



**Автономная некоммерческая организация
Профессиональная образовательная организация
«КОЛЛЕДЖ ИНФОРМАТИКИ И ДИЗАЙНА»
(АНО ПОО «Колледж информатики и дизайна»)**

109029, г. Москва, ул. Нижегородская, д.32, стр. 16, комн.301
ИНН 9723269190, КПП 772301001, ОГРН 1267700052620
тел. 8(495)774-72-74, 8(495)222-54-55
официальный сайт kid-spo.ru

Приложение 3
к ОП СПО 09.02.11

Разработка и управление программным обеспечением

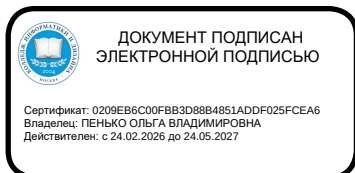
Утверждаю

Директор АНО ПОО

«Колледж информатики и дизайна»

О.В. Пенько

13 мая 2026г.



РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ПРОГРАММА ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА ПО
СПЕЦИАЛЬНОСТИ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

**09.02.11 Разработка и управление программным обеспечением
на базе основного общего образования**

Форма обучения очная
(очная, заочная, очно-заочная)

Москва, 2026

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) **09.02.11 ПРОГРАММА ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА ПО СПЕЦИАЛЬНОСТИ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**, утвержденного приказом Министерства просвещения Российской Федерации от 10 марта 2025 г. N 184.

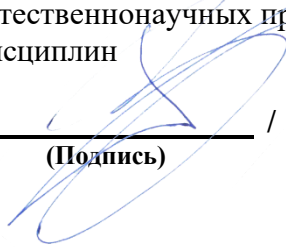
Организация-разработчик: АНО ПОО «Колледж информатики и дизайна»

ОДОБРЕНА

Предметно-цикловой комиссией
общих гуманитарных и социально-
экономических, математических и
общих естественнонаучных,
профессиональных дисциплин

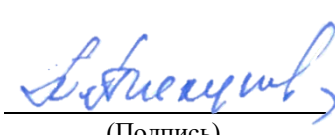
Протокол № 8
от « 29 » апреля 20 26 г.

Председатель предметно-цикловой комиссии
общих гуманитарных и социально-
экономических, математических и общих
естественнонаучных профессиональных
дисциплин



(Подпись) / В.В. Гаах
(Ф.И.О.)

Заместитель директора по учебно-
методической работе



(Подпись) / П.В. Пискунова
(Ф.И.О.)

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	стр. 2
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	2
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ	5
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	7
5. ПРИЛОЖЕНИЕ 1. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ УЧЕБНОЙ ДИСЦИПЛИНЫ	8

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины «ОП.05 Основы информационной безопасности»: формирование представлений об основах выбора материала с учетом его состава, структуры, термической обработки и достигающихся при этом эксплуатационных и технологических свойств, необходимых для приборостроения, а представления об основных технологических методах получения деталей из конструкционных материалов.

Дисциплина «ОП.05 Основы информационной безопасности» включена в обязательную часть общепрофессионального цикла образовательной программы.

1.2. Планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3.3 ПОП-П).

В результате освоения дисциплины обучающийся должен:

<i>Код ОК, ПК</i>	Уметь	Знать	Владеть навыками
ОК 01 ОК 02 ОК 05 ОК 09	- применять программное обеспечение для защиты от несанкционированного доступа; - применять программное обеспечение для защиты от вирусного заражения компьютера; - зашифровывать и дешифровывать сообщения различными методами	- основные понятия и определения, эволюция подходов к обеспечению информационной безопасности. - основы криптографии - основные методы и приемы защиты от несанкционированного доступа - компьютерные вирусы и антивирусные программы - криптографические методы защиты информации - организационно-правовое обеспечение информационной безопасности	-

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	Объем в часах	В т.ч. в форме практ. подготовки
Учебные занятия	64	66
<i>Курсовая работа (проект)</i>	-	-
Самостоятельная работа		-
Промежуточная аттестация (<i>дифференцированный зачет</i>)	2	-
Всего	66	66

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Основы безопасности информационных систем		6 /4	
Тема 1.1. Основные понятия. Угрозы безопасности	Практические занятия и лабораторные работы	4	ОК 01, ОК 02, ОК 05, ОК 09
	Практическое занятие №1. Определение основных принципов информационной безопасности (ИБ): целостности, конфиденциальность, доступности.	2	
	Практическое занятие №2. Определение угроз ИБ: информационные, программно-математические, физические и организационные угрозы.	2	
	Контрольная работа по теме « Основы безопасности информационных систем».	2	ОК 01, ОК 02, ОК 05, ОК 09
Раздел 2. Защита информации в АИС		60/58	
Тема 2.1. Основные принципы построения подсистемы защиты информации	Практические занятия и лабораторные работы	18	ОК 01, ОК 02, ОК 05, ОК 09
	Практическое занятие №3. Идентификация и аутентификация.	2	
	Практическое занятие №4. Создание электронной цифровой подписи.	2	
	Практическое занятие №5. Проверка электронной цифровой подписи.	2	
	Практическое занятие №6. Работа с криптографическими механизмами конфиденциальности, целостности и аутентичности информации.	2	
	Практическое занятие №7. Шифрование информации в одной из традиционных криптосистем.	2	
	Практическое занятие №8. Дешифрование информации.	2	
	Практическое занятие №9. Обнаружение и противодействие атакам.	2	
	Практическое занятие №10. Создание АРМ шифровальщика.	2	
	Контрольная работа/ тест	2	
Тема 2.2. Защита информации от	Практические занятия и лабораторные работы	10	ОК 01, ОК 02, ОК 05, ОК 09
	Практическое занятие №11. Использование основных принципов, средств и механизмов защиты информации от НСД .	2	

несанкционированного доступа (НСД)	Практическое занятие №12. Создание программ по защите информации.	2	
	Практическое занятие №13. Использование пароля с проверкой.	2	
	Практическое занятие №14. Создание программ по защите информации.	2	
	Практическое занятие №15. Использование пароля без проверки.	2	
Тема 2.3. Управление доступом в АИС	Практические занятия и лабораторные работы	16	ОК 01, ОК 02, ОК 05, ОК 09
	Практическое занятие №16. Анализ принципов организации разноуровневого доступа в АИС. Определение клиента, прав доступа, объекта доступа.	2	
	Практическое занятие №17. Работа с учетными записями пользователей АИС.	2	
	Практическое занятие №18. Обеспечение безопасности ресурсов с помощью разрешений NTFS для папок и файлов.	2	
	Практическое занятие №19. Планирование, установка и изменение разрешений NTFS.	2	
	Практическое занятие №20. Изменение параметров учетных записей.	2	
	Практическое занятие №21. Управление группами.	2	
	Практическое занятие №22. Настройка параметров безопасности операционной системы.	2	
	Контрольная работа/ тест	2	
Тема 2.4. Защита от воздействия вирусов	Практические занятия и лабораторные работы	8	ОК 01, ОК 02, ОК 05, ОК 09
	Практическое занятие №23. Реализация методов защиты от воздействия вирусов.	2	
	Практическое занятие №24. Использование современных антивирусных программ	2	
	Практическое занятие №25. Установка антивирусного программного обеспечения.	2	
	Практическое занятие №26. Работа с антивирусной программой.	2	
Тема 2.5. Организационно-правовое обеспечение ИБ	Практические занятия и лабораторные работы	10	ОК 01, ОК 02, ОК 05, ОК 09
	Практическое занятие №27. Использование организационных методов защиты информации.	2	
	Практическое занятие №28. Организация работ по обеспечению ИБ.	2	
	Практическое занятие №29. Определение порядка создания, утверждения и исполнения должностных инструкций.	2	
	Практическое занятие №30. Составление должностной инструкции.	2	
	Практическое занятие №31. Анализ концепции правового обеспечения ИБ РФ.	2	
Дифференцированный зачет		2	
Всего:		66/64	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Дисциплина реализуется в кабинете, оснащённом оборудованием и техническими средствами обучения:

Столы – 20 шт.

Стулья – 40 шт.

Комплект мебели для преподавателя – 1 шт.

Компьютер – 1 шт.

Аудиоколонки – 1 шт.

Экран настенный – 1 шт.

Доска ученическая – 1 шт. Проектор - 1 шт.

Комплект информационных стендов и стеллажей для наглядные пособия; раздаточные материалы.

3.2. Учебно-методическое обеспечение

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные и/или электронные издания

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с.

2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с..

3. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Нисов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с..

3.2.2. Дополнительные источники

1. Бабаш А. В., Баранова Е. К., Ларин Д. А. Информационная безопасность. История защиты информации в России. М.: КДУ. 2017. 736 с.

2. Баранова Е. К., Бабаш А. В. Основы информационной безопасности. Учебник. М.: РИОР. 2019. 202 с.

3. Богомазова Г. Н. Обеспечение информационной безопасности компьютерных сетей. М.: Academia. 2017. 224 с.

4. Бубнов А. А. Информационная безопасность и защита информации. М.: Academia. 2006. 256 с.

5. Бубнов А. А. Основы информационной безопасности. М.: Academia. 2018. 256 с.

6. Гилязова Р. Н. Информационная безопасность. Лабораторный практикум. Учебное пособие. М.: Лань. 2020. 44 с.

7. Гришина Н. В. Информационная безопасность предприятия. Учебное пособие. М.: Форум. 2015. 239 с.

8. Краковский Ю. М. Защита информации. Учебное пособие. М.: Феникс. 2017. 348 с.

9. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с..
10. Осавелюк Е. А. Информационная безопасность государства и общества в контексте деятельности СМИ. М.: Лань. 2020. 92 с.
11. Платонов В. В. Программно-аппаратные средства защиты информации. М.: Academia. 2020. 288 с.
12. Степченко И. Г., Погонишева Д. А., Ерохин В. В. Безопасность информационных систем. Учебное пособие. М.: Флинта. 2016. 184 с.

Интернет-ресурсы

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность <http://www.itsec.ru> –
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
11. Федеральный портал «Российское образование» www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоённости	Методы оценки
Знает: сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности.	Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)
Умеет: классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации;		

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. Общие положения

Фонд оценочных средств (ФОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины **ОП.05 Основы информационной безопасности**.

ФОС включают контрольные материалы для промежуточной аттестации в форме дифференцированного зачета в 4 семестре.

2. Результаты освоения дисциплины, подлежащие проверке

КОД	Освоенные умения, усвоенные знания
31	Понятие информационной безопасности, основные понятия и определения. Эволюция подходов к обеспечению информационной безопасности.
32	Организационно-правовое обеспечение информационной безопасности
33	Основы криптографии. Криптографические методы защиты информации
34	Основные методы и приемы защиты от несанкционированного доступа.
35	Компьютерные вирусы и антивирусные программы.
У1	Применять программное обеспечение для защиты от несанкционированного доступа
У2	Применять программное обеспечение для защиты от вирусного заражения компьютера
У3	Зашифровывать и дешифровывать сообщения различными методами

3. Структура контрольного задания

3.1. Дифференцированный зачет в 4 семестре проводится по результатам тестирования и выполнения практического задания.

Задание 1. Тестирование.

Проверяемые результаты обучения: 31, 32, 33, 34, 35.

Вопросы теста

1. Перечислите методы обеспечения информационной безопасности (ИБ).

- Организационные, морально-этические, законодательные, инженерно-технические, программно-аппаратные, криптографические
- Персональная ответственность руководителей, определение состава конфиденциальных сведений, наличие специализированной службы безопасности
- Препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение

2. К каким средствам относятся средства защиты, которые реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи. Эти нормы не являются обязательными, но несоблюдение их ведет обычно к потере авторитета и престижа человека?

- Морально-этические
- Организационные
- Принуждение

3. Назовите главные требования к организации эффективной работы системы защиты информации (СЗИ) фирмы.

- Организационные, морально-этические, законодательные, инженерно-технические, программно-аппаратные, криптографические
- Персональная ответственность руководителей, определение состава конфиденциальных сведений, определение порядка доступа персонала и наличие специализированной службы безопасности
- Препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение

4. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.)?

- Организационный
- Препятствие
- Управление доступом

5. Как называется метод защиты информации регулированием использования всех ресурсов системы (элементов БД, программных и технических средств)?
 - а) Определение состава конфиденциальных сведений
 - б) Программно-аппаратный
 - в) Управление доступом
6. Какие средства предназначены для противодействия средствам технической разведки и формирования рубежей охраны территории и здания с помощью технических средств?
 - а) Маскировка
 - б) Организационные
 - в) Инженерно-технические
7. Как называется метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности НСД к ней сводились бы к минимуму?
 - а) Принуждение
 - б) Организационный
 - в) Регламентация
8. К каким средствам относятся меры управленческого, режимного и технологического характера, побуждающие персонал соблюдать правила СЗИ фирмы?
 - а) Принуждение
 - б) Организационные
 - в) Инженерно-технические
9. Могут ли лица, проектирующие и модернизирующие систему защиты, контролирующие и анализирующие ее работу, быть пользователями этой системы ?
 - а) Не могут быть
 - б) Могут быть
10. Что является главным элементом любой, даже самой технически совершенной, СЗИ?
 - а) Подбор, расстановка и обучение персонала
 - б) Сознательность, обученность и ответственность персонала
 - в) Пропускной режим на территории, в здании и помещениях фирмы
11. Перечислите средства обеспечения ИБ.
 - а) Организационные, морально-этические, законодательные, инженерно-технические, программно-аппаратные, криптографические
 - б) Персональная ответственность руководителей, определение состава конфиденциальных сведений, наличие специализированной службы безопасности
 - в) Препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение
12. Как называется метод защиты информации регулированием использования всех ресурсов системы (элементов БД, программных и технических средств)?
 - а) Определение состава конфиденциальных сведений
 - б) Программно-аппаратный
 - в) Управление доступом
13. Какие средства предназначены для защиты информации в компьютерах и серверах?
 - а) Препятствие
 - б) Организационные
 - в) Программно-аппаратные
14. Как называется метод защиты информации путем ее криптографического закрытия?
 - а) Маскировка
 - б) Программно-аппаратный
 - в) Криптографический
15. К каким средствам относятся средства, предназначенные для защиты конфиденциальной информации методами криптографии?
 - а) Маскировка

- б) Криптографические
 - в) Программно-аппаратные
- 16. Какой организацией разрабатываются и меняются составные части криптографической защиты, коды, пароли и другие ее атрибуты?**
- а) ГОСТом
 - б) Инженерно-технической
 - в) Специализированной
- 17. Что нужно делать с содержанием составных частей элементов, методов и средств защиты информации в рамках любой системы защиты с целью предотвращения их раскрытия заинтересованным лицом?**
- а) Регулярно изменять
 - б) Шифровать
 - в) Ставить пароли
- 18. Как называется такой метод защиты, который побуждает пользователя и персонал системы не нарушать сложившиеся моральные и этические нормы (как регламентированные, так и "неписанные")?**
- а) Принуждение
 - б) Морально-этический
 - в) Побуждение
- 19. Допускается ли применение пользователями собственных систем шифровки?**
- а) Допускается
 - б) Не допускается
- 20. К каким средствам защиты относятся сооружения инженерной защиты (заборы, решетки, стальные двери, кодовые замки, сейфы и др.)?**
- а) Принуждение
 - б) Организационные
 - в) Инженерно-технические
- 21. Что является угрозой для компьютерной системы (КС)?**
- а) условия, предоставляющие потенциальную возможность для нанесения ей ущерба
 - б) внешние электромагнитные наводки
 - в) работа в автономном режиме
- 22. Как называются угрозы, направленные на изменение или полное уничтожение информации?**
- а) Угрозы нарушения целостности
 - б) Угрозы нарушения работоспособности
 - в) Угрозы нарушения конфиденциальности информации
- 23. Как называются угрозы, направленные на снижение работоспособности системы, либо на блокирование доступа к некоторым ресурсам?**
- а) Угрозы нарушения целостности
 - б) Угрозы нарушения работоспособности
 - в) Угрозы нарушения конфиденциальности информации
- 24. К какому типу угроз относятся угрозы, связанные с целенаправленными действиями нарушителя: служащего, посетителя, конкурента, наемника и т.д?**
- а) Случайные воздействия
 - б) Преднамеренные угрозы
 - в) Угрозы нарушения целостности
- 25. К какому типу угроз компонентам КС относятся угрозы, связанные с временным прекращением центральным процессором текущей работы для выполнения некоторых посторонних действий, по завершении которых процессор возвращается в прежнее состояние и продолжает прерванную работу?**
- а) Прерывание

- б) Перехват
 - в) Модификация
 - г) Подделка (фальсификация)
- 26. Как называется процесс, в результате которого злоумышленник может добавить некоторый фальшивый процесс в систему для выполнения нужных ему, но не учитываемых системой действий, либо подложные записи в файлы системы или других пользователей?**
- а) Прерывание
 - б) Перехват
 - в) Модификация
 - г) Подделка (фальсификация)
- 27. К какому типу относится прерывание, которое инициируется изнутри основной программы при помощи специальных команд процессора?**
- а) Программное
 - б) Аппаратное
 - в) Перехват
- 28. Что такое закладка?**
- а) Несанкционированное изменение структуры КС
 - б) Несанкционированный доступ в КС
 - в) Несанкционированное изменение программы в КС
- 29. Что является основной задачей на этапе эксплуатации КС?**
- а) Исключение ошибок и возможности внедрения закладок
 - б) Выявление закладок и ошибок, а также обеспечение целостности, неизменности структур
 - в) Дублирование информации
- 30. Что является универсальным средством проверки адекватности и работоспособности КС?**
- а) Дублирование
 - б) Тестирование
 - в) Многослойная «фильтрация»
- 31. Как называются угрозы, направленные на разглашение конфиденциальной или секретной информации, когда информация становится известной лицам, которые не должны иметь к ней доступ?**
- а) Угрозы нарушения целостности
 - б) Угрозы нарушения работоспособности
 - в) Угрозы нарушения конфиденциальности информации
- 32. К какому типу угроз относятся аварийные ситуации из-за стихийных бедствий и отключений электропитания, отказы и сбои аппаратуры, ошибки в программном обеспечении, ошибки в работе обслуживающего персонала и пользователей, помехи в линиях связи из-за воздействия внешней среды?**
- а) Случайные воздействия
 - б) Преднамеренные угрозы
 - в) Угрозы нарушения целостности
- 33. Как называется процесс, в результате которого злоумышленник получает доступ к программным средствам и различного рода физическим носителям информации?**
- а) Прерывание
 - б) Перехват
 - в) Модификация
 - г) Подделка (фальсификация)
- 34. Как называется процесс, в результате которого злоумышленник получает не только доступ к компонентам (БД, программам, аппаратным элементам) компьютерной системы, но и манипулирует ими (изменяет, видоизменяет)?**
- а) Прерывание
 - б) Перехват

- в) Модификация
 - г) Подделка (фальсификация)
- 35. К какому типу относится прерывание, которое возникает тогда, когда какое-либо устройство нуждается в экстренном обслуживании, и, как правило, такое прерывание - большая неожиданность для центрального процессора?**
- а) Программное
 - б) Аппаратное
 - в) Перехват
- 36. Как называется процесс получения нарушителем доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности?**
- а) Перехват
 - б) Модификация
 - в) Несанкционированный доступ
- 37. Что является основной задачей на этапе разработки и при модернизации КС?**
- а) Исключение ошибок и возможности внедрения закладок
 - б) Выявление закладок и ошибок, а также обеспечение целостности, неизменности структур
 - в) Дублирование информации
- 38. Как называется независимая (возможно разными организациями) разработка одного и того же блока алгоритма программы или устройства КС?**
- а) Дублирование
 - б) Тестирование
 - в) Многослойная «фильтрация»
- 39. Что предполагает поэтапное выявление ошибок и закладок определенного класса КС?**
- а) Дублирование
 - б) Тестирование
 - в) Многослойная «фильтрация»
- 40. Как влияет автоматизация процесса разработки на возможности внедрения закладок?**
- а) Не влияет
 - б) Существенно снижает
 - в) Повышает
- 41. Что является целью аутентификации электронных документов?**
- а) их защита от возможных видов злоумышленных действий (перехват, маскарад и т.д.)
 - б) статистическая обработка произвольного или фиксированного текста
 - в) присвоение субъектам доступа идентификаторов
- 42. Для чего используется ЭЦП?**
- а) для статистической обработки произвольного или фиксированного текста
 - б) для присвоения субъектам доступа идентификаторов
 - в) для аутентификации текстов, передаваемых по телекоммуникационным каналам
- 43. В чём состоит основное достоинство ЭЦП?**
- а) удостоверяет, что подписанный текст исходит от лица, поставившего подпись; не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом; гарантирует целостность подписанного текста
 - б) удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
 - в) гарантирует целостность подписанного текста
- 44. Из каких процедур состоит система ЭЦП?**
- а) процедура постановки подписи
 - б) процедура постановки подписи и процедура проверки подписи
 - в) процедура проверки подписи
- 45. Какой ключ используется в процедуре постановки подписи?**
- а) секретный ключ отправителя сообщения

- б) открытый ключ отправителя сообщения
 - в) секретный и открытый ключ отправителя сообщения
- 46. Какой ключ используется в процедуре проверки подписи?**
- а) секретный ключ отправителя сообщения
 - б) открытый ключ отправителя сообщения
 - в) секретный и открытый ключ отправителя сообщения
- 47. Какой ключ генерируется для каждого из абонентов, посылающих друг другу подписанные электронные документы?**
- а) секретный и открытый
 - б) секретный ключ
 - в) открытый ключ
- 48. Позволяет ли открытый ключ вычислить секретный ключ?**
- а) позволяет
 - б) не позволяет
 - в) в зависимости от степени секретности
- 49. Какую информацию содержит каждая подпись?**
- а) дату подписи; срок окончания действия ключа данной подписи; собственно цифровую подпись
 - б) дату подписи; информацию о лице, подписавшем файл; собственно цифровую подпись
 - в) дату подписи; срок окончания действия ключа данной подписи; информацию о лице, подписавшем файл; идентификатор подписавшего (имя открытого ключа); собственно цифровую подпись
- 50. Для чего предназначена хэш-функция?**
- а) для сжатия подписываемого документа М до нескольких десятков или сотен бит
 - б) для расшифровки секретного ключа
 - в) для получения открытого ключа отправителя
- 51. Какие карты являются наименее защищенными от фальсификации?**
- а) Виганд
 - б) магнитные
 - в) смарт-карты
- 52. Какие карты имеют максимальную защищенность?**
- а) смарт-карты
 - б) Виганд
 - в) штриховые
- 53. В каких идентификаторах идентификационный признак слабо или совсем не связан с личностью предъявителя?**
- а) атрибутивных
 - б) биометрических
 - в) автоматизированных
- 54. Какие идентификаторы основаны на использовании индивидуальных биологических особенностей человека?**
- а) атрибутивные
 - б) биометрические
 - в) автоматизированные
- 55. Что используется для биометрической идентификации человека?**
- а) пластиковые карты, папиллярные узоры пальцев, узоры сетчатки глаз, форма кисти руки
 - б) папиллярные узоры пальцев, узоры сетчатки глаз, форма кисти руки, особенности речи, форма и размеры лица, динамика подписи, ритм работы на клавиатуре
 - в) пластиковые карты, особенности речи, форма и размеры лица, динамика подписи, ритм работы на клавиатуре

56. Как называется метод идентификации, в котором папиллярные узоры считываются с пальца специальным сканером?

- а) Дактилоскопический
- б) Параметрический
- в) Биометрический

57. Какой метод идентификации используется в системах «Кордон» и «Папилон»?

- а) Биометрический
- б) Параметрический
- в) Дактилоскопический

58. Какие методы идентификации пока не нашли широкого применения?

- а) по ритму работы на клавиатуре
- б) по форме кисти рук
- в) по запаху и термическим характеристикам тела

59. В чём заключается достоинство биометрических методов идентификации?

- а) они не требуют дополнительных аппаратных затрат
- б) очень высокая вероятность обнаружения попыток несанкционированного доступа
- в) идентификация проводится с использованием всех признаков

60. На чём основывается идентификация по ритму работы на клавиатуре?

- а) на измерении скорости печати
- б) на измерении времени между последовательным нажатием двух клавиш
- в) на интенсивность нажатия клавиш

Критерии оценивания результатов тестирования

За правильный ответ на вопросы теста выставляется положительная оценка – 1 балл. За неправильный ответ на вопросы теста выставляется отрицательная оценка – 0 баллов. Общая сумма баллов за тест является одной частью общей оценки.

Критерии оценки:

- Оценка «5»: — от 90% и выше правильных ответов.
- Оценка «4»: — от 70% до 89% правильных ответов.
- Оценка «3»: — от 50% до 69% правильных ответов.
- Оценка «2»: — менее 50% правильных ответов.

Задание 2. Практическое задание.

Проверяемые результаты обучения: 31, 32, 33, 34, 35 У1, У2, У3.

Варианты практического задания

Задание 1: Зашифровать стихотворение в одной из традиционных криптосистем своего варианта.

Задание 2: Подготовить к отправке сообщение своего варианта с присоединённой ЭЦП, для этого:

- а) Зашифровать двоичным кодом текст сообщения своего варианта, используя данные таблицы.
- б) Вычислить хэш-функцию.
- с) Придумать и записать в тетрадь секретный ключ K_x .
- д) Вычислить значение ЭЦП.
- е) Записать сообщение M_1 , для удобства проверки отделять байты пробелом.
- ф) Вычислить значение открытого ключа отправителя K_u .

Задание 3: Проверьте диск С с помощью антивирусных пакетов и запишите время, затраченное программой на полную проверку диска.

Сравните и запишите в тетрадь количество обнаруженных вирусов и время проверки для разных антивирусных пакетов.

Пролечите флешку с вирусами с помощью любого пакета.

4. Критерии оценивания выполнения практического задания

Таблица 3

Оценка « отлично »	Практическое задание выполнено в полном объеме. Студент точно ответил на контрольные вопросы, свободно ориентируется в предложенном решении, может его модифицировать при изменении условия задачи.
Оценка « хорошо »	Практическое задание выполнено в полном объеме. Студент испытывает небольшие затруднения при ответе на теоретические вопросы, не на высоком уровне ориентируется в предложенном решении, испытывает затруднения при модификации условий задачи.
Оценка « удовлетворительно »	Студент правильно выполнил практическое задание, но может ответить только на общие вопросы по работе, плохо ориентируется в решении задачи, не может полностью объяснить полученные результаты.
Оценка « неудовлетворительно »	Студент не выполнил в полном объеме практическое задание и не может объяснить полученные результаты.

Общая оценка по итогам тестирования и выполнения практического задания складывается из двух оценок:

- оценки за тестирование;
- оценки по результатам выполнения практического задания.

Порядок выставления общей оценки дифференцированного зачета по дисциплине - по результатам тестирования и практического задания:

Оценка «**отлично**»

Оценка за тестирование	5	4				
Оценка за практическое задание	5	5				

Оценка «**хорошо**»

Оценка за тестирование	5	4	3	3		
Оценка за практическое задание	4	4	5	4		

Оценка «**удовлетворительно**»

Оценка за тестирование	5	4	3	2	2	2
Оценка за практическое задание	3	3	3	5	4	3

Оценка «**неудовлетворительно**»

Оценка за тестирование	5	4	3	2		
Оценка за практическое задание	2	2	2	2		

5. Время на подготовку и выполнение:

- подготовка 10 мин.;
- выполнение 1 час 30 мин.;
- оформление и сдача 20 мин.;
- всего 2 часа 0 мин.

6. Перечень материалов, оборудования и информационных источников, используемых для аттестации

Место выполнения задания: кабинет Информатики.

7. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

3.2.1. Основные печатные и/или электронные издания

- Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с.
- Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с..

3. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с..

3.2.2. Дополнительные источники

1. Бабаш А. В., Баранова Е. К., Ларин Д. А. Информационная безопасность. История защиты информации в России. М.: КДУ. 2017. 736 с.
2. Баранова Е. К., Бабаш А. В. Основы информационной безопасности. Учебник. М.: РИОР. 2019. 202 с.
3. Богомазова Г. Н. Обеспечение информационной безопасности компьютерных сетей. М.: Academia. 2017. 224 с.
4. Бубнов А. А. Информационная безопасность и защита информации. М.: Academia. 2006. 256 с.
5. Бубнов А. А. Основы информационной безопасности. М.: Academia. 2018. 256 с.
6. Гилязова Р. Н. Информационная безопасность. Лабораторный практикум. Учебное пособие. М.: Лань. 2020. 44 с.
7. Гришина Н. В. Информационная безопасность предприятия. Учебное пособие. М.: Форум. 2015. 239 с.
8. Краковский Ю. М. Защита информации. Учебное пособие. М.: Феникс. 2017. 348 с.
9. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с..
10. Осавелюк Е. А. Информационная безопасность государства и общества в контексте деятельности СМИ. М.: Лань. 2020. 92 с.
11. Платонов В. В. Программно-аппаратные средства защиты информации. М.: Academia. 2020. 288 с.
12. Степченко И. Г., Погоньшева Д. А., Ерохин В. В. Безопасность информационных систем. Учебное пособие. М.: Флинта. 2016. 184 с.

Интернет-ресурсы

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность <http://www.itsec.ru> –
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
11. Федеральный портал «Российское образование» www.edu.ru