

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

26 мая 2020 г.



Кафедра «Управление и защита информации»

Автор Алексеев Виктор Михайлович, д.т.н., профессор

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Объекты защиты информации»

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>2020</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">С.В. Володин</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 16 21 мая 2020 г. Заведующий кафедрой</p>  <p style="text-align: right;">Л.А. Баранов</p>
---	--

Москва 2020 г.

1. Цели освоения учебной дисциплины

Целью изучения дисциплины «Объекты защиты информации» является обеспечение приобретения специалистами знаний о видах и направлениях защиты информации, сущности и свойств объектов, на которые направлена деятельность, называемая защитой информации.

Основной целью изучения учебной дисциплины «Объекты защиты информации» является формирование у обучающегося компетенций для следующих видов деятельности:

контрольно-аналитическая;
эксплуатационная;
специализация №8.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

контрольно-аналитическая деятельность:

выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты и анализ результатов;

проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности компьютерной системы;

эксплуатационная:

установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения;

специализация №8 "Информационная безопасность объектов информатизации на базе компьютерных систем":

разработка проектных решений и анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации, в том числе разработка модели угроз и формирование требования к обеспечению информационной безопасности.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Объекты защиты информации" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПКР-2	Способен проводить моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации
ПКР-9	Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой
ПКС-2	Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации
ПКС-3	Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также

	процессов их проектирования, создания и модернизации
ПКС-4	Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем
ПКС-5	Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Объекты защиты информации» 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 классическими лекционными (объяснительно-иллюстративными), и на 70 % с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция. 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 (диалоговых) 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 4 раздела, представляющих собой логически завершенный объем 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

Защита информации как деятельность. Виды защиты информации

1. Основные понятия в области технической защиты информации. Концептуальные основы защиты информации. Система документов по технической защите информации. Органы по технической защите информации в РФ. Лицензирование деятельности в области технической защиты информации.
2. Сертификация средств защиты информации. Аттестация объекта информатизации по требованиям безопасности информации. Классификация угроз и объектов защиты.

РАЗДЕЛ 2

Цели, направления и объекты защиты информации. Защита информации от непреднамеренного воздействия

1. Объект информатизации. Классификация объектов защиты. Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе ТСР/IP. Программно-математическое воздействие.
2. Требования и рекомендации по защите информации. Порядок обеспечения защиты информации в АС.

РАЗДЕЛ 2

Цели, направления и объекты защиты информации. Защита информации от непреднамеренного воздействия

Устный опрос

РАЗДЕЛ 3

Каналы утечки информации

1. Классификация технических каналов утечки информации. Информационный сигнал и его характеристики. Технические каналы утечки акустической информации. Побочные электромагнитные излучения и наводки.
2. Побочные электромагнитные излучения и наводки. Методы защиты информации от утечки через ПЭМИН.

РАЗДЕЛ 4

Методы и средства защиты от утечки информации

1. Средства и методы обнаружения технических каналов утечки информации.
2. Мероприятия по выявлению технических каналов утечки информации.
3. Оценка защищенности информации от утечки по ТКУИ.

РАЗДЕЛ 4

Методы и средства защиты от утечки информации

Устный опрос

РАЗДЕЛ 5

Зачет с оценкой