государственное бюджетное общеобразовательное учреждение Самарской области
средняя общеобразовательная школа «Образовательный центр» с.Александровка
муниципального района Большеглушицкий Самарской области

РАССМОТРЕНО	ПРОВЕРЕНО	УТВЕРЖДЕНО
на заседании МО	ответственным за выполнение	директором ГБОУ СОШ "ОЦ"
классных руководителей	функций зам.директора по ВР	с. Александровка
Протокол № 1 от «24»08.2023 г.	_____ Тюмасева О.В.	_____Айтасовой Л.И.
Руководитель МО	Протокол №1от «28»08.2023г.	Приказ №209 от «31»08.2023г.
_____/Тюмасева О.В.		

Рабочая программа внеурочной деятельности

«Информационная безопасность»

Направление внеурочной деятельности по обеспечению безопасности жизни и здоровья обучающихся.

Ц**елью** изучения курса «Информационная безопасность» являются обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз, и формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Программа рассчитана на 10-11 классы

Составитель: Айтасов Р.Ж.,
учитель информатики и ОБЖ

C=RU, O="ГБОУ СОШ ""ОЦ"" с. Александровка", CN=Айтасова Л.И., E=alexander_sch@samara.edu.ru
00b7fc6a7aee4c654c
2023.09.28 12:58:47+04'00'

с. Александровка
2023 год

Пояснительная записка

Программа внеурочной деятельности «Информационная безопасность» составлена на основе федерального государственного образовательного стандарта основного общего образования по предметным образовательным областям «Математика и информатика», «Физическая культура и основы безопасности жизнедеятельности» и Примерной рабочей программы учебного курса «Цифровая гигиена» основного общего образования, рекомендованного Координационным советом учебно-методических объединений в системе общего образования Самарской области (протокол № 27 от 21.08.2019) и реализуется в ГБОУ СОШ «ОЦ» с. Александровка в рамках социального направления развития личности по плану внеурочной деятельности в ОО.

Целью изучения курса «Информационная безопасность » являются обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз, и формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

1. сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
2. создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
3. сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
4. сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
5. сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Общая характеристика учебного курса

Курс внеурочной деятельности «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.

Программа учебного курса рассчитана на 68 учебных часов, 34 часа в 10 и 34 часа в 11 классе. Внеурочной деятельности «Информационная безопасность » отводится по 1 часу в неделю в 10 и 11 классах.

Планируемые результаты освоения учебного курса

Личностные:

− готовность и способность к самостоятельной, творческой и ответственной деятельности;

− 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;

− эстетическое отношение к миру, включая эстетику научного и технического творчества;

− осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов; отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем.

Метапредметные:

− умение самостоятельно определять цели деятельности и составлять планы деятельности;

− самостоятельно осуществлять, контролировать и корректировать деятельность;

− умение продуктивно общаться и взаимодействовать в процессе совместной деятельности;

− владение навыками познавательной, учебно-исследовательской и проектной деятельности, способность и готовность к самостоятельному поиску методов решения практических задач;

− готовность и способность к самостоятельной информационно-познавательной деятельности, включая умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;

− умение использовать средства информационных и коммуникационных технологий (далее – ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;

− умение использовать средства ИКТ при построении бизнес процессов в различных сферах жизнедеятельности в соответствии с общей концепцией развития технологий связи.

− умение настраивать домашние и офисные сети связи, а также осознанно использовать технологии связи, заложенные в устройства связи, такие как смартфоны, компьютеры, микрокомпьютеры и умная бытовая техника.

− умение внедрять инновации на основе концепции интернета вещей.

Предметные:

− овладение систематическими знаниями и приобретение опыта осуществления целесообразной и результативной деятельности;

− развитие логического мышления; умение применять предметные знания при решении практических задач и оценивать полученные результаты;

− развитие умений применять изученные понятия, результаты, методы для решения задач практического характера и задач из смежных дисциплин с использованием при необходимости справочных материалов, компьютера;

− развитие инновационной творческой деятельности обучающихся в процессе решения учебных задач;

− осознание роли техники и технологий для прогрессивного развития общества;

формирование целостного представления о техносфере, сущности технологической культуры и культуры труда;

− овладение методами решения творческих задач, оценки возможностей и использования сетевых устройств, применение прямых соединений между устройствами, развертывания сетей связи;

− развитие умений применять технологии представления, преобразования и использования информации, оценивать возможности и области применения средств и инструментов ИКТ в современном производстве;

− развитие способности к непрерывному самообразованию, овладению ключевыми компетентностями, составляющими основу умения:

самостоятельному приобретению и интеграции знаний, коммуникации и сотрудничеству, эффективному разрешению проблем, осознанному использованию информационных и коммуникационных технологий, самоорганизации и саморегуляции;

− обеспечение профессиональной ориентации обучающихся.

Содержание внеурочной деятельности

1. Сети передачи данных. Вводное занятие. Сеть Интернет. Пакетные сети. Передача данных пакетным способом. Сети передачи данных. Услуги в IP-сетях.

Классификация сетей связи: от PAN до GAN. Изучение элементов сети передачи данных с использованием сетевой инфраструктуры класса ТС. Виды сетевого кабеля. Принципы построения сетей передачи данных. Шина данных. Шина, звезда, кольцо. Соединение устройств через концентратор (hub). Соединение устройств точка-точка.

2. Оборудование и технологии передачи данных, сетевые интерфейсы. Уровни OSI. Стек TCP/IP. Концепция эталонной модели взаимодействия открытых систем (OSI). Концепция стека TCP/IP. Расположение и задачи физической среды передачи, Ethernet, IP, TCP, UDP, и протоколов прикладного уровня. Оборудование передачи данных: ПК, сервер, концентратор (hub), коммутатор, маршрутизатор. Сетевые интерфейсы оборудования и их параметры. Сбор данных о технических характеристиках элементов сети передачи данных. Работа «Визуальное знакомство с сетевой инфраструктурой класса ТС»: изучение устройств сетевой инфраструктуры класса ТС и элементов, входящих в его состав. Работа «Программное знакомство с сетевой инфраструктурой класса ТС»: изучение программного обеспечения элементов комплекта сетевой инфраструктуры класса ТС.

3. Операционные системы часть 1. ОС Windows и Linux, особенности файловой системы, mc. Консольные команды. Работа «Действия с файлами»: использование команд интерфейса командной строки для управления каталогами и файлами в ОС Windows и Linux. Работа «Права доступа и создание учетной записи пользователя»: добавление новой учетной записи пользователя в операционной системе Windows и Linux, изучение прав доступа к файлам в системах с многопользовательским режимом, изучение возможностей повышения полномочий. Работа «Управление процессами»: изучение работы диспетчера задач и основных принципов управления процессами в операционной системе.

4. Операционные системы часть 2. Работа «Основные аспекты работы в консоли»: изучение основных аспектов работы в консоли компьютера в ОС Windows и Linux. Данные о сетевых подключениях в операционной системе. Работа «Сетевые утилиты»: сетевые утилиты (ipconfig/ifconfig, ping, traceroute, ip-route, netstat, nslookup/dig, netsh) в ОС Windows и Linux. Работа «Основные аспекты работы в консоли маршрутизатора»: Знакомство с основными принципами работы с интерфейсом командной строки операционной системы маршрутизатора. Работа «DNS-клиент»: применение специализированных программ для отправки DNS запросов и получения DNS записей. Организация и подключение проводной сети передачи данных. Работа «Знакомство с проводной сетью комплекта сетевой инфраструктуры класса ТС»: изучение устройства компьютерных сетей на примере ПК, маршрутизатора сервера. Рассмотрение проводной сети связи комплекта сетевой инфраструктуры класса ТС. Изучение сетевых кабелей и световых индикаторов сетевых интерфейсов, используемых в сетевой инфраструктуре класса ТС для построения сети передачи данных. Веб-страница веб-сервера комплекта сетевой инфраструктуры класса ТС. Рассмотрение работоспособности сети при выходе из строя элементов комплекта сетевой инфраструктуры класса ТС. Изучение передаваемой информации в IP-сети. Стек TCP/IP. Понятие сетевого протокола. Понятие модели OSI. Стек протоколов TCP/IP. Сравнение протоколов UDP и TCP. Принципы работы веб-страниц. Веб-клиент. Веб-сервер. Технологии DNS/HTTP. Изучение уровней OSI. Адресная информация канального, сетевого и транспортного уровня. Адресация в пакетных сетях. MAC-адрес, IP-адрес, транспортный порт. Программа анализа передаваемых данных Wireshark. Работа «Изучение передаваемой информации в IP-сети»: изучение профессионального инструмента для перехвата и анализа информации, передаваемой по сети. Использование фильтрации данных. Рассмотрение принципов работы веб-сервера и веб-клиента, а также понятий доменного имени и протоколов DNS и

HTTP. Работа «Изучение уровней OSI»: изучение протоколов, используемых в модели OSI на НСТ. Перехват пакетов при обращении к веб-страничке. Анализ стека протоколов. Поиск адресной информации канального, сетевого и транспортного уровня. Изучение данных, передаваемых в протоколах DNS и HTTP.

5. Интернет протокол и вспомогательные протоколы. Интернет протокол (IP). IPадреса и их классы. Ipv4 и IPv6. Адрес подсети. Маски подсетей. Расчет числа устройств в сети. Протокол ICMP. Принцип работы протокола ARP. Работа «Протокол IP»: Знакомство с принципами адресации и маршрутизации в сети Интернет, изучение процесса фрагментации пакетов. Работа «Вспомогательный протокол сетевого уровня»: Знакомство с принципами работы протокола ICMP и исследование примеров сценариев работы протокола ICMP. Работа «Протоколы TCP UDP»: Знакомство с принципами работы протоколов UDP и TCP, изучение сценариев работы этих протоколов, а также сравнение производительности протоколов с помощью утилиты iperf.

6. Клиент-серверная архитектура. Конфигурация сетевых интерфейсов и маршрутизации. IP-адресация и конфигурация IP-адресов на сетевых устройствах. Сетевые интерфейсы. Конфигурация маршрутизатора. Маршрутизация. Настройка взаимодействия нескольких сетей. Ручное и автоматическое назначение IP-адресов. Работа «Добавление ПК в сеть в ручном режиме»: Настройка на ПК адресации для работы в проводной сети. Указание с помощью графического интерфейса программы Wicd - IP-адреса, сетевой маски, шлюза и DNS-сервера на ПК. Сброс IP-адреса на ПК, проверка работы сетевых библиотек с помощью программы gnome-nettool, настройка IP-адреса на ПК с помощью программы Wicd, сбор информации о работе канального уровня с помощью утилит mii-tool и ethtool. Работа «Маршрутизация ПК тренажера»: изучение таблицы маршрутизации ПК с помощью графической программы gnome-nettool и консольной команды ip route.

7**. Конфигурация сетевого оборудования.** Понятие клиент и сервер. Протокол DHCP. Сервер DHCP. Сервис доменных имен (DNS) и работа браузера (HTTP/HTML). Сервер DNS. Web-сервер. Конфигурация сетевых интерфейсов и маршрутизации на ПК и маршрутизаторе. Работа «Добавление ПК в сеть в автоматическом режиме (DHCP)»: Настройка DHCP-клиента на ПК для автоматического получения IP-адреса. Использование графического (Wicd) и консольного (udhcpc) DHCP-клиента. Поиск в таблице маршрутизации ПК IP-адрес шлюза для передачи данных. Обнаружение с помощью утилиты DNS-запросов (dig/nslookup) - IP-адреса DNS-сервера. Работа «Настройка соединения между маршрутизатором и сервером комплекта сетевой инфраструктуры класса ТС»:

8. Применение различных типов беспроводных сетей связи: Развитие радиосвязи. Сети подвижной связи (1-5G). Беспроводные технологии (Wi-Fi). Особенности среды передачи по радиоканалу. Эволюция систем радиосвязи. Методы сканирования радиоэфира. Определение существующих беспроводных сетей. Аналоговые (1G), цифровые (2G), цифровые универсальные (3-5G). Соты, Handover, Rouming. Идентификаторы IMSI и IMEI. Технологии Wi-Fi (802.11) и Wi-Max (802.16). SSID идентификаторы. Применяемые типы шифрования. Беспроводные компьютерные сети. Мобильные точки доступа.

9. Радиотехнологии интернета вещей. Конфигурация оборудования с применением Wi-Fi часть 1. Персональные беспроводные сети (Bluetooth, ZigBee). Радиотехнологии интернета вещей. NFC и RFID. Wi-Fi сети. Подключение к Wi-Fi сети. Настройка беспроводной Wi-Fi сети на маршрутизаторе. Организация точки доступа Wi-Fi на смартфоне. Объединение сетей передачи данных по беспроводной связи. Беспроводное соединение между маршрутизаторами. Удаленный доступ к компьютеру со смартфона по Wi-Fi сети. Работа «Знакомство с беспроводными сетевыми интерфейсами Wi-Fi»: Получение информации о беспроводных интерфейсах Wi-Fi на ПК, маршрутизаторе и смартфоне. Работа «Подключение ПК комплекта сетевой инфраструктуры класса ТС по беспроводной сети к маршрутизатору»: посредством

беспроводного соединения осуществляется подключение к маршрутизатору и смена названия Wi-Fi сети (SSID). Подключение ПК к Wi-Fi сети маршрутизатора. Проверка доступности маршрутизатора, с включенным и выключенным проводным интерфейсом. Просмотр в веб- интерфейсе маршрутизатора списка подключенных к беспроводной сети устройств. Работа «Беспроводное подключение смартфона к маршрутизатору»: подключение посредством беспроводного соединения смартфона к маршрутизатору. Проверка доступности маршрутизатора и сервера, путем открытия со смартфона их вебстраниц. Просмотр данных в веб-интерфейсе маршрутизатора об устройствах,подключенных по Wi-Fi. Смена названия Wi-Fi сети (SSID).

9. Конфигурация оборудования с применением Wi-Fi часть 2. Работа «Настройка беспроводной сети на маршрутизаторе комплекта сетевой инфраструктуры класса ТС»: настройка Wi-Fi сети на маршрутизаторе. Подключение ПК к маршрутизатору по беспроводной сети. Выключение проводного интерфейса на ПК. Проверка доступа к серверу. Работа «Организация точки доступа Wi-Fi на смартфоне»: организация Wi-Fi сети на смартфоне. Подключение ПК к смартфону по Wi-Fi сети. Получение информации о подключенных к смартфону устройствах. Работа «Беспроводное соединение между маршрутизаторами двух комплектов сетевой инфраструктуры
класса ТС»: масштабирование при объединении нескольких компьютерных сетей на примере беспроводного объединения двух комплектов сетевой инфраструктуры в одну сеть.

10. Применение технологии Bluetooth. Технология Bluetooth. Подключение ПК к смартфону по Bluetooth. Подключение персональных устройств к компьютеру. Применение Bluetooth. Работа «Подключение микрокомпьютера к смартфону по Bluetooth»: активация Bluetooth на смартфоне и подключение микрокомпьютера к смартфону по Bluetooth. Работа «Подключение персональных устройств к компьютеру»: подключение смартфона или персонального устройства к ПК с использованием технологии Bluetooth. Работа «Применение Bluetooth»: подключение смартфона к ПК с использованием Bluetooth. Передача файла с ПК на смартфон. Получение доступа к файловой системе смартфона с ПК и чтение ранее переданного файла.

11. Мультимедийные сервисы и серверы. Вводное занятие. Мультимедийные сервисы: IP-телефония, передача данных, передача видео. Понятие сервер услуг. Понятие телефонной станции. Видеотрансляции. Видео-сервер. Видеосервисы. IPTV. Мультимедийные службы мгновенных сообщений. Современные технологии IP-телефонии. Технология VoIP. Протоколы RTP и SIP. Концепция IMS.

12. Технологии сетевых сервисов. Программно-конфигурируемые сети. Технологии DNS, HTTP, E-mail. Электронная почта. Сервер электронной почты. Знакомство с принципами работы протокола DNS, изучение сценариев работы протокола, а также знакомство с работой и настройкой клиентских и серверных приложений. Работа «Электронная почта»: настройка клиента электронной почты

13. Технологии передачи, обработки и хранения данных (Центры обработки данных и облачные хранилища данных). Технология FTP. Протокол HTTP. Базы данных. Центры обработки данных. Облачные хранилища данных. Доступ к облачным данным. Сети контент-провайдера. Работа «Протокол TFTP»: Знакомство с принципами работы протокола TFTP, изучение сценариев работы протокола, а также знакомство с работой и настройкой клиентских и серверных приложений. Работа «Протокол FTP»: Знакомство с принципами работы протокола FTP, изучение сценариев работы протокола, а также знакомство с работой и настройкой клиентских и серверных приложений. Работа «Протокол HTTP»: Знакомство с принципами работы протокола HTTP, изучение сценариев работы протокола, а также знакомство с работой и настройкой клиентских и серверных приложений.

14. Технологии и оборудование связи (IP-телефония: АТС, телефоны, смартфоны). Концепция и технологии интернета вещей. Туманные (пограничные) вычисления.

Понятие мультисервисной сети начала XXI века. Технология оптической сети PON. Совместное применение PON и беспроводного доступа Wi-Fi. VoIP. IP-телефон, смартфон. IP-Автоматическая телефонная станция (IP-АТС). Концепция интернета вещей. Радиотехнологии интернета вещей. Протокол MQTT. Архитектура сетевой инфраструктуры современной сети с интернетом вещей. Туманные (пограничные) вычисления для обработки данных.

15. Вводное занятие. Обзорный курс: объект, субъект, атака, угроза, уязвимость.

Понятие информационной безопасности. Изучение основных аспектов информационной безопасности. Понятие атаки, угрозы, уязвимости, актива и их различия. Специальные разделы математики, используемые в информационной безопасности: модульная арифметика, интерполяционные формулы, расширенный алгоритм Евклида, квадратичные вычеты.

16. Кибербезопасность.

Изучение понятия кибербезопасности. Основные отличия кибербезопасности от информационной безопасности. Понятие цифровой атаки. Изучение основных способов получения несанкционированного доступа к конфиденциально информации. Изучение механизмов кибербезопасности.

17. Математические основы криптологии.

Понятие криптологии. Основы теории чисел. Понятия группы, кольца, поля. Понятие отношения эквивалентности, изоморфизма, гомоморфизма. Понятие кольца классов вычетов. Применение методов математической криптологии в современной криптографии.

18. Введение в криптографию.

Понятие криптографии. Классификация шифров. Определение параметров, основных свойств и особенностей. Классическая криптография: шифр Цезаря, шифр Виженера, шифр Плейфера. Понятие симметрической криптографии. Понятие асимметрической криптографии. Шифры замены, перестановки, потоковые шифры. Понятие хэш-функции, свойства требования и особенности. Криптографические примитивы для цифровой подписи.

19. Основы теории информации в вопросах обеспечения ИБ.

Понятие количественной меры информации. Понятие энтропии. Понятие информационной системы. Дискретные и непрерывные информационные системы. Системы защиты информации с точки зрения теории информации.

20. Технические средства защиты информации.

Понятие технической защиты информации. Классификация технических каналов утечки информации. Изучение средств противодействия утечкам по электромагнитному, виброаккустическому и видовому каналам утечки информации.

21. Приемы обеспечения информационной безопасности личного пространства.

Понятие персональной информационной безопасности. Анализ методов социальной инженерии. Изучение основ персональной информационной безопасности. Формирование компьютерной этики для противодействия действиям злоумышленника в целях личной безопасности.

22. Основы вирусологии.

Понятие компьютерного вируса. Классификация вредоносных программ, определения, основные свойства и особенности. Понятие резидента, троянского коня, червя. Способы заражения программ. Классификация антивирусных программ. Изучение основных способов противодействия вирусным атакам.

23. Проблема вирусного заражения и структура современных вирусов.

Предпосылки формирования и совершенствование системы защиты информации в России, нормативные и правовые акты в области защиты информации России в период XV-XVII вв. до наших дней.

Образование Российского государства. Формирование органов государственного

управления. Складывание элементов защиты информации в XV-XVII вв.; достоинства и недостатки системы защиты информации в Российской империи в XIX – нач. XX в.;

24. Законодательная и нормативная базы по информационной безопасности.
Базовые законы в области информационной безопасности, защиты информации, информационных технологий. Понятие тайны. Основные виды тайн. Кодексы, включающие в себя правовые вопросы защиты охраняемой законом тайны.

25. Основные понятия и практика применения Закона о государственной тайне.
Закон РФ «О государственной тайне». Основные понятия. Принципы засекречивания и рассекречивания сведений, составляющих государственную тайну. Допуск и доступ к сведениям, составляющих государственную тайну. Лицензирование деятельности предприятий в вопросах государственной тайны.

26. Коммерческая тайна на предприятии.
Основные понятия. Режим коммерческой тайны. Предоставление сведений, составляющих коммерческую тайну. Правоприменение положений Закона о коммерческой тайне на предприятии.

27. Правовые вопросы защиты персональных данных.
Нормативная документация в области защиты персональных данных. Правоприменение положений нормативных документов в условиях предприятия. Вопросы защиты персональных данных в судебном порядке. Описание политики защиты персональных данных и организационных мер по их защите.

28. Организационные вопросы защиты информации на предприятии.
Основные виды угроз информационной безопасности. Зоны безопасности. Организация охраны предприятия. Виды охраны. Внутриобъектовый режим на предприятии. Прием на работу персонала и работа с постоянными сотрудниками. Защита информации при работе со СМИ и при рекламной деятельности. Организация совещаний и конференций. Модели угроз информационной безопасности.

29. Лицензирование видов деятельности в области защиты информации.
Государственная система лицензирования и сертификации средств защиты информации в Российской Федерации. Органы лицензирования и сертификации, их задачи и функции. Ответственность за правонарушения в области защиты информации. Основные правонарушения в сфере безопасности информации ограниченного доступа, не относящейся к государственной тайне.

30. Международная информационная безопасность.
Правовые основы информационной безопасности в странах Европы, США, Азии. Государственное регулирование функционирования сети Интернет. Национальная защита коммерческой и государственной тайны. Законодательство в области компьютерных преступлений.

31. Структуры вычислительных сетей. Основные понятия и определения в системах разграничения и контроля доступа.
Понятие вычислительной сети. Изучение основных топологий сети. Изучение структуры модели OSI. Понятие системы разграничения и контроля доступа. Модели разграничения доступа.

32. Основные сетевые протоколы безопасности.
Понятие технологии VPN. Изучение протоколов PPP, PPTP, L2TP, IPSec. Протокол Kerberos. Протоколы PAP и CHAP. Протокол RADIUS. Архитектура протокола IPSec.

33. Аутентификация: определения, свойства, требования.
Понятие многофакторной аутентификации, свойства, примеры. Локальная и удаленная аутентификация, основные особенности и свойства. Понятие протокола аутентификации. Протоколы аутентификации без разглашения.

34. Безопасность в автоматизированных информационных системах.
Понятие автоматизированной системы. Структура системы защиты информации автоматизированной системы. Системы защиты информации от

несанкционированного доступа (SecretNet, DallasLock).
35. Средства мониторинга вычислительных сетей.
Понятие системы обнаружения вторжений. Изучение сканеров безопасности (XSpaider, Сканер-ВС, nmap). Тестирование локальной вычислительной сети на проникновение. Изучение методов «белого» и «черного» ящиков.
36. Мультиагентные системы - понятие, структура и типы. Примеры МАС.
Анализ уязвимостей, угроз и атак на информационную безопасность МАС. Проблемы информационной безопасности МАС. Подходы к их решению.
Вопросы информационной безопасности МАС. Уязвимости МАС. Атаки на ИБ МАС, признаки атак на ИБ. Методы обеспечения ИБ МАС. Методы обнаружения атак. Методы противодействия атакам. Подходы к оценке применимости методов обеспечения ИБ МАС.
Алгоритмы безопасного взаимодействия агентов в МАС, подходы и средства контроля показателей эффективности функционирования МАС и обеспечения информационной
37. Интеллектуальные методы управления МАС.
Методы самоорганизации распределенных систем. Методы интеллектуального управления МАС. Смешанные стратегии управления. Роевой интеллект. Примеры применения. Разработка сценариев применения МАС. Проектирование МАС.
38. Основы функциональной безопасности МАС.
Концепция функциональной безопасности. Основные понятия, показатели, методы обеспечения функциональной безопасности МАС. Примеры. Нормативно-правовая основа.
39. Моделирование деструктивного воздействия на МАС.
Основы математического моделирования. Введение в имитационное моделирование. Инструменты имитационного моделирования. Моделирование МАС. Планирование экспериментов. Построение моделей МАС.\

Поурочное планирование

№	Темы	Количество часов
1. Технологии передачи данных и проводных сетей		
1.	Сети передачи данных	1
2.	Оборудование и технологии передачи данных.	1
3.	Сетевые интерфейсы	1
4.	Сетевые интерфейсы	1
5.	Операционные системы	1
6.	Организация и подключение проводной сети передачиданных	1
7.	Интернет протокол и вспомогательные протоколы	1
8.	Интернет протокол и вспомогательные протоколы	1
9.	Конфигурация сетевых интерфейсов и маршрутизации	1
10.	Конфигурация сетевого оборудования	1
2. Технологии беспроводных сетей		
11.	Применение различных типов беспроводных сетей связи: Развитие радиосвязи	1
12.	Сети подвижной связи (1-5G)	1
13.	Сети подвижной связи (1-5G)	1
14.	Беспроводные технологии (Wi-Fi)	1
15.	Беспроводные технологии (Wi-Fi)	1

16.	Радиотехнологии интернета вещей	1
17.	Радиотехнологии интернета вещей	1
18.	Конфигурация оборудования с применением Wi-Fi	1
19.	Конфигурация оборудования с применением Wi-Fi	1
3. Сетевые сервисы		
20.	Мультимедийные сервисы и серверы	1
21.	Технологии сетевых сервисов	1
22.	Технологии сетевых сервисов	1
23.	Программно-конфигурируемые сети	1
24.	Технологии передачи, обработки и хранения данных (Центры обработки данных и облачные хранилища данных)	1
4. Конвергентные сети		
25.	Технологии и оборудование связи	1
26.	Технологии и оборудование связи	1
27.	IP-телефония: АТС, телефоны, смартфоны	1
28.	Концепция и технологии интернета вещей	1
29.	Туманные (пограничные) вычисления	1
5. Введение в информационную безопасность		
30.	Знакомство с понятиями: "объект", "субъект", "атака","угроза", "уязвимость".	1
31.	Кибербезопасность	1
32.	Математические основы криптологии	1
33.	Математические основы криптологии	1
34.	Введение в криптографию	1
35.	Введение в криптографию	1
36.	Основы теории информации в вопросах обеспечения информационной безопасности	1
37.	Технические средства защиты информации	1
38.	Приемы обеспечения информационной безопасностиличного пространства	1
39.	Основы вирусологии	1
6. Правовые аспекты информационной безопасности		
40.	Предпосылки формирования и совершенствование системы защиты информации в России, нормативные и правовые акты в области защиты информации России в период XV-XVII вв. до наших дней	1
41.	Законодательная и нормативная базы по информационной безопасности	1
42.	Основные понятия и практика применения Закона о государственной тайне	1
43.	Коммерческая тайна на предприятии	1
44.	Правовые вопросы защиты персональных данных	1
45.	Организационные вопросы защиты информации на предприятии	1
46.	Лицензирование видов деятельности в области защиты информации	1

47.	Международная информационная безопасность	1
7. Элементы сетевой безопасности		
48.	Структуры вычислительных сетей	1
49.	Структуры вычислительных сетей	1
50.	Основные понятия и определения в системах разграничениях контроля доступа	1
51.	Основные сетевые протоколы безопасности	1
52.	Основные сетевые протоколы безопасности	2
53.	Аутентификация: определения, свойства, требования	1
54.	Безопасность в автоматизированных информационных системах	1
55.	Средства мониторинга вычислительных сетей	1
8. Безопасность мультиагентных систем (МАС)		
56.	Анализ уязвимостей, угроз и атак на информационную безопасность МАС	1
57.	Проблемы информационной безопасности МАС. Подходы ких решению	1
58.	Алгоритмы безопасного взаимодействия агентов в МАС	1
59.	Подходы и средства контроля показателей эффективности функционирования МАС	1
60.	Интеллектуальные методы управления МАС	1
61.	Основы функциональной безопасности МАС	1
62.	Моделирование деструктивного воздействия на МАС	2
63.	Моделирование деструктивного воздействия на МАС	1
64.	Моделирование деструктивного воздействия на МАС	1
65	Резервное время	2
	Итого	68

Список Литературы

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2020. – 432с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2021. – 182с.
3. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2022. – 558с.
4. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, – 64с.