МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Вычислительные системы, сети и информационная безопасность»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Гуманитарные аспекты информационной безопасности»

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2020

1. Цели освоения учебной дисциплины

Целью освоения дисциплины "Гуманитарные аспекты информационной безопасности" является формирование системного социально-ориентированного мышления студентов и умений: анализировать гуманитарные аспекты информационной безопасности, связанные с социальной сущностью информационных процессов в цифровом обществе; уметь критически оценивать и понимать процессы информационного воздействия на установки и поведение людей, как в ходе глобально ведущейся информационно-психологической борьбы за мировое влияние, так и в ходе получения информации ограниченного доступа потенциальными нарушителями прииспользовании так называемой «социальной инженерии»; уметь работать с персоналом организации по формированию навыков обеспечения информационной безопасности.
Задачи преподавания дисциплины:
- помочь студентам уяснить особенности гуманитарной составляющей информационной безопасности в её философских, политических, правовых, экономических, социально-психологических и других аспектах, атакуемых в информационно-психологическом противоборстве между государствами, а также потенциальными нарушителями информационной безопасности организации;
- оказать содействие процессам вузовского образовательно-воспитательного воздействия на сознание и чувства студентов для форми-рования у них активной национально-ориентированной гражданской позиции и умения отстаивать эту позицию в практической деятельности;
- сформировать практические навыки анализа и оценки содержания защищаемой информации и потенциальных угроз информационной безопасности личности, общества и государства, связанных с человеческим фактором;
- сформировать практические навыки работы с персоналом организации по обучению приемам обеспечения информационной безопасности, противостоянию потенциальным нарушителям с целью завладения информацией ограниченного доступа.
Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности):
эксплуатационная деятельность:
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта;
- участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;
проектно-технологическая деятельность:
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов;
экспериментально-исследовательская деятельность:
- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;

- проведение вычислительных экспериментов с использованием стандартных программных средств;
организационно-управленческая деятельность:
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Гуманитарные аспекты информационной безопасности" 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:

ОПК-7	Способен организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК-12	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире, в том числе для формирования гражданской позиции и развития патриотизма

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

В качестве образовательных технологий используются: печатные издания (книги основной и дополнительной литературы), интернет-ресурсы (электронные энциклопедии, электронные учебники), интерактивная электронная доска, демонстрация через проектор слайдов, подготовленных в формате PowerPoint и Word пакета Microsoft Office. Преподавание дисциплины осуществляется в форме лекций и практических занятий. Лекции проводятся в традиционной форме. Практические занятия проводятся с использованием интерактивных технологий. Ряд занятия носят характер семинара-диалога и семинара-тренинга. На таких занятиях в процессе диалога студенты обсуждают поставленные вопросы, ищут пути и варианты решения поставленной учебной задачи. Это может быть как выбор одного из предложенных вариантов или нахождение и обоснование собственного варианта решения вопроса. Самостоятельная работа студента проводиться с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отдельных тем по учебным пособиям. К интерактивным технологиям относятся работа студентов с электронными информационными ресурсами с целью подготовки и написания рефератов, докладов, и других письменных работ на заданные темы с демонстрацией презентаций

через видеопроектор, подготовленных в формате PowerPoint.. Фонды оценочных средств освоенных компетенций включают вопросы теоретического характера для оценки знаний и задания практического характера для оценки умений и навыков. Теоретические знания проверяются путем индивидуальных и групповых опросов .

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

РАЗДЕЛ 1
Методологические основы гуманитарных аспектов информационной безопасности.

Тема: Введению в дисциплину «Гуманитарные аспекты информационной безопасности».

Тема: Теоретические аспекты развития информационного общества. Основные теории информации. Информационные революции. Эволюция создания информационного общества, цифровой экономики и цифровизации общественных процессов.

РАЗДЕЛ 2
Исторические аспекты информационной борьбы между государствами
Выполнение практических работ

Тема: Информационно-психологическое воздействие. Понятие, виды, средства, субъекты и мишени.

Тема: Приемы психологического воздействия на личность и общество, способы защиты от манипулирования

Тема: Информационная война и методы её ведения. Средства ведения информационных войн.

Тема: Информационные операции: понятие, виды, структура. Приемы информационного противоборства.

РАЗДЕЛ 3
Человеческий фактор в вопросах обеспечения информационной безопасности

Тема: Социально-психологическая характеристика внутреннегои внешнего нарушителя, использование методов «социальной инженерии» для получения информации ограниченного доступа. Приемы противоборства методам «социальной инженерии». Информационная концепция В. Ставицко-го. Главная цель, закономерности, условия эффективности информационной агрессии

Тема: Вопросы ИБ в управлении персоналом. Подбор персонала на должности, связанные с работой с информацией ограниченного доступа. Приемы обучения сотрудников навыкам обеспечения информационной безопасности в организации.

РАЗДЕЛ 4
Итоговая аттестация