МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

25 мая 2018 г.

Кафедра «Управление и защита информации»

Автор Павлинов Дмитрий Васильевич

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Защита в операционных системах»

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2018

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 21 мая 2018 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 16 15 мая 2018 г. Заведующий кафедрой  Л.А. Баранов

Москва

1. Цели освоения учебной дисциплины

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. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Защита в операционных системах" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-10	способностью оценивать эффективность 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-18	способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
ПСК-8.4	способностью участвовать в создании системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Защита в операционных системах» осуществляется в форме лекций и лабораторных работ.Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью являются традиционными классически-лекционными (объяснительно-иллюстративные).Лабораторные работы организованы с использованием технологий развивающего обучения. В ходе выполнения курсовой работы реализуются проектные и исследовательские методы обучения. Это позволяет развивать индивидуальные творческие способности обучающихся, более осознанно подходить к профессиональному и социальному самоопределению, самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося.Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относиться отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы. .

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1
Понятие защищенной операционной системы. Управление доступом.

Тема: 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.

РАЗДЕЛ 2
Управление доступом в операционных системах семейства UNIX

Тема: Субъекты, объекты, методы и права доступа, UID, EUID, GID, EGID.
Средства динамического изменения полномочий субъектов: SUID/SGID.

РАЗДЕЛ 3
Управление доступом в операционных системах семейства Windows

Тема: Субъекты, объекты, методы и права доступа, привилегии субъекта. Порядок проверки прав доступа

Тема: Средства динамического изменения полномочий субъектов. мандатный контроль целостности, контроль учетных записей. Элементы изолированной программной среды

РАЗДЕЛ 4
Идентификация, аутентификация и авторизация

Тема: 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

РАЗДЕЛ 5
Аутентификация на основе паролей.

Тема: Средства и методы защиты от компроментации и подбора паролей. Парольная аутентификаци в UNIX

Тема: Парольная аутентификация в Windows. Средства управления параметрами аутентификации

РАЗДЕЛ 6
Аутентификация на основе внешних носителей ключа

Тема: Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы рассылки и смены ключей

РАЗДЕЛ 7
Биометрическая аутентификация

Тема: Общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации

РАЗДЕЛ 8
Аудит в операционных системах UNIX и WINDOWS

Тема: Необходимость аудита в защищенной системе. Требования к подсистеме аудита ОС.

Тема: Реализация аудита в UNIX и WINDOWS

РАЗДЕЛ 9
Интеграция защищенных операционных систем в защищенную сеть

Тема: Преимущества доменной архитектуры локальной сети. Понятие домена. Сквозная аутентификация. Проблемы и способы их решения.

РАЗДЕЛ 10
Централизованное управление политикой безопасности

Тема: Управление политикой безопасности в домене.

Тема: Порядок наделения пользователей домена полномочиями на отдельных компьютерах

РАЗДЕЛ 11

Доменная архитектура WIN-DOWS

Тема: Ее преимущества по сравнению с доменной архитектурой Windows NT. Идентификация компьютеров в сети.

Тема: Средства и методы синхронизации баз данных контроллеров разных доменов. Аутентификация по Kerberos. Групповая политика.

Экзамен