой браузер).
Операционная система Microsoft Windows.
Microsoft Office.
Пакет прикладных программ GNS3,
Пакет прикладных программ VirtualBox.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Курсовая работа в 8 семестре.
Экзамен в 8 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

Д.В. Павлинов

Согласовано:

Заведующий кафедрой ИУиИБ	Л.А. Баранов
Заведующий кафедрой УиЗИ	Л.А. Баранов
Председатель учебно-методической комиссии	Н.А. Андриянова