МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором 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

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2023

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 при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-10 - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

ОПК-15 - Способен администрировать компьютерные сети и контролировать корректность их функционирования;

ОПК-16 - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;

ОПК-17 - Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма;

ПК-6 - Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-11 - Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации;

ПК-27 - Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем.

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

Знать:

- методики и инструментарий, определяет критерии и осуществляет проверку эффективности систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.
- основные принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении.
- программно-аппаратных средств защиты информации в операционных системах, системах управления базами данных, компьютерных сетях

Уметь:

- Строить, анализировать и реализовывать алгоритмы, в том числе криптографические, в современных программных комплексах.

- Строить, анализировать и реализовывать протоколы, в том числе криптографические, в современных программных комплексах.

- Выполнять задачи по администрированию подсистем и средств защиты информации в сетях.

- проводить дифференциацию и декомпозицию задач мониторинга эффективности различных программно-аппаратных средств защиты информации в операционных системах, системах управления базами данных, компьютерных сетях.

- анализировать полученные результаты мониторинга эффективности программно-аппаратных средств защиты информации в операционных системах, системах управления базами данных, компьютерных сетях и делать соответствующие выводы

Владеть:

- навыками сравнительного анализа эффективности программно-аппаратных средств защиты информации в операционных системах.

- методами и средствами оценки эффективности операционных систем и систем управления базами данных.

- навыками создания систем обеспечения информационной безопасности.

- методами и средствами мониторинга эффективности программно-аппаратных средств защиты информации в операционных системах, системах управления базами данных, компьютерных сетях.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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	Сем. №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 64 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

№ п/п	Тематика лекционных занятий / краткое содержание
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. - 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.

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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.

№ п/п	Вид самостоятельной работы
2	Подготовка к лабораторным работам.
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.
6	Выполнение курсовой работы.
7	Подготовка к промежуточной аттестации.
8	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	Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах В.Г.Проскурин, С.В.Крутов, И.В.Мацкевич Радио и связь , 2000	НТБ (фб.); НТБ (чз.2)
2	Безопасность операционных систем В.П. Соловьев, Н.В. Павленко, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации" Однотомное издание МИИТ , 2007	НТБ (ЭЭ); НТБ (фб.); НТБ (чз.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 УиЗИ	Л.А. Баранов
Председатель учебно-методической комиссии	С.В. Володин