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

«Организационное и правовое обеспечение 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

Цели и задачи изучения дисциплины «ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» соотносятся с общими целями ГОС ВПО по специальности/направлению подготовки. Слушатель получает систематизированные теоретические знания в области законодательных основ обеспечения информационной безопасности и их практического применения на российских предприятиях различных форм собственности.
В курсе изучаются: государственная политика в сфере обеспечения информационной безопасности РФ, основы российского законодательства в области обеспечения информационной и компьютерной безопасности, правовой, организационный и программно-технический уровни обеспечения информационной безопасности на современном предприятии, основные методы обеспечения целостности, доступности и конфиденциальности информации, проблемы обеспечения информационной безопасности в задачах управления и управленческого контроля.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами 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 "Организационное и правовое обеспечение 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-6	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации (учреждении, предприятии)
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
ПКО-9	Способность проводить сбор, изучение научно-технической информации, отечественного и зарубежного опыта по вопросам обеспечения информационной безопасности
ПКР-4	Способность осуществлять организационно-правовое обеспечение и управление информационной безопасностью, оценивать угрозы объекта защиты

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Для освоения дисциплины «Организационное и правовое обеспечение информационной безопасности», получения знаний и формирования профессиональных компетенций используются следующие образовательные технологии:• лекция с элементами дискуссии, постановкой проблем• лекции — электронные презентации;• дискуссия;• работа в малых группах;• презентация;• демонстрация;• комментирование научной статьи;• подготовка обзора научной литературы по теме;• комментирование ответов студентов;• решение задач;• анализ конкретных ситуаций;• круглый стол;• интервьюирование;• составление таблиц и схем;• тестирование и др. Указанные технологии могут быть применены преподавателем для диагностики «входных» знаний студентов; могут применяться во время занятий (на лекциях и практических занятиях) и после — для аттестации, контроля и диагностики компетентностей «на выходе». При достаточных технических возможностях аудиторий, может быть использована демонстрация слайдов и видеофильмов. В целом в учебном процессе интерактивные формы составляют не менее 20% аудиторных занятий. Какие именно аудиторные занятия проводятся с использованием интерактивных методов обучения, определяет преподаватель, проводящий аудиторные занятия со студентам .

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

РАЗДЕЛ 1
Информационная безопасность: сущность и содержание.
Информация как один из наиболее важных ресурсов современности. Понятие «информация». Виды и свойства информации. Понятие информационной безопасности.

Понятие национальной безопасности. Понятия «информационная безопасность», «компьютерная безопасность», «кибербезопасность», «защита информации». Задачи информационной безопасности общества. Правовой, организационный и программно-технический уровни обеспечения информационной безопасности. Целостность, доступность и конфиденциальность информации.

РАЗДЕЛ 2
Государственная политика в сфере обеспечения информационной безопасности. Понятие государственной политики в информационной сфере. Содержательный и технологический аспекты государственной информационной политики. Объекты государственной информационной политики. Доктрина информационной безопасности РФ. Функции государства в обеспечении ИБ. Принципы законности, баланса интересов граждан, общества и государства в информационной сфере. Совершенствование нормативно-правовой базы регулирования информационных отношений. Контроль за соблюдением и исполнением законодательства в информационной сфере. Развитие современных информационных и телекоммуникационных технологий как одна из приоритетных задач государственной политики в сфере информационной безопасности..

РАЗДЕЛ 3
Основные законы, регламентирующие организационно-правовую базу в области информационной безопасности.
ФЗ № 149 «Об информации, информационных технологиях и защите информации». Основные понятия: информация, обладатель информации, информационные технологии, конфиденциальность, предоставление и распространение информации, электронный документ. Права и обязанности обладателя информации. ФЗ №152 «О персональных данных». Основные понятия: персональные данные, обработка персональных данных. Согласие субъекта персональных данных на обработку его персональных данных. Доктрина информационной безопасности РФ. Виды угроз информационной безопасности РФ. Угрозы безопасности информационных и телекоммуникационных средств. Внешние и внутренние источники угроз информационной безопасности РФ. Основные принципы государственной политики обеспечения ИБ. ФЗ №187 «О безопасности критической информационной инфраструктуры». Понятия «критической информационной инфраструктуры», «значимый объект критической информационной инфраструктуры», «компьютерная атака». Принципы обеспечения безопасности критической информационной инфраструктуры. Категорирование объектов критической информационной инфраструктур. Основные задачи системы безопасности значимого объекта критической информационной инфраструктуры. ФЗ №98 «О коммерческой тайне». Основные понятия: «коммерческая тайна», «режим коммерческой тайны», «доступ», «предоставление», «передача» информации. Сведения, которые не могут составлять коммерческую тайну.

РАЗДЕЛ 3
Основные законы, регламентирующие организационно-правовую базу в области информационной безопасности.
защита пр. работы 1

РАЗДЕЛ 4
Основные задачи обеспечения информационной безопасности.
Обеспечение информационной безопасности как комплексная задача. Организационно-технические, правовые и экономические методы обеспечения информационной безопасности. Регламентирование доступа к объектам. Идентификация и аутентификация. Шифрование файлов. Обеспечение безопасности соединения. Обязанности руководства

организации по обеспечению ИБ (ISO 27001). Общие задачи обеспечения информационной безопасности. Режим государственной, коммерческой, личной (семейной) тайны. Разработка стратегии обеспечения информационной безопасности России. Обоснование государственной политики в условиях глобализации информационных процессов, формирования геоинформационных сетей. Разработка научно-практических основ формирования и проведения государственной политики в области обеспечения информационной безопасности.

РАЗДЕЛ 4
Основные задачи обеспечения информационной безопасности.
защита пр. работы 2

РАЗДЕЛ 5
Угрозы информационной безопасности.
Понятие «угроза». Классификации угроз ИБ. Внешние и внутренние угрозы информационной безопасности. Компьютерные сети и информационная безопасность. Понятие и виды атак на компьютерную систему. Классификации атак на компьютерную систему. Вредоносные программы, их виды и направления применения. Понятие и виды антивирусного программного обеспечения. Правовой, организационный и программно-технический способы нейтрализации угроз информационной безопасности. Электронная подпись и ее виды.

РАЗДЕЛ 6
Формирование нормативно-правовой базы обеспечения информационной безопасности.
Разработка нормативно-правовых и организационно-методических документов, регламентирующих деятельность органов государственной власти в области информационной безопасности; взаимоотношения субъектов информационной деятельности в части обеспечения информационной безопасности. Государственная регламентация процессов функционирования и развития рынка средств информации, информационных продуктов и услуг. Разработка концепции информационной безопасности. Регулирование правового статуса субъектов системы информационной безопасности, пользователей информационных и телекоммуникационных систем. Силы обеспечения ИБ: Президент РФ, Федеральное Собрание, Правительство РФ, Совет Безопасности РФ, Федеральные органы исполнительной власти РФ, ФСБ РФ, ФСО РФ, ФСТЭК РФ, Минобороны РФ, МВД РФ, Минкомсвязи РФ, Роскомнадзор РФ,

РАЗДЕЛ 6
Формирование нормативно-правовой базы обеспечения информационной безопасности.
защита пр. работ
3, 4, 5

РАЗДЕЛ 7
Развитие современных методов обеспечения информационной безопасности.
Разработка методов комплексного исследования деятельности персонала информационных систем. Разработка практических рекомендаций по сохранению и укреплению политической стабильности в обществе; обеспечению прав и свобод граждан; укреплению законности и правопорядка методами информационной безопасности. Формирование подходов и способов обеспечения органов государственной власти и управления, граждан и их объединений достоверной, полной и своевременной информацией. Выработка основных направлений деятельности по предотвращению негативных информационных воздействий на индивидуальное, групповое и общественное

сознание. Обоснование направлений противодействия информационному оружию.

РАЗДЕЛ 7
Развитие современных методов обеспечения информационной безопасности.
ПК-2,

РАЗДЕЛ 8
Проблемы повышения эффективности обеспечения информационной безопасности на современном этапе.
Обеспечение согласованности решений органов, ответственных за реализацию государственной политики в сфере обеспечения информационной безопасности в рамках единого информационного пространства. Политика протекционизма, направленная на поддержку деятельности отечественных производителей средств информатизации и защиты информации. Защита внутреннего рынка от проникновения некачественных средств информатизации и информационных продуктов. Необходимость формирования программы информационной безопасности, объединяющую усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности.

РАЗДЕЛ 8
Проблемы повышения эффективности обеспечения информационной безопасности на современном этапе.
защита пр. работ
6, 7
тестирование

РАЗДЕЛ 9
Итоговая аттестация