МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»

УТВЕРЖДАЮ
Ректор СГТУ имени Гагарина Ю.А., профессор
_____ Е.Ю. Наумов
«24» декабря 2024 г.

Утверждено Ученым советом СГТУ имени Гагарина Ю.А.
Протокол № 18
от «26» декабря 2024 г.

**Дополнительная профессиональная программа повышения квалификации**
**«Организация и технология защиты информации»**
**по профилю специальности 10.02.05 – «Обеспечение информационной безопасности автоматизированных систем»**

Объем программы 40 часов

Саратов – 2024

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

## 1.1. Нормативные правовые основания разработки программы

Нормативную правовую основу разработки программы составляют:

– Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

– приказ Минтруда России от 12 апреля 2013 г. № 148н «Об утверждении уровней квалификаций в целях разработки проектов профессиональных стандартов»;

– приказ Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– Положение о порядке организации и осуществления образовательной деятельности по дополнительным профессиональным программам в ФГБОУ ВО «Саратовский государственный технический университет имени Гагарина Ю.А.»

– Программа разработана на основе требований ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденный приказом Минобрнауки РФ от 09.12.2016 №1553.

– Программа разработана с учетом профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации №525н от 14 сентября 2022.

## 1.2. Категория слушателей

Лица, желающие освоить дополнительную профессиональную программу, должны иметь среднее профессиональное или высшее образование, или получать среднее профессиональное или высшее образование. Наличие образования должно подтверждаться соответствующим документом.

## 1.3. Цель и планируемые результаты обучения

Целью реализации программы является совершенствование профессиональных компетенций, необходимых для выполнения следующих видов профессиональной деятельности и соответствующих профессиональных компетенций:

- Эксплуатация автоматизированных (информационных) систем в защищенном исполнении;
- Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

ПК 1. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 2. Осуществлять установку и настройку отдельных программных, программноаппаратных средств защиты информации.
ПК 3. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 4. Осуществлять тестирование функций отдельных программных и программноаппаратных средств защиты информации.

**Планируемые результаты обучения**

В результате освоения программы слушатель должен приобрести следующие знания и умения:
слушатель должен знать:

- Администрирование систем защиты информации автоматизированных систем
- Управление защитой информации в автоматизированных системах
- Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций
- Мониторинг и аудит защищенности информации в автоматизированных системах
- Установка и настройка средств защиты информации в автоматизированных системах
- Анализ уязвимостей внедряемой системы защиты информации

слушатель должен уметь:

- производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней
- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
- применять средства информационных технологий для решения профессиональных задач;
- использовать современное программное обеспечение
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации

## 1.4. Срок обучения

Трудоемкость обучения по данной программе – 40 часов, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя. Общий срок обучения – 5 недель.

## 1.5. Форма обучения и сведения о языка(х), на котором(ых) осуществляется обучение

Форма обучения – очная. Обучение проводится на русском языке.

## 1.6. Структурное подразделение, реализующее программу

Профессионально-педагогический колледж Федерального государственного бюджетного образовательного учреждения высшего образования «Саратовский государственный технический университет имени Гагарина Ю.А.»

# 2. СОДЕРЖАНИЕ ПРОГРАММЫ

## 2. 1. Учебный план

*Учебный план определяет перечень, трудоемкость, последовательность и распределение учебных предметов, курсов, дисциплин (модулей), практик, стажировок(ки) и иных видов учебной деятельности слушателей, а также указание видов аттестации.*

| № п/п | Наименование учебных курсов, дисциплин (модулей), практик, стажировок | Общая трудо-емкость, час. | Всего ауди-торных занятий, час. | В том числе | | СРС, час. | Коды профессиональных компетенций и трудовых функций | Форма контроля |
|---|---|---|---|---|---|---|---|---|
| | | | | лекции, час. | практи-ческие занятия, час. | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
| 1 | **Модуль 1. «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении** | | | | | | | |
| 1.1 | Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении | **8** | 8 | 2 | 6 | 0 | ПК.1 | - |
| 1.2 | Использование информационных технологий в профессиональной деятельности | **2** | 2 | - | 2 | 0 | ПК.1 | зачет |
| | **Итого в модуле:** | **10** | **10** | **2** | **8** | **0** | | |
| 2 | **Модуль 2. «Защита информации в автоматизированных системах программными и программно- аппаратными средствами»** | | | | | | | |
| 2.1 | Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации | **8** | 8 | 2 | 6 | 0 | ПК.2, ПК.3, ПК4 | |
| 2.2 | Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами | **12** | 12 | 8 | 4 | 0 | ПК.2, ПК.3, ПК.4 | зачет |
| 2.3 | Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации | **6** | 4 | 2 | 2 | 2 | ПК.2, ПК.3, ПК4 | - |
| | **Итого в модуле:** | **26** | **24** | **12** | **12** | **2** | | |
| | **Итоговая аттестация*** | **4** | | | | | Квалификационный экзамен | |
| | **Всего:** | **40** | | | | | | |

## 2.2. Календарный учебный график

| № п/п | Наименование учебных курсов, дисциплин (модулей), практик, стажировок | Виды учебной нагрузки | Всего часов | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 месяц | | | | 2 месяц | | | | ИТОГО |
| | | | 1 неделя | 2 неделя | 3 неделя | 4 неделя | 1 неделя | 2 неделя | 3 неделя | 4 неделя | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 1. | Тема 1.1 Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении | Л | 2 | | | | | | | | 2 |
| 2. | Практическое занятие №1. Администрирование автоматизированных систем в защищенном исполнении | П | 2 | | | | | | | | 2 |
| 3. | Практическое занятие №2. Установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем | П | 2 | | | | | | | | 2 |
| 4. | Практическое занятие №3. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление | П | 2 | | | | | | | | 2 |
| 5. | Тема 1.2 Практическая работа №4 Использование информационных технологий в профессиональной деятельности | П | | 2 | | | | | | | 2 |
| 6. | Тема 2.1 Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации | Л | | 2 | | | | | | | 2 |
| 7. | Практическое занятие №5. Установка и настройка программных и программно-аппаратных средств защиты информации | П | | 2 | | | | | | | 2 |
| 8. | Практическое занятие №6. Использование программных и программно-аппаратных средств для защиты информации в сети | П | | 2 | | | | | | | 2 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 9. | Практическое занятие №7. Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами | П | | | 2 | | | | | | 2 |
| 10. | Тема 2.2 Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. Использование типовых программных криптографических средств | Л | | | 4 | 4 | | | | | 8 |
| 11. | Практическое занятие №8. Развертывание VPN | П | | | 2 | | | | | | 2 |
| 12. | Практическое занятие №9. Развёртывание и настройка инфраструктуры открытого ключа с корпоративным центом сертификации | П | | | | 2 | | | | | 2 |
| 13. | Тема 2.3 Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации | Л | | | | 2 | | | | | 2 |
| 14. | Практическое занятие №9. Тестирование функций работоспособности программных и программно-аппаратных средств защиты информации | П | | | | | 2 | | | | 2 |
| 15. | Тема 2.3 Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации | С | | | | | 2 | | | | 2 |
| | **Итоговая аттестация** | | | | | | 4 | | | | 4 |
| | **Всего часов в неделю** | | **8** | **8** | **8** | **8** | **8** | | | | **40** |

**Обозначения:** Л - лекции, П - практические занятия, СРС - стажировка/самостоятельная работа

## 2.3. Режим занятий

4 часа в день, 2 раза в неделю – всего 8 часов в неделю

## 2.4. Рабочая программа

| **Наименование модулей, разделов (дисциплин) и тем** | **Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных работ, практических занятий (семинаров), самостоятельной работы, используемых образовательных технологий и рекомендуемой литературы** | **Объем часов (по учебному плану)** |
|---|---|---|
| **Рабочая программа к Модулю 1. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении** | | |
| Тема 1.1. Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении | Установка, адаптация и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы | 2 |
| Практическое занятие 1 | Администрирование автоматизированных систем в защищенном исполнении Конфигурирование, настройка компонент систем защиты информации автоматизированных систем, обеспечивать работоспособности АС. | 2 |
| Практическое занятие 2 | Установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем | 2 |
| Практическое занятие 3 | Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление | 2 |
| Тема 1.2 Использование информационных технологий в профессиональной деятельности | | |
| Практическое занятие 4 | Использование информационных технологий в профессиональной деятельности | 2 |
| Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы | 1. Костров Б.В. Сети и системы передачи информации: учебник/ Б.В. Костров, В.Н. Ручкин: (2-е изд.) (в электронном формате) 2019. https://academia-library.ru<br>2. Внуков, А. А. Основы информационной безопасности: защита | |

| Наименование модулей, разделов (дисциплин) и тем | Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных работ, практических занятий (семинаров), самостоятельной работы, используемых образовательных технологий и рекомендуемой литературы | Объем часов (по учебному плану) |
|---|---|---|
| | информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт[сайт]. — URL: https://urait.ru | |
| **Рабочая программа к Модулю 2. Защита информации в автоматизированных системах программными и программно- аппаратными средствами** | | |
| Тема 2.1 Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации | Установка и настройка программных и программно-аппаратных средств защиты информации | 2 |
| Практическое задание 5 | Установка и настройка программных и программно-аппаратных средств защиты информации | 2 |
| Практическое задание 6-7 | Использование программных и программно-аппаратных средств для защиты информации в сети | 4 |
| Тема 2.2. Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами | Защита автономных автоматизированных систем. Защита информации в локальных сетях. Задачи защиты. Объекты защиты. Планирование и реализация систем защиты. Методы защиты информации. Средства разграничения доступа. Протоколирование. Защита автономных автоматизированных систем. Основы защиты автономных автоматизированных систем. Защита программ от изучения. Вредоносное программное обеспечение. Защита программ и данных от несанкционированного копирования. Защита информации на машинных носителях. Аппаратные средства идентификации и аутентификации пользователей. Системы обнаружения атак и вторжений. Мониторинг систем защиты. Мониторинг систем защиты. Изучение мер защиты информации в информационных системах. Изучение современных программно-аппаратных комплексов | 8 |
| Практическое занятие 8 | Развертывание VPN<br>Использование типовых программных криптографических средств | 2 |

| Наименование модулей, разделов (дисциплин) и тем | Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных работ, практических занятий (семинаров), самостоятельной работы, используемых образовательных технологий и рекомендуемой литературы | Объем часов (по учебному плану) |
|---|---|---|
| Практическое задание 9 | Развёртывание и настройка инфраструктуры открытого ключа с корпоративным центом сертификации | 2 |
| Тема 2.3. Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации | Тестирование средств защиты информации в отдельных программных и программно-аппаратных средствах защиты информации | 2 |
| Практическое задание 10 | Тестирование функций работоспособности программных и программно-аппаратных средств защиты информации | 2 |
| Самостоятельная работа | Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации | 2 |
| Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы | 1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // ЭБС Юрайт [сайт].—URL: https://urait.ru<br>2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. - Москва : ИД "ФОРУМ" : ИНФРА-М, 2021. - 416 с. -(Среднее профессиональное образование). ISBN 978-5-8199-0754- | |
| Используемые образовательные технологии | Предусматривается решение профессиональных задач на компьютере. | |

## 3. ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

Оценка качества освоения программы включает текущий контроль знаний, промежуточную аттестацию обучающихся в форме проверки выполнения индивидуальных заданий, итоговую аттестацию в форме квалификационного экзамена.
Текущий контроль знаний и промежуточная аттестация проводится по результатам освоения разделов программы, выполнения практических заданий, предусмотренных учебным планом.
К итоговой аттестации допускаются лица, выполнившие требования, предусмотренные настоящей программой. Итоговая аттестация проводится для определения соответствия полученных знаний, умений и навыков программе обучения.

Итоговая аттестация производится в соответствии с критериями оценки:

| Процент результативности | Качественная оценка индивидуальных образовательных достижений |
|---|---|
| 90 ÷ 100 | отлично |
| 80 ÷ 89 | хорошо |
| 70 ÷ 79 | удовлетворительно |
| менее 70 | неудовлетворительно |

## 4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

| **Наименование специализированных аудиторий, кабинетов, лабораторий** | **Вид занятий** | **Наименование оборудования, программного обеспечения** |
|---|---|---|
| Кабинет информационной безопасности | лекции | компьютер, мультимедийный проектор, экран, доска |
| Лаборатория программных и программно-аппаратных средств | практические и занятия | ЦПУ: Процессор не менее 3,2 ГГц с поддержкой виртуализации или Аналог, не менее 6 физических ядер не менее 12 потоков, не менее 32 |

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятий | Наименование оборудования, программного обеспечения |
|---|---|---|
| защиты информации. | | ГБ ОЗУ, не менее 500 ГБ SSD со свободным местом не менее 300 ГБ, не менее 100 ГБ свободного места на этом же или дополнительных носителях (HDD/SSD) для хранения резервных образов, в случае ноутбука необходим дополнительный монитор, ОС с графическим интерфейсом, ПО для виртуализации с поддержкой драйверов для операционных систем семейства UNIX, офисный пакет, текстовый редактор с подсветкой синтаксиса, браузер, ssh-клиент, sftp/scp-клиент, ftp-клиент<br>ПО для просмотра документов в формате PDF<br>ПО для архивации<br>ПО для офисной работы<br>ПО среда разработки с библиотеками<br>Система управления базами данных |

## 5. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

### 5.1. Сведения о штатных научно-педагогических работниках (внешних совместителях), привлекаемых к реализации программы

| № п/п | Ф.И.О. преподавателей | Ученое звание, степень, должность | Год рождения | Общий стаж работы | Важнейшие публикации за последние пять лет *(не более трех)* |
|---|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | Закревская Ольга Васильевна | Преподаватель ППК СГТУ имени Гагарина Ю.А. | 1975 | 24 | Закревкая О.В. Имитационное моделирование работы компьютерной СЕТИ В CISCO PACKET TRACER»; / Закревкая О.В., Е.Р. Кожанова, Л.В. Кожанов https://elibrary.ru/item.asp?id=44172751 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Саратов, 2020.-212стр.<br>2 Закревская О.В. IT-РИНГ/ [Электронный ресурс] https://fond21veka.ru/publication/20/48/337448/ .2021 |

### 5.2. Использование наглядных пособий и других учебных материалов при реализации программы

1. Мультимедийные презентации к лекционным и практическим занятиям.
2. Электронный образовательный ресурс https://profspo.ru
3. Электронный образовательный ресурс https://urait.ru
4. Электронная образовательная среда https://eios-ppk.sstu.ru

## 6. СОСТАВИТЕЛИ ПРОГРАММЫ

Класс Ю.Н., преподаватель высшей категории ППК СГТУ имени Гагарина Ю.А. , Исакова М.И., начальник учебно-производственного отдела ППК СГТУ имени Гагарина Ю.А.

| | |
|---|---|
| Руководитель Института дополнительного и довузовского образования | С.В. Аношина |
| Заместитель руководителя<br>Института дополнительного и довузовского образования | Н.А. Трофимова |
| Директор ППК СГТУ имени Гагарина Ю.А. | Т.И. Кузнецова |
| Начальник отдела среднего профессионального образования | А.Л. Задорожная |
| Руководитель программы, преподаватель высшей категории<br>ППК СГТУ имени Гагарина Ю.А. | Ю.Н. Класс |

**Фонд оценочных средств**
**по дополнительной профессиональной программе повышения квалификации**
**«Организация и технология защиты информации»**

## 1.Паспорт фонда оценочных средств

Настоящий фонд оценочных средств (далее – ФОС) предназначен для организации и проведения аттестации по дополнительной профессиональной программе повышения квалификации «Организация и технология защиты информации».

ФОС разработан на основе требований к результатам освоения дополнительной профессиональной программе повышения квалификации «Организация и технология защиты информации».

| № п\п | Контролируемые модули (дисциплины) | Оценочные средства для текущего контроля | |
|---|---|---|---|
| | | Вид | Количество |
| | | 1.Промежуточная аттестация | |
| 1. | Модуль 1. «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении | Итоговая практическая работа №1 | 1 |
| 2. | Модуль 2. «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» | Итоговая практическая работа №2 | 1 |
| | | 2.Итоговая аттестация | |
| | Итоговая аттестация (экзамен) | Комплект билетов для проведения экзамена | 1 |
| | | Итого: | 3 |

**Фонд оценочных средств для промежуточной аттестации**

**Итоговая практическая работа №1 по модулю**
**«Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»**

**Задание:** Изучите возможности системы защиты информации от несанкционированного доступа «Страж NT»:

- назначение,
- запуск и регистрация системы защиты,
- создание пользователей,
- реализация мандатной модели разграничения доступа,
- реализация дискреционной модели разграничения доступа,
- обеспечение замкнутости программной среды,
- контроль целостности,
- организация учета съемных носителей информации,
- регистрация событий,
- гарантированное удаление данных.

**Материально-техническое обеспечение необходимое для выполнения задания:**

Персональный компьютер в составе:

ЦП с тактовой частотой - не менее 2400 мГц, физический ядер – не менее 4, техпроцесс – не старше 14 нм, объём кэш-памяти – не менее 6 Мб.

ОЗУ объём – не менее 8 Гб, частота – не менее 1800 мГц.

Накопитель объём – не менее 500 Гб, скорость чтения/записи – не менее 500 МБ/с Монитор, клавиатура, мышь, сетевой адаптер с выходом в сеть Интернет.
Поддержка виртуализации.

Программное обеспечение:

Операционная система Windows 10, Oracle VM VirtualBox, пакет офисных приложений с поддержкой форматов .doc/.docx/.xls/.xlsx, архиватор с поддержкой формата .rar, дистрибутивы (установочные комплекты) операционных систем Windows XP, Windows 7, Windows 10, Ubuntu 20.04.04, комплексы СЗИ: Страж NT, Dallas Lock, Secret NET 5.0-C.

**Задание:** Изучите возможности системы защиты информации от несанкционированного доступа «Dallas Lock»:

- назначение,
- запуск и регистрация системы защиты,
- создание пользователей,
- реализация мандатной модели разграничения доступа,
- реализация дискреционной модели разграничения доступа,
- обеспечение замкнутости программной среды,
- контроль целостности,
- регистрация событий,
- гарантированное удаление данных,
- печать штампа,
- реализация запрета загрузки ПЭВМ в обход.

**Материально-техническое обеспечение необходимое для выполнения задания:**

Персональный компьютер в составе:

ЦП с тактовой частотой - не менее 2400 мГц, физический ядер – не менее 4, техпроцесс – не старше 14 нм, объём кэш-памяти – не менее 6 Мб.

ОЗУ объём – не менее 8 Гб, частота – не менее 1800 мГц.

Накопитель объём – не менее 500 Гб, скорость чтения/записи – не менее 500 МБ/с Монитор, клавиатура, мышь, сетевой адаптер с выходом в сеть Интернет.

Поддержка виртуализации.

Программное обеспечение:

Операционная система Windows 10, Oracle VM VirtualBox, пакет офисных приложений с поддержкой форматов .doc/.docx/.xls/.xlsx, архиватор с поддержкой формата .rar, дистрибутивы (установочные комплекты) операционных систем Windows XP, Windows 7, Windows 10, Ubuntu 20.04.04, комплексы СЗИ: Страж NT, Dallas Lock, Secret NET 5.0-C.

**Задание: Изучите возможности системы защиты информации от несанкционированного доступа «Secret NET 5.0-C»:**

- назначение,
- запуск и регистрация системы защиты,
- создание пользователей,
- реализация мандатной модели разграничения доступа,
- реализация дискреционной модели разграничения доступа,
- обеспечение замкнутости программной среды,
- контроль целостности,
- регистрация событий,
- гарантированное удаление данных,
- печать штампа,
- настройка механизма шифрования.

**Материально-техническое обеспечение необходимое для выполнения задания:**

Персональный компьютер в составе:

ЦП с тактовой частотой - не менее 2400 мГц, физический ядер – не менее 4, техпроцесс – не старше 14 нм, объём кэш-памяти – не менее 6 Мб.

ОЗУ объём – не менее 8 Гб, частота – не менее 1800 мГц.

Накопитель объём – не менее 500 Гб, скорость чтения/записи – не менее 500 МБ/с Монитор, клавиатура, мышь, сетевой адаптер с выходом в сеть Интернет.
Поддержка виртуализации.

Программное обеспечение:

Операционная система Windows 10, Oracle VM VirtualBox, пакет офисных приложений с поддержкой форматов .doc/.docx/.xls/.xlsx, архиватор с поддержкой формата .rar, дистрибутивы (установочные комплекты) операционных систем Windows XP, Windows 7, Windows 10, Ubuntu 20.04.04, комплексы СЗИ: Страж NT, Dallas Lock, Secret NET 5.0-C.

**Итоговая практическая работа №2 по модулю**
**«Защита информации в автоматизированных системах программными и программно - аппаратными средствами»**

**Задание:** Сформировать полное описание АС для выполнения последующих работ по защите информации на выбранной АС.
В практической работе необходимо придумать организацию, можно взять реальную организацию/компанию/предприятие , в которой используются автоматизированные системы.
Придумать 5 разных типов сотрудников, которые работают в этой организации с использованием автоматизированной системы. Эти сотрудники должны работать с разной информацией в автоматизированной системе.
Нужно описать организацию, ее специфику в нескольких предложениях.
Описать сотрудников и то с какой информацией они работают.
Описать какие происходят процессы в выбранной АС (ввод, обработка, вывод, обратная связь).
Отчет должен содержать:

- Описание организации, ее специфика.
- Описание перечня защищаемых информационных ресурсов АС;
- Описание перечня лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий; - Описание процессов в АС.

**Материально-техническое обеспечение необходимое для выполнения заданий:**

Персональный компьютер в составе:

ЦП с тактовой частотой - не менее 2400 мГц, физический ядер – не менее 4, техпроцесс – не старше 14 нм, объём кэш-памяти – не менее 6 Мб.
ОЗУ объём – не менее 8 Гб, частота – не менее 1800 мГц.

Накопитель объём – не менее 500 Гб, скорость чтения/записи – не менее 500 МБ/с Монитор, клавиатура, мышь, сетевой адаптер с выходом в сеть Интернет.
Поддержка виртуализации.

Программное обеспечение:

Операционная система Windows 10, Oracle VM VirtualBox, пакет офисных приложений с поддержкой форматов .doc/.docx/.xls/.xlsx, архиватор с поддержкой формата .rar, дистрибутивы (установочные комплекты) операционных систем Windows XP, Windows 7, Windows 10, Ubuntu 20.04.04

**Фонд оценочных средств для итоговой аттестации по дополнительной профессиональной программе повышения квалификации «Организация и технология защиты информации»**

Итоговая аттестация по Квалификационный экзамен направлен на определение уровня освоения выпускником материала, предусмотренного образовательной программой, и степени сформированности профессиональных умений и навыков путем проведения независимой экспертной оценки выполненных выпускником практических заданий в условиях реальных или смоделированных производственных процессов. Квалификационный экзамен состоит из двух частей: теоретической и практической.

**Перечень вопросов для теоретической части Квалификационного экзамена**

2. Охарактеризуйте основные этапы процесса информационного поиска.
3. Перечислите основные и технологические объекты, используемые при поиске.
4. Определите назначение «обратной связи» в процессе информационного поиска.
5. Охарактеризуйте основные интерфейсные средства подготовки и модификации поисковых запросов.
6. Охарактеризуйте основные интерфейсные средства развития поисковых запросов.
7. Приведите типологию сценариев формирования выражения поискового запроса на ИПЯ.
8. Охарактеризуйте сценарии типа «укажи и выбери».
9. Охарактеризуйте сценарии типа «укажи и получи».
10. Дайте характеристику интерфейсным средствам использования тезаурусных связей при модификации поисковых запросов.
11. Охарактеризуйте интерфейсные средства использования терминологических структур при подготовке и модификации запросов.
12. Перечислите информационные объекты, используемые для реализации технологии «обратной связи» в процессе информационного поиска.

13. Перечислите типы информационной потребности пользователя и определите их связь с уровнями информационных объектов.
14. Дайте сравнительную оценку характера деятельности человека и компьютерной системы.
15. Приведите основные процессы в уровневой модели взаимодействия пользователя и системы.
16. Дайте определение понятия «интерфейс пользователя».
17. Охарактеризуйте модели взаимодействия пользователя с АИПС и базой данных.
18. Охарактеризуйте влияние интерфейсных средств на адаптацию пользователя.
19. Приведите примеры диалоговых интерфейсных средств обучения пользователя работе с АИПС и БД.
20. Виртуальная частная сеть. Функции, назначение, принцип построения..
21. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.
22. Основные типы угроз. Модель нарушителя.
23. Классификация сетевых мониторов.
24. Безвозвратное удаление данных. Принципы и алгоритмы.
25. Использование сетевых снифферов в качестве систем обнаружения атак и вторжений .

## Перечень заданий для практической части Квалификационного экзамена

**Задание 1:**

С помощью технологии виртуальных машин для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах
(Главный офис — виртуальные машины, Офис филиал — виртуальные машины).

При выполнении заданий необходимо при помощи текстового редактора, сформировать отчет, в котором представить скриншоты ключевых настроек. В ходе выполнения данного задания нужно установить основное ПО на рабочие станции будущей защищенной сети, задать пароли пользователей и администраторов сети.

Для правильной работы сети надо создать или убедиться в наличии 4 сетей: Host only или внутренняя сеть адаптер для сети центрального офиса Host only или внутренняя сеть адаптер для сети филиала
Host only или внутренняя сеть адаптер для сети межсетевого взаимодействия;
Host only адаптер, NAT или Bridge для виртуального «Интернета».
IP адреса защищенных сетей:
Центральный офис «Сеть 1 ЦО»: 172.16.224.224/27 Офис филиал «Сеть 1 Филиал»: 10.10.20.128/25 Офис сеть 2 «Сеть 2 Офис»: 192.168.88.64/26
«Интернет» для всех координаторов: 10.8.248.0/24 Адреса выбираются самостоятельно из указанного диапазона.

В связи с особенностями работы системы на различных версиях пользовательских или серверных ОС, может потребоваться установка компонентов системы вручную (например, БД, сервер ЦУС, клиент ЦУС) используя пакеты MSI в подпапках дистрибутивов.

**Задача 1.1** Установить базу данных MSSQL на виртуальную машину Net1- Open (незащищенный узел).
Необходимые приложения: отсутствуют.

**Задание 2:**

Развертывание ПК Administrator в качестве центра сертификации Установить и настроить рабочее место администратора (на базе виртуальной машины Net1-AdminCA (ЦО)): Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД. Установить клиент ЦУС на ВМ Net1-Open (незащищенный узел).

**Задача 2.1 .** Инициализация VPN Coordinator и установка ПО VPN Client
На виртуальной машине Net1-AdminCA (ЦО) установить ПО Client (Пользовательская или серверная ОС), рабочее место администратора, на виртуальной машине Net1-Coord (ЦО) инициализировать Coordinator HW-VA. Задача 2.3 .
Инициализация VPN Coordinator и установка ПО VPN Client для организации сети филиала

На виртуальной машине Net2-Coord (филиал) инициализировать Coordinator HW-VA, на виртуальной машине Net2-Client (филиал) установить ПО Client, рабочее место пользователя. В отчете необходимо зафиксировать процесс установки скриншотами форм.

**Задача 2.2** Развертывание удостоверяющего центра в составе защищенной сети
Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

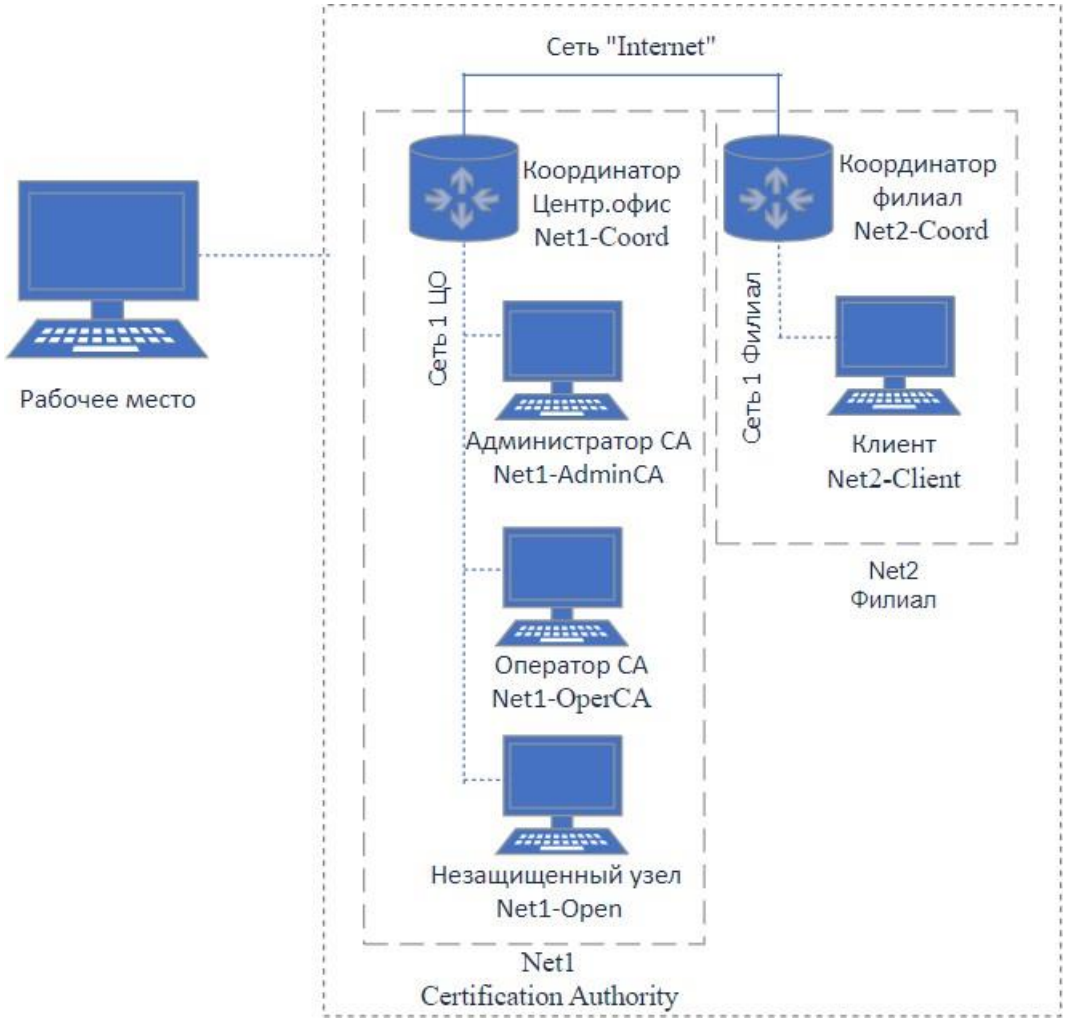


Рисунок 1 Схема защищенной сети

## Критерии оценок квалификационного экзамена

Схема оценивания представлена в таблице:

| | Оценка | Критерии |
|---|---|---|
| **Схема оценивания** | **5** | 1. Ответил на теоретический вопрос в полной мере. Демонстрирует глубокое, полное знание и понимание программного материала<br>2. Практическая часть: действие (операция) выполнено в полной мере согласно установленным требованиям |
| | **4** | 1. Ответил на теоретический вопрос полной мере. Недостаточно последовательно, но самостоятельно раскрывает основное содержание вопроса<br>2. Практическая часть: действие (операция) выполнено, но ниже установленных требований (имеются незначительные ошибки) |
| | **3** | 1. Ответил на теоретический вопрос не в полной мере. Излагает программный материал фрагментарно, не всегда последовательно.<br>2. Практическая часть: действие (операция) выполнено, но ниже установленных требований (имеются значительные ошибки) |
| | **2** | 1. Слушатель демонстрирует незнание и непонимание программного материала.<br>2.Практическая часть: действие (операция) не выполнено, результат отсутствует |