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

«Защита информации в интернет и интранет 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	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 16 21 мая 2020 г. Заведующий кафедрой  Л.А. Баранов

Москва 2020 г.

1. Цели освоения учебной дисциплины

Дисциплина «Защита информации в интернет и интранет системах» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 100501 « Компьютерная безопасность». Дисциплина «Защита информации в интернет и интранет системах» относится к числу обязательных дисциплин специализации №8.
Целью преподавания дисциплины «Защита информации в интернет и интранет системах» является изложение слушателям основных принципов и методов защиты информации, комплексного проектирования и анализа защищенных компьютерных систем КС.
Задачами изучения дисциплины являются:
изучение основ устройства и принципов функционирования,
методологии проектирования и построения защищенных,
критериев и методов оценки защищенности КС,
средств и методов защиты от несанкционированного доступа (НСД) к информации.
Основной целью изучения учебной дисциплины «Защита информации в интернет и интранет системах» является формирование у обучающегося компетенций для организационно-управленческого, эксплуатационного видов деятельности, а также для специализированых профессиональных компетенций специализации №8 "Информационная безопасность объектов информатизации на базе компьютерных систем".
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):
Организационно-управленческая деятельность:
организация работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих государственную тайну и конфиденциальной информации).
Эксплуатационная деятельность:
установка, наладка, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем;
установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии со специализацией):
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;
разработка проектов нормативных правовых актов, руководящих и методических документов предприятия, учреждения, регламентирующих деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Защита информации в интернет и интранет системах" 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-8	Способен подготовить обоснование необходимости защиты информации в автоматизированной системе
ПКР-9	Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой
ПКС-1	Способен разрабатывать модели угроз, формировать требования по защите 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

4. Общая трудоемкость дисциплины составляет

5 зачетных единиц (180 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Защита информации в интернет и интранет системах» 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.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 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. Весь курс разбит на 3 раздела, представляющих собой логически завершенный 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
Выбор мер защиты информации для их реализации в рамках системы защиты информации в сети интернет и интранет
1. Классификация информационноі? системы по требованиям защиты информации
2. Определение угроз безопасности информации
3. Выбор мер защиты информации для их реализации в рамках ее системы защиты информации

РАЗДЕЛ 2
Меры защиты информации в сети интернет и интранет
1. Идентификация и аутентификация субъектов доступа и объектов доступа.
2. Управление доступом субъектов доступа к объектам доступа.
3. Ограничение программноі? среды.
4. Защита машинных носителеі? информации.
5. Регистрация событиі? безопасности.
6. Антивирусная защита.
7. Обнаружение (предотвращение) вторжениі?.
8. Контроль (анализ) защищенности информации.
9. Обеспечение целостность информации.
10. Обеспечение доступности информации.

РАЗДЕЛ 2
Меры защиты информации в сети интернет и интранет
опросы

РАЗДЕЛ 3
Меры защиты информации в сети интернет и интранет
1. Обеспечение доступности информации.
2. Защита среды виртуализации.
3. Защита технических средств.
4. Защита средств и систем связи и передачи данных.

РАЗДЕЛ 3
Меры защиты информации в сети интернет и интранет
опросы, защита курсового проекта

РАЗДЕЛ 4
Зачет с оценкой