МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИПСС

Т.В. Шепитько

26 мая 2020 г.

Кафедра «Системы автоматизированного проектирования»

Авторы Смирнов Владимир Юрьевич, к.т.н., доцент
Смирнова Ольга Владимировна, к.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы информационной безопасности

Направление подготовки:	09.03.01 – Информатика и вычислительная техника
Профиль:	Системы автоматизированного проектирования
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 5 25 мая 2020 г. Председатель учебно-методической комиссии М.Ф. Гуськова	Протокол № 10 15 мая 2020 г. Заведующий кафедрой И.В. Нестеров

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины (модуля) «Защита информации» является выработка у обучающегося:
? базовых знаний об основных методах защиты компьютерной информации,
? навыков по способам защиты при работе в глобальных (Интернет) и локальных сетях, при работе с электронной почтой.
? базовых знаний об программах-вирусах и антивирусных пакетах
? основных методах шифрования данных и создания электронной подписи.

В результате изучения дисциплины студенты должны:
? знать способы защиты компьютерной информации при работе в сети,
? знать способы борьбы с программами-вирусами и уметь бороться с ними,
? знать алгоритмы шифрования и проверки электронной подписи.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Основы информационной безопасности " относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

2.2. Наименование последующих дисциплин

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1 Знать общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети, архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети, инструкции по установке администрируемых сетевых устройств, инструкции по эксплуатации администрируемых сетевых устройств, инструкции по установке администрируемого программного обеспечения, инструкции по эксплуатации администрируемого программного обеспечения, протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем, модель ISO для управления сетевым трафиком, модели IEEE, регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе, требования охраны труда при работе с сетевой аппаратурой администрируемой сети. ОПК-3.2 Уметь настраивать параметры современных программно-аппаратных межсетевых экранов, пользоваться нормативно-технической документацией в области инфокоммуникационных технологий, сегментировать элементы администрируемой сети. ОПК-3.3 Владеть навыками параметризации операционных систем дополнительных средств защиты администрируемой сети от несанкционированного доступа, установки специализированных программных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа, установки межсетевых экранов, гибких коммутаторов, средств предотвращения атак виртуальной частной сети.
2	ОПК-4 Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил	ОПК-4.1 Знать законодательство Российской Федерации в области обеспечения безопасности и защиты персональных данных, методики разработки регламента аудита систем безопасности на уровне БД. ОПК-4.2 Уметь разрабатывать комплекс организационно-технических мероприятий по обеспечению безопасности данных на уровне БД, оценивать степень защиты данных от угроз безопасности на уровне БД. ОПК-4.3 Владеть навыками выбора критериев оценки результатов аудита данных на уровне БД, разработки методик аудита системы безопасности данных на уровне БД, аудита системы безопасности и оценка ее эффективности.
3	ПКО-7 Способность администрировать процесс контроля использования сетевых устройств и программного обеспечения	ПКО-7.1 Знать общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; архитектуру аппаратных, программных и

№ п/п	Код и название компетенции	Ожидаемые результаты
		программно-аппаратных средств администрируемой сети; инструкции по установке администрируемых сетевых устройств; инструкции по эксплуатации администрируемых сетевых устройств; инструкции по установке администрируемого программного обеспечения; инструкции по эксплуатации администрируемого программного обеспечения; протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; модель ISO для управления сетевым трафиком; модели IEEE; регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе; требования охраны труда при работе с сетевой аппаратурой администрируемой сети. ПКО-7.2 Уметь работать с контрольно-измерительными аппаратными и программными средствами; использовать современные измерительные приборы и программное обеспечение; пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; анализировать корреляции различных параметров при изменениях производительности. ПКО-7.3 Владеть навыками установки кабельных и сетевых анализаторов для контроля изменения номиналов сетевых устройств и программного обеспечения администрируемой сети в целом и отдельных подсистем инфокоммуникационной системы; контроля изменения номиналов сетевых устройств и программного обеспечения администрируемой сети в целом и отдельных подсистем инфокоммуникационной системы с применением утилит операционных систем; анализа параметров производительности администрируемой сети за установленный период (сутки, неделя, месяц, квартал, год); сравнения параметров производительности администрируемой сети за установленный период (сутки, неделя, месяц, квартал, год); составления отчетов о производительности администрируемой сети.
4	ПКО-8 Способность разрабатывать компоненты системных программных продуктов	ПКО-8.1 Знать архитектуру целевой аппаратной платформы, для которой разрабатывается программное обеспечение; синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования; системы команд процессора целевой аппаратуры; способы адресации памяти целевой аппаратной платформы; технологии разработки компиляторов; конструкции распределенного и параллельного программирования; методы и основные этапы трансляции; принципы организации, состав и схемы работы операционных систем; принципы управления ресурсами; стандарты информационного взаимодействия систем; методики тестирования разрабатываемого программного обеспечения; локальные правовые акты, действующие в организации; английский язык на уровне чтения технической документации в области информационных и компьютерных технологий; государственные стандарты ЕСПД.

№ п/п	Код и название компетенции	Ожидаемые результаты
		ПКО-8.2 Уметь применять языки программирования, определенные в техническом задании на разработку драйвера, для написания программного кода; применять технологию разработки компиляторов; создавать блок-схемы алгоритмов функционирования разрабатываемых программных продуктов; оценивать вычислительную сложность алгоритмов функционирования разрабатываемых программных продуктов; работать со стандартными контроллерами устройств (графическим адаптером, клавиатурой, мышью, сетевым адаптером); работать с документацией, прилагаемой разработчиком устройства; осуществлять отладку программных продуктов для целевой операционной системы. ПКО-8.3 Владеть навыками получения технической документации устройства, для которого разрабатывается драйвер; получения технической документации по языку программирования, системе команд процессора устройства, адресации памяти и регистров процессора устройства; изучения технической документации устройства, для которого разрабатывается драйвер; изучения технической документации по языку программирования, системе команд процессора устройства, адресации памяти и регистров процессора устройства; разработки блок-схемы драйвера устройства, компиляторов, загрузчиков, сборщиков, утилиты; написания исходного кода драйвера устройства, компиляторов, загрузчиков, сборщиков, утилиты; отладки разработанного драйвера устройства, компиляторов, загрузчиков, сборщиков, утилиты; разработки эксплуатационной документации на разработанный драйвер, компиляторов, загрузчиков, сборщиков, утилиты; сопровождения разработанного драйвера устройства, компиляторов, загрузчиков, сборщиков, утилиты; реинжиниринга разработанного драйвера устройства, компиляторов, загрузчиков, сборщиков.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

3 зачетных единиц (108 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 4
Контактная работа	32	32,15
Аудиторные занятия (всего):	32	32
В том числе:		
лекции (Л)	16	16
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	16	16
Самостоятельная работа (всего)	76	76
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗаО	ЗаО

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

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	4	Раздел 1 Понятие информационной безопасности	6	6			48	60	
2	4	Тема 1.1 Понятие информационной безопасности. Законы о защите информации	2	2			16	20	
3	4	Тема 1.2 Технические средства обеспечения информационной безопасности.	2	2			16	20	
4	4	Тема 1.3 Защита персонального компьютера (ПК) от сбоев.	2	2			16	20	ПК1
5	4	Раздел 2 Безопасность в глобальных и локальных сетях	6	6			14	26	
6	4	Тема 2.1 Безопасность в глобальных и локальных сетях.	2	2			10	14	
7	4	Тема 2.2 Аутентификация пользователей.	2	2			2	6	
8	4	Тема 2.3 Атаки изнутри системы. Троянские кони. Логические бомбы. Потайные двери.	2	2			2	6	ПК2
9	4	Раздел 3 Вирусы и антивирусы	4	4			6	14	
10	4	Тема 3.1 Атаки системы снаружи. Вирусы.	2	2			2	6	
11	4	Тема 3.2 Антивирусные программы и анти-антивирусные технологии.	2	2			2	6	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
12	4	Тема 3.3 Предохранение от вирусов. Восстановление после вирусной атаки.					2	2	
13	4	Раздел 4 Вирусы и антивирусы					4	4	
14	4	Тема 4.1 Шифрование информации. Симметричные шифры.					2	2	
15	4	Тема 4.2 Метод Касицкого. Метод Фридмана					2	2	
16	4	Раздел 5 Современная криптография					4	4	
17	4	Тема 5.3 Теоретические основы кодирования с открытым ключом.					2	2	
18	4	Тема 5.4 Алгоритм построения криптосистемы RSA.					2	2	
19	4	Экзамен						0	ЗаО
20		Тема 5.1 Кодирование с секретным ключом.							
21		Тема 5.2 Кодирование с открытым ключом. Система RSA.							
22		Тема 5.5 Электронная подпись. Проверка электронной подписи.							
23		Тема 5.6 Хэш-функции. Стеганография.							
24		Всего:	16	16			76	108	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 16 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	4	РАЗДЕЛ 1 Понятие информационной безопасности	Понятие информационной безопасности. Законы о защите информации	2
2	4	РАЗДЕЛ 1 Понятие информационной безопасности	Технические средства обеспечения информационной безопасности.	2
3	4	РАЗДЕЛ 1 Понятие информационной безопасности	Защита персонального компьютера (ПК) от сбоев.	2
4	4	РАЗДЕЛ 2 Безопасность в глобальных и локальных сетях	Безопасность в глобальных и локальных сетях.	2
5	4	РАЗДЕЛ 2 Безопасность в глобальных и локальных сетях	Аутентификация пользователей.	2
6	4	РАЗДЕЛ 2 Безопасность в глобальных и локальных сетях	Атаки изнутри системы. Троянские кони. Логические бомбы. Потайные двери.	2
7	4	РАЗДЕЛ 3 Вирусы и антивирусы	Атаки системы снаружи. Вирусы.	2
8	4	РАЗДЕЛ 3 Вирусы и антивирусы	Антивирусные программы и анти-антивирусные технологии.	2
			ВСЕГО:	16/0

4.5. Примерная тематика курсовых проектов (работ)

1. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами сетевых фильтров.
2. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами сетевых фильтров.
3. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами сетевых фильтров.
4. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение извне доступа к ресурсам компьютера за исключением двух доверенных узлов. Реализуйте политику средствами сетевых фильтров.
5. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение доступа к Web-ресурсам определенного узла. Реализуйте политику средствами сетевых

фильтров.
6. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только получение доступа к Web-ресурсам двух определенных узлов. Реализуйте политику средствами сетевых фильтров.
7. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами сетевых фильтров.
8. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами протокола IPSec.
9. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами протокола IPSec.
10. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами протокола IPSec.
11. С использованием программы «Брандмауэр Windows» (Windows Firewall) выполнить настройки, запрещающие использование всех портов защищаемого узла за исключением TCP-порта 3389.
12. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами протокола IPSec.
13. Сгенерируйте и получите в виде файла сертификат открытого ключа с использованием образа ОС Windows Server 2003.
14. Настройте Web-сервер для организации защищенного доступа к Web-странице с использованием протокола SSL. Выполнить с использованием образа ОС Windows Server 2003. Файл-сертификат открытого ключа прилагается.
15. Настройте входящее подключение VPN с использованием протокола PPTP. Настроить и установить подключение клиентского узла. Выполнить с использованием образа ОС Windows Server 2003.
16. Осуществите криптографическую защиту сетевого трафика средствами протокола IPSec в ОС Windows XP. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В качестве основной формы проведения практических занятий по учебной дисциплине «Защита информации» рекомендуется индивидуальное выполнение лабораторных работ. Рекомендуется также заслушивать и обсуждать доклады, подготовленные обучающимися в ходе самостоятельной работы.

Во вводной части занятия необходимо проверить наличие студентов и их готовность к лабораторному занятию, объявить тему, цели и учебные вопросы занятия.

Далее следует разобрать пример задания, а затем выдать задания для самостоятельного решения.

В конце занятия рекомендуется объявить тему для самостоятельной работы и выдать задания для самостоятельного решения дома.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	4	РАЗДЕЛ 1 Понятие информационной безопасности	Понятие информационной безопасности. Законы о защите информации	16
2	4	РАЗДЕЛ 1 Понятие информационной безопасности	Технические средства обеспечения информационной безопасности.	16
3	4	РАЗДЕЛ 1 Понятие информационной безопасности	Защита персонального компьютера (ПК) от сбоев.	16
4	4	РАЗДЕЛ 2 Безопасность в глобальных и локальных сетях	Безопасность в глобальных и локальных сетях.	10
5	4	РАЗДЕЛ 2 Безопасность в глобальных и локальных сетях	Аутентификация пользователей.	2
6	4	РАЗДЕЛ 2 Безопасность в глобальных и локальных сетях	Атаки изнутри системы. Троянские кони. Логические бомбы. Потайные двери.	2
7	4	РАЗДЕЛ 3 Вирусы и антивирусы	Атаки системы снаружи. Вирусы.	2
8	4	РАЗДЕЛ 3 Вирусы и антивирусы	Антивирусные программы и анти-антивирусные технологии.	2
9	4	РАЗДЕЛ 3 Вирусы и антивирусы	Предохранение от вирусов. Восстановление после вирусной атаки.	2
10	4	РАЗДЕЛ 4 Вирусы и антивирусы	Шифрование информации. Симметричные шифры.	2
11	4	РАЗДЕЛ 4 Вирусы и антивирусы	Метод Касицкого. Метод Фридмана	2
12	4	РАЗДЕЛ 5 Современная криптография	Теоретические основы кодирования с открытым ключом.	2
13	4	РАЗДЕЛ 5 Современная криптография	Алгоритм построения криптосистемы RSA.	2
			ВСЕГО:	76

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Криптография: скоростные шифры	Молдовян А.А., Молдовян Н.А.	СПб.: БХВ-Петербург, 2002	Все разделы
2	Современные операционные системы	Э. Таненбаум	Питер, 2002 НТБ (фб.); НТБ (чз.1)	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	Программирование алгоритмов защиты информации	Домашев А.В., Грунтович М.М. и др.	М.: Нолидж, 2002	Все разделы
4	Алгоритмы: построение и анализ	Кормен Т., Лейзерсон Ч., Ривест Р.	М.: МЦНМО, 2009	Все разделы
5	Алгоритмы шифрования	В.Ю. Смирнов, О.В. Смирнова; МИИТ. Каф. "САПР транспортных конструкций и сооружений"	МИИТ, 2005 НТБ (ЭЭ); НТБ (уч.1)	Все разделы

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

http://www.academiaxxi.ru/ - интернет-сообщество Academia XXI для обмена идеями и методами, относящимися к образованию, науке и инженерному творчеству.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения занятий необходимо, чтобы на компьютере было установлено следующее программное обеспечение: MS Visual Studio C++.

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения занятий необходима аудитория, оснащенная компьютером и проектором.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания для обучения по освоению дисциплины представлены в методических указаниях и учебном пособии, разработанном на кафедре.