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 - программа 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: 01.06.2022

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:

Владеть:

Строит, анализирует и реализует алгоритмы, в том числе криптографические, в современных программных комплексах

Владеть:

Строит, анализирует и реализует протоколы, в том числе криптографические, в современных программных комплексах.

Владеть:

Строит, анализирует и учитывает новые методы защиты в системах управления базами данных, сетей и систем передачи информации.

Уметь:

Выполняет задачи по администрированию подсистем и средств защиты информации в КС.

Уметь:

Выполняет задачи по администрированию подсистем и средств защиты информации в сетях.

Владеть:

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

Уметь:

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

Уметь:

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

Владеть:

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

Владеть:

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

Уметь:

Умеет применять на практике методы и средства оценки эффективности операционных систем и систем управления базами данных.

Уметь:

Умеет проводить дифференциацию и декомпозицию задач оценки эффективности реализации действующих политик безопасности операционных систем и систем управления базами данных.

Уметь:

Умеет анализировать результаты оценки эффективности реализации действующих политик безопасности операционных систем и систем управления базами данных; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов.

Владеть:

Владеет методами и средствами контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях.

Уметь:

Умеет применять на практике методы и средства контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях.

Уметь:

Умеет проводить дифференциацию и декомпозицию задач контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях.

Уметь:

Умеет анализировать результаты контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов.

Знать:

Подбирает 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.

Уметь:

Обосновывает критерии и рассчитывает показатели эффективности защиты обрабатываемой информации.

Уметь:

Составляет методики тестирования, подбирает инструментарии? и осуществляет проверку эффективности функционирования программных, программно-аппаратных и технических средств, подсистем защиты информации.

Уметь:

Выполняет работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации.

Знать:

Знать основные принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении.

Уметь:

Уметь создавать системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации.

Владеть:

Владеть навыками создания систем обеспечения информационной безопасности.

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	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 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. Управление доступом.
2	Угрозы и классификация наиболее распространенных угроз. 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
4	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
6	Субъекты, объекты, методы и права доступа, привилегии субъекта. Порядок проверки прав доступа
7	Средства динамического изменения полномочий субъектов. мандатный контроль целостности, контроль учетных записей. Элементы изолированной программной среды
8	Идентификация, аутентификация и авторизация
9	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
10	Аутентификация на основе паролей.
11	Средства и методы защиты от компроментации и подбора паролей. Парольная аутентификаци в UNIX
12	Парольная аутентификация в Windows. Средства управления параметрами аутентификации
13	Аутентификация на основе внешних носителей ключа
14	Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы рассылки и смены ключей
15	Биометрическая аутентификация
16	Общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации
17	Аудит в операционных системах UNIX и WINDOWS

№ п/п	Тематика лекционных занятий / краткое содержание
18	Необходимость аудита в защищенной системе. Требования к подсистеме аудита ОС.
19	Реализация аудита в UNIX и WINDOWS
20	Интеграция защищенных операционных систем в защищенную сеть
21	Преимущества доменной архитектуры локальной сети. Понятие домена. Сквозная аутентификация. Проблемы и способы их решения.
22	Централизованное управление политикой безопасности
23	Управление политикой безопасности в домене.
24	Порядок наделения пользователей домена полномочиями на отдельных компьютерах
25	Доменная архитектура WIN-DOWS
26	Ее преимущества по сравнению с доменной архитектурой Windows NT. Идентификация компьютеров в сети.
27	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	ЛР1 Управление доступом в Unix
2	ЛР2 Создание политик безопасности для разграничения доступа ОС Linux
3	ЛР3 Настройка штатных механизмов защиты в современных ОС Windows
4	ЛР4 Отработка задания по безопасности для подсистемы аудита в ОС Windows
5	ЛР5 Удаленная авторизация на серверах по паролю. Разграничение прав доступа в многопользовательской системе
6	ЛР6 ПК1-текущий контроль РИТМ-МИИТ
7	ЛР7 Схемы биометрической аутентификации
8	ЛР8 Реализация аудита в UNIX и WINDOWS
9	ЛР9 Организация безопасного доступа из внешних сетей к внутрисетевым ресурсам
10	ЛР10 Экранирование приватных вычислительных сетей.
11	ЛР11 Создание и управление доменной сетью.

№ п/п	Наименование лабораторных работ / краткое содержание
12	ЛР12 Управление доменами в Windows
13	ЛР13 ПК2-текущий контроль РИТМ-МИИТ

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: [1, стр.4-10, 14-19] 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
2	СР2 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.62) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела
3	СР3 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.26) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
4	СР4 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.26) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
5	СР5 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.72-99) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
6	СР6 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.72-99) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
7	СР7 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (2, стр.184) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
8	СР8 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (2, стр.143-161) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
9	СР9 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: [2, стр. 31] 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
10	СР10 1. Проработка лекционного материала по данному разделу.2. Проработка учебной литературы из приведенных источников: (1, стр 110-114, 2, стр.213-217) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.

№ п/п	Вид самостоятельной работы
11	СР11 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр 110-114, 2, стр.213-217) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
12	СР12 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (2 стр. 163-180) (1, стр.149) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
13	СР13 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.149) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела
14	СР14 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.149) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
15	СР15 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.134-149) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
16	СР16 1. Проработка лекционного материала по данному разделу. 2. Проработка учебной литературы из приведенных источников: (1, стр.134-149) 3. Изучение электронных документов, библиотек и порталов, связанных с тематикой данного раздела.
17	Выполнение курсовой работы.
18	Подготовка к промежуточной аттестации.
19	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).

1. http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ. 2. http://elibrary.ru/ - научно-электронная библиотека. 3. http://lissyara.su 4. http://linux.org 5. http://freebsd.org 6. http://sysadmins.ru 7. http://opennet.ru 8. Поисковые системы: Yandex, Google, Mail.

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

Для проведения лекционных занятийнеобходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.Для проведения практических занятийнеобходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами: Microsoft Office не ниже Microsoft Office 2007 (2013), пакет прикладных программ GNS3, пакет прикладных программ VirtualBox.

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

Для проведения аудиторных занятий и самостоятельной работы требуется:1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET. 2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской. 3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANETДля проведения

лабораторных занятий:компьютерный класс; компьютеры с минимальными требованиями – Intel i3, ОЗУ 8 ГБ, HDD 500 ГБ, USB 3.0.

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:

доцент кафедры «Управление и защита информации» Д.В. Павлинов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин