

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»**

Кафедра            «Управление и защита информации»

**АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ**

**«Защита программ и данных»**

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

## 1. Цели освоения учебной дисциплины

Целью дисциплины «Защита программ и данных» является теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий анализа программных реализаций, защиты программ и программных систем от анализа и вредоносных программных воздействий. Основной целью изучения учебной дисциплины «Защита программ и данных» является формирование у обучающегося компетенций для научно-исследовательского и эксплуатационного видов деятельности.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видом деятельности):  
сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;  
участие в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах;  
изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте;  
разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов;  
установка, наладка, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем;  
установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения;  
проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

## 2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Защита программ и данных" 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-1	способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности
ПК-20	способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций

#### **4. Общая трудоемкость дисциплины составляет**

5 зачетных единиц (180 ак. ч.).

#### **5. Образовательные технологии**

Преподавание дисциплины «Защита программ и данных» осуществляется в форме лекций, лабораторных работ и практических занятий. Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 30 % являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 70 % с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция (36 часов). Практические занятия и лабораторные работы организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговые) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а так же использованием компьютерной тестирующей системы. 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 относятся 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. Весь курс разбит на 6 разделов, представляющих собой логически завершённый объём учебной информации. 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, решение тестов с использованием компьютеров или на бумажных носителях..

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

##### **РАЗДЕЛ 1**

##### **Анализ программных реализаций**

1. Задача анализа программных реализаций. Метод экспериментов, статический метод, динамический метод. Принципы функционирования отладчиков. Факторы, ограничивающие возможности отладчиков.
2. Методы поиска функций защиты в машинном коде: метод маяков, метод Step-Trace.
3. Анализ потоков данных. Особенности анализа оверлейного кода, параллельного кода.
4. Особенности анализа машинного кода в среде, управляемой сообщениями.

## РАЗДЕЛ 2

### Защита программ от анализа

1. Защита от дизассемблирования. Защита от отладки.
2. Методы встраивания защиты в программное обеспечение.

## РАЗДЕЛ 2

### Защита программ от анализа

#### Устный опрос

## РАЗДЕЛ 3

### Программные закладки

1. Понятие программной закладки. Классификация программных закладок.
2. Модель «наблюдатель»: модульная структура закладки, организация информационного взаимодействия между клиентской и серверной частями.
3. Модель «перехват»: перехватчики паролей первого, второго и третьего рода, защита от перехватчиков паролей первого рода в Windows, средства и методы перехвата сетевого трафика, перехват обращений пользователя к документам, электронной почте и веб-страницам.
4. Модель «искажение»: применение программных закладок для несанкционированного повышения полномочий пользователя.

## РАЗДЕЛ 4

### Внедрение программных закладок

1. Предпосылки к внедрению программных закладок: уязвимости программного обеспечения, уязвимости политики безопасности, человеческий фактор.
2. Методы внедрения программных закладок: маскировка под «безобидное» программное обеспечение, подмена, прямое и косвенное ассоциирование.

## РАЗДЕЛ 5

### Противодействие программным закладкам

1. Методы выявления программных закладок: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки.
2. Принципы построения политики безопасности, обеспечивающей высокую защищенность от программных закладок.

## РАЗДЕЛ 5

### Противодействие программным закладкам

#### Устный опрос

## РАЗДЕЛ 6

### Компьютерные вирусы как особый класс программных закладок

1. Бинарные вирусы Windows и Linux: структура, порядок инициализации, алгоритмы поиска и заражения жертвы.
2. Сетевые вирусы: онлайн-вирусы, почтовые вирусы, IM-вирусы. Скриптовые вирусы: макровирусы, shell-вирусы, HTML-вирусы. Комбинированные вирусы.
3. Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению: стелс-технологии, полиморфные преобразования кода.

экзамен