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

УТВЕРЖДАЮ
Проректор
по учебно-методической работе
_____ А.А.Панфилов
«15» 01 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ЗАЩИТА ИНФОРМАЦИИ»

(наименование дисциплины)

Направление подготовки 09.03.01 – Информатика и вычислительная техника

Профиль/программа подготовки _____

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоемкость, зач. ед./ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачёт)
8	5/180	36	–	18	90	Экзамен (36)
Итого	**5/180**	**36**	**–**	**18**	**90**	**Экзамен (36)**

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины (модуля) «Защита информации» являются:

1) обучение студентов основам построения систем безопасности;

2) создание фундаментальной основы знаний, необходимой при проектировании программных продуктов для вычислительных систем;

3) изучение основных методов защиты данных в информационно-вычислительных системах;

4) освоение студентами основных приемов программирования типовых задач криптографии (алгоритм Виженера, методы перестановки, аналитические методы);

5) изучение особенностей реализации систем защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Защита информации» относится к вариативной части ОПОП по направлению 09.03.01 – «Информатика и вычислительная техника» бакалавриат.

Дисциплина логически, содержательно и методически тесно связана с рядом теоретических дисциплин и практик ОПОП.

Для успешного изучения дисциплины «Защита информации» студенты должны быть знакомы с дисциплинами, которые формируют необходимые для изучения данной дисциплины способности к обобщению и анализу информации, знания математического анализа и алгоритмов, структурных блоков ЭВМ, способов представления данных в ЭВМ, способность использовать персональный компьютер и системы программирования для разработки программного обеспечения, готовность понимать актуальность совершенствования языков программирования, подходов к проектированию программных систем, программного обеспечения в аспектах технического и научного прогресса.

Без освоения дисциплины «Защита информации» невозможна дальнейшая успешная подготовка студентов по направлению 09.03.01.

Дисциплина предоставляет саму возможность изучения практически всех дисциплин вариативной части, поскольку в процессе изучения используются ЭВМ и языки высокого уровня как средства и инструменты для исследований и получения результатов, для решения специализированных задач. Происходит ознакомление студентов с общей проблемой информационной безопасности информационных систем и методах её преодоления, изучение российских и международных стандартов информационной безопасности, содержащих рекомендации о процедурном и программно-техническом уровнях информационной безопасности.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) **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 (ОК-4);

2) **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 (ОПК-5);

3) **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 (ОПК-5).

Перечень компетенций:

ОК-4 – способность использовать основы правовых знаний в различных сферах деятельности;

ОПК-5 – способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности.

Курс «Защита информации» связан с дисциплинами «Высшая математика», «Организация ЭВМ и систем», «Программирование на ЯВУ», «Операционные системы», «Системное программное обеспечение».

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Защита информации» составляет 5 зачетных единиц, 180 часов.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоёмкость (в часах)						Объём учебной работы с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра),* форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1	Введение	8	1	2						1 час/50%	
2	Информационно-вычислительные системы как объекты защиты информации	8	1-2	4				10		3 часа/75%	
3	Информация. Категории информации	8	2-3	4				10		2 часа/50%	Рейтинг-контроль №1
4	Стандарты и спецификации в области информационной безопасности	8	3-4	4		4		20		2 часа/25%	
5	Методы защиты информации в ИВС	8	4-6	8		4		10		4 часа/33%	Рейтинг-контроль №2
6	Защита информации в локальных сетях	8	6-7	6		4		20		2 часа/20%	
7	Контроль защиты информации	8	8-9	6		6		20		2 часа/17%	
8	Заключение	8	9	2						1 час/50%	Рейтинг-контроль №3
Всего				**36**		**18**		**90**		**17 часов/31%**	**Экзамен**

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При освоении дисциплины используются следующие сочетания видов учебной работы с методами и формами активизации познавательной деятельности бакалавров для достижения запланированных результатов обучения и формирования компетенций:

- изучение теоретического материала дисциплины на лекциях с использованием компьютерных технологий;
- самостоятельное изучение теоретического материала дисциплины с использованием Интернет-ресурсов, информационных баз, методических разработок, специальной учебной и научной литературы;
- закрепление теоретического материала при проведении лабораторных работ с использованием современной вычислительной техники и систем программирования, выполнения проблемно-ориентированных, поисковых, творческих заданий;
- самостоятельная работа студента, направленная на углубление и закрепление знаний, развитие практических умений, комплекса универсальных (общекультурных) и профессиональных компетенций, повышение творческого потенциала, заключается в работе с лекционным материалом, поиске и анализе литературы и электронных источников информации по заданной проблеме, переводе материалов из тематических информационных ресурсов с иностранных языков, изучении тем, вынесенных на самостоятельную проработку, подготовке докладов и презентаций по результатам выполненной работы, изучении теоретического материала к лабораторным занятиям, подготовке к экзамену.

Удельный вес занятий, проводимых в интерактивной форме, составляет 31% от аудиторной нагрузки.

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

8 семестр

6.1. Оценочные средства для текущего контроля

Рейтинг-контроль № 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).

7. 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). Отразить весь процесс шифрования (таблица замены, исходная фраза, ключ, зашифрованное сообщение).

8. 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.

Рейтинг-контроль № 2

1. Перечислите достоинства физических генераторов случайных чисел.
2. Перечислите недостатки физических генераторов случайных чисел.
3. Перечислите достоинства табличных генераторов случайных чисел.
4. Перечислите недостатки табличных генераторов случайных чисел.
5. Перечислите достоинства алгоритмических генераторов случайных чисел.
6. Перечислите недостатки алгоритмических генераторов случайных чисел.
7. Как Вы думаете, почему в криптографии широко используется матричная алгебра?
8. Какими свойствами обладает текст после применения шифра замены?
9. Какими свойствами обладает текст после применения шифра перестановки?
10. Какими свойствами обладает текст после применения гаммирования?
11. Зашифровать любое сообщение методом двойной перестановки. В качестве ключа использовать свои фамилию и имя. Сообщение должно быть достаточной длины.

Рейтинг-контроль № 3

1. Какими характеристиками обладает двоичная последовательность на выходе регистра скремблера?
2. Выполните классификацию алгоритма шифрования DES.

3. Перечислите основные режимы использования блочных шифров.

4. Перечислите основные принципы, лежащие в основе асимметричных криптоалгоритмов.

5. Перечислите достоинства асимметричных криптоалгоритмов.

6. Какие свойства приобретает текст после шифрования по алгоритму DES? Ответ пояснить.

7. Опишите, чем принципиально отличается стеганография от криптографии.

6.2. Промежуточная аттестация

Список вопросов к экзамену

1. Основные виды и источники атак на информацию
2. Категории информационной безопасности.
3. Абстрактные модели защиты информации
4. Комплексный поиск возможных методов доступа
5. Терминалы защищенной информационной системы
6. Получение пароля на основе ошибок администратора и пользователей
7. Получение пароля на основе ошибок в реализации
8. Симметричные криптоалгоритмы
9. Скремблеры
10. Блочные шифры
11. AES: стандарт блочных шифров
12. Функции криптосистем
13. Алгоритмы создания цепочек
14. Методы рандомизации сообщений
15. Генераторы случайных и псевдослучайных последовательностей
16. Архивация
17. Общие принципы архивации. Классификация методов
18. Общая схема симметричной криптосистемы
19. Асимметричные криптоалгоритмы
20. Общие сведения об асимметричных криптоалгоритмах
21. Асимметричные криптосистемы
22. Сетевая безопасность
23. Ошибки, приводящие к возможности атак на информацию
24. Основные положения по разработке ПО
25. Комплексная система безопасности

6.3. Самостоятельная работа 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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Основная литература

1. Защита информации [Электронный ресурс]: учебное пособие / Ю.М. Краковский - Ростов н/Д : Феникс, 2016. - (Высшее образование). - http://www.studentlibrary.ru/book/ISBN9785222269114.html

2. Информационная безопасность и защита информации[Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 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"). - http://www.studentlibrary.ru/book/ISBN5984530155.html

7.2. Дополнительная литература

1. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 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 "Информационнаябезопасность")." - 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. - 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. - http://www.studentlibrary.ru/book/ISBN9785991203791.html

5. Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html

7.3. Интернет-ресурсы

1. Беляев А.В."Методы и средства защиты информации" (курс лекций). http://citforum.ru/internet/infsecure/index.shtml

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Электронные средства обучения

Набор слайдов, методические указания к выполнению лабораторных и практических работ, к курсовому проекту, учебная цифровая вычислительная машина, контрольные тесты.

8.2. Лабораторное оборудование

Лабораторные занятия проводятся в компьютерной лаборатории с использованием персональных компьютеров с установленной лицензионной средой разработки Visual Studio

При проведении лабораторных работ используется мультимедиа проектор и интерактивная доска.

8.3. Средства вычислительной техники и демонстрационное оборудование

Лекции читаются в аудитории кафедры ВТ, оснащенной мультимедиа проектором. При выполнении самостоятельной работы по освоению дисциплины студенты имеют возможность работать в компьютерном классе кафедры ВТ с выходом в сеть Интернет, используя лицензионное прикладное и системное программное обеспечение, а также электронные методические материалы.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 09.03.01 – Информатика и вычислительная техника

Рабочую программу составил _____ ст. преп. кафедры ВТ Трофимов М.А.
(ФИО, подпись)

Рецензент(ы) к.т.н., доцент кафедры ВТ К.В.Куликов
(представитель работодателя) ведущий инженер-программист встраиваемых систем ЗАО «Синтелс» Г.А.Лобачёв
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ВТ

Протокол № 6 от 15 февраля 2016 года

Заведующий кафедрой _____ В.Н.Ланцов
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления _____

Протокол № 1 от 15 февраля 2016 года

Председатель комиссии _____ В.Н.Ланцов
(ФИО, подпись)