


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)**

Институт информационных технологий и радиоэлектроники

УТВЕРЖДАЮ:
Директор института

Галкин А.А.
« 31 » 08 2021 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

направление подготовки / специальность

09.03.01 Информатика и вычислительная техника

направленность (профиль) подготовки

Системы автоматизированного проектирования микроэлектроники

г. Владимир

2021 Год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Защита информации» являются 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.

Задачи:

- 1) классификация аспектов защиты информации;
- 2) изучение основных криптографических методов;
- 3) изучение законов РФ в области защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

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

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции (код, содержание индикатора)	Результаты обучения по дисциплине	
ПК-3 Способен проводить научно-исследовательские и опытно-конструкторские разработки по отдельным разделам темы	ПК-3.1 Знает инструментарий математического анализа дискретных объектов и систем ПК 3.2 Умеет анализировать и формализовать полученные на практике или при исследованиях результаты и делать на их основе обоснованные выводы ПК 3.3 Владеет навыками применения методов решения теоретических задач в области схемотехники цифровых устройств	Знать основные концепции информационной безопасности; методы и средства защиты информации в программных системах и сетях; стандарты информационной безопасности. Уметь проектировать систему на базе типовых функциональных узлов; обосновывать принимаемые проектные решения, настраивать и налаживать программно-аппаратные комплексы. Владеть базовыми навыками формирования электрических структурных, функциональных и принципиальных схем, в том числе, с использованием технической и справочной литературы; современными инструментальными средствами и технологиями; навыками работы с компьютером как средством управления информацией	Тестовые вопросы Практико-ориентированное задание

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа

Тематический план форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные работы	в форме практической подготовки		
1	Информационно-вычислительные системы как объекты защиты информации	8	1	2	1	0		4	
2	Информация. Категории информации	8	2	2	1			2	
3	Методы защиты информации в ИВС	8	3-6	8	16	18		24	Рейтинг-контроль №1
4	Современные криптографические методы защиты информации	8	7	2				20	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	Экзамен
Наличие в дисциплине КП/КР									Нет
Итого по дисциплине				18	18	18		54	Экзамен

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 (семестр 8)

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 (семестр 8)

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

5.1. Текущий контроль успеваемости

(семестр 8)

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. Отрастить весь процесс шифрования (ключ $(N+10)$, таблица замены, исходная фраза, зашифрованное сообщение).

Вопросы рейтинг-контроля №2

1. Используя алгоритм Вижинера и свою фамилию в качестве ключа, зашифруйте фразу: «Рейтинг-контроль номер 1». Базовый алфавит состоит из всех (!) букв кириллицы и пробела (всего 34 символа). Отрастить 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?

5.2. Промежуточная аттестация

Вопросы к экзамену (8 семестр)

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.

5.3. Самостоятельная работа обучающегося.

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.

Задания для самостоятельной работы студентов (семестр 8)

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 материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
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	2010	http://www.studentlibrary.ru/book/ISBN9785940745181.html

В.Ф. - М. : ДМК Пресс, 2010.		
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

6.2. Периодические издания

Журналы (<https://elibrary.ru/>):

1. Вестник компьютерных и информационных технологий
2. Вычислительные технологии
3. Радиотехнические и телекоммуникационные системы

6.3. Интернет-ресурсы

<http://www.studentlibrary.ru>

<http://library.vlsu.ru/>

<http://citforum.ru/>

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий *лекционного типа, занятий практического/лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.* Практические/лабораторные работы проводятся в аудиториях 424-2, 401-2, 412-2 и 416-2.

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



Рецензент

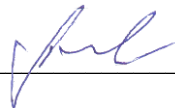
(представитель работодателя) _____ Генеральный директор ООО "Диаграмма" Протягов И.В.



Программа рассмотрена и одобрена на заседании кафедры ВТ и СУ

Протокол № 1 от 31 августа 2021 года

Заведующий кафедрой Ланцов В.Н.

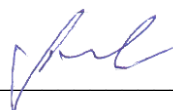


Рабочая программа рассмотрена и одобрена

на заседании учебно-методической комиссии направления 09.03.01 информатика и вычислительная техника

Протокол № 1 от 31 августа 2021 года

Председатель комиссии Ланцов В.Н. зав. каф. ВТиСУ



**ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ**

Рабочая программа одобрена на 20 22 / 20 23 учебный года

Протокол заседания кафедры № 1 от 29.08.22 года

Заведующий кафедрой  Куликов К.В.

Рабочая программа одобрена на 20 ____ / 20 ____ учебный года

Протокол заседания кафедры № ____ от ____ года

Заведующий кафедрой _____

Рабочая программа одобрена на 20 ____ / 20 ____ учебный года

Протокол заседания кафедры № ____ от ____ года

Заведующий кафедрой _____