Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А.Панфилов
«_25_» _02_____ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки: 09.03.01 – Информатика и вычислительная техника

Профиль/программа подготовки: Высокопроизводительные и распределенные вычисления

Уровень высшего образования: бакалавриат

Форма обучения: очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточной аттестации (экзамен/зачет/зачет с оценкой)
8	4/144	18	18	18	54	Экзамен (36)
Итого	**4/144**	**18**	**18**	**18**	**54**	**Экзамен (36)**

Владимир 2021

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Защита информации» – создание фундаментальной основы знаний, необходимой при проектировании программных продуктов для вычислительных систем и проектировании систем безопасности. знакомство с основными принципами криптографических алгоритмов, основными аспектами защиты информации и законами РФ в области защиты информации.

Задачами являются:

1) классификация аспектов защиты информации;

2) изучение основных криптографических методов;

3) изучение законов РФ в области защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Защита информации» относится к части, формируемой участниками образовательных отношений.

Пререквизиты дисциплины: «Математика», «Программирование», «Введение в специальность», «Сети и телекоммуникации», «Дискретная математика и математическая логика».

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесённые с планируемыми результатами освоения ОПОП

Код формируемых компетенций	Уровень освоения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций (показатели освоения компетенции)
1	2	3
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности	Частичное	**знать**: основные концепции информационной безопасности; возможные источники, риски и формы атак на информацию; потенциальные каналы утечки информации в ИС при вводе, выводе, передаче, обработке, накоплении и хранении информации; алгоритмические методы криптографической защиты информации, а также методы шифрования данных; стандарты информационной безопасности; методы и средства защиты информации в сетях; **уметь**: осваивать методики использования программных средств для решения практических задач, разрабатывать компоненты программных комплексов и баз данных, использовать современные инструментальные средства и технологии программирования; обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности; настраивать и налаживать программно-аппаратные комплексы. **владеть**: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения; способностью находить организационно-управленческие решения в нестандартных ситуациях; основными законами естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования; навыками работы с компьютером как средством управления информацией; способностью работать с информацией в глобальных компьютерных сетях
ПК-2 Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности	Частичное	**знать**: основные принципы построения вычислительных систем и устройств. **уметь:** проектировать систему на базе типовых функциональных узлов. **владеть:** базовыми навыками формирования электрических структурных, функциональных и принципиальных схем, в том числе, с использованием технической и справочной литературы

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоёмкость дисциплины составляет 4 зачётные единицы, 144 часа.

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	СРС		
1	Информационно-вычислительные системы как объекты защиты информации	8	1	2	1	0	4	1/33%	
2	Информация. Категории информации	8	2	2	1		2	1/33%	
3	Методы защиты информации в ИВС	8	3-6	8	16	18	24	16/38%	Рейтинг-контроль №1
4	Современные криптографические методы защиты информации	8	7	2			20	1/50%	Рейтинг-контроль №2
5	Стандарты и спецификации. Оранжевая книга	8	8	2			2		
6	Законы РФ в области защиты информации. Персональные данные	8	9	2			2		Рейтинг-контроль №3
Всего за 8 семестр:				18	18	18	54	19/35%	Экзамен (36)
Наличие в дисциплине КП/КР									Нет
Итого по дисциплине				18	18	18	54	19/35%	Экзамен (36)

Содержание лекционных занятий по дисциплине

Раздел 1. Информационно-вычислительные системы как объекты защиты информации
Раздел 2. Информация. Категории информации
Раздел 3. Методы защиты информации в ИВС
Раздел 4. Современные криптографические методы защиты информации
Раздел 5. Стандарты и спецификации. Оранжевая книга
Раздел 6. Законы РФ в области защиты информации. Персональные данные

Содержание лабораторных занятий по дисциплине

1. Исследование методов полиалфавитной подстановки
2. Шифрование методом перестановки
3. Исследование гаммирования при шифровании
4. Шифрование с помощью аналитических преобразований

Содержание практических занятий по дисциплине

1. Каналы утечки информации. Аспекты защиты данных.
2. Криптоанализ шифров подстановки: общие подходы.
3. Криптоанализ шифров Гронсфельда и Вижинера.
4. Криптоанализ шифров перестановки.
5. Анализ алгоритмических генераторов псевдослучайных чисел.
6. Анализ результатов шифрования методом гаммирования.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «Защита информации» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Интерактивная лекция (темы № 1-3, 5);

Групповая дискуссия (темы №5,6,7,8);

Ролевые игры (темы №1, 3)

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Текущий контроль успеваемости

Вопросы рейтинг-контроля №1

1. Определение термина «информация».
2. В чём заключается физический аспект защиты данных? Приведите примеры.
3. Перечислите критерии классификации алгоритмов шифрования.
4. В чём заключается технический аспект защиты данных? Приведите примеры.
5. Как Вы понимаете словосочетание «период применения контура» в полиалфавитной многоконтурной подстановке?
6. Используя шифр простой замены, зашифруйте свою фамилию. В качестве алфавита для замены используйте исходный алфавит, циклически сдвинутый на (N+10) позиций влево, где N – номер по списку. Отразить весь процесс шифрования (ключ (N+10), таблица замены, исходная фраза, зашифрованное сообщение).

Вопросы рейтинг-контроля №2

1. Используя алгоритм Виженера и свою фамилию в качестве ключа, зашифруйте фразу: «Рейтинг-контроль номер 1». Базовый алфавит состоит из всех (!) букв кириллицы и пробела (всего 34 символа). Отразить весь процесс шифрования (таблица замены, исходная фраза, ключ, зашифрованное сообщение).
2. Требуется зашифровать фразу «автолокализованная квазичастица». Выбран шифр полиалфавитной одноконтурной монофонической подстановки. Сформируйте вариант таблицы монофонической замены, поясните, почему именно такая таблица должна использоваться. Выполните шифрование.
3. Перечислите достоинства физических генераторов случайных чисел.
4. Перечислите недостатки физических генераторов случайных чисел.
5. Перечислите достоинства табличных генераторов случайных чисел.
6. Перечислите недостатки табличных генераторов случайных чисел.

Вопросы рейтинг-контроля №3

1. Перечислите достоинства алгоритмических генераторов случайных чисел.
2. Перечислите недостатки алгоритмических генераторов случайных чисел.
3. Как Вы думаете, почему в криптографии широко используется матричная алгебра?
4. Какими свойствами обладает текст после применения шифра замены?
5. Какими свойствами обладает текст после применения шифра перестановки?
6. Какими свойствами обладает текст после применения гаммирования?

Промежуточная аттестация по итогам освоения дисциплины

Список вопросов к экзамену

1. Категории информационной безопасности.
2. Категории для информационных систем.
3. Аспекты проблемы защиты информации.
4. Каналы утечки информации и возможные последствия атак на информацию.
5. Классификация криптоалгоритмов.
6. Основные принципы симметричных и асимметричных криптоалгоритмов.
7. Основные принципы блочных и потоковых криптоалгоритмов.
8. Генераторы случайных чисел.
9. Скремблеры.
10. Обмен информацией по открытому каналу. Алгоритм Диффи-Хеллмана.
11. Простая перестановка.
12. Перестановка, усложнённая по таблице.
13. Перестановка, усложнённая по маршрутам.
14. Простая замена.
15. Полиалфавитная одноконтурная обыкновенная замена.
16. Полиалфавитная одноконтурная монофоническая замена.
17. Полиалфавитная многоконтурная замена.

18. Шифрование гаммированием.
19. Аналитическое преобразование по правилам алгебры матриц.
20. Аналитическое преобразование: алгоритм RSA.
21. Алгоритм DES.
22. Электронная цифровая подпись.

Самостоятельная работа студентов

Целью самостоятельной работы являются формирование личности студента, развитие его способности к самообучению и повышению своего профессионального уровня.

Самостоятельная работа заключается в изучении содержания тем курса по конспектам, учебникам и дополнительной литературе, подготовке к лабораторным и практическим занятиям, выполнении заданий для самостоятельной работы, оформлении отчетов по лабораторным работам, подготовке к промежуточной аттестации и экзаменам.

Задания для самостоятельной работы студентов

1. Сеть Фейштеля
2. Блочный шифр TEA
3. Алгоритм Хаффмана
4. Алгоритм Лемпеля-Зива
5. Хеширование паролей
6. Алгоритм RSA
7. Технологии цифровых подписей
8. Механизм распространения открытых ключей
9. Обмен ключами по алгоритму Диффи-Хеллмана
10. Транспортное кодирование
11. Создание политики информационной безопасности
12. Методы обеспечения безотказности

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ	
		Количество экземпляров изданий в библиотеке ВлГУ в соответствии с ФГОС ВО	Наличие в электронной библиотеке ВлГУ
1	2	3	4
Основная литература			
1. Защита информации [Электронный ресурс]: учебное пособие / Ю.М. Краковский - Ростов н/Д : Феникс, 2016. - (Высшее образование).	2016		http://www.studentlibrary.ru/book/ISBN9785222269114.html
2. Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014.	2014		http://www.studentlibrary.ru/book/ISBN9785940747680.html
3. Защита от хакеров корпоративных сетей [Электронный ресурс] / Ахмад Д.М. и др. ; Пер. с англ. А.А. Петренко. - Второе издание. - М. : ДМК Пресс, 2016. - (Серия "Информационная безопасность").	2016		http://www.studentlibrary.ru/book/ISBN5984530155.html

Дополнительная литература			
1. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2010.	2010		http://www.studentlibrary.ru/book/ISBN9785940745181.html
2. Защита от хакеров Web-приложений [Электронный ресурс] /Джефф Форристал, Крис Брумс, Дрю Симонис, Брайн Бегнолл, Майкл Дайновиц, Джей Д. Дайсон, Джо Дьюлэй, Майкл Кросс, Эдгар Даниелян, Дэвид Г. Скабру ; Пер. с англ. В. Зорина. - М. : ДМК Пресс, 2008. - (Серия "Информационная безопасность").	2008		http://www.studentlibrary.ru/book/ISBN5940742580.html
3. Технические средства и методы защиты информации [Электронный ресурс] : Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. Под ред. А.П. Зайцева и А. А. Шелупанова. - 7-е изд., испр. - М. : Горячая линия - Телеком, 2012.	2012		http://www.studentlibrary.ru/book/ISBN9785991202336.html
4. Защита в операционных системах [Электронный ресурс] : Учебное пособие для вузов / Проскурин В.Г. - М. : Горячая линия - Телеком, 2014.	2014		http://www.studentlibrary.ru/book/ISBN9785991203791.html
5. Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А.А. - М. : ДМК Пресс, 2012.	2012		http://www.studentlibrary.ru/book/ISBN9785940746478.html

7.2. Периодические издания

Журналы (https://elibrary.ru/):

1. Вестник компьютерных и информационных технологий
2. Вычислительные технологии
3. Известия вузов: электроника
4. Радиотехнические и телекоммуникационные системы

7.3. Интернет-ресурсы

1. Электронная библиотека www.citforum.ru
2. Электронная энциклопедия wikipedia.org

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий практического типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы. Лабораторные работы проводятся в учебно-исследовательской лаборатории «Центра микроэлектронного проектирования и обучения».

Рабочую программу составил ст. преподаватель кафедры ВТиСУ Трофимов М.А.

Рецензент
(представитель работодателя) Генеральный директор ООО «Диаграмма»
Протягов И.В.

Программа рассмотрена и одобрена на заседании кафедры ВТ и СУ
Протокол № 6 от 25.02.2021 года
Заведующий кафедрой ВТ и СУ Ланцов В.Н.
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 09.03.01
Протокол № 2 от 25.02.2021 года
Председатель комиссии Ланцов В.Н.

(ФИО, подпись)