МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Первый проректор

В.С. Тимонин

14 января 2022 г.

Кафедра «Цифровые технологии управления транспортными процессами»

Автор Давыдовский Михаил Альбинович, к.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации. Методы и алгоритмы

Направление подготовки:	09.03.01 – Информатика и вычислительная техника
Профиль:	Программное обеспечение средств вычислительной техники и автоматизированных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2018

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 4 30 апреля 2020 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 1 27 апреля 2020 г. Доцент В.Е. Нутович

Москва 2022 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Защита информации. Методы и алгоритмы» являются ознакомление студентов с основными видами угроз информационной безопасности, изучение основных приемов защиты информации и интеллектуальной собственности и приобретение практических навыков использования и создания алгоритмов шифрования.
Основной целью изучения учебной дисциплины «Защита информации. Методы и алгоритмы» является формирование компетенций в области проектирования и использования баз данных, необходимых при создании информационных систем, для следующих видов деятельности:
- научно-исследовательская;
- проектно-конструкторская.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):
научно-исследовательская деятельность:
изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
проведение измерений и наблюдений, составление описания проводимых исследований, подготовка данных для составления обзоров, отчетов и научных публикаций;
составление отчета по выполненному заданию, участие во внедрении результатов исследований и разработок;
проектно-конструкторская деятельность:
сбор и анализ исходных данных для проектирования;
разработка и оформление проектной и рабочей технической документации;

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Защита информации. Методы и алгоритмы" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

2.1. Наименования предшествующих дисциплин

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

2.1.1. Базы данных. Модели и языки:

Знания: понятия, определения, термины баз данных

Умения: разрабатывать модели предметной области, создавать базы данных в одной или нескольких СУБД

Навыки: средствами описания и доступа к базе данных

2.1.2. Программирование :

Знания: основные конструкции языка Java, позволяющие создать удобные меню для работы с программой.

Умения: определить форму запроса и получения результата.

Навыки: навыком предвидения нестандартных ситуаций в ходе выполнения задачи.

2.1.3. Сети и телекоммуникации. Архитектура и протоколы:

Знания:

Умения:

Навыки:

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-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знать и понимать: основные типы угроз информационной безопасности, методы организации защиты информации, современные программные и аппаратные средства защиты информации Уметь: защищать личную информацию и интеллектуальную собственность, использовать функционал программных средств, операционных систем и оболочек для защиты информации, разрабатывать собственные средства защиты информации Владеть: основными способами получения, хранения и обработки информации, современными инструментами защиты информации

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 8
Контактная работа	54	54,15
Аудиторные занятия (всего):	54	54
В том числе:		
лекции (Л)	18	18
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	36	36
Самостоятельная работа (всего)	54	54
Экзамен (при наличии)	36	36
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1	ПК1
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	8	Раздел 1 Введение	3					3	
2	8	Тема 1.1 Основные термины и определения	1					1	
3	8	Тема 1.2 Угрозы информационной безопасности	2					2	
4	8	Раздел 2 Криптографическая защита информации	6	26/6			31	63/6	
5	8	Тема 2.3 Основы шифрования	2	6/6			5	13/6	
6	8	Тема 2.4 Симметричные алгоритмы шифрования	2	10			12	24	
7	8	Тема 2.5 Ассиметричные алгоритмы шифрования	2	10			14	26	ПК1, Отчеты по ЛР 1, 2
8	8	Раздел 3 Защита баз данных	4/3				12	16/3	
9	8	Тема 3.6 Методы и средства защиты	2/3				4	6/3	
10	8	Тема 3.7 Уязвимость SQL запросов	1				4	5	
11	8	Тема 3.8 Способы защиты запросов	1				4	5	
12	8	Раздел 4 Защита сетевого уровня	5/3	10			11	26/3	
13	8	Тема 4.9 Сетевые атаки	2/3					2/3	
14	8	Тема 4.10 Межсетевые экраны	1				4	5	, Отчет по ЛР 3
15	8	Тема 4.11 Виртуальные защищенные сети	1				3	4	
16	8	Тема 4.12 Протоколы, используемые в виртуальных сетях	1	10			4	15	
17	8	Экзамен						36	ЭК

№ 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
18		Всего:	18/6	36/6			54	144/12	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 36 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	8	РАЗДЕЛ 2 Криптографическая защита информации Тема: Основы шифрования	Разработка генератора простых чисел и алгоритма проверки чисел на простоту	6 / 6
2	8	РАЗДЕЛ 2 Криптографическая защита информации Тема: Симметричные алгоритмы шифрования	Реализация симметричного блочного алгоритма шифрования информации на примере DES,BlowFish,RC2,RC5	10
3	8	РАЗДЕЛ 2 Криптографическая защита информации Тема: Ассиметричные алгоритмы шифрования	Реализация асимметричного алгоритма шифрования информации на примере RSA	10
4	8	РАЗДЕЛ 4 Защита сетевого уровня	Протоколы, используемые в виртуальных сетях	10
			ВСЕГО:	36/6

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Защита информации. Методы и алгоритмы» осуществляется в форме лекций, лабораторных работ, самостоятельной работы студентов.
Лекции проводятся в форме мультимедиа-лекций, на которых демонстрируются презентации. Студенты имеют возможность ознакомиться с материалами презентации до начала лекции.
Лабораторные занятия проводятся в компьютерном классе с установленным программным обеспечением, необходимым для разработки индивидуальных заданий. На лабораторных работах выполняются индивидуальные задания, демонстрируются готовые части выполненных заданий и отчета по заданию. Часть лабораторных работ (20 часов) проводится в форме традиционных занятий (проверка отчетов по выполненным индивидуальным заданиям). Остальная часть лабораторных работ (6 часов) проводится с использованием интерактивных технологий. Разработка программ по индивидуальным заданиям ведется с применением интерактивной среды разработки программ на языке C++ или Java.
Самостоятельная работа студента организованна с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы (20 часов) относятся отработка лекционного материала и отработка отдельных тем по учебной литературе. К интерактивным (диалоговым) технологиям (31 часов) относится отработка отдельных тем с использованием электронных информационных ресурсов и разработка индивидуальных проектов в интерактивном режиме в среде автоматизированного проектирования программного обеспечения.
Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 4 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 (индивидуальные задания для выполнения лабораторных работ) для оценки умений и навыков. Теоретические знания проверяются на экзамене и в ходе проверки отчетов по выполненным индивидуальным заданиям.

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	8	РАЗДЕЛ 2 Криптографическая защита информации Тема 3: Основы шифрования	1.Подготовка к лабораторной работе №1 2.Изучение учебной литературы: [1, стр. 122-123]	5
2	8	РАЗДЕЛ 2 Криптографическая защита информации Тема 4: Симметричные алгоритмы шифрования	1. Подготовка к лабораторной работе №2 2. Изучение учебной литературы: [1, стр. 124-137] [4, стр. 117-136]	12
3	8	РАЗДЕЛ 2 Криптографическая защита информации Тема 5: Ассиметричные алгоритмы шифрования	1. Подготовка к лабораторной работе №3 2. Изучение учебной литературы: [1, стр. 183-192, 257-270, 316-322] [4, стр. 137-147], [6, стр. 12-70]	14
4	8	РАЗДЕЛ 3 Защита баз данных Тема 6: Методы и средства защиты	1. Изучение методов защиты базы данных Oracle 2. Изучение учебной литературы: [2, стр. 271-293]	4
5	8	РАЗДЕЛ 3 Защита баз данных Тема 7: Уязвимость SQL запросов	1. Изучение примеров внедрения SQL-кода 2. Изучение учебной литературы: [3, стр. 384-416], [4, стр. 262-292]	4
6	8	РАЗДЕЛ 3 Защита баз данных Тема 8: Способы защиты запросов	1. Изучение способов защиты SQL запросов 2. Изучение учебной литературы: [2, стр. 120-147]	4
7	8	РАЗДЕЛ 4 Защита сетевого уровня	Виртуальные защищенные сети	3
8	8	РАЗДЕЛ 4 Защита сетевого уровня Тема 10: Межсетевые экраны	1. Подготовка к лабораторной работе №3 2. Изучение учебной литературы: [3, стр. 384-416], [4, стр. 262-292]	4
9	8	РАЗДЕЛ 4 Защита сетевого уровня Тема 12: Протоколы, используемые в виртуальных сетях	1. Изучение протоколов IPSEC 2. Изучение учебной литературы: [3, стр. 257-260, 331-370, 417-452], [4, стр. 293-322, 346-379]	4
			ВСЕГО:	54

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	Н. Смарт	М.: Техносфера, 2006 - 525 с.ISBN 5-94836-043-1 НТБ МИИТ 004 С50(фб.-3)	Раздел 2 [124-137, 183-192, 257-270, 316-322]
2	Безопасность Oracle глазами аудитора: нападение и защита	Поляков, А.М.	М. : ДМК Пресс, 2010 -336 с. http://e.lanbook.com/book/1121	Раздел 3 [120-147, 271-293]
3	Защита информации в компьютерных системах и сетях	Шаньгин В.Ф.	М. : ДМК Пресс, 2012 - 592 с. ISBN 978-5-94074-637-9 http://e.lanbook.com/book/3032	Раздел 4 [257-260, 331-370, 384-416, 417-452]

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
4	Защита компьютерной информации	Шаньгин В.Ф.	М. : ДМК Пресс, 2010 -544 с. ISBN 978-5-94074-518-1 http://e.lanbook.com/book/1122	Раздел 2 [117-147], Раздел 4 [262-322, 346-379]
5	Методика противодействия атакам типа SQLINJECTION	Богданов Н.В., Кротова Е.Л., Шабуров А.С.	Наука и бизнес: пути развития. №6, 2015 http://elibrary.ru/item.asp?id=24066266	Раздел 3 [39-41]
6	Построение защищенных корпоративных сетей.	Ачилов Р.Н.	М. : ДМК Пресс -250 с., 2013 http://e.lanbook.com/book/66472	Раздел 2 [12-70]

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

- http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ
- https://ru.wikipedia.org - Википедия
- www.citforum.ru – материалы по информационным технологиям

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

Используемые информационные технологии:
- объектно-ориентированное программирование;
- объектно-ориентированное проектирование.

Поисковые системы:

- Google;
- Яндекс.

Для выполнения лабораторных требуется следующее программное обеспечение:
- Операционная система Windows;
- Среда разработки на языке C++ Microsoft Visual Studio;
- Среда разработки на языке Java Eclipse или NetBeens.

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

Для выполнения лабораторных работ группе студентов необходима аудитория с ПК (компьютерный класс).
При изучении дисциплины используется лекционная аудитория, оборудованная мультимедийным проектором и экраном. Для каждой лекции готовится презентация.

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

1. В лекционном курсе рассматриваются основные вопросы по данной дисциплине. Дополнительные вопросы, необходимые студентам при выполнении своих индивидуальных заданий, изучаются студентами самостоятельно и контролируются преподавателем.
2. Задания по всем лабораторным работам выдаются студентам в начале семестра, чтобы студенты имели возможность самостоятельно изучить дополнительные теоретические сведения, необходимые им при выполнении индивидуальных заданий, и спланировать график выполнения заданий с учетом их специфики.
3. Прежде чем приступить к выполнению конкретного задания студент должен изучить:
- материалы лекций по теме задания;
- дополнительные материалы, относящиеся к специфике индивидуального задания;
- программные средства, используемые при выполнении задания.
4. Выполнение индивидуальных заданий и их сдача осуществляется по определенному графику и учитывается при периодической аттестации студентов.
5. Лекции по дисциплине, подготовленные в электронном виде, рекомендуется выдавать студентам в начале семестра с целью лучшего освоения материала и возможности досрочного изучения вопросов, необходимых для выполнения индивидуальных заданий.
6. Индивидуальные задания, требующие разработки сложных программных систем, могут выдаваться на группу студентов, но при этом необходимо контролировать знание каждым студентом всего задания в целом.
7. Для полноценного освоения дисциплины необходимо:
- посещение лекций и практических занятий;
- изучение лекционного материала;
- освоение теоретического материала, вынесенного на самостоятельное изучение, по предложенным источникам (литература, интернет-ресурсы);
- изучение программного обеспечения, необходимого, для выполнения индивидуальных заданий;
- консультации с преподавателем в ходе выполнения индивидуальных заданий и обсуждение промежуточных результатов выполнения индивидуальных заданий;
- своевременное выполнение индивидуальных заданий;
- своевременное предоставление отчетов по индивидуальным заданиям и защита выполненных работ.