Муниципальное автономное общеобразовательное учреждение города Новосибирска
«Лицей №22 «Надежда Сибири»
Главный корпус на Советской: г. Новосибирск, ул. Советская, 63, тел. 222-35-15,
e-mail: l_22@edu54.ru
Корпус 99 на Чаплыгина: г. Новосибирск, ул. Чаплыгина, 59, тел. 223-74-15

РАССМОТРЕНО на заседании инженерной кафедры протокол № 1 от 25.08.2025 Кириленко К.А. *ФИО руководителя кафедры*	СОГЛАСОВАНО Заместитель директора Н.А.Данилова от 29.08.2025

РАБОЧАЯ ПРОГРАММА

Информатика. Компьютерные сети и информационная безопасность

10 «ИП» класса

(уровень среднего общего образования)

Разработчик:

Кириленко Ксения Алексеевна

2025

Рабочая программа по учебному предмету «Информатика. Компьютерные сети и информационная безопасность (предметная область «Математика и информатика») (далее соответственно – программа по компьютерным сетям и информационной безопасности, компьютерные сети и информационная безопасность) составлена на основе Федеральной рабочей программы по информатике и является авторской, включает пояснительную записку, содержание обучения, планируемые результаты освоения программы по компьютерным сетям и тематическое планирование.

Пояснительная записка отражает общие цели и задачи изучения компьютерных сетей и информационной безопасности, место в структуре учебного плана, а также подходы к отбору содержания, к определению планируемых результатов.

Содержание обучения раскрывает содержательные линии, которые предлагаются для обязательного изучения в 10 классе на уровне среднего общего образования.

Планируемые результаты освоения программы по компьютерным сетям и информационной безопасности включают личностные, метапредметные результаты за период обучения в 10 классе на уровне среднего общего образования, а также предметные достижения обучающегося.

1. Пояснительная записка

Общая характеристика учебного предмета " Компьютерные сети и информационная безопасность "

Компьютерные сети и информационная безопасность представляют собой фундаментальную и критически важную междисциплинарную область, объединяющую информатику, телекоммуникации и правоведение, направленную на создание, управление и защиту цифровой инфраструктуры современного мира. Изучение основ сетевых технологий и кибербезопасности в школе открывает учащимся возможность не просто быть пассивными пользователями, а стать архитекторами и защитниками цифрового пространства, развивая глубокое понимание принципов передачи данных и продвинутые навыки системного администрирования, лежащие в основе глобального интернета, облачных сервисов и безопасной коммуникации.

Функциональная значимость предмета для школьников заключается в освоении фундаментальных принципов построения и функционирования сетей, включая такие ключевые концепции, как модель OSI/TCP-IP, IP-адресация, маршрутизация, DNS, а также основы криптографии, аутентификации и защиты от угроз. Эти знания переводят абстрактные представления о «всемирной паутине» в конкретные технические реализации, позволяя решать прикладные задачи из области системного администрирования, DevOps, пентеста и обеспечения безопасности персональных данных.

Знание принципов сетей и информационной безопасности и умение применять инструменты, такие как Wireshark, Nmap или Cisco Packet Tracer, важно для каждого школьника, стремящегося понять, как устроено цифровое взаимодействие в

современном мире. Понимание того, как пакет данных путешествует от отправителя к получателю, какие уязвимости возникают на его пути и как их устранить, помогает учащимся развивать системное и аналитическое мышление, а также способность к проектированию отказоустойчивых и защищенных систем.

Сетевые симуляторы и инструменты анализа, выполняя свои основные функции, позволяют учащимся абстрагироваться от дорогостоящего физического оборудования и сосредоточиться на концептуальном проектировании сетевой архитектуры. Они предоставляют безопасную sandbox-среду для моделирования работы коммутаторов, маршрутизаторов и протоколов, что дает возможность сосредоточиться на постановке задачи, анализе трафика и поиске уязвимостей, что является ключевым этапом в любой профессиональной деятельности, связанной с сетевыми технологиями.

Обучение компьютерным сетям и безопасности направлено на развитие интеллектуальных и технических способностей учащихся, включая умение работать с сетевыми стеками протоколов, настраивать сервисы, проводить аудит безопасности, оценивать риски и реагировать на инциденты. Это способствует развитию критического и предупредительного мышления, понимания векторов кибератак и методов защиты, что является crucial для успешного обучения и дальнейшей профессиональной реализации в сфере кибербезопасности и сетевой инженерии.

Содержание программы ориентировано также на развитие функциональной и правовой грамотности учащихся, включая умение читать и понимать сетевые диаграммы и техническую документацию RFC, использовать базовые средства шифрования, понимать принципы действия вредоносного ПО, оценивать этические и правовые последствия кибератак, а также применять полученные знания для обеспечения собственной цифровой гигиены и защиты приватности, расширяя свои компетенции и профессиональные горизонты в эпоху тотальной цифровизации.

Цели и задачи изучения учебного предмета «Компьютерные сети и информационная безопасность».

Изучение Компьютерных сетей и информационной безопасности направлено на достижение следующих целей:

- Формирование целостного представления о компьютерных сетях как о фундаментальной основе цифрового мира, связывающей теоретические модели передачи данных (такие как OSI и TCP/IP) с их практической реализацией для обеспечения коммуникации между устройствами и глобального доступа к информации.
- Развитие компетенций в области проектирования, анализа и защиты сетевой инфраструктуры — от базовых понятий IP-адресации и DNS до сложных задач настройки виртуальных частных сетей (VPN), межсетевых экранов и систем обнаружения вторжений с использованием современных симуляторов (Cisco Packet Tracer, GNS3) и инструментов анализа (Wireshark, Nmap).

- Стимулирование интереса к исследовательской и инженерной деятельности в сферах сетевой инженерии, DevOps и кибербезопасности через моделирование реальных сетевых сценариев, анализ уязвимостей и разработку стратегий защиты от современных киберугроз.

Задачи изучения предмета:

- Развивать системное и аналитическое мышление через понимание и практическую реализацию сетевых протоколов (HTTP/S, TCP, UDP, ICMP), анализ сетевого трафика и диагностику неисправностей в работе сети.
- Сформировать навыки сквозной проектной деятельности в области сетевых технологий и безопасности: от проектирования топологии сети и расчета IP-подсетей до настройки сервисов, тестирования на проникновение и разработки политик безопасности.
- Воспитывать критическое и ответственное мышление, понимая ценность и уязвимость данных, принципы конфиденциальности, целостности и доступности (CIA-триада), а также этические и правовые последствия кибератак и неправомерного использования сетевых ресурсов.
- Развивать умение самостоятельного освоения сложного инструментария: работать с технической документацией (RFC), использовать командную строку для диагностики (ping, tracert, ipconfig, netstat), изучать и применять актуальные методы защиты и средства автоматизации (например, с использованием Python для сетевых задач), активно участвуя в профессиональных сообществах, посвященных информационной безопасности.

Особенности классов

Рабочая программа по предмету «Информатика. Компьютерные сети и информационная безопасность» для 10-го «ИП» класса предназначена для углубленного изучения учащимися информационно-технологического профиля в группе «Информационная безопасность». На изучение данного модуля отведено 33 часа в 10-м классе.

Место предмета в учебном плане лицея

Учебный план на изучение «Информатика. Компьютерное зрение» в 10 «ИП» классе среднего общего образования отводит 1 учебный час в неделю (всего 33 учебных часов) за счёт части, формируемой участниками образовательных отношений.

Учебный год	Количество часов
	10 «ИП»
2025/2026	33

К тематическому планированию применяется модульный принцип построения образовательной программы, что позволяет выстраивать индивидуальную образовательную парадигму и обеспечивать саморазвитие при индивидуальном темпе работы с учебным материалом, контроль и самоконтроль знаний.

Используемые образовательные технологии, в том числе дистанционные

Обучение искусственному интеллекту может осуществляться с использованием дистанционных образовательных технологий (далее ДОТ), которое предполагает как самостоятельное прохождение учебного материала учеником, так и с помощью сопровождения учителя. При применении ДОТ используются платформы: лицейская платформа дистанционного обучения Moodle, ФГИС «Моя школа», ГИС «Электронная школа» Новосибирской области.

При реализации рабочей программы могут быть использованы материалы для подготовки к профилям олимпиады КД НТИ и стандартов Всероссийского чемпионатного движения по профессиональному мастерству «Профессионалы».

Информация о промежуточной аттестации

Промежуточная аттестация осуществляется по окончании учебного модуля с целью проверки степени и качества усвоения материала по результатам изучения тематических модулей и проводится в форме аттестационных работ.

Текущий контроль осуществляются с целью проверки степени и качества усвоения материала в ходе его изучения в следующих формах: самостоятельных и проверочных работ.

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением об осуществлении текущего контроля успеваемости и промежуточной аттестации обучающихся, их формах, периодичности и порядке проведения муниципального автономного общеобразовательного учреждения города Новосибирска «Лицей № 22 «Надежда Сибири» (протокол педагогического совета №1 от 29.08.2023).

Итоговая аттестация проводится в соответствии с законодательством РФ.

Промежуточная аттестация
по компьютерным сетям и информационной безопасности в 10 «ИП» классе

№ модульной	**Название модуля**	**Количество часов в модуле**	**Номер урока ПА**	**Форма ПА**
МР № 1	Расчет IP-адресов и схемы топологий.	8	8	Практическая работа
МР № 2	Схемы маршрутизации, работа с DNS и VPN.	8	16	Практическая работа
МР № 3	Анализ угроз,	8	24	Практическ

	схемы защиты, тестирование.			ая работа
МР № 4	Анализ предложенного сценария (школьная/домашняя/корпоративная сеть), определение топологии, настройка адресации, выявление угроз безопасности и предложение мер защиты.	9	33	Практическая работа

2. Содержание учебного предмета

Модуль 1 «Расчет IP-адресов и схемы топологий.»

Понятие сети, виды сетей (LAN, MAN, WAN), цели изучения дисциплины. Сетевые карты, кабели, маршрутизаторы, коммутаторы, точки доступа. Шина, звезда, кольцо, смешанные топологии; достоинства и недостатки. 7 уровней модели, их назначение, примеры протоколов. Основные уровни, сравнение с OSI, ключевые протоколы. Ethernet, IP, TCP, UDP — назначение и особенности. IP-адреса, маски подсетей, MAC-адреса.

Модуль 2 «Схемы маршрутизации, работа с DNS и VPN.»

Особенности построения, пример домашней сети. Принципы работы Интернета, провайдеры, магистральные сети. Маршрутизатор, коммутатор, точка доступа, их функции. Работа системы доменных имен, основные принципы маршрутизации. Wi-Fi, Bluetooth, мобильные сети; безопасность Wi-Fi. E-mail, WWW, FTP, облачные сервисы. Принципы работы, защита трафика, примеры использования.

Модуль 3 «Анализ угроз, схемы защиты, тестирование»

Определение ИБ, основные угрозы и принципы защиты. Вирусы, черви, трояны, шпионские программы; способы защиты. Пароли, шифрование, антивирусы, межсетевые экраны. Симметричное и асимметричное шифрование, цифровая подпись. DDoS, фишинг, перехват трафика, социальная инженерия. Методы проверки подлинности пользователей, роли и права доступа. WPA/WPA2, угрозы Wi-Fi, защита домашних и школьных сетей.

Модуль 4 «Анализ предложенного сценария (школьная/домашняя/корпоративная сеть), определение топологии, настройка адресации, выявление угроз безопасности и предложение мер защиты»

Методы бэкапа, облачное хранение, стратегии защиты данных. Парольная политика, контроль доступа, правила пользователей. Законодательство РФ, GDPR, правила хранения и обработки. Методы обмана, примеры атак, правила безопасности.

Защита аккаунтов, работа с соцсетями, безопасное поведение. Антивирусы, обновления, правила установки ПО, мобильная безопасность. Киберугрозы, кибервойны, искусственный интеллект в безопасности. Построение небольшой локальной сети (виртуально или на схеме), настройка IP-адресов, проверка связи, настройка пароля Wi-Fi и межсетевого экрана.

Планируемые образовательные результаты освоения учебного предмета Искусственный интеллект

Личностные результаты

1. сформированность мировоззрения, соответствующего современному уровню развития науки и техники;
2. готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности;
3. навыки сотрудничества со сверстниками, детьми младшего возраста, взрослыми в образовательной, учебно-исследовательской, проектной и других видах деятельности;
4. эстетическое отношение к миру, включая эстетику научного и технического творчества;

Метапредметные результаты:

1.2.5	Анализировать полученные в ходе решения задачи результаты, критически оценивать их достоверность, прогнозировать изменение в новых условиях
1.2.6	Уметь переносить знания в познавательную и практическую области жизнедеятельности; уметь интегрировать знания из разных предметных областей; осуществлять целенаправленный поиск переноса средств и способов действия в профессиональную среду
1.2.7	Способность и готовность к самостоятельному поиску методов решения практических задач, применению различных методов познания; ставить и формулировать собственные задачи в образовательной деятельности и жизненных ситуациях; ставить проблемы и задачи, допускающие альтернативные решения; выдвигать новые идеи, предлагать оригинальные подходы и решения; разрабатывать план решения проблемы с учетом анализа имеющихся материальных и нематериальных ресурсов
1.3	Работа с информацией
1.3.1	Владеть навыками получения информации из источников разных типов, самостоятельно осуществлять поиск, анализ, систематизацию и интерпретацию информации различных видов и форм представления
1.3.2	Создавать тексты в различных форматах с учетом назначения информации и целевой аудитории, выбирая оптимальную форму представления и визуализации
1.3.3	Оценивать достоверность, легитимность информации, ее соответствие правовым и морально-этическим нормам
1.3.4	Использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности
1.3.5	Владеть навыками распознавания и защиты информации, информационной безопасности личности
2	Коммуникативные УУД
2.1	Общение
2.1.1	Осуществлять коммуникации во всех сферах жизни; владеть различными способами общения и взаимодействия
2.1.2	Развернуто и логично излагать свою точку зрения с использованием языковых средств
2.1.3	Аргументированно вести диалог
3	
3.1	Самоорганизация
3.1.1	Самостоятельно осуществлять познавательную деятельность, выявлять проблемы, ставить и формулировать собственные задачи в образовательной деятельности и жизненных ситуациях; давать оценку новым ситуациям
3.1.2	Самостоятельно составлять план решения проблемы с учетом имеющихся ресурсов, собственных возможностей и предпочтений; делать осознанный выбор, аргументировать его, брать ответственность за решение; оценивать приобретенный опыт; способствовать формированию и проявлению широкой эрудиции в разных областях знаний
3.2	Самоконтроль

3.2.1	Давать оценку новым ситуациям, вносить коррективы в деятельность, оценивать соответствие результатов целям
3.2.2	Владеть навыками познавательной рефлексии как осознания совершаемых действий и мыслительных процессов, их результатов и оснований; использовать приемы рефлексии для оценки ситуации, выбора верного решения; уметь оценивать риски и своевременно принимать решения по их снижению
3.3	Эмоциональный интеллект, предполагающий сформированность: саморегулирования, включающего самоконтроль, умение принимать ответственность за свое поведение, способность адаптироваться к эмоциональным изменениям и проявлять гибкость, быть открытым новому; внутренней мотивации, включающей стремление к достижению цели и успеху, оптимизм, инициативность, умение действовать, исходя из своих возможностей

Выпускник научится:

1. самостоятельно определять цели деятельности и составлять планы деятельности; самостоятельно осуществлять, контролировать и корректировать деятельность; использовать все возможные ресурсы для достижения поставленных целей и реализации планов деятельности; выбирать успешные стратегии в различных ситуациях;
2. продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников деятельности, эффективно разрешать конфликты;
3. владеть навыками познавательной, учебно-исследовательской и проектной деятельности, навыками разрешения проблем;
4. использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Выпускник получит возможность научиться:

1. быть готовым и способным к самостоятельной информационно-познавательной деятельности, включая умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;
2. быть способным и готовым к самостоятельному поиску методов решения практических задач, применению различных методов познания.

Регулятивные универсальные учебные действия

1. самостоятельно определять цели, задавать параметры и критерии, по которым можно определить, что цель достигнута;
2. оценивать возможные последствия достижения поставленной цели в деятельности, собственной жизни и жизни окружающих людей, основываясь на соображениях этики и морали;
3. ставить и формулировать собственные задачи в образовательной деятельности и жизненных ситуациях;
4. оценивать ресурсы, в том числе время и другие нематериальные ресурсы, необходимые для достижения поставленной цели;
5. выбирать путь достижения цели, планировать решение поставленных задач, оптимизируя материальные и нематериальные затраты;
6. организовывать эффективный поиск ресурсов, необходимых для достижения поставленной цели;
7. сопоставлять полученный результат деятельности с поставленной заранее целью.

Познавательные универсальные учебные действия

1. искать и находить обобщенные способы решения задач, в том числе, осуществлять развернутый информационный поиск и ставить на его основе новые (учебные и познавательные) задачи;
2. критически оценивать и интерпретировать информацию с разных позиций, распознавать и фиксировать противоречия в информационных источниках;
3. использовать различные модельно-схематические средства для представления существенных связей и отношений, а также противоречий, выявленных в информационных источниках;
4. находить и приводить критические аргументы в отношении действий и суждений другого; спокойно и разумно относиться к критическим замечаниям в отношении собственного суждения, рассматривать их как ресурс собственного развития;
5. выходить за рамки учебного предмета и осуществлять целенаправленный поиск возможностей для широкого переноса средств и способов действия;
6. выстраивать индивидуальную образовательную траекторию, учитывая ограничения со стороны других участников и ресурсные ограничения;
7. менять и удерживать разные позиции в познавательной деятельности.

Коммуникативные универсальные учебные действия

1. осуществлять деловую коммуникацию как со сверстниками, так и со взрослыми (как внутри образовательной организации, так и за ее пределами), подбирать партнеров для деловой коммуникации исходя из соображений результативности взаимодействия, а не личных симпатий;
2. при осуществлении групповой работы быть как руководителем, так и членом команды в разных ролях (генератор идей, критик, исполнитель, выступающий, эксперт и т.д.);
3. координировать и выполнять работу в условиях реального, виртуального и комбинированного взаимодействия;
4. развернуто, логично и точно излагать свою точку зрения с использованием адекватных (устных и письменных) языковых средств;
5. распознавать конфликтогенные ситуации и предотвращать конфликты до их активной фазы, выстраивать деловую и образовательную коммуникацию, избегая личностных оценочных суждений.

Предметные результаты

Выпускник будет демонстрировать:

1) систематизация знаний, относящихся к *математическим объектам информатики*; умение строить математические объекты информатики, в том числе логические формулы;

2) сформированность базовых навыков и умений по соблюдению требований *техники безопасности*, гигиены и ресурсосбережения при работе со средствами информатизации;

3) владение опытом построения и использования *компьютерно-математических моделей*, проведения экспериментов и статистической обработки данных с помощью компьютера, интерпретации результатов, получаемых в ходе моделирования реальных процессов; умение оценивать числовые параметры моделируемых объектов и процессов; сформированность представлений о необходимости *анализа соответствия модели* и моделируемого объекта (процесса);

4) сформированность представлений о способах хранения и простейшей обработке данных; умение пользоваться *базами данных* и справочными системами; владение основными сведениями о базах данных, их структуре, средствах создания и работы с ними;

Выпускник получит возможность продемонстрировать:

1. владение системой базовых знаний, отражающих *вклад информатики* в формирование современной научной картины мира;

2. владение навыками *алгоритмического мышления* и понимание необходимости формального описания алгоритмов.

ПРОВЕРЯЕМЫЕ НА ЕГЭ ПО ИНФОРМАТИКЕ ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ СРЕДНЕГО ОБЩЕГО ОБРАЗОВАНИЯ

Код проверяемого требования	Проверяемые требования к предметным результатам освоения основной образовательной программы среднего общего образования
1.	*Знать (понимать)*
1.1	Понимание основных принципов устройства и функционирования современных стационарных и мобильных компьютеров; тенденций развития компьютерных технологий; владение навыками работы с операционными системами и основными видами программного обеспечения для решения учебных задач по выбранной специализации
1.4	Понимание базовых алгоритмов обработки числовой и текстовой информации (запись чисел в позиционной системе счисления, делимость целых чисел; нахождение всех простых чисел в заданном диапазоне; обработка многоразрядных целых чисел; анализ символьных строк и других), алгоритмов поиска и сортировки
1.5	Знание функциональные возможности инструментальных средств среды разработки
1.6	Владение основными сведениями о базах данных, их структуре, средствах создания и работы с ними
1.7	Понимание возможностей и ограничений технологий искусственного интеллекта в различных областях; наличие представлений об использовании информационных технологий в различных профессиональных сферах
2.	*Уметь*
2.1	Умение использовать компьютерно-математические модели для анализа объектов и процессов: формулировать цель моделирования, выполнять анализ результатов, полученных в ходе моделирования; оценивать адекватность модели моделируемому объекту или процессу; представлять результаты моделирования в наглядном виде
2.2	Умение классифицировать основные задачи анализа данных (прогнозирование, классификация, кластеризация, анализ отклонений); понимать последовательность решения задач анализа данных: сбор первичных данных, очистка и оценка

Код проверяемого требования	Проверяемые требования к предметным результатам освоения основной образовательной программы среднего общего образования
	качества данных, выбор и (или) построение модели, преобразование данных, визуализация данных, интерпретация результатов
2.9	Умение анализировать алгоритмы с использованием таблиц трассировки; определять без использования компьютера результаты выполнения несложных программ, включающих циклы, ветвления и подпрограммы, при заданных исходных данных
2.10	Умение определять сложность изучаемых в курсе базовых алгоритмов (суммирование элементов массива, сортировка массива, переборные алгоритмы, двоичный поиск) и приводить примеры нескольких алгоритмов разной сложности для решения одной задачи
2.11	Владение универсальным языком программирования высокого уровня (Паскаль, Python, Java, C++, C#), представлениями о базовых типах данных и структурах данных; умение использовать основные управляющие конструкции; умение осуществлять анализ предложенной программы: определять результаты работы программы при заданных исходных данных; определять, при каких исходных данных возможно получение указанных результатов; выявлять данные, которые могут привести к ошибке в работе программы; формулировать предложения по улучшению программного кода
2.12	Умение реализовывать на выбранном для изучения языке программирования высокого уровня (Паскаль, Python, Java, C++, C#) типовые алгоритмы обработки чисел, числовых последовательностей и массивов: представление числа в виде набора простых сомножителей; нахождение максимальной (минимальной) цифры натурального числа, записанного в системе счисления с основанием, не превышающим 10; вычисление обобщённых характеристик элементов массива или числовой последовательности (суммы, произведения среднего арифметического, минимального и максимального элементов, количества элементов, удовлетворяющих заданному условию); сортировку элементов массива; умение использовать в программах данные различных типов с учётом ограничений на диапазон их возможных значений, применять при решении задач структуры данных (списки, словари, стеки, очереди, деревья); применять стандартные и собственные подпрограммы для обработки числовых данных и символьных строк; использовать

Код проверяемого требования	Проверяемые требования к предметным результатам освоения основной образовательной программы среднего общего образования
	при разработке программ библиотеки подпрограмм; умение использовать средства отладки программ в среде программирования

ПЕРЕЧЕНЬ ЭЛЕМЕНТОВ СОДЕРЖАНИЯ, ПРОВЕРЯЕМЫХ НА ЕГЭ ПО ИНФОРМАТИКЕ

Код	Проверяемый элемент содержания
3	Алгоритмы и программирование
3.1	Формализация понятия алгоритма. Машина Тьюринга как универсальная модель вычислений
3.2	Оценка сложности вычислений. Время работы и объём используемой памяти, их зависимость от размера исходных данных. Оценка асимптотической сложности алгоритмов. Алгоритмы полиномиальной сложности. Переборные алгоритмы. Примеры различных алгоритмов решения одной задачи, которые имеют различную сложность
3.3	Определение возможных результатов работы простейших алгоритмов управления исполнителями и вычислительных алгоритмов. Определение исходных данных, при которых алгоритм может дать требуемый результат
3.4	Алгоритмы обработки натуральных чисел, записанных в позиционных системах счисления: разбиение записи числа на отдельные цифры, нахождение суммы и произведения цифр, нахождение максимальной (минимальной) цифры. Представление числа в виде набора простых сомножителей. Алгоритм быстрого возведения в степень. Поиск простых чисел в заданном диапазоне с помощью алгоритма «решето Эратосфена»
3.5	Многоразрядные целые числа, задачи длинной арифметики
3.6	Язык программирования (Паскаль, Python, Java, C++, C#). Типы данных: целочисленные, вещественные, символьные, логические. Ветвления. Сложные условия. Циклы с условием. Циклы по переменной. Обработка данных, хранящихся в файлах. Текстовые и двоичные файлы. Файловые переменные (файловые указатели). Чтение из файла. Запись в файл. Разбиение задачи на подзадачи. Подпрограммы (процедуры и функции). Использование стандартной библиотеки языка программирования
3.7	Рекурсия. Рекурсивные процедуры и функции. Использование стека для организации рекурсивных вызовов

Код	Проверяемый элемент содержания
3.8	Численные методы. Точное и приближённое решения задачи. Численное решение уравнений с помощью подбора параметра. Численные методы решения уравнений: метод перебора, метод половинного деления. Приближённое вычисление длин кривых. Вычисление площадей фигур с помощью численных методов (метод прямоугольников, метод трапеций). Поиск максимума (минимума) функции одной переменной методом половинного деления
3.9	Обработка символьных данных. Встроенные функции языка программирования для обработки символьных строк. Алгоритмы обработки символьных строк: подсчёт количества появлений символа в строке, разбиение строки на слова по пробельным символам, поиск подстроки внутри данной строки, замена найденной подстроки на другую строку. Генерация всех слов в некотором алфавите, удовлетворяющих заданным ограничениям. Преобразование числа в символьную строку и обратно
3.10	Массивы и последовательности чисел. Вычисление обобщённых характеристик элементов массива или числовой последовательности (суммы, произведения, среднего арифметического, минимального и максимального элементов, количества элементов, удовлетворяющих заданному условию). Линейный поиск заданного значения в массиве. Алгоритмы работы с элементами массива с однократным просмотром массива. Сортировка одномерного массива. Простые методы сортировки (метод пузырька, метод выбора, сортировка вставками). Сортировка слиянием. Быстрая сортировка массива (алгоритм QuickSort). Двоичный поиск в отсортированном массиве
3.11	Двумерные массивы (матрицы). Алгоритмы обработки двумерных массивов: заполнение двумерного числового массива по заданным правилам, поиск элемента в двумерном массиве, вычисление максимума (минимума) и суммы элементов двумерного массива, перестановка строк и столбцов двумерного массива
3.12	Словари (ассоциативные массивы, отображения). Хэш-таблицы. Построение алфавитно-частотного словаря для заданного текста
3.13	Стеки. Анализ правильности скобочного выражения. Вычисление арифметического выражения, записанного в постфиксной форме. Очереди. Использование очереди для временного хранения данных
3.14	Алгоритмы на графах. Построение минимального остовного дерева взвешенного связного неориентированного графа. Количество различных путей между вершинами ориентированного ациклического графа. Алгоритм Дейкстры
3.15	Деревья. Реализация дерева с помощью ссылочных структур. Двоичные (бинарные) деревья. Построение дерева для заданного арифметического

Код	Проверяемый элемент содержания
	выражения. Рекурсивные алгоритмы обхода дерева. Использование стека и очереди для обхода дерева
3.16	Динамическое программирование как метод решения задач с сохранением промежуточных результатов. Задачи, решаемые с помощью динамического программирования: вычисление рекурсивных функций, подсчёт количества вариантов, задачи оптимизации
3.17	Понятие об объектно-ориентированном программировании. Объекты и классы. Свойства и методы объектов. Объектно-ориентированный анализ. Разработка программ на основе объектно-ориентированного подхода. Инкапсуляция, наследование, полиморфизм
4	Информационные технологии
4.1	Анализ данных. Основные задачи анализа данных: прогнозирование, классификация, кластеризация, анализ отклонений. Последовательность решения задач анализа данных: сбор первичных данных, очистка и оценка качества данных, выбор и (или) построение модели, преобразование данных, визуализация данных, интерпретация результатов. Программные средства и Интернет-сервисы для обработки и представления данных. Большие данные. Машинное обучение
4.2	Анализ данных с помощью электронных таблиц. Вычисление суммы, среднего арифметического, наибольшего (наименьшего) значения диапазона. Вычисление коэффициента корреляции двух рядов данных. Построение столбчатых, линейчатых и круговых диаграмм. Построение графиков функций. Подбор линии тренда, решение задач прогно-зирования. Решение задач оптимизации с помощью электронных таблиц

3. Тематическое планирование

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
Модуль №1 «Расчет IP-адресов и схемы топологий» - 8 часов					
1.1	Расчет IP-адресов и схемы топологий.	7			
1.2	Самостоятельная работа «Расчет IP-адресов и схемы топологий»	1		1	
Модуль №2 «Схемы маршрутизации, работа с DNS и VPN» - 8 часов					

2.1	Схемы маршрутизации, работа с DNS и VPN	7			
2.2	Самостоятельная работа «Схемы маршрутизации, работа с DNS и VPN»	1		1	
Модуль №3 «Анализ угроз, схемы защиты, тестирование» - 8 часов					
3.1	Анализ угроз, схемы защиты, тестирование.	7			
3.2	Самостоятельная работа «Анализ угроз, схемы защиты, тестирование»	1		1	
Модуль №4 «Анализ предложенного сценария (школьная/домашняя/корпоративная сеть), определение топологии, настройка адресации, выявление угроз безопасности и предложение мер защиты» - 9 часов					
3.1	Анализ предложенного сценария (школьная/домашняя/корпоративная сеть), определение топологии, настройка адресации, выявление угроз безопасности и предложение мер защиты.	8			
3.2	Аттестационная работа «Введение в глубокое обучение»	1		1	

5. Приложения к программе

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ

№ п/п	Наименование разделов и тем программы	Количество часов			Электронные (цифровые) образовательные ресурсы
		Всего	Контрольные работы	Практические работы	
Модуль №1 «Расчет IP-адресов и схемы топологий» - 8 часов					
1.1	Введение в компьютерные сети	1			
1.2	Аппаратное обеспечение сетей	1			
1.3	Сетевые топологии	1			
1.4	Модель OSI	1			
1.5	Модель TCP/IP	1			
1.6	Протоколы передачи данных	1			
1.7	Адресация в сетях	1			
1.8	**Самостоятельная работа №1**	1		1	
Модуль №2 «Схемы маршрутизации, работа с DNS и VPN» - 8 часов					
2.1	Локальные сети	1			
2.2	Глобальные сети и Интернет	1			
2.3	Сетевые устройства	1			
2.4	DNS и	1			

	маршрутизация				
2.5	Беспроводные сети	1			
2.6	Сетевые службы	1			
2.7	Виртуальные частные сети (VPN)	1			
2.8	**Самостоятельная работа №2**	1		1	
Модуль №3 « Анализ угроз, схемы защиты, тестирование» - 8 часов					
3.1	Основы информационной безопасности	1			
3.2	Вредоносное ПО	1			
3.3	Методы защиты информации	1			
3.4	Криптография: основы	1			
3.5	Сетевые атаки	1			
3.6	Аутентификация и авторизация	1			
3.7	Безопасность беспроводных сетей	1			
3.8	**Самостоятельная работа №3**	1		1	
Модуль №4 «Анализ предложенного сценария (школьная/домашняя/корпоративная сеть), определение топологии, настройка адресации, выявление угроз безопасности и предложение мер защиты» - 9 часов					
4.1	Резервное копирование и восстановление	1			

4.2	Политика безопасности в организациях	1			
4.3	Персональные данные и их защита	1			
4.4	Социальная инженерия и фишинг	1			
4.5	Безопасность в Интернете	1			
4.6	Цифровая гигиена	1			
4.7	Современные тенденции ИБ	1			
4.8	Настройка и защита сети	1			
4.9	**Итоговая контрольная работа**	1		1	

КИМ

Модуль 1 «Расчет IP-адресов и схемы топологий»

Цель: Закрепить на практике знания о сетевом оборудовании, топологиях, моделях OSI/TCP-IP и принципах адресации. Развить навыки проектирования и конфигурирования простой сети.

Задача: Спроектировать сеть для небольшого офиса, выбрать оборудование, топологию, настроить базовую IP-адресацию и проанализировать процесс передачи данных.

Часть 1: Проектирование сети (Теоретическая)

1. Техническое задание:
В офисе есть:

5 стационарных компьютеров в разных кабинетах.
1 сетевой принтер.
2 беспроводных устройства (ноутбук и смартфон).

Необходим доступ в интернет.

2. Выбор оборудования:
Используя пройденный материал, составьте список активного и пассивного сетевого оборудования, необходимого для построения этой сети. Обоснуйте свой выбор.

Пример: Коммутатор (Switch) на 8 портов, т.к. нужно подключить 5 ПК и принтер, а также оставить порт для подключения к маршрутизатору...
Маршрутизатор (Router) с функцией Wi-Fi точки доступа для раздачи интернета и подключения беспроводных устройств...
Сетевые кабели (витая пара, UTP 5e)...

3. Выбор топологии:
Выберите и обоснуйте тип топологии (звезда, кольцо, шина) для проводной части вашей сети. Нарисуйте ее схему, подписав все устройства.

Пример: «Выбираю топологию «Звезда», так как она обеспечивает высокую надежность: обрыв кабеля у одного компьютера не приведет к отказу всей сети...»
Часть 2: Моделирование и адресация (Практическая в Cisco Packet Tracer или на листе бумаги)

1. Создание схемы:
Смоделируйте свою сеть в программе Cisco Packet Tracer (или детально нарисуйте на бумаге).

Добавьте все устройства из техзадания.
Соедините их виртуальными «кабелями», правильно подключив устройства к коммутатору, а коммутатор — к маршрутизатору.

2. Настройка IP-адресации:
Ваш маршрутизатор получил от провайдера адрес 212.45.78.99. Вам нужно создать частную сеть.

Шаг 1: Выберите частную IP-сеть (например, из диапазона 192.168.1.0).
Шаг 2: Придумайте маску подсети, которой хватит на все ваши устройства (с запасом). Например, 255.255.255.0 (/24).
Шаг 3: Назначьте IP-адреса каждому устройству в вашей сети.

Маршрутизатор (шлюз по умолчанию) — 192.168.1.1
Компьютер 1 — 192.168.1.10
Компьютер 2 — 192.168.1.11
... и так далее.
Шаг 4: Укажите на каждом компьютере адрес шлюза (192.168.1.1).

3. Таблица адресов:

Создайте таблицу соответствия устройств, их IP- и MAC-адресов.

Устройство	IP-адрес	MAC-адрес
PC1	192.168.1.10	(будет в симуляторе)
Router (Gateway)	192.168.1.1	...
...	...	...

Часть 3: Анализ (Письменный отчет)

Ответьте на вопросы, используя знания о моделях OSI и TCP/IP.

Уровневый анализ: Какие протоколы и на каких уровнях модели OSI будут задействованы, когда компьютер с адресом 192.168.1.10 отправляет запрос на печать на сетевой принтер 192.168.1.20?

Пример: «На канальном уровне (L2) будут использоваться протокол Ethernet и MAC-адреса... На сетевом уровне (L3) — протокол IP и IP-адреса...»

Сравнение протоколов: Чем будет отличаться процесс передачи, если вместо отправки файла на печать компьютер откроет веб-страницу? Укажите, какие протоколы транспортного уровня (TCP или UDP) будут использоваться в каждом случае и почему.
Поиск неисправности: Представьте, что компьютер не может выйти в интернет, но «видит» другие компьютеры в локальной сети. Используя утилиты командной строки (ping, ipconfig), опишите алгоритм диагностики этой проблемы. К каким устройствам вы будете последовательно отправлять ping?

Модуль 2 «Схемы маршрутизации, работа с DNS и VPN»

Цель: Закрепить на практике знания о построении домашних сетей, работе интернета, сетевом оборудовании, ключевых сервисах и основах безопасности. Развить навыки анализа, проектирования и обеспечения базовой защиты сетевой инфраструктуры.

Задача: Проанализировать предложенный сценарий, спроектировать схему сети, настроить ключевые сервисы и разработать рекомендации по безопасности.

Часть 1: Анализ и проектирование (Теоретическая)

Сценарий:

Семья из трех человек переехала в новую квартиру. Им необходимо организовать подключение к интернету и настроить домашнюю сеть.

Требования:

Подключить 2 ноутбука, 3 смартфона, Smart-TV и сетевой принтер.
Обеспечить стабильный Wi-Fi по всей квартире.
Настроить доступ к общим файлам и принтеру.
Организовать безопасный доступ для гостей.
Активно использовать облачные сервисы (Google Диск, Netflix), онлайн-банкинг и видеозвонки.
Задание 1: «Выбор провайдера и оборудования»

Объясните, какую роль играет провайдер и магистральные сети в подключении этой квартиры к интернету.
Составьте список необходимого сетевого оборудования. Обоснуйте, почему вам нужен именно маршрутизатор (роутер), а не просто коммутатор или точка доступа.
Нарисуйте схему сети в виде топологии «звезда», указав все устройства и то, как они подключены (проводное/беспроводное).
Часть 2: Настройка и объяснение принципов работы (Практико-ориентированная)

Задание 2: «Объяснение ключевых процессов»
Ответьте на вопросы, подробно описывая принципы работы сетей:

DNS: Опишите пошагово процесс преобразования доменного имени www.youtube.com в IP-адрес, когда пользователь вводит его в браузере. Объясните, для чего это нужно.
Маршрутизация: Объясните путь пакета данных от ноутбука в квартире до сервера YouTube. Какие устройства (с указанием их функций) он пройдет на своем пути? (Локальный маршрутизатор -> провайдер -> магистральные сети...).
Сервисы: Чем отличаются протоколы, используемые для просмотра веб-страниц (HTTP/HTTPS), передачи файлов (FTP) и отправки почты (SMTP/POP3/IMAP)? Какой из них наиболее безопасный и почему?
Задание 3: «Настройка Wi-Fi и безопасности»

Перечислите не менее 3 обязательных мер безопасности для домашней Wi-Fi сети.
Объясните, чем опасен открытый Wi-Fi в кафе и какие меры предосторожности нужно соблюдать при его использовании.
Сравните технологии Wi-Fi и Bluetooth по целям использования, радиусу действия и потреблению энергии.
Предположим, что ваш маршрутизатор поддерживает гостевую сеть. Объясните, зачем нужна эта функция и как она повышает безопасность основных устройств в сети.
Часть 3: Кейс-задача «Безопасное использование облачных сервисов» (Аналитическая)

Ситуация:
Один из членов семьи активно работает с финансовыми отчетами через онлайн-банкинг и хранит их копии на Google Диске. Другой — постоянно смотрит фильмы через Smart-TV. Третий — качает файлы для учебы через FTP-сервер.

Задание:

Анализ рисков: Определите по 2 основных киберриска для каждого описанного сценария использования (банкинг, стриминг, FTP).
Разработка рекомендаций: Составьте памятку «Правила цифровой гигиены для моей семьи» на основе пройденного материала. Памятка должна содержать не менее 5 пунктов, охватывающих:

Защиту Wi-Fi.
Безопасное использование публичных сетей.
Выявление подозрительных писем (e-mail).
Безопасную работу с облачными сервисами (использование HTTPS, двухфакторной аутентификации).
Осознанное использование публичных FTP-серверов.

Модуль 3 «Анализ угроз, схемы защиты, тестирование»

Цель: Закрепить на практике знания об основных угрозах информационной безопасности и принципах защиты. Научиться применять cryptographic-методы, анализировать риски и разрабатывать эффективные меры противодействия.

Задача: Выступить в роли специалиста по кибербезопасности и разработать персональный план защиты для вымышленного студента Алексея, который активно пользуется интернетом для учебы и общения.

Часть 1: Анализ угроз и уязвимостей

Сценарий:
Алексей использует:

Слабый пароль 123456 для всех аккаунтов (соцсети, почта, облако).
Подключается к открытому Wi-Fi в университете и кафе.
Качает рефераты с сомнительных сайтов.
Получил письмо от «банка» с просьбой «проверить данные» карты по ссылке.
Задание 1: «Классификация угроз»

Составьте таблицу, в которой для каждого действия Алексея укажите:

- Конкретную угрозу (вирус, фишинг, перехват трафика и т.д.).
- К какому типу вредоносного ПО она относится (троян, шпионское ПО).

- Возможные последствия (кража данных, потеря денег, шпионаж).

Действие/Ситуация	**Угроза (название)**	**Тип вредоносного ПО**	**Последствия**
Слабый пароль	Брутфорс-атака	-	Кража всех аккаунтов
Подключение к открытому Wi-Fi	**Man-in-the-Middle**	**Шпионское ПО**	**Перехват логинов и паролей**
...	...	...	...

Часть 2: Разработка системы защиты

Задание 2: «Применение принципов защиты»
Для каждой угрозы из Задания 1 предложите конкретные меры защиты, основанные на пройденных принципах.

Пароли и аутентификация:

Объясните, почему пароль Алексея ненадежен. Сформулируйте 3 правила создания сильного пароля.
Предложите более безопасный метод — менеджер паролей или двухфакторную аутентификацию (2FA). Объясните их преимущество.
Шифрование:

Алексей хочет пересылать одногруппнику конфиденциальные учебные материалы. Объясните, почему нельзя делать это через личные сообщения в соцсетях.
Предложите два безопасных способа на основе шифрования:

Использование симметричного шифрования (например, запароленный ZIP-архив). В чем его недостаток?
Использование асимметричного шифрования (например, PGP). Объясните его принцип и преимущество.
Для чего в этом сценарии можно использовать цифровую подпись?
Защита периметра:

Объясните, как межсетевой экран (файрвол) и антивирус дополняют друг друга в защите ноутбука Алексея.
Дайте рекомендацию по выбору антивируса (платный/бесплатный, на что смотреть).
Часть 3: Кейс-задача «Защита домашней сети»

Задание 3: «Аудит Wi-Fi безопасности»

Алексей купил роутер и хочет настроить домашнюю Wi-Fi сеть.

Выбор протокола: Объясните, почему нужно выбрать WPA2 или WPA3, а не устаревшие и небезопасные WEP или Open.
Настройка безопасности: Составьте чек-лист из 5 обязательных пунктов для настройки безопасной Wi-Fi сети (например: «Сменить пароль администратора роутера по умолчанию», «Скрыть SSID», «Включить шифрование WPA2» и т.д.).
Социальная инженерия: К Алексею в гости приходят друзья и просят пароль от Wi-Fi. Как он может предоставить им доступ, не раскрывая основной пароль? (Используйте концепцию гостевой сети).
Задание 4: «Отпись фишинга»
Алексей получил подозрительное письмо. Опишите алгоритм из 3-5 действий, как ему следует поступить, чтобы не стать жертвой фишинга. (Например: «1. Не переходить по ссылке. 2. Проверить адрес отправителя. 3. Связаться с банком по официальному телефону...»).

Модуль 4 «Анализ предложенного сценария (школьная/домашняя/корпоративная сеть), определение топологии, настройка адресации, выявление угроз безопасности и предложение мер защиты»

Цель работы: Проверка умений анализировать сетевую инфраструктуру, разрабатывать схемы адресации, выявлять уязвимости и предлагать комплексные меры защиты для различных сценариев. Работа направлена на формирование системного подхода к проектированию и защите сетей.

Постановка задачи:
Проанализировать предложенный сценарий организации сети, выполнить следующие задания:
1. Определить и графически отобразить топологию сети.
2. Разработать и обосновать схему IP-адресации (выбрать приватную сеть, разбить на подсети, назначить адреса ключевым устройствам).
3. Выявить потенциальные угрозы информационной безопасности для каждого сетевого segment и устройства.
4. Предложить комплекс мер защиты (организационных и технических) для устранения выявленных угроз.

Рекомендации по выполнению
1. Выделите все устройства, пользователей, сервисы и связи между ними.
2. Разбейте работу на этапы: топология, адресация, угрозы, информационная безопасность.
3. Для рисования топологии используйте GNS 3 или любой редактор схем. Для расчета подсетей воспользуйтесь калькулятором.
4. Будьте конкретны в принимаемых решениях в построении топологии сети и мерах информационной безопасности.

Варианты заданий

Вариант 1: Современная школа

Сценарий: В школе развернута Wi-Fi сеть для учащихся, учителей и администрации. Есть компьютерные классы, сервер с электронным дневником, система видеонаблюдения с выходом в интернет, умные доски в каждом классе. Учащиеся используют личные устройства.

Задача: Предложить топологию, разделить сеть на сегменты, выделить угрозы доступа к электронному дневнику и видеонаблюдению, предложить меры защиты.

Вариант 2: Домашняя сеть с умными устройствами (IoT)

Сценарий: В квартире есть персональные компьютеры, смартфоны, умный телевизор, голосовой помощник (умная колонка), IP-камеры для няни, smart-розетки и система умного освещения. Все устройства подключены к одному домашнему маршрутизатору.

Задача: Нарисовать топологию, предложить схему адресации, проанализировать риски утечки данных через IoT-устройства, предложить правила для маршрутизатора.

Вариант 3: Небольшой офис

Сценарий: В офисе есть рабочие места администраторов (ПК), касса онлайн-платежей, публичный Wi-Fi для клиентов, локальный сервер с базой данных клиентов и их платежными данными, принтер.

Задача: Разделить сеть на подсети (гостевая/рабочая/серверная), предложить правила межсетевого экрана, выделить угрозы к базе данных, предложить способы защиты платежных транзакций.

Вариант 4: Сеть загородного дома

Сценарий: Двухэтажный дом, участок. Есть основной маршрутизатор, Wi-Fi покрывает не весь участок, поэтому добавлена вторая точка доступа (репитер). Устройства: камеры по периметру, умный замок на калитке, датчики освещения, ПК, ноутбуки.

Задача: Предложить топологию для устойчивого покрытия, настроить адресацию, выделить угрозы безопасности умного замка и камер, предложить меры по шифрованию трафика.

Вариант 5: Сеть небольшой кофейни

Сценарий: Есть кассовая система, ноутбук бухгалтера, терминал для бесконтактной оплаты, гостевая Wi-Fi сеть для посетителей, камера над кассой.

Задача: Изолировать гостевой трафик, защитить кассовую систему и транзакции, предложить способ безопасно передавать данные бухгалтеру на дом.

Вариант 6: Интернет вещей (IoT) на ферме

Сценарий: В теплицах и на полях установлены датчики влажности и температуры, управляемые клапаны полива, камеры. Все данные передаются на сервер в хозблоке по Wi-Fi. Хозяин контролирует все со своего смартфона из дома.

Задача: Предложить схему сети, выделить угрозы перехвата управления или ложных данных с датчиков, предложить меры аутентификации устройств и шифрования данных.

Вариант 7: Домашняя сеть геймера

Сценарий: Несколько игровых консолей, мощный игровой ПК, NAS-сервер с медиатекой и резервными копиями, смартфон, умный телевизор. Важны низкие задержки (ping) и высокая скорость.
Задача: Оптимизировать топологию для игр, настроить QoS, выделить угрозы для NAS-сервера с данными, предложить схему резервного копирования и защиты от внешних атак.
Вариант 8: Сеть для удаленной работы (фриланс)
Сценарий: Домашний офис фрилансера: ноутбук, смартфон, принтер, облачные сервисы для работы, VPN-доступ к серверам клиентов. Частая работа в публичных Wi-Fi сетях (кафе, коворкинги).
Задача: Предложить меры защиты домашней сети. Сформулировать правила безопасной работы в публичных сетях. Предложить выбор и настройку VPN.
Вариант 9: Небольшая интернет-магазин
Сценарий: Складской ПК с программой учета товаров, ноутбук менеджера, онлайн-касса, принтер для этикеток. Все подключены к роутеру. Доступ к интернет-магазину и почте осуществляется через браузер.
Задача: Предложить меры по защите учетных записей на площадках, защите от фишинга, обеспечению безопасности ПК с базой товаров, организации безопасного доступа к почте.
Вариант 10: Школьный класс
Сценарий: В классе 15 учебных компьютеров, 3D-принтер, управляемый по сети, сервер для проектов, программируемые роботы, подключенные по Wi-Fi. Ученики приносят свои ноутбуки.
Задача: Разработать сетевую топологию, изолировать критичное оборудование (3D-принтер, сервер), предложить правила для гостевого доступа, защиту от несанкционированного доступа к роботам.