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)

Отделение среднего профессионального образования

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____Д.Е. Андрианов
«_19_» ___05___ 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

для специальности 09.02.11 Разработка и управление программным обеспечением

Муром, 2026 г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее - ФГОС) по специальности среднего профессионального образования (далее - СПО) 09.02.11 Разработка и управление программным обеспечением №138 от 24 февраля 2025 года.

Кафедра-разработчик: информационных систем.

Рабочую программу составил: преподаватель СПО кафедры ИС Панкратов Д.А.

_____ от «05» мая 2026 г.
(подпись)

Рабочая программа рассмотрена и одобрена на заседании кафедры ИС.

Протокол № 21 от «05» мая 2026 г.

Заведующий кафедрой ИС *Андрианов Д.Е.* _____
(подпись)

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы информационной безопасности

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании, для получения дополнительных компетенций, умений и знаний, необходимых для обеспечения конкурентоспособности выпускника на рынке труда и продолжения образования по специальности.

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена

Дисциплина ОП.05 Основы информационной безопасности является общепрофессиональной дисциплиной

Дисциплина «Основы информационной безопасности» — это базовая методика обеспечения защиты информации, которая обеспечивает понимание основ и концепций информационной безопасности, а также подходов при разработке мер защиты информационных систем. Курс базируется на знаниях, полученных студентами в процессе изучения дисциплин: информатика, основы алгоритмизации и программирования, операционные системы, компьютерные сети, технологии объектно-ориентированного программирования. Углубление и расширение вопросов, изложенных в данном курсе, будет осуществляться во время работы студентов над дисциплинами модуля ПМ.02 Разработка и интеграция модулей программного обеспечения, модуля ПМ.03 Проектирование и разработка информационных систем, а также при написании выпускных квалификационных работ.

1.3. Цели и задачи учебной дисциплины - требования к результатам освоения учебной дисциплины:

Цель дисциплины Ознакомление студентов с методологией обеспечения информационной безопасности; формирование способностей выявлять угрозы и уязвимости, осуществлять сертификацию объектов информатизации, проектировать базовые и прикладные системы защиты информации и разрабатывать средства реализации политик информационной безопасности

В результате освоения дисциплины обучающийся должен знать:

- Знать основные виды угроз информационной безопасности, принципы защиты информации и базовые средства обеспечения безопасности (ОК 01., ОК 09., ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7., ОК 02.).

В результате освоения дисциплины обучающийся должен уметь:

- Уметь применять базовые методы защиты информации при решении простых профессиональных задач (ОК 01., ОК 09., ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7., ОК 02.).

В результате освоения дисциплины обучающийся должен владеть следующими общими (ОК) и профессиональными (ПК) компетенциями:

- ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;
- ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках;
- ПК 1.1. Проектировать базы данных;
- ПК 1.4. Администрировать базы данных;

- ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации;
- ПК 3.1. Собирать исходные данные для разработки проектной документации на информационную систему;
- ПК 3.2. Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика;
- ПК 3.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием;
- ПК 3.5. Интегрировать информационную систему с существующими информационными системами заказчика;
- ПК 3.7. Разрабатывать техническую документацию на эксплуатацию информационной системы;
- ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

1.4. Количество часов на освоение программы учебной дисциплины:

Максимальной учебной нагрузки обучающегося 94 часа, в том числе:
обязательной аудиторной нагрузки обучающегося 80 часов;
самостоятельной нагрузки обучающегося 14 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
	3 семестр
Максимальная учебная нагрузка (всего)	94
Обязательная аудиторная учебная нагрузка (всего)	80
В том числе:	
лекционные занятия	32
практические занятия	32
лабораторные работы	16
контрольные работы	
курсовая работа / индивидуальный проект	0
Самостоятельная работа обучающегося (всего)	14
Итоговая аттестация в форме	Экзамен

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
	3 семестр		
Раздел 1	**Основы информационной безопасности**		
Тема 1.1 Международные стандарты информационного обмена	*Содержание учебного материала*		
	Лекционные занятия. Основные понятия и определения. Понятие и задачи информационной безопасности. Структуры, обеспечивающие информационную безопасность. Этапы развития информационной безопасности. Нормативно-правовые аспекты информационной безопасности.	10	1
	Практические занятия. Шифр Цезаря. Аффинная система шифрования Цезаря. Шифр Цезаря с ключевым словом. Шифр Атбаш. Шифрующие таблицы. Шифрующие таблицы с ключевым словом. Шифрующие таблицы с двойной перестановкой. Квадрат Полибия. Метод тюремной азбуки. XOR - одноразовый блокнот.	20	2
	Самостоятельная работа обучающихся. Гаммирование с обратной связью. Генераторы псевдослучайных чисел. Современные симметричные методы шифрования. Современные асимметричные методы шифрования.	14	3
Тема 1.2 Криптографические методы защиты	*Содержание учебного материала*		
	Лекционные занятия. Информационные угрозы. Хакерские атаки. Фишинговые атаки. Спам и защита от него. Вредоносные программы. Компьютерные преступления. Многоуровневая защита информации. Антивирусная защита.	22	1

	Системы аутентификации пользователей. SQL-инъекции. криптографические методы защиты информации.		
	Практические занятия. RSA. Эль-Гамаль.	4	2
	Лабораторные работы. Шифр Вижинера. Шифр Гамильтона. Гаммирование. Рюкзачный шифр.	16	3
Тема 1.3 Методы кодирования и сжатия информации	*Содержание учебного материала*		
	Практические занятия. Код Шеннона-Фано. Код Хаффмана.	4	2
Тема 1.4 Резервное хранение информации	*Содержание учебного материала*		
	Практические занятия. Контроль целостности.	2	2
Тема 1.5 Электронно-цифровая подпись и хеширование	*Содержание учебного материала*		
	Практические занятия. Хэш-функция.	2	2
Всего:		94	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально – техническому обеспечению

Лаборатория ГИС и САПР

Сервер; 12 персональных компьютеров; проектор Sanyo PDG-DSU20; экран настенный Drapper Apex Star

Лаборатория разработки информационных систем

12 персональных компьютеров; проектор View Sonic PG603X DLP; экран настенный Lumien

Лаборатория распределенных систем

12 персональных компьютеров; проектор Nec V300X; экран настенный Lumien Master Picture

Лаборатория информатики и программирования

12 персональных компьютеров; проектор Sanyo PDG-DSU20; экран настенный Drapper Apex Star.

Компьютерный класс

Проектор ViewSonic PG603X DLP Экран Lumien Персональный компьютер RUSCO – 19 шт. Коммутатор D-Link Маршрутизатор беспроводной N ASUS RT-AC66U

Программное обеспечение:

РЕД ОС (Соглашение №140/05-21У от 18.05.2021 года о сотрудничестве в области науки, развития инновационной деятельности)

Pycharm Community Edition (проприетарная лицензия и Apache License 2.0)

Python 3.9.4 (Python Software Foundation License)

РЕД ОС (Соглашение №140/05-21У от 18.05.2021 года о сотрудничестве в области науки, развития инновационной деятельности)

QT Creator ((L)GPL)

Python 3 (PSF License Agreement)

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, интернет – ресурсов, дополнительной литературы.

Основные источники:

1. Основы информационной безопасности : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2023. — 287 c. . https://www.iprbookshop.ru/141624.html
2. Мельников А.В. Основы информационной безопасности : учебное пособие / Мельников А.В., Зарубин С.В.. — Москва : Российский государственный университет правосудия имени В.М. Лебедева, 2025. — 220 c.. https://www.iprbookshop.ru/152309.html
3. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 266 c. . https://www.iprbookshop.ru/142285.html

Дополнительные источники:

1. Суворова, Г. М. Основы информационной безопасности : учебное пособие для СПО / Г. М. Суворова. — 2-е изд. — Саратов : Профобразование, 2024. — 135 c.. https://www.iprbookshop.ru/142816.html
2. Зенков А.В. Основы информационной безопасности : учебное пособие / Зенков А.В.. — Москва, Вологда : Инфра-Инженерия, 2022.. https://www.iprbookshop.ru/124242.html

3. Гультяева Т.А. Основы информационной безопасности : учебное пособие / Гультяева Т.А.. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 c.. https://www.iprbookshop.ru/91640.html

Интернет-ресурсы:
1. Электронная библиотечная система - iprbookshop.ru
2. Электронная библиотека ВлГУ - e.lib.vlsu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Уметь применять базовые методы защиты информации при решении простых профессиональных задач.	контрольная работа, устный опрос
Знать основные виды угроз информационной безопасности, принципы защиты информации и базовые средства обеспечения безопасности.	контрольная работа, устный опрос

Приложение

Фонд оценочных материалов (средств) по дисциплине
Основы информационной безопасности

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных
тест_20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация, характеризуемая:
+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации
22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность
- Доступность
- Актуальностьl
23) Угроза информационной системе (компьютерной сети) – это:
+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически
24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

+ Программные, технические, организационные, технологические

- Серверные, клиентские, спутниковые, наземные

- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети

- Администратор сети

- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности

- Инструкций, алгоритмов поведения пользователя в сети

- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер

- Аудит, анализ безопасности

+ Аудит, анализ уязвимостей, риск-ситуаций

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	Контрольная работа, практические работы, лабораторные работы	20
Рейтинг-контроль 2	Контрольная работа, практические работы, лабораторные работы	20
Рейтинг-контроль 3	Контрольная работа, практические работы, лабораторные работы	20
Посещение занятий студентом		10
Дополнительные баллы (бонусы)		10
Выполнение семестрового плана самостоятельной работы		20

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)

1. Информационная безопасность, основные понятия и определения
2. Задачи информационной безопасности
3. Классификация угроз информационной безопасности.
4. Классификация сетевых атак
5. Принципы обеспечения информационной безопасности
6. Методы и средства обеспечения информационной безопасности
7. Структуры обеспечивающие информационную безопасность
8. Этапы развития информационной безопасности.
9. Действия и события нарушающие информационную безопасность
10. Способы воздействия угроз на информационные объекты

11. Внутренние и внешние угрозы
12. Вредоносные программы
13. SQL инъекции
14. Хакерские атаки
15. Фишинговые атаки
16. Спам и защита от него.
17. Асинхронные методы шифрования

Методические материалы, характеризующих процедуры оценивания

При проведении промежуточных аттестаций используются вопросы, приведенные в пункте "Оценочные средства для промежуточной аттестации". Из каждого раздела, освоенного студентом, выбирается по два теоретических и одному практическому вопросу. Теоретические вопросы раскрываются в устной, либо в письменной форме. Практические задания как правило реализуются с помощью персонального компьютера.

При проверке знаний, приобретенных в рамках выполнения практических и лабораторных работ, используются контрольные вопросы, приведенные в методических указаниях к практическим работам. Защита практических и лабораторных работы также является средством промежуточной аттестации.

Максимальная сумма баллов, набираемая студентом по дисциплине равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	***Уровень сформированности компетенций***
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	***Высокий уровень***
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	***Продвинутый уровень***

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	***Пороговый уровень***
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	***Компетенции не сформированы***

3. Задания в тестовой форме по дисциплине

Примеры заданий:

Предоставляющий свои ресурсы пользователям сети компьютер – это:

- Пользовательский
- Клиент
+ Сервер

Центральная машина сети называется:

- Центральным процессором
+ Сервером
- Маршрутизатором

Правильно утверждение "Звезда"

- Топологию «Звезда» можно собрать из нескольких топологий «Кольцо»
+ Топологию «Дерево» можно собрать из нескольких топологий «Звезда»
- Топологию «Шина» можно собрать из нескольких топологий «Дерево»

Сетевая топология определяется способом, структурой:

- Аппаратного обеспечения
- Программного обеспечения
+ Соединения узлов каналами сетевой связи

Система – это

1) совокупность внутренних устойчивых связей между элементами системы, определяющая ее основные свойства.

2) совокупность элементов, объединенная связями между ними и обладающая определенной целостностью.

3) совокупность экономико-математических методов и моделей обработки информации.

4) набор целенаправленных правил взаимоотношений между элементами.

Укажите правильный ответ.

Информационная услуга представляет собой

Тиражирование информационного продукта для доведения до потребителя.

Производственная деятельность с информационной продукцией.

Информационная деятельность по доведению информационной продукции до потребителей.

Обслуживание потребителей в интернет-клубах.

Особенности экспертных систем (ЭС):

Ограничена определенной предметной областью.

Способна «рассуждать» при сомнительных исходных данных.

Способна «объяснить» цепочку сделанных ею рассуждений.

Строится так, чтобы имелась возможность сохранять стабильность наполнения программы.

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=4562

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