МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор РОАТ

 В.И. Апатцев

21 мая 2019 г.

Кафедра «Железнодорожная автоматика, телемеханика и связь»

Автор Носиловский Евгений Антонович, к.ф.-м.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографическая защита бизнес-информации

Направление подготовки:	09.04.03 – Прикладная информатика
Магистерская программа:	Прикладная информатика в обеспечении безопасности бизнеса
Квалификация выпускника:	Магистр
Форма обучения:	заочная
Год начала подготовки	2019

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 1 10 октября 2019 г. Председатель учебно-методической комиссии  С.Н. Климов	Протокол № 3 03 октября 2019 г. Заведующий кафедрой  А.В. Горелик

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Криптографическая защита бизнес информации» является формирование у обучающихся компетенций в соответствии с федеральными государственными образовательными стандартами по специальности «Прикладная информатика» и приобретение ими:
- знаний о шифровании с помощью симметричных и ассиметричных ключей;
- умений использовать математические методы в криптографии;
- навыков применения методов криптографической защиты бизнес информации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Криптографическая защита бизнес-информации" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Современные системы программирования:

Знания: различные научные подходы к автоматизации информационных процессовосновы информационных процессов и системметодологию и технологию создания ИС предприятий и организаций

Умения: развивать информатизацию предприятий и организацийиспользовать инновационные инструментальные средстваосуществлять анализ проектовпо информатизации прикладных задач

Навыки: навыками исследовать различные научные подходы к автоматизации информационных процессовнавыками адаптации современных ИКТ к задачам прикладных ИСпроектами по информатизации прикладных задач

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Научно-исследовательская работа

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	ПКС-51 Способен обеспечить кибербезопасность в бизнес-процессах при проектировании и эксплуатации информационных систем, управлении проектами в области информационных технологий	ПКС-51.1 Разрабатывает эффективные методы управления информационными системами ПКС-51.2 Использует знания в области информационных технологий для решения поставленных задач ПКС-51.3 Активно применяет инструменты управления информационными системами с учетом современных информационных технологий

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

4.1. Общая трудоемкость дисциплины составляет:

4 зачетные единицы (144 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 2
Контактная работа	16	16,35
Аудиторные занятия (всего):	16	16
В том числе:		
лекции (Л)	8	8
практические (ПЗ) и семинарские (С)	8	8
Самостоятельная работа (всего)	119	119
Экзамен (при наличии)	9	9
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
Текущий контроль успеваемости (количество и вид текущего контроля)	КР (1)	КР (1)
Виды промежуточной аттестации (экзамен, зачет)	ЭК	ЭК

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	2	Раздел 1 Раздел 1. Математика криптографии. Модульная арифметика, сравнения и матрицы. Алгебраические структуры. Простые числа и уравнения сравнения.	3		4		26	33	
2	2	Раздел 2 Раздел 2. Введение в основы современных шифров с симметричным ключом. Современные блочные шифры. Современные шифры потока. Стандарты шифрования DES и AES.	1		4		30	35	КР
3	2	Раздел 3 Раздел 3. Криптография с ассиметричным ключом Криптографические системы RSA. Криптосистемы Рабина и Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых.	3				30	33	
4	2	Раздел 4 Раздел 4. Некоторые вопросы криптографии	1				33	34	КР

№ 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
		Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись.							
5	2	Экзамен						9	КР, ЭК
6	2	Раздел 8 Курсовая работа						0	КР
7		Всего:	8		8		119	144	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 8 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	2	Раздел 1. Математика криптографии.	Практическое занятие	4
2	2	Раздел 2. Введение в основы современных шифров с симметричным ключом.	Практическое занятие	4
			ВСЕГО:	8/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые проекты (работы) по теме: "Разработка приложений с криптографической защитой"

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии, используемые для реализации компетентностного подхода и с целью формирования и развития профессиональных навыков студентов по усмотрению преподавателя в учебном процессе могут быть использованы в различных сочетаниях активные и интерактивные формы проведения занятий, включая: Лекционные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; средства и устройства манипулирования аудиовизуальной информацией; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ).Лабораторные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; виртуальные лабораторные работы. Практические занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ).Самостоятельная работа. Дистанционное обучение - интернет-технология, которая обеспечивает студентов учебно-методическим материалом, размещенным на сайте академии, и предполагает интерактивное взаимодействие между преподавателем и студентами. Контроль самостоятельной работы. Использование тестовых заданий, что предполагает интерактивное взаимодействие между преподавателем и студентами. При изучении дисциплины используются технологии электронного обучения(информационные, интернет ресурсы, вычислительная техника) и, при необходимости, дистанционные образовательные технологии, реализуемые в основном с применениеминформационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающегося и педагогических работников.

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	2	Раздел 1. Математика криптографии.	самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом [осн.: 1, доп.:1].	26
2	2	Раздел 2. Введение в основы современных шифров с симметричным ключом.	самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом [осн.: 1, доп 1].	30
3	2	Раздел 3. Криптография с ассиметричным ключом	самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом; решение заданий из контрольной работы [осн.: 1, доп.:1].	30
4	2	Раздел 4. Некоторые вопросы криптографии	самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом [осн.: 1, доп 1].	33
			ВСЕГО:	119

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 и безопасность сетей.	Б.А. Фороузан	М.: Изд-во Бином, 2010 г, библиотека РОАТ	Используется при изучении разделов, номера страниц 1(54 – 60), 2(120 – 134), 3(219 – 224), 4(261 – 270)
2	Криптографические методы защиты информации: учебник и практикум	Васильева И.Н.	М.: ЮРАЙТ, 2016. ЭБС ЮРАЙТ	Используется при изучении разделов, номера страниц 1-6
3	Электронно-библиотечная система издательства «Лань»		0 http://e.lanbook.com	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
4	Защита информации в компьютерных системах	Ю.В. Романец, П.А. Тимофеев, В.А. Шаньгин	М.: Радио и связь, 2007г. Библиотка РОАТ.	Используется при изучении разделов, номера страниц 1(52 – 69), 2(128 – 147), 3(158 – 231), 4(264 – 309)
5	Электронно-библиотечная система Научно-технической библиотеки МИИТ		0 http://library.miit.ru/	Все разделы

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

Официальный сайт РУТ (МИИТ) (http://miit.ru/)
Электронно-библиотечная система Научно-технической библиотеки МИИТ (http://library.miit.ru/)
Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/)
Электронно-библиотечная система ibooks.ru (http://ibooks.ru)/
Электронно-библиотечная система «УМЦ» (http://www.umczdt.ru/)
Электронно-библиотечная система «Intermedia» (http:// www .intermedia-publishing.ru/)
Электронно-библиотечная система РОАТ (http://biblioteka.rgotups.ru/jirbis2/)

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

Программное обеспечение должно позволять выполнить все предусмотренные учебным планом виды учебной работы по дисциплине «Криптографическая защита бизнес информации»: теоретический курс, задания на контрольную работу, тестовые и экзаменационные вопросы по курсу.
- Программное обеспечение для выполнения практических заданий включает в себя программные продукты общего применения
- Программное обеспечение для проведения лекций, демонстрации презентаций и ведения интерактивных занятий: Microsoft Office 2003 и выше.
- Программное обеспечение, необходимое для оформления отчетов и иной документации: Microsoft Office 2003 и выше.
- Программное обеспечение для выполнения текущего контроля успеваемости: Браузер Internet Explorer 6.0 и выше.

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

Для проведения аудиторных занятий и самостоятельной работы требуется:
1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET.
2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.
3. Компьютерный класс с кондиционером. Рабочие места студентов в компьютер¬ном классе, подключённые к сетям INTERNET и INTRANET
4. Для проведения практических занятий: компьютерный класс; кондицио¬нер; компьютеры с минимальными требованиями - Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

Технические требования к оборудованию для осуществления учебного процесса сиспользованием дистанционных образовательных технологий:
колонки, наушники или встроенный динамик (для участия в аудиоконференции);микрофон или гарнитура (для участия в аудиоконференции); веб-камеры (для участия в
видеоконференции);
для ведущего: компьютер с процессором Intel Core 2 Duo от 2 ГГц (или аналог) ивыше, от 2 Гб свободной оперативной памяти.

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

В процессе освоения дисциплины студенты должны посетить лекции, выполнить лабораторные работы и курсовую работу в соответствии с учебным планом, получить оценку по курсовой работе и сдать экзамен.
1. Указания (требования) для выполнения курсовой работы.
1.1. Методические рекомендации по выполнению курсовой (проект) размещены студент получает у преподавателя в начале установочной сессии.
1.2. Курсовая работа должна быть выполнена в установленные сроки
и оформлена в соответствии с утверждёнными требованиями, которые приведены в методических рекомендациях.
1.3. Выполнение курсовой работы (проект) рекомендуется не откладывать на длительный срок: решить большую часть задач имеет смысл практически после аудиторных занятий, пока хорошо помнишь то, что было рассказано на лекции.

При таком подходе возникает возможность получить оперативную очную консультацию у лектора в течение периода прохождения сессии.
1.4. Если возникают трудности по выполнению курсовой работы (проект), можно получить консультацию по решению у преподавателя между сессиями.
1.5. В установленные сроки производится защита курсовых работ (проект) по изучаемому теоретическому материалу.
2. Указания для освоения теоретического материала и сдачи экзамена
2.1. Обязательное посещение лекционных занятий по дисциплине с конспектированием излагаемого преподавателем материала в соответствии с расписанием занятий.
2.2. Получение в библиотеке рекомендованной учебной литературы и электронное копирование конспекта лекций, презентаций и методических рекомендаций по выполнению курсовой работы (проект).
2.3. Копирование (электронное) перечня вопросов к экзамену по дисциплине, а также списка рекомендованной литературы из рабочей программы дисциплины.
2.4. Рекомендуется следовать советам лектора, связанным с освоением предлагаемого материала, провести самостоятельный Интернет - поиск информации (видеофайлов, файлов-презентаций, файлов с учебными пособиями) по ключевым словам курса и ознакомиться с найденной информацией при подготовке к экзамену по дисциплине.
2.5. После проработки теоретического материала согласно рабочей программе курса необходимо подготовить ответы на вопросы для защиты курсовой работы и вопросы к экзамену.
2.6. Студент допускается до сдачи экзамена, если выполнена и защищена курсовая работа.
Контактная работа осуществляется в соответствии с расписанием занятий.
Контактная работа может быть организована с использованием дистанционныхобразовательных технологий.
Если дисциплина осваивается с использованием элементов дистанционныхобразовательных технологий:
Лекционные занятия проводятся в формате вебинара врежиме реального времени.
Практические занятия проводятся в формате вебинара илионлайн формате в режиме реального времени. Практические занятия проводятся в интерактивном (диалоговом) режиме
Если лабораторные работы могут быть выполнены с использованиемдистанционных образовательных технологий. В этом случае студенту с помощью сети Internet предоставляется доступ к дистанционному лабораторному стенду, размещенномуна сервере академии
Для выполнения лабораторных работ используется свободно распространяемое программного обеспечение