

Министерство науки и высшего образования Российской Федерации  
**Муромский институт (филиал)**  
федерального государственного бюджетного образовательного учреждения высшего образования  
**«Владимирский государственный университет  
имени Александра Григорьевича и Николая Григорьевича Столетовых»**  
(МИ ВлГУ)

Кафедра *ФПМ*

«УТВЕРЖДАЮ»  
Заместитель директора по УР  
\_\_\_\_\_ Д.Е. Андрианов  
\_\_\_\_\_ 23.05.2023

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

*Основы информационной безопасности*

**Направление подготовки**

*10.03.01 Информационная безопасность*

**Профиль подготовки**

*Безопасность компьютерных систем (по  
отрасли или в сфере профессиональной  
деятельности)*

Семестр	Трудоем- кость, час./зач. ед.	Лек- ции, час.	Практи- ческие занятия, час.	Лабора- торные работы, час.	Консультация, час.	Конт- роль, час.	Всего (контакт- ная работа), час.	СРС, час.	Форма промежу- точного контроля (экз., зач., зач. с оц.)
4	144 / 4	32	16		5,2	0,35	53,55	63,8	Экз.(26,65)
Итого	144 / 4	32	16		5,2	0,35	53,55	63,8	26,65

Муром, 2023 г.

## 1. Цель освоения дисциплины

Цель дисциплины: дать понятие о существующих угрозах информационной безопасности и их источниках;

дать понятие о существующих средствах обеспечения информационной безопасности и тенденциях их развития.

научить анализировать имеющуюся ситуацию на предприятии;

научить определять круг мер и средств для повышения информационной безопасности.

## 2. Место дисциплины в структуре ОПОП ВО

Базовые дисциплины: Введение в специальность, Математика, Дискретная математика.

## 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	Результаты обучения по дисциплине	
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.1 Оценивает и систематизирует информацию, обрабатываемую в информационных системах	знать о существующих угрозах информационной безопасности и их источниках (ОПК-1.1) Уметь оценивать роль и значение информации, информационных технологий и информационной безопасности (ОПК-1.1)	Вопросы к устному опросу, тесты
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.3 Применяет информационные технологии для решения профессиональных задач	знать о существующих средствах обеспечения информационной безопасности и тенденциях их развития (ОПК-2.3) Уметь решать задачи профессиональной деятельности на основе существующих компьютерных технологий (ОПК-2.3) Владеть навыками разработки и реализации политики управления доступом в компьютерных системах (ОПК-2.3)	Вопросы к устному опросу, тесты

#### 4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

##### 4.1. Форма обучения: очная

Уровень базового образования: среднее общее.

Срок обучения 4г.

##### 4.1.1. Структура дисциплины

№ п/п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Основы информационной безопасности	4	32	16						63,8	Устный опрос, тестирование
Всего за семестр		144	32	16				5,2	0,35	63,8	Экз.(26,65)
Итого		144	32	16				5,2	0,35	63,8	26,65

##### 4.1.2. Содержание дисциплины

###### 4.1.2.1. Перечень лекций

###### Семестр 4

###### Раздел 1. Основы информационной безопасности

###### Лекция 1.

Актуальность проблемы информационной безопасности. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Основные понятия и определения (2 часа).

###### Лекция 2.

Политика государства в области информационной безопасности. Правовые основы обеспечения информационной безопасности (2 часа).

###### Лекция 3.

Угрозы безопасности информации. Источники угроз (2 часа).

###### Лекция 4.

Модель угроз безопасности информации. Модель нарушителя безопасности информации (2 часа).

###### Лекция 5.

Меры и методы обеспечения защиты информации. Организационные(процедурные, административные) меры защиты информации (2 часа).

**Лекция 6.**

Инженерно-технические меры защиты информации (2 часа).

**Лекция 7.**

Идентификация и аутентификация. Управление доступом (2 часа).

**Лекция 8.**

Межсетевое экранирование. Обеспечение высокой доступности (2 часа).

**Лекция 9.**

Протоколирование и аудит. Системы обнаружения и предотвращения компьютерных атак (2 часа).

**Лекция 10.**

Криптографические методы защиты информации. Электронная цифровая подпись. Контроль целостности (2 часа).

**Лекция 11.**

Вредоносные программы и защита от них. Защита информации в компьютерных сетях. Тестирование на проникновение. Социальная инженерия (2 часа).

**Лекция 12.**

Меры по обеспечению безопасности данных при их обработке в информационных системах персональных данных и государственных информационных системах (2 часа).

**Лекция 13.**

Лицензирование и сертификация в области ИБ (2 часа).

**Лекция 14.**

Аттестация объектов информатизации. Выбор средств ИБ. Управление рисками ИБ (2 часа).

**Лекция 15.**

Компьютерные преступления, инциденты ИБ и их расследование. Форензика (2 часа).

**Лекция 16.**

Основные стандарты и спецификации в области информационной безопасности. Цифровая гигиена (2 часа).

#### **4.1.2.2. Перечень практических занятий**

**Семестр 4***Раздел 1. Основы информационной безопасности***Практическое занятие 1**

Реализация дискреционной модели политики безопасности (2 часа).

**Практическое занятие 2**

Простые симметричные криптосистемы (2 часа).

**Практическое занятие 3**

Простые симметричные криптосистемы (2 часа).

**Практическое занятие 4**

Алгоритм XOR. Одноразовый блокнот (2 часа).

**Практическое занятие 5**

Протокол Фиата-Шамира (2 часа).

**Практическое занятие 6**

Защита от копирования (2 часа).

**Практическое занятие 7**

Контроль целостности (2 часа).

**Практическое занятие 8**

Хэш-функции (2 часа).

#### **4.1.2.3. Перечень лабораторных работ**

Не планируется.

#### **4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы**

Перечень тем, вынесенных на самостоятельное изучение:

1. Объединение блочных шифров.
2. Криптосистемы на эллиптических кривых.
3. Совершенные шифры.
4. Близкие к совершенным шифры.
5. Экстремальные шифры.
6. Аппаратные средства защиты.
7. Программные и аппаратные средства сетевой защиты в различных операционных системах.
8. Протоколы защищенной передачи информации в сети.
9. Корпоративные системы обеспечения информационной безопасности.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

#### **4.1.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР** Не планируется.

#### **4.1.2.6. Примерный перечень тем курсовых работ (проектов)** Не планируется.

### **5. Образовательные технологии**

В процессе изучения дисциплины применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). Задачи решаются синхронно со студентами с пояснением шагов решения.

### **6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.** Фонды оценочных материалов (средств) приведены в приложении.

## **7. Учебно-методическое и информационное обеспечение дисциплины.**

### **7.1. Основная учебно-методическая литература по дисциплине**

1. Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/101992.html>. — Режим доступа: для авторизир. пользователей - <https://www.iprbookshop.ru/101992.html>
2. Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие - Санкт-Петербург: СПб: Университет ИТМО, 2015, 2015. - 93 с. - <http://books.ifmo.ru/file/pdf/1763.pdf>
3. Маркина Т.А. Основные механизмы защиты в ОС MS Windows. Методические рекомендации по выполнению лабораторных работ. Учебно-методическое пособие - Санкт-Петербург: СПб: Университет ИТМО, 2015, 2015. - 48 с. - <http://books.ifmo.ru/file/pdf/1766.pdf>

### **7.2. Дополнительная учебно-методическая литература по дисциплине**

1. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/108227.html> . — Режим доступа: для авторизир. пользователей. - DOI: <https://doi.org/10.23682/108227> - <https://www.iprbookshop.ru/108227.html>

### **7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем**

В образовательном процессе используются информационные технологии, реализованные на основе информационно-образовательного портала института ([www.mivlgu.ru/iop](http://www.mivlgu.ru/iop)), и инфокоммуникационной сети института:

- предоставление учебно-методических материалов в электронном виде;
- взаимодействие участников образовательного процесса через локальную сеть института и Интернет;
- предоставление сведений о результатах учебной деятельности в электронном личном кабинете обучающегося.

Информационные справочные системы:

- 1) Информационно-поисковая система Консультант Плюс (<http://www.consultant.ru>)
- 2) Информационный портал Совета Безопасности Российской Федерации (<http://www.scrf.gov.ru/documents/6/>)
- 3) Информационно-аналитический портал ISO27000.RU / ЗАЩИТА-ИНФОРМАЦИИ.SU (<http://iso27000.ru>)
- 4) Каталог решений и услуг по Информационной Безопасности (<http://www.ru-ib.ru>)

Программное обеспечение:

LibreOffice (Mozilla Public License v2.0)

Microsoft Windows 10 Professional (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Microsoft Visual Studio (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

### **7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

[iprbookshop.ru](http://iprbookshop.ru)  
[books.ifmo.ru](http://books.ifmo.ru)  
[consultant.ru](http://consultant.ru)  
[scrif.gov.ru](http://scrif.gov.ru)  
[iso27000.ru](http://iso27000.ru)  
[ru-ib.ru](http://ru-ib.ru)  
[mivlgu.ru/iop](http://mivlgu.ru/iop)

## **8. Материально-техническое обеспечение дисциплины**

Лаборатория программно-аппаратных средств защиты информации

Программно-аппаратный комплекс RadioInspector WIFI 2 ; портативный RFID считыватель cipherLab 1862; компьютер для проведения мультимедиалекций Raspberry; персональный компьютер Mini PC Android MK808 B; ПК CPU-Intel Core i5-4460 BOX - 12 шт.; ПК — 1шт.; экран DRAPPER Apex STAR; видеопроектор InFocus; коммутатор. Доступ к сети Интернет.

## **9. Методические указания по освоению дисциплины**

Для успешного освоения теоретического материала обучающийся: знакомится со списком рекомендуемой основной и дополнительной литературы; уточняет у преподавателя, каким дополнительным пособиям следует отдать предпочтение; ведет конспект лекций и прорабатывает лекционный материал, пользуясь как конспектом, так и учебными пособиями.

На практических занятиях пройденный теоретический материал подкрепляется решением задач по основным темам дисциплины. Занятия проводятся в компьютерном классе, используя специальное программное обеспечение. Каждой подгруппе обучающихся преподаватель выдает задачу, связанную с разработкой и программной реализацией

алгоритмов обработки информации. В конце занятия обучающие демонстрируют полученные результаты преподавателю и при необходимости делают работу над ошибками.

Выполнение самостоятельной работы студентом основано на ознакомлении с материалами, расширяющими знания по темам, вынесенным на СРС, в источниках литературы и интернет ресурсах, рекомендованных преподавателем.

Форма заключительного контроля при промежуточной аттестации – экзамен. Для проведения промежуточной аттестации по дисциплине разработаны фонд оценочных средств и балльно-рейтинговая система оценки учебной деятельности студентов. Оценка по дисциплине выставляется в информационной системе и носит интегрированный характер, учитывающий результаты оценивания участия студентов в аудиторных занятиях, качества и своевременности выполнения заданий в ходе изучения дисциплины и промежуточной аттестации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *10.03.01 Информационная безопасность* и профилю подготовки *Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)*  
Рабочую программу составил к.т.н., доцент Астафьев А.В. \_\_\_\_\_

Программа рассмотрена и одобрена на заседании кафедры *ФПМ*

протокол № 19 от 26.04.2023 года.

Заведующий кафедрой *ФПМ* \_\_\_\_\_ *Орлов А.А.*

(Подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета

протокол № 9 от 19.05.2023 года.

Председатель комиссии ФИТР \_\_\_\_\_ *Рыжкова М.Н.*

(Подпись)

(Ф.И.О.)



**Фонд оценочных материалов (средств) по дисциплине**  
**Основы информационной безопасности**

**1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине**

Темы для устного опроса:

Актуальность проблемы информационной безопасности.  
 Национальные интересы Российской Федерации в информационной сфере и их обеспечение.  
 Основные понятия и определения.  
 Политика государства в области информационной безопасности.  
 Правовые основы обеспечения информационной безопасности.  
 Угрозы безопасности информации.  
 Источники угроз.  
 Модель угроз безопасности информации.  
 Модель нарушителя безопасности информации.  
 Меры и методы обеспечения защиты информации.  
 Организационные(процедурные, административные) меры защиты информации.  
 Инженерно-технические меры защиты информации.  
 Идентификация и аутентификация.  
 Управление доступом.  
 Межсетевое экранирование.  
 Обеспечение высокой доступности.  
 Протоколирование и аудит.  
 Системы обнаружения и предотвращения компьютерных атак.  
 Криптографические методы защиты информации.  
 Электронная цифровая подпись.  
 Контроль целостности.  
 Вредоносные программы и защита от них.  
 Защита информации в компьютерных сетях.  
 Тестирование на проникновение.  
 Социальная инженерия.  
 Меры по обеспечению безопасности данных при их обработке в информационных системах персональных данных и государственных информационных системах.  
 Лицензирование и сертификация в области ИБ.  
 Аттестация объектов информатизации.  
 Выбор средств ИБ.  
 Управление рисками ИБ.  
 Компьютерные преступления, инциденты ИБ и их расследование.  
 Форензика.  
 Основные стандарты и спецификации в области информационной безопасности.  
 Цифровая гигиена.

**Общее распределение баллов текущего контроля по видам учебных работ для студентов**

Рейтинг-контроль 1	Контрольная работа, лабораторные работы, практические работы	15
Рейтинг-контроль 2	Контрольная работа, лабораторные работы, практические работы	30

Рейтинг-контроль 3	Контрольная работа, лабораторные работы, практические работы	45
Посещение занятий студентом		5
Дополнительные баллы (бонусы)		5
Выполнение семестрового плана самостоятельной работы		5

## **2. Промежуточная аттестация по дисциплине**

### **Перечень вопросов к экзамену / зачету / зачету с оценкой.**

### **Перечень практических задач / заданий к экзамену / зачету / зачету с оценкой (при наличии)**

Темы для устного опроса:

Актуальность проблемы информационной безопасности.  
 Национальные интересы Российской Федерации в информационной сфере и их обеспечение.  
 Основные понятия и определения.  
 Политика государства в области информационной безопасности.  
 Правовые основы обеспечения информационной безопасности.  
 Угрозы безопасности информации.  
 Источники угроз.  
 Модель угроз безопасности информации.  
 Модель нарушителя безопасности информации.  
 Меры и методы обеспечения защиты информации.  
 Организационные(процедурные, административные) меры защиты информации.  
 Инженерно-технические меры защиты информации.  
 Идентификация и аутентификация.  
 Управление доступом.  
 Межсетевое экранирование.  
 Обеспечение высокой доступности.  
 Протоколирование и аудит.  
 Системы обнаружения и предотвращения компьютерных атак.  
 Криптографические методы защиты информации.  
 Электронная цифровая подпись.  
 Контроль целостности.  
 Вредоносные программы и защита от них.  
 Защита информации в компьютерных сетях.  
 Тестирование на проникновение.  
 Социальная инженерия.  
 Меры по обеспечению безопасности данных при их обработке в информационных системах персональных данных и государственных информационных системах.  
 Лицензирование и сертификация в области ИБ.  
 Аттестация объектов информатизации.  
 Выбор средств ИБ.  
 Управление рисками ИБ.  
 Компьютерные преступления, инциденты ИБ и их расследование.  
 Форензика.

Основные стандарты и спецификации в области информационной безопасности.  
Цифровая гигиена.

### **Методические материалы, характеризующие процедуры оценивания**

Промежуточные аттестации проводятся 3 раза за семестр (на 6, 12 и 17 учебных неделях) в форме письменной контрольной работы.

В зависимости от объема пройденного материала на момент проведения контрольной работы в нее включаются вопросы из пункта 18, соответствующие пройденному материалу. При проведении контрольной работы студенты делятся на 2 варианта. Каждому варианту предоставляется индивидуальный набор контрольных вопросов.

Оценка работ проводится по критерию полноты ответа.

Вопросы, выносимые на промежуточные контрольные работы, используются так же при проведении экзамена. Экзамен проводится в форме устной беседы и включает в себя ответ на вопросы билета (2 шт.) и выполнение практической части.

В случае невыполнения практической части экзаменационная работа студента может быть оценена не более чем на оценку "Хорошо".

Оценка экзаменационной работы осуществляется по критерию полноты ответа и самостоятельности его изложения.

Уровень знаний студента может быть уточнен 1-2 дополнительными вопросами (так же берутся из вопросника в пункте 18).

Максимальная сумма баллов, набираемая студентом по дисциплине равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	<i>Уровень сформированности компетенций</i>
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	<b><i>Высокий уровень</i></b>
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	<b><i>Продвинутый уровень</i></b>

50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	<b><i>Пороговый уровень</i></b>
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	<b><i>Компетенции не сформированы</i></b>

### 3. Задания в тестовой форме по дисциплине

Примеры заданий:

Что является активным компонентом системы, который может стать причиной потока информации или изменения состояния системы.

- : Объект
- : Субъект
- :Arteфакт
- : Уязвимость

Что является пассивным компонентом системы, хранящим, принимающий или передающим информацию.

- : Объект
- : Субъект
- :Arteфакт
- : Уязвимость

Что обеспечивается в случае, если данные в системе в семантическом отношении не отличаются от данных в исходных документах?

- : Конфиденциальность
- : Целостность
- : Доступность
- : Санкционированность

Полный перечень тестовых заданий с указанием правильных ответов, размещен в банке вопросов на информационно-образовательном портале института по ссылке <https://www.mivlgu.ru/iop/question/edit.php?courseid=405&cat=24885%2C10661&category=24877%2C10661&qbshowtext=0&recurse=0&recurse=1&showhidden=0>

Оценка рассчитывается как процент правильно выполненных тестовых заданий из их общего числа.