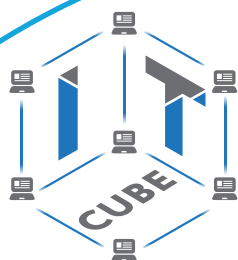




МИНИСТЕРСТВО
ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ОБРАЗОВАНИЕ

НАЦИОНАЛЬНЫЕ
ПРОЕКТЫ
РОССИИ



СЕТЬ ЦЕНТРОВ ЦИФРОВОГО
ОБРАЗОВАНИЯ ДЕТЕЙ «ИТ-КУБ»

РЕАЛИЗАЦИЯ
ДОПОЛНИТЕЛЬНОЙ
ОБЩЕОБРАЗОВАТЕЛЬНОЙ
ПРОГРАММЫ
ПО ТЕМАТИЧЕСКОМУ
НАПРАВЛЕНИЮ

«КИБЕРГИГИЕНА И РАБОТА
С БОЛЬШИМИ ДАННЫМИ»

С ИСПОЛЬЗОВАНИЕМ
ОБОРУДОВАНИЯ ЦЕНТРА
ЦИФРОВОГО ОБРАЗОВАНИЯ
ДЕТЕЙ «ИТ-КУБ»

МОСКВА 2021



С. Г. Григорьев

А. Ю. Львов

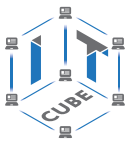
Е. В. Старостина

**Реализация дополнительной общеобразовательной программы по
тематическому направлению «Кибергигиена и работа с большими
данными» с использованием оборудования центра цифрового
образования детей «IT-куб»**

Методическое пособие

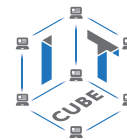
под редакцией С. Г. Григорьева

Москва, 2021



Содержание

Введение	3
Пояснительная записка	4
Нормативная база	4
Основные понятия и термины	5
Описание материально-технической базы	7
Примерная рабочая программа	9
Тематическое планирование	9
Методические рекомендации по проведению уроков.	14
Дидактические материалы	16
Введение в курс. Инструктаж по технике безопасности.	16
Человек в цифровом пространстве.	17
Интернет. История развития и современное состояние.	21
Программное обеспечение. Вредоносное программное обеспечение	26
Финансовая деятельность. Электронные платежи	29
Трансформация понятия частной собственности	33
Общение в сети. Социальные сети и системы обмена сообщениями	34
Цифровой портрет. Социальный рейтинг	39
Цифровая безопасность вне дома	40
Настройка оборудования	41
Поиск и обработка данных. Основные принципы	43
Аналитический подход к информации. Структурирование информации	45
Правонарушения в сфере компьютерной информации	52
Планы учебных занятий	55
Тема урока «Человек в цифровом пространстве»	55
Тема урока «Интернет. История развития»	57
Тема урока «Создание надёжного пароля»	59
Тема урока «Поиск и обработка информации»	62
Тема урока «Создание интеллект-карт»	64
Описание лабораторных работ	68
Лабораторная работа 1. Выбор и установка антивирусного ПО	68
Лабораторная работа 2. Создание надежных паролей	69
Лабораторная работа 3. Настройка Wi-Fi роутера	70
Лабораторная работа 4. Поиск и обработка информации	71
Лабораторная работа 5. Анализ предметной области «Музыкальный сервис»	72
Список доступных источников	77
Материалы для организации и проведения учебно-исследовательской и проектной деятельности	81
Примерные темы по развитию учебно-исследовательских и проектных навыков ...	81



Введение

Сегодня трудно представить современного человека в мире без цифровых технологий. Мобильная связь, Интернет, «большие данные», машинное обучение — эти и многие другие понятия уже прочно вплелись в общественную и культурную жизнь. За последние четверть века цифровизация охватила все сферы человеческой деятельности и трансформировала их. Для примера можно выделить следующие характерные направления, формирующие тенденции современного общества:

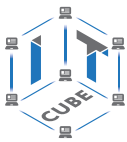
- мобильные устройства;
- умные датчики и интернет вещей;
- технологии, основанные на определении местоположения;
- аутентификация, авторизация и идентификация;
- аналитика и визуализация больших данных;
- доступность вычислительных ресурсов по запросу;
- продвинутые интерфейсы взаимодействия человека и компьютера;
- машинное обучение.

Человечество входит в пору четвёртой промышленной революции, которая кардинально изменит образ жизни человека: систему ценностей, критерии важности, принципы взаимоотношений в обществе. Информация становится доступнее, и, как следствие, образование и самообразование, а также способы самореализации выходят на качественно иной уровень.

Основная среда для использования цифровых технологий — глобальная сеть. При этом современные технологии размывают границы использования цифровой техники в рамках Сети или локально до такой степени, что большинство пользователей даже не задумывается о том, что использует Интернет. Интернет из академического мира шагнул сначала в каждый дом, а дальше стал постоянным спутником человека без привязки к конкретному месту и в любой момент времени. Снижение цен на электронные устройства и на тарифы доступа к Интернету, развитие мобильного интернета и высокоскоростных линий передачи данных являются катализаторами этого процесса. В России пользователей Интернета на данный момент более 80% населения [<https://www.internetworldstats.com/stats4.htm#europe>]. И с каждым годом эта цифра увеличивается. При этом пользователями Интернета являются не только взрослые. Как показывают различные исследования, дети начинают пользоваться Интернетом уже в возрасте 6-8 лет. Становится очевидным, что учиться жить в новых реалиях — необходимость, а бурное развитие цифровых технологий обуславливает потребность наличия соответствующих образовательных материалов, затрагивающих все аспекты их применения.

Важно отметить, что учиться использовать новые технологии нужно не только с позиции грамотного применения и достижения полезного эффекта, но и с точки зрения безопасности. Любая технология имеет обратную сторону. В свою очередь, доступность современных цифровых технологий формирует повышенную активность преступников и правонарушителей в этой сфере, именно поэтому изучение потенциальных факторов кибер-угроз, умение их распознать и противостоять, является неотъемлемой частью образовательного процесса.

Умение использовать цифровые технологии, и Интернет, в частности, нашло свое отражение в виде включения данного умения в Федеральный государственный стандарт общего образования. Но в рамках школьной программы достаточно сложно подробно осветить все аспекты современной цифровой жизни общества, что обуславливает актуальность отдельного курса, посвящённого этим вопросам.



Пояснительная записка

Программа дополнительного образования по тематическому направлению «Кибергиена и работа с большими данными» имеет техническую направленность. Целью программы является формирование у учащихся основных понятий о современных цифровых технологиях, глобальной сети Интернет, основах информационной безопасности. Также программа позволяет получить представления о персональных данных и возможности работы с ними, получить практические навыки анализа и структурирования данных.

Для достижения поставленной цели планируется решить следующие задачи:

Образовательные:

- формирование навыков поиска достоверной информации в Интернете;
- формирование аналитического подхода при работе с большими данными;
- формирование навыков безопасного и рационального использования личных и персональных данных;
- формирование навыков распознавания угрозы в интернет-ресурсах и противодействия им;
- формирование навыков выявления закономерностей в данных.

Развивающие:

- развитие аналитического мышления;
- развитие умения грамотного разделения процесса достижения целей на этапы;
- развитие умения поиска необходимой информации;
- формирование мотивации к соблюдению правил безопасности при использовании цифровых ресурсов.

Воспитательные:

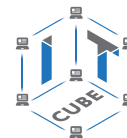
- воспитание умения работать индивидуально и в группе для решения поставленной задачи;
- воспитание трудолюбия, упорства, желания добиваться поставленной цели;
- воспитание ответственности, культуры поведения и общения, информационной культуры.

Программа рассчитана на учащихся в возрасте от 11-ти до 18-ти лет, не требует предварительных знаний и входного тестирования.

Занятия проводятся в группах до 12-ти человек, продолжительность занятия 45 минут, общая продолжительность программы 36 часов.

Нормативная база

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)
2. Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 31.07.2020) «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2020)
3. Паспорт национального проекта «Образование» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 N 16)
4. Государственная программа Российской Федерации «Развитие образования» (Утверждена Постановлением Правительства РФ от 26.12.2017 N 1642 (ред. от 22.02.2021) «Об утверждении государственной программы Российской Федерации «Развитие образования»
5. Стратегия развития воспитания в Российской Федерации на период до 2025 года (Утверждена распоряжением Правительства РФ от 29.05.2015 N 996-р «Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года»)



6. Профессиональный стандарт «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании), (воспитатель, учитель)» (ред. от 16.06.2019 г.) (Приказ Министерства труда и социальной защиты РФ от 18 октября 2013г. № 544н, с изменениями, внесенными приказом Министерства труда и соцзащиты РФ от 25 декабря 2014г. № 1115н и от 5 августа 2016г. № 422н)

7. Профессиональный стандарт «Педагог дополнительного образования детей и взрослых» (Приказ Министерства труда и социальной защиты РФ от 5 мая 2018 г. N 298н «Об утверждении профессионального стандарта «Педагог дополнительного образования детей и взрослых»)

8. Федеральный государственный образовательный стандарт основного общего образования (Утвержден приказом Министерства образования и науки Российской Федерации от 17 декабря 2010 г. N 1897) (ред. 21.12.2020)

9. Федеральный государственный образовательный стандарт среднего общего образования (Утвержден приказом Министерства образования и науки Российской Федерации от 17 мая 2012 г. N 413) (ред. 11.12.2020)

10. Методические рекомендации по созданию и функционированию детских технопарков «Кванториум» на базе общеобразовательных организаций (Утверждены распоряжением Министерства просвещения Российской Федерации от 12 января 2021 г. N P-4)

11. Методические рекомендации по созданию и функционированию центров цифрового образования «ИТ-куб» (Утверждены распоряжением Министерства просвещения Российской Федерации от 12 января 2021 г. N P-5)

12. Методические рекомендации по созданию и функционированию в общеобразовательных организациях, расположенных в сельской местности и малых городах, центров образования естественно-научной и технологической направленностей («Точка роста») — (Утверждены распоряжением Министерства просвещения Российской Федерации от 12 января 2021 г. N P-6)

13. Федеральный закон о защите детей от информации, причиняющей вред их здоровью и развитию 436-ФЗ в ред. Федерального закона от 28.07.2012

14. Федеральный закон «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации».

15. Законодательство в области борьбы с преступлениями против несовершеннолетних.

Основные понятия и термины

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

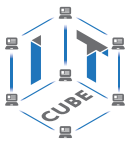
Адрес электронной почты — запись, установленная по RFC 5322, однозначно идентифицирующая почтовый ящик, в который следует доставить сообщение электронной почты.

Видимая сеть — часть Всемирной паутины (~4%), находящаяся в открытом лёгком доступе для широкой публики и индексируемая поисковыми системами.

Вирус — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по различным каналам связи.

Вредоносное программное обеспечение — программы, которые так или иначе наносят пользователям компьютеров ущерб.

Глубокая сеть — множество веб-страниц Всемирной паутины (~96%), не индексируемых поисковыми системами.



Даркнет — изолированная часть, для доступа к которой используются специальные протоколы и программное обеспечение.

Интеллект-карта — метод структуризации концепций с использованием графической записи в виде диаграммы. Реализуется в виде древовидной схемы, на которой изображены слова, идеи, задачи или другие понятия, связанные ветвями, отходящими от центрального понятия или идеи.

Интернет — всемирная система объединённых компьютерных сетей для хранения и передачи информации.

Информация — сведения (сообщения, данные) независимо от формы их представления; сведения об окружающем мире и протекающих в нём процессах, воспринимаемые человеком или специальным устройством; сообщения, осведомляющие о положении дел, о состоянии чего-нибудь; осознанные сведения (знания, выраженные в сигналах, сообщениях, известиях, уведомлениях и т. д.) об окружающем мире, которые являются объектом хранения, преобразования, передачи и использования.

Носители информации — любые материальные объекты, способные без использования дополнительных устройств достаточно длительное время сохранять зафиксированную на них информацию.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор персональных данных — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Оффтоп или оффтопик — сетевое сообщение, выходящее за рамки заранее установленной темы общения.

Персональные данные — любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.

Преступления в сфере компьютерной информации — общественно опасные деяния (предусмотренные главой 28 Раздела 11 УК РФ), которые посягают на сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Программа для ЭВМ — представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определённого результата.

Программное обеспечение — это совокупность всех программ, размещённых на компьютере.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Руткит — программа или набор программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения.

Сетевой этикет — правила поведения, общения в Сети, традиции и культуры интернет-сообщества, которых придерживается большинство.



Спам — сообщения рекламного характера.

Троян — разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения.

Флейм — неожиданно возникшее бурное обсуждение, в развитие которого участники обычно забывают о первоначальной теме, переходят на личности и не могут остановиться.

Флуд — это сообщения в интернет-форумах и чатах, не несущие никакой полезной информации.

Червь — разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные (Интернет) компьютерные сети.

NFC — технология беспроводной передачи данных малого радиуса действия, которая даёт возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров.

Web 2.0 — методика проектирования систем, которые путём учёта сетевых взаимодействий становятся тем лучше, чем больше людей ими пользуются.

World Wide Web — распределённая система, предоставляющая доступ к связанным между собой документам, расположенным на различных компьютерах, подключенных к сети Интернет.

Описание материально-технической базы

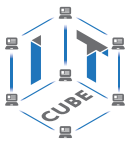
Для организации учебного процесса в рамках реализации дополнительной общеобразовательной программы по тематическому направлению «Кибергигиена и работа с большими данными» согласно распоряжению «Об утверждении методических рекомендаций по созданию и функционированию центров цифрового образования «ИТ-куб» от 12.02.2021 рекомендуется следующее оборудование лаборатории:

Рабочее место преподавателя и ученика:

- ноутбук с жёсткой неотключаемой клавиатурой;
- экран: не менее 15,6 дюймов с разрешением не менее 1920x1080 пикселей;
- процессор: не менее 4-ёх ядер с частотой не менее 1 ГГц;
- объём установленной оперативной памяти должен быть не менее 8 Гбайт (до 24 Гбайт); объём поддерживаемой оперативной памяти (для возможности расширения): не менее 24 Гбайт;
- объём накопителя SSD: не менее 240 Гбайт;
- время автономной работы от батареи: не менее 6 часов;
- вес ноутбука с установленным аккумулятором: не более 1,8 кг;
- внешние интерфейсы:
 - USB стандарта не ниже 3.0: не менее трёх свободных штук;
 - сетевые и беспроводные интерфейсы: LAN, Wi-Fi (с поддержкой стандарта IEEE 802.11n или современнее);
- web-камера;
- манипулятор «мышь»;
- предустановленная операционная система с графическим пользовательским интерфейсом, обеспечивающая работу распространённых образовательных и общесистемных приложений.

Дополнительное оборудование:

- МФУ;
- web-камера;



- интерактивный моноблочный дисплей с диагональю экрана не менее 65 дюймов и разрешением не менее 3840×2160 пикселей.
- Wi-Fi роутер.

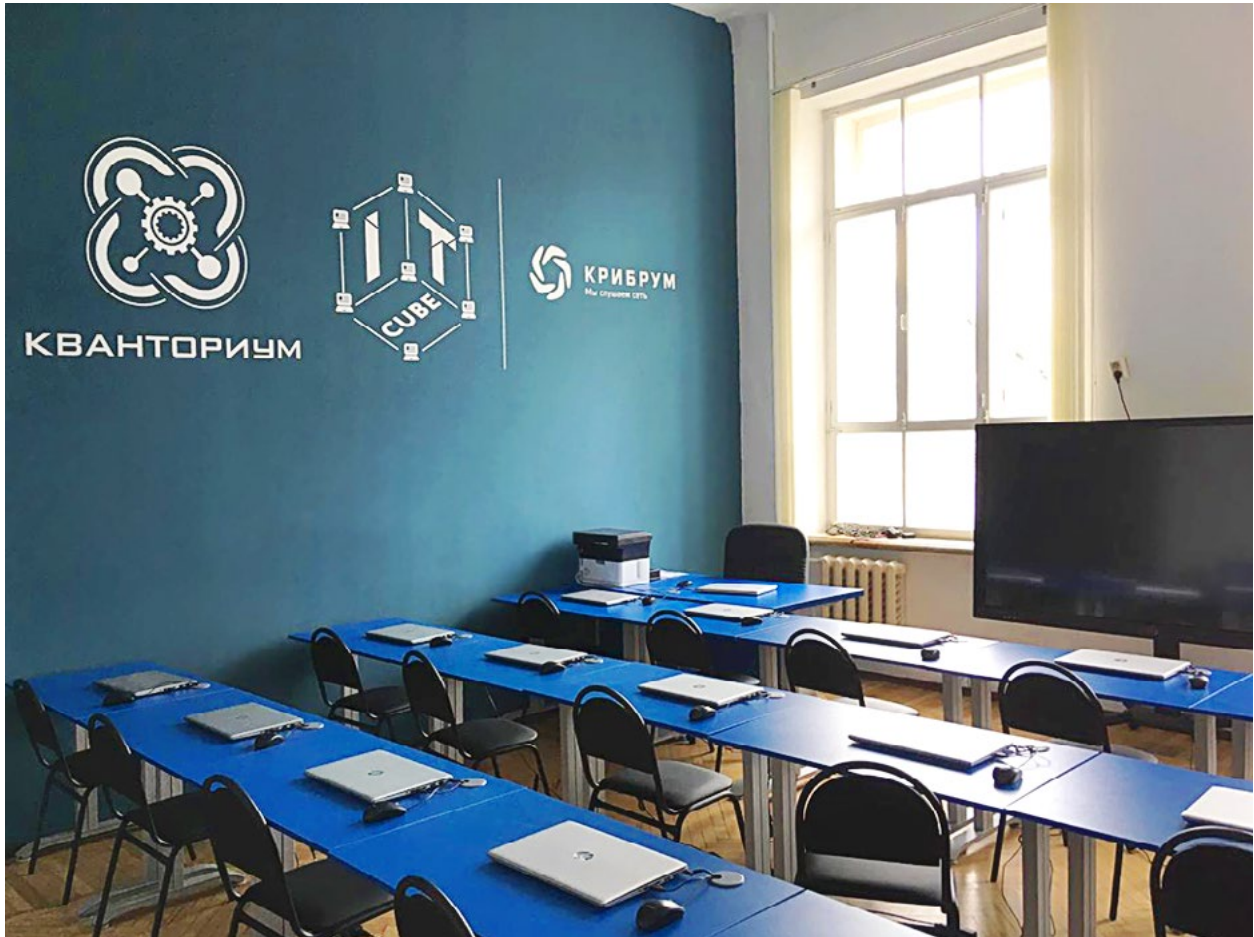
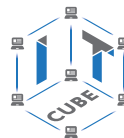


Рис. 1. Аудитория



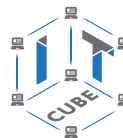
Примерная рабочая программа для организации работы по тематическому направлению «Кибергигиена и работа с большими данными»

Тематическое планирование

№ п/п	Тема	Содержание	Целевая установка урока	Кол-во часов	Основные виды деятельности обучающихся на уроке/внеурочном занятии	Использование оборудования
1	Введение в курс. Инструктаж по технике безопасности.	Введение в курс «Кибергигиена и работа с большими данными». Инструктаж по технике безопасности при работе с оборудованием в аудитории и на рабочем месте ученика.	Ознакомление с проблематикой курса, темами, которые будут рассмотрены на занятиях. Проведение инструктажа по правилам поведения в аудитории и обращению с вычислительной и оргтехникой.	1	Наблюдение за работой учителя, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.
2	Человек в цифровом пространстве.	Основные тенденции современного общества, взаимосвязь реального мира и цифрового. Роль человека в рамках понятия «персональных данных».	Законодательство в цифровую эпоху. Персональные данные. Цифровые данные: Соглашение пользователя. Статистика пользования ресурсами и программным обеспечением. Личные аккаунты.	3	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.
3	Интернет. История развития и современное состояние.	История возникновения и развития вычислительных сетей. Трансформация знания глобальной сетей в XXI веке. Текущее положение в сфере информационных технологий. Зоны Интернета: белая, чёрная, серая.	История возникновения и развития вычислительных сетей. Становление Интернета. «Подводная часть айсберга» — нахождение Интернета в окружающих процессах. Формирование понятия о благонадёжности сетевых ресурсов. Критерии разделения на зоны.	3	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.

Продолжение

№ п/п	Тема	Содержание	Целевая установка урока	Кол-во часов	Основные виды деятельности обучающихся на уроке/внеурочном занятии	Использование оборудования
4	Программное обеспечение. Вредоносное программное обеспечение.	Понятие «программное обеспечение». Трансформация данного понятия в контексте систем облачных вычислений. Вредоносное ПО: типы, принципы, угрозы. Методы противодействия вредоносному ПО.	Ознакомление с понятием программного обеспечения. Трансформация принципов использования ПО. Вредоносное ПО: типы (майнеры, кей-логгеры, ботнеты, вирусы/черви, шифровальщики, модифицированное ПО) и угрозы.	3	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.
5	Финансовая деятельность. Электронные платежи.	Криптовалюта, электронные деньги, игровые валюты. Банковские карты. *Pay/NFC. Онлайн платежи.	Введение в финансовую деятельность. Платёжные системы, системы интернет-банка. Меры безопасности при проведении электронных платежей.	2	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.
6	Трансформация понятия частной собственности.	Подписки как стиль потребления. Типы сервисов: развлечения (музыка, кино, книги, обучение), услуги (каршеринг, доставка). Перенос в реальный мир — ограничение функциональности. Потенциальные риски при использовании подписных сервисов.	Формирование критического взгляда на тенденции в области современного распространения сервисов. Формирование представления о подписных сервисах, отличиях от частной собственности. Очевидные плюсы и минусы.	2	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.
7	Общение в сети. Социальные сети и системы обмена сообщениями.	История средств общения в Интернете. Электронная почта. Современные системы обмена сообщениями. Социальные сети. Сетевой	Формирование норм поведения и потребления в социальных сетях. Этические нормы. Сетевой этикет. Социализация через виртуальность.	4	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.

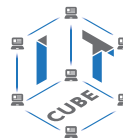


Продолжение

№ п/п	Тема	Содержание	Целевая установка урока	Кол-во часов	Основные виды деятельности обучающихся на уроке/внеурочном занятии	Использование оборудования
		этикет. Потенциальные угрозы, связанные с социальными сетями. Законодательные нормы.	Возможные проблемы, опасности и способы их нейтрализации.			
8	Цифровой портрет. Социальный рейтинг.	Что попало в Интернет — навсегда осталось в нём. Создание репутации с момента начала пользования цифровыми услугами. Родительский контроль. Влияние цифрового портрета на социализацию.	Формирование цифровой грамотности с первых шагов, умения создавать «чистый» цифровой портрет.	2	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, интерактивная доска.
9	Мобильные устройства — ключ в персональный мир.	Современные мобильные устройства, как центр персональной цифровой вселенной. Опасности, связанные с использованием мобильных устройств, минимизация рисков.	Формирование системы представления о трансформации цифровой современной жизни, где мобильное устройство одновременно и ключ к ресурсам и дверь в личное пространство, где и то, и то необходимо оберегать.	2	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, интерактивная доска.
10	Цифровая безопасность вне дома.	Банковские карты/*Pay/NFC. Современные системы видеонаблюдения и их возможности (штрафы для пешеходов, оплата проезда и покупок).	Совокупность современных технологий, позволяющих достичь повышенного комфорта в повседневной жизни: очевидные плюсы и потенциальные угрозы, связанные с подобными сервисами.	2	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, интерактивная доска.

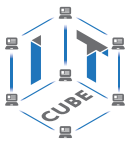
Продолжение

№ п/п	Тема	Содержание	Целевая установка урока	Кол-во часов	Основные виды деятельности обучающихся на уроке/внеурочном занятии	Использование оборудования
		Отслеживание перемещений на основе геолокации, данных мобильного устройства.	Способы минимизации критических отрицательных факторов.			
11	Настройка оборудования.	Типы устройств. Потенциальные проблемные места. Возможные угрозы. Методы предотвращения и защиты от несанкционированного доступа.	Базовая настройка компьютера, телефона, роутера с целью предотвращения несанкционированного доступа к личной информации. Создание надежных и простых паролей.	4	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.
12	Поиск и обработка данных. Основные принципы.	Отправные точки в изучении предметной области. Принципы разделения источников. Принцип последовательного углубления.	Ознакомление с базовыми принципами поиска достоверной информации на основе обработки множественных источников с последовательным углублением.	2	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.
13	Аналитический подход к информации. Структурирование информации.	Классификация, структуризация, анализ полученной информации. Выстраивание системы понятий, организованных в таксономию, формирование семантических связей.	Обработка полученной информации посредством структурирования, классифицирования и последующего анализа предметной области. Выстраивание системы понятий предметной области. Формирование семантических связей между сущностями.	4	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.



Продолжение

№ п/п	Тема	Содержание	Целевая установка урока	Кол-во часов	Основные виды деятельности обучающихся на уроке/внеурочном занятии	Использование оборудования
14	Правонарушения в сфере компьютерной информации.	Основы формирования компьютерного права. Понятие «компьютерное правонарушение». Состав компьютерных правонарушений.	Знакомство с правовыми аспектами, системой понятий, критериями правонарушений в сфере компьютерной информации.	2	Наблюдение за работой учителя, самостоятельная работа, ответы на контрольные вопросы.	Компьютер, проектор, интерактивная доска.
	Итого			36		



Методические рекомендации по проведению уроков.

С одной стороны, ранняя вовлечённость детей и подростков в современные информационные процессы неизбежно приводит к тому, что они сталкиваются не только с их положительными аспектами, но и с негативными. С другой, повышенная динамика развития современных технологий, в частности, цифровых, приводит к тому, что даже специалистам в соответствующих областях необходима постоянная актуализация знаний. Изучая и анализируя эти проблемы, можно определить, что вопросы цифровой гигиены и анализа информационных потоков уже не относятся к компетенции только информатики. В сферу интеграции вовлечены различные предметы из школьной программы: ОБЖ, математика, экономика, история, основы права и многие другие. В сложившихся условиях возникает необходимость формирования единого методического инструментария, который соответствует следующему набору критериев:

— Модульное представление материала с возможностью строить как обзорные уроки, так и углубленно рассматривать некоторые темы.

— Возможность частичного использования материалов в упрощенном виде в рамках интегрированных уроков по разным предметам.

— Представление адаптированного материала к различным возрастным категориям.

— Систематизация возможностей современных цифровых технологий и угроз, которые им сопутствуют, а также методов их выявления и противодействия.

— Примерные материалы, на базе которых возможно построение занятий.

— База знаний в удобном для использования виде с возможностью оперативного изменения и дополнения с учетом развития современных информационных технологий.

Данные методические рекомендации содержат описание предлагаемого инструментария и соответствующие предполагаемые сценарии их использования. Методические рекомендации составлены на основе опыта проведения школьных уроков и занятий в ВУЗе, посвященных вопросам кибербезопасности и рациональному использованию цифровых технологий, опираются на актуальную нормативно-правовую базу, требования ФГОС.

Дополнительно в методическое руководство включены:

- базовые тематические материалы, которые могут быть использованы как основа при построении уроков либо как самостоятельный материал;
- примерные конспекты уроков;
- дидактические материалы;
- примеры контрольно-измерительных материалы с критериями оценивания;
- перечень доступных источников информации, в который включены электронные образовательные ресурсы, тематические подборки материалов в привязке к изучаемым темам.

Цели, которые ставятся в рамках данного курса можно сформулировать следующим образом:

- систематизация знаний в области современных технологий;
- формирование навыков их безопасного использования;
- формирование умений распознавания и адекватного реагирования на проблемы и угрозы, связанные с использованием цифровых технологий.

Достижение поставленных целей зависит от решения конкретных задач соответствующих учебных занятий, а именно:

- систематизация знаний обучающихся в области цифровых технологий по следующим направлениям:
 - Общая компьютерная грамотность.
 - Роль человека в современном цифровом пространстве.



- Персональное и общественное цифровое пространство.
- Общение в Сети.
- Финансово-экономические аспекты современного мира.
- Проблемы и угрозы, связанные с использованием современных технологий.
- связь навыков повседневного использования цифровых технологий с вопросами безопасности и формирование на основе этого соответствующих навыков;
- формирование устойчивых навыков и осознанных подходов к противодействию угрозам и правонарушениям с использованием цифровых технологий;
- формирование устойчивого представления о том, что в сложных и критических ситуациях большую важность имеет тесное взаимодействие детей и взрослых (родителей, учителей, тьюторов, социальных педагогов).

В рамках подготовки к урокам важно помнить о том, что все соответствующие материалы должны соответствовать следующим дидактическим принципам:

- активной вовлеченности;
- доступности;
- мотивации;
- рефлексивности;
- системности;
- открытости содержания.

Под этим подразумевается, что в процессе изучения материала происходит обращение к личному опыту ребенка и развитие этого опыта на основе получения новых знаний или систематизации имеющихся. При этом подача материала должна учитывать возрастные характеристики участников занятия, их социальный статус и жизненный опыт, а также уровень полученных в процессе обучения знаний и иметь форму, которая будет стимулировать к использованию полученных знаний в повседневной жизни, подталкивать к самостоятельному поиску новой информации. В комплексе это дает ребенку возможность соотнести полученные знания и собственный опыт, корректировать модели собственного поведения.

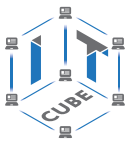
Структурированная информация, представленная в форме простых правил и лаконичных формулировок, как основа новых знаний, дополняет и уточняет единую информационную картину, а также предполагает, что преподаватель имеет возможность свободного частичного или полного использования существующих материалов, а также их актуализации.

При подготовке к фактическому занятию преподаватель на основе методических рекомендаций и дидактических материалов создаёт собственное занятие, дополняя и расширяя его собственными методическими разработками.

При подготовке к уроку необходимо учитывать:

- уровень собственной подготовки;
- состояние материально-технической базы;
- возрастные особенности и уровень развития детей;
- вектор последующей активности по данной теме и ее месте в процессе обучения.

При проведении уроков следует учитывать, что технологии развиваются сверх динамично, создавая тем самым фактическое отставание методик их освоения. Возраст вовлечения детей во взаимодействие с современными технологиями также стремительно снижается. Совокупность этих предпосылок формирует в детях ложное представление о том, что старшее поколение отстает от них в области освоения новых технологий, а также формирует стремление «проверить» преподавателя «каверзными» вопросами и соотнести материал с собственным опытом. При этом необходимо следить за тем, чтобы строго соблюдался комплексный подход к изучению учебных материалов и формированию необходимых навыков.



Дидактические материалы

Введение в курс. Инструктаж по технике безопасности.

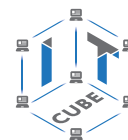
Введение в курс «Кибергигиена и работа с большими данными» и проведение инструктажа по технике безопасности при работе с оборудованием в аудитории и на рабочем месте ученика — первые две ступени, которые необходимо пройти при освоении курса. При этом тесная взаимосвязь этих двух составляющих — залог прочного фундамента всего курса. С первых шагов преподаватель на окружающих примерах вводит учащихся в курс дела, формирует осознанное соблюдение правил техники безопасности и поведения при работе с вычислительной техникой и цифровыми технологиями. Преподаватель знакомит учеников с оборудованием, на котором им придется работать, с особенностями функционирования тех или иных элементов материально-технической базы. В процессе ознакомления, преподаватель в режиме постоянного диалога может выяснить уровень подготовленности учеников, возможность выполнения ими определенных заданий в домашних условиях, задавая простые вопросы, например:

- **У кого дома нет компьютера или ноутбука?**
- **Кто знает какая операционная система на ваших домашних устройствах?**
- **У кого стоит MacOS? У кого Windows? А может быть у кого-то есть Linux?**
- **А какая именно версия операционной системы у вас установлена?**
- **Какие еще операционные системы вы знаете?**

При этом, даже если вопросы кажутся излишне простыми или нелепыми, на основе ответов на каждый из них можно получить достаточно важные для последующей работы данные. Не секрет, что современные мобильные устройства по своим характеристикам и вычислительной мощности зачастую превосходят настольные компьютеры десятилетней давности, поэтому отсутствие компьютера или ноутбука в современном доме — реальность, так как огромное количество повседневных задач возможно решать и без их использования: общение в сети, просмотр фильмов, чтение книг, новостных лент, управление домашними системами, игры и т. п. Знание операционной системы и ее версии показывает наличие любознательности, заинтересованности. Знание альтернативных операционных систем также указывает на наличие любознательности и обширного кругозора по данной теме.

Такой диалог позволяет плавно перейти к ознакомительной части занятия, делая акцент на том, что у каждого из присутствующих в той или иной мере происходит постоянное ежедневное взаимодействие с современными технологиями, что эти технологии тесно вплетены в обиход:

- **Вы умываетесь и чистите зубы по утрам?**
- **Уходя из дома вы закрываете дверь?**
- **Вы оставляете ключи от дома под ковриком перед дверью?**
- **Вы оставляете пароль от своего аккаунта, записанным на бумажке на видном месте?**
- **Вы переходите дорогу на красный свет?**
- **Вы общаетесь на улице с незнакомыми, агрессивными и т. п. людьми?**
- **Вы разлогиниваетесь из своих аккаунтов, используя компьютеры общего пользования?**



— **Вы оставляете свой телефон/ноутбук/планшет разблокированным на парте?**

— **Ваши друзья имеют доступ к вашему аккаунту почты, например, для входа в игру?**

— **Вы рассказываете малознакомым людям о том, что у вас есть в квартире компьютер, ноутбук (особенно на MacOS)?**

— **Часто вы вступаете в спор (конфликты) с незнакомыми людьми в чатах или в обсуждениях?**

— **Вы моете руки возвращаясь домой с улицы? Почему?**

Практически в игровой форме «Вопрос-ответ» до учеников доносится тот факт, что элементы правил безопасности и гигиены в обычной повседневной жизни и в цифровой взаимосвязаны.

Ознакомление с проблематикой курса и темами, которые будут рассмотрены на занятиях, проводится в виде краткого изложения содержания и целевых установок каждого модуля курса.

Человек в цифровом пространстве.

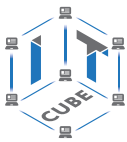
На земле живет более 7,5 миллиардов человек. Каждый из них имеет уникальный набор характеристик: пол, раса, национальность, имя, возраст, рост, вес, цвет глаз и волос, год, месяц, дата и место рождения, и другие. Также человек идентифицируется в современном обществе на основе различных документов и иной информации: свидетельство о рождении, паспорт, СНИЛС, ИНН, адрес, семейное положение, образование, профессия и т. д. В цифровом мире также существует набор данных, связанных с конкретным человеком. Некоторые типы данных дублируют в цифровой форме аналогичные из реальной жизни, а некоторые являются специфичными для цифровой среды. Все это так или иначе является персональными данными. По сути, вся информация о человеке формирует его цифровой двойник.

Любые действия с персональными данными подпадают под регулирование законом и закон детально регламентирует все аспекты данного вопроса (Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 30.12.2020) “О персональных данных” (с изм. и доп., вступ. в силу с 01.03.2021) — см. QR-код слева).



Данный закон следующим образом трактует основные понятия:

- **персональные данные** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- **оператор** — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- **обработка персональных данных** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;



- **автоматизированная обработка персональных данных** — обработка персональных данных с помощью средств вычислительной техники;
- **распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределённому кругу лиц;
- **предоставление персональных данных** — действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.

Ещё недавно мы вносили личную информацию где и когда угодно — для розыгрыша мгновенной лотереи, для получения скидочной карты, и много чего где. Реалии современного информационного общества диктуют новые требования к безопасности персональных данных, а также необходимость формирования культуры обращения с нашей информацией.

Итак, персональные данные — любая информация, которая относится к определённому человеку, или информация, которая позволит однозначно определить какого-либо человека. Если в разговоре со своим другом вы рассказали о каком-то человеке что-либо, что позволит вашему собеседнику узнать, кто это — вы передали персональные данные.

К персональным данным относятся: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, серия и номер паспорта, и другая информация, содержащаяся в тексте Федерального закона, в статье 3.

Кто такой оператор персональных данных? Например, регистрируясь на каком-либо сайте, вводя информацию о себе, или устраиваясь на работу, заполняя формы в отделе кадров, вы передаёте свои данные операторам персональных данных, будь то владелец сайта, работник отдела кадров или организатор какого-либо опроса.

Также в Федеральном законе сказано, что оператор персональных данных — это государственный орган, муниципальный орган, юридическое или физическое лицо, организующее обработку персональных данных.

А что же значит обработка персональных данных?

Представьте, что мы с вами регистрируемся в системе, где нас просят ввести свои Ф.И.О., дату рождения и пол. В этом случае оператором персональных данных выступает организатор данного сайта. Процесс же обработки наших данных может выглядеть как сам факт сбора этих данных, или как хранение, изменение и удаление этой информации из базы данных сайта, как использование наших данных, например, для того, чтобы предложить нам какой-то товар или услугу, основываясь на том, какого мы возраста и пола и т. д.

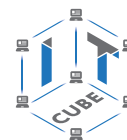
Текст закона о персональных данных может показаться сложным для восприятия, поэтому необходимо запомнить самое главное:

- информация, содержащая любые персональные данные, не принадлежит никому кроме нас;
- если кто-то хочет её получить, он должен обосновать это желание и получить наше разрешение, либо иметь на обработку законные основания;
- этот человек (или компания) должен обеспечить безопасность этой информации.

Наши персональные данные могут обрабатывать только для чётко определённых целей, никто не может их обрабатывать просто так! Если нас при регистрации на конкурс просят указать свои паспортные данные, то это лишняя информация, которая не требуется для участия в конкурсе, и такой сбор **незаконен**.

Также личные данные можно классифицировать по степени их важности:

1. Критические персональные данные:
 - a. СНИЛС
 - b. Паспортные данные
 - c. Биометрические данные



- d. Номер телефона
- 2. Не критические
 - a. Регион проживания
 - b. Электронная почта
- 3. Зависящие от условий предоставления
 - a. Местожительство
 - b. Семейные условия
 - c. Личные фотографии

Как уже было сказано выше, предоставление персональных данных возможно только с личного согласия. В цифровом мире зачастую этот вопрос регулируется пользовательским соглашением.

Ответьте на вопрос:

Часто вы полностью и внимательно читаете пользовательское соглашение?

Прочитайте внимательно пользовательское соглашение компании Яндекс. Оно находится по адресу <https://yandex.ru/legal/rules/> или воспользуйтесь QR-кодом для перехода:

В пользовательском соглашении может быть прописано, что личные данные могут быть использованы не только для нужд сервиса, но и в коммерческих целях, включая **передачу третьей стороне**, то есть для обработки кем-то еще, кроме владельцев сервиса.

Иногда создание личной учетной записи порой является необходимостью. Аккаунт Google, Apple ID, учетная запись на сайте Госуслуг — это ключи, открывающие двери к современным цифровым услугам. Аккаунты в социальных сетях, сервисах обмена сообщениями, игровые аккаунты (которые можно оценить даже в рамках затраченного времени и вложенных средств).



Ответьте на вопросы:

- Сколько важной и ценной информации может храниться за «цифровыми дверями»?
- Готовы ли вы отдать ключи кому-либо «от квартиры, где деньги лежат» (места, где хранятся все/большая часть личных данных)?

Ответы на эти вопросы очевидны — доступ к подобной информации необходимо тщательно оберегать и следить за тем, чтобы никто не имел несанкционированного доступа к ней!

Иной интересный момент, на который необходимо обратить внимание при использовании цифровых продуктов — сбор статистики. Как ни странно, но практически каждое действие в Интернете так или иначе фиксируется и полученные данные подвергаются анализу. С одной стороны, на основе такой статистики поисковые сервисы стараются выдать наиболее актуальную для нас информацию, электронные магазины подобрать интересующие товары и т. п. С другой стороны, владельцы сервиса могут строить цифровой портрет пользователя, рекламные системы — рекламировать соответствующие товары и услуги. Грань между положительными и отрицательными результатами такой обработки информации очень зыбкая.

Помимо этого, собирается статистика использования программного обеспечения, как на мобильных устройствах, так и на ПК. Часто, по умолчанию, данное действие разрешается фактом согласия с пользовательским соглашением. Для того чтобы отключить сбор статистики, нужно найти соответствующий пункт в настройках. Разберем это на примере популярного приложения «Google Keyboard».

После установки это приложение по умолчанию осуществляет отправку обезличенных статистических данных в целях улучшения качества приложения.

Ответьте на вопрос:

Кто пользуется этим приложением? Вы уже отключили сбор статистики?

Отключить это возможно в настройках приложения.

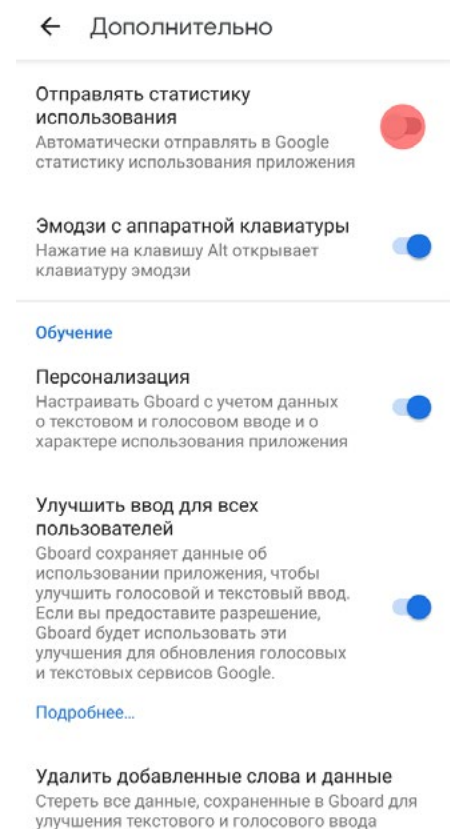
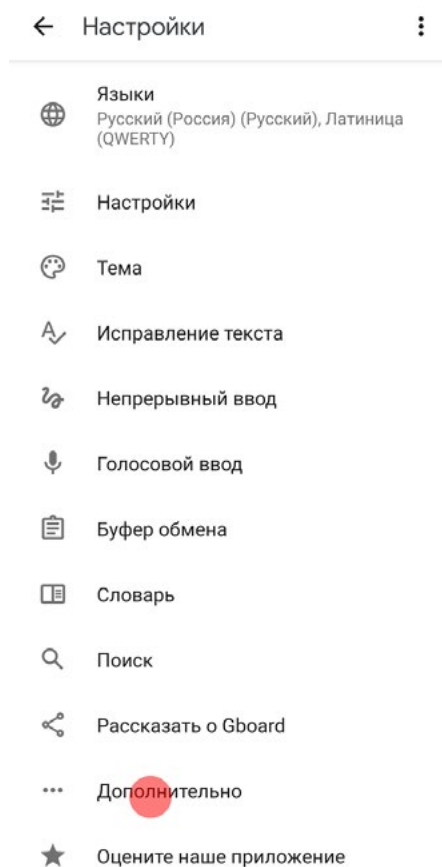
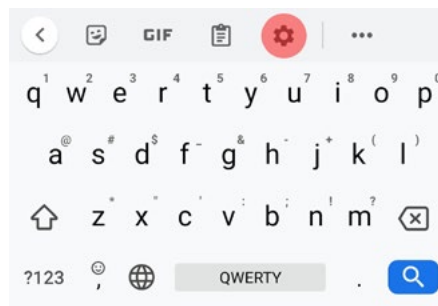


Рис. 4,5,6. Последовательность действий по отключению. сбора статистики



Ответьте на вопрос и выполните задание:

А ваше любимое приложение собирает и отправляет статистику?
Проверьте!

В таком сборе статистики существует дополнительный подводный камень — она передается через Интернет в фоновом режиме, что увеличивает объем трафика.

Ответьте на вопрос:

Почему порой так быстро достигается лимит трафика?

Интернет. История развития и современное состояние.

Для современного человека Интернет вполне естественная среда. История его возникновения и развития уходит в 60-е годы XX века.

Сеть ARPANET, предшествовавшая современному Интернету, была академическим исследовательским проектом, который был профинансирован Агентством передовых исследовательских проектов (Advanced Research Projects Agency, ARPA). Это агентство являлось частью ВПК (военно-промышленного комплекса), в его задачи входило финансирование исследовательских проектов, у которых нет непосредственного коммерческого или военного применения. Изначально сеть связывала Университет Юты с тремя исследовательскими центрами в Калифорнии.



The ARPANET in December 1969

Рис. 7. Карта ARPANET, 1969 год

Проект ARPANET был тестовой площадкой для новой технологии — коммутации пакетов, позволяющей разбивать данные на небольшие «пакеты», чтобы их можно было эффективно передавать по сети. Кроме того, проект имел более практическую цель: повысить эффективность использования дорогих вычислительных ресурсов. Одним из первых приложений ARPANET был протокол Telnet, который позволял подключаться к компьютерам, находящимся на других объектах ARPANET.

К концу 1970 года ARPANET выросла до 13-ти узлов. К ней присоединились учебные заведения Восточного побережья, такие как Гарвард и MIT. Среди ранних узлов была инженерно-консалтинговая компания Bolt, Beranek, and Newman (BBN), которая выполнила инженерную работу по созданию ARPANET.

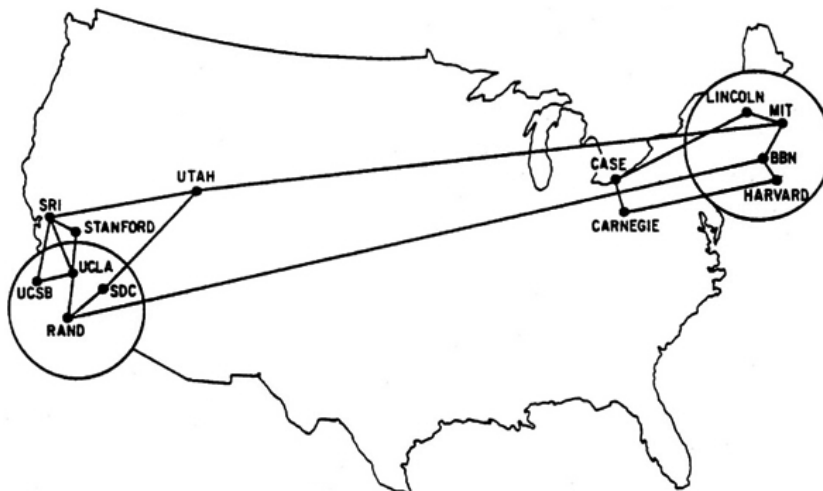


Рис. 8. Карта ARPANET, 1970 год

В 1971 году была разработана первая программа для отправки электронной почты по сети. Эта программа сразу стала популярна среди пользователей сети. Тогда же появились первые списки почтовой рассылки, новостные группы и доски объявлений.

В 1973 году к сети были подключены через трансатлантический телефонный кабель первые иностранные организации из Великобритании и Норвегии, сеть стала международной.

В 1977 году ARPANET состояла из 111 хост-компьютеров, а уже в 1983 году — из 4 000, которые располагались на всей территории США, была налажена спутниковая связь с Гавайями и Европой.

Становилось понятно, что рано или поздно централизованная сеть, продолжая расти, станет неуправляемой. Было принято решение, что ARPANET следует реорганизовать в децентрализованную «сеть сетей». Согласно этой схеме, разные сети контролировались бы разными организациями, но все сети могли бы взаимодействовать по открытым стандартам. 1 января 1983 года сеть ARPANET перешла на протокол TCP/IP (разработан группой исследователей под руководством Винта Серфа и Боба Кана), который успешно применяется до сих пор для объединения сетей. Именно в 1983 году термин «Интернет» закрепился за сетью ARPANET, а 1 января 1983 принято считать официальной датой рождения Интернета.

В 1984 году была разработана система доменных имён (Domain Name System, DNS), что позволило обращаться к узлам сети удобным для человека способом.

Также 1984 год был примечателен тем, что у сети ARPANET появился серьёзный соперник — Национальный фонд науки США (NSF) основал обширную межуниверситетскую сеть NSFNet, которая имела гораздо большую пропускную способность, нежели ARPANET и за год к ней подключились около 10 тыс. компьютеров, название «Интернет» начало плавно переходить к NSFNet.

В 1988 году был разработан протокол Internet Relay Chat (IRC), благодаря чему в Интернете стало возможно общение в реальном времени (чат).

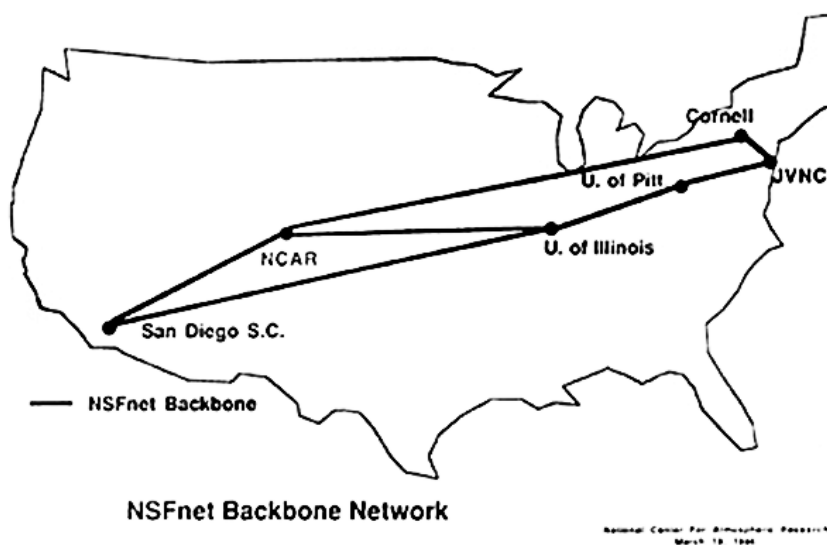


Рис. 9. Карта опорной магистрали NSFnet

2 ноября 1988 года было парализовано около шести тысяч узлов ARPANET сетевым червём. Этот червь получил название Червь Морриса в честь своего создателя — аспиранта Корнельского университета Роберта Таппана Морриса. Это был первый вирус, получивший значительное внимание в средствах массовой информации. Это было одно из первых компьютерных преступлений. Также эта эпидемия показала, как опасно безоговорочно доверять компьютерным сетям. В результате были выработаны новые, более жёсткие, нормы компьютерной безопасности, касающиеся безопасности кода программ, администрирования сетевых узлов и выбора защищённых паролей.

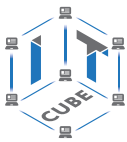
В 1989 году в Европе, в стенах Европейского совета по ядерным исследованиям (ЦЕРН, CERN), родилась концепция Всемирной паутины — World Wide Web. Её предложил знаменитый британский учёный Тим Бернерс-Ли. Он же в течение двух лет разработал протокол HTTP, язык HTML и идентификаторы URI.

В 1990 году сеть ARPANET прекратила своё существование, полностью проиграв конкуренцию NSFNet. В том же году было зафиксировано первое подключение к Интернету по телефонной линии.

В 1991 году Всемирная паутина стала общедоступна в Интернете, а в 1993 году появился знаменитый веб-браузер NCSA Mosaic. Всемирная паутина стала набирать популярность.

В 1995 году Всемирная паутина стала основным поставщиком информации в Интернете, обогнав по трафику протокол пересылки файлов FTP. Формируется Консорциум Всемирной паутины (W3C). Тем самым, Всемирная паутина преобразила Интернет и создала его современный облик и с 1996 года Всемирная паутина почти полностью подменяет собой понятие «Интернет».

В 1990-е годы Интернет объединил в себе большинство существовавших тогда сетей. Объединение выглядело привлекательным благодаря отсутствию единого руководства, а также благодаря открытости технических стандартов Интернета, что делало сети независимыми от бизнеса и конкретных компаний. К 1997 году в Интернете насчитывалось уже около 10 млн. компьютеров, было зарегистрировано более 1 млн доменных имён. Интернет стал очень популярным средством для обмена информацией. Начиная с середины 1990-х годов Интернет имеет кардинальное влияние на культуру, торговлю и технологии, в том числе за счёт распространения практически мгновенного общения через электрон-



ную почту, мгновенного обмена сообщениями, телефонной связи по интернет-протоколу, телефонных звонков, видеосвязи, онлайн-игр, а также Всемирной паутины с дискуссионными форумами, блогами, социальными сетями и интернет-магазинами. Завышенные рыночные ожидания от этих процессов в 2000 году привели к биржевому краху, известному как «Пузырь доткомов».

Начало XXI века было ознаменовано возникновением новой концепции, известной как Web 2.0. По сути, термин «Web 2.0» обозначает проекты и сервисы, активно развиваемые и улучшаемые самими пользователями: блоги, вики-проекты, социальные сети и т. д. Катализация запущенных процессов трансформации была осуществлена лишь спустя некоторое время за счёт роста в сфере мобильных устройств. Следствием данной мобильной революции стало использование многими людьми компьютеров в виде смартфонов, которые они стали повсюду носить с собой, использовать для связи, фото- и видеосъёмки и мгновенного обмена этими данными, а также поиска информации «на ходу», а также использовать в социальной жизни вместо применяемых дома или на работе настольных компьютеров.

На текущий момент Интернет и сетевые технологии пронизывают все сферы человеческой жизни. Порой наличие сетевого взаимодействия настолько прозрачно, что на первый взгляд кажется, что его и вовсе нет.

Ответьте на вопросы:

- Назовите неочевидные примеры использования сетевых технологий?
- Подумайте над тем, в каких сферах сетевое взаимодействие и цифровые технологии активно вытесняют или полностью вытеснили взаимодействие на физическом уровне?

Доступность, огромное количество разнородной информации, широкие возможности — все это привело к тому, что Интернет по своему содержанию начал расслаиваться, это привело к появлению сайтов с непроверенной информацией, содержащих нежелательное или нарушающее законодательство содержимое — так называемая темная сторона Интернета. Обратная — «белая» сторона — сайты государственных организаций, официальные новостные агентства, образовательные ресурсы.

Существует также следующая градация:

- **Видимая сеть** — часть Всемирной паутины (~4%), находящаяся в открытом лёгком доступе для широкой публики и индексируемая поисковыми системами.
- **Глубокая сеть** — множество веб-страниц Всемирной паутины (~96%), не индексируемых поисковыми системами.
- **Даркнет** — изолированная часть, для доступа к которой используются специальные протоколы и программное обеспечение.

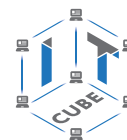
По содержанию можно распределить таким образом:

Белая зона — Видимая сеть:

1. Госсайты
2. Сайты крупного бизнеса
3. Образовательные ресурсы

Серая зона — Глубокая сеть:

1. Социальные сети
2. Новостные сайты
3. Различные сервисы
4. и многое другое



Темная зона:

1. Darknet
2. Фишинговые сайты
3. Контент для взрослых
4. Казино / Букмекерство
5. Нелегальный контент

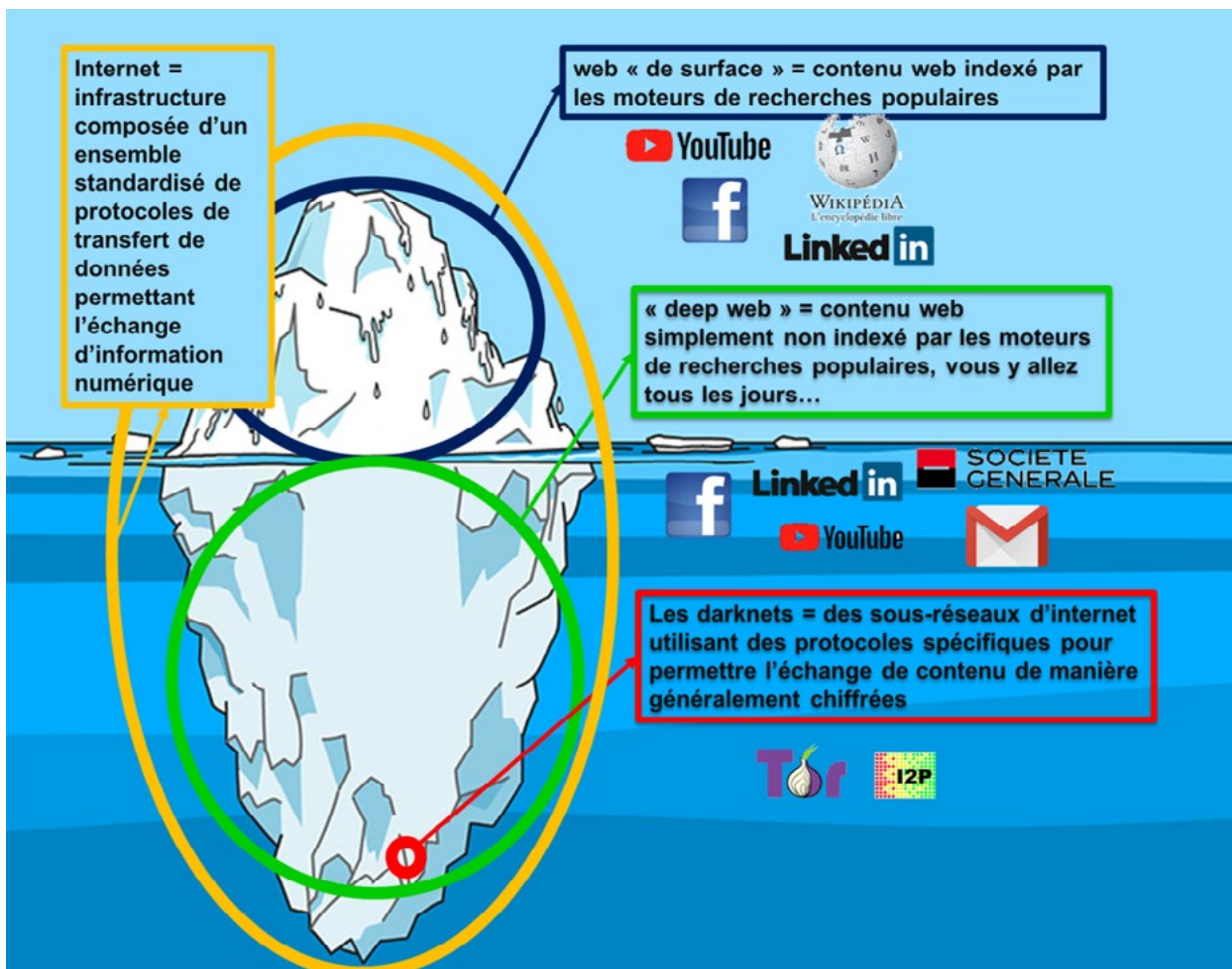


Рис. 10. Зоны Интернета.

Ответьте на вопросы:

- Будете ли вы гулять один ночью в незнакомом малоосвещенном районе с плохой репутацией?
- Будете ли вы выстраивать свое мнение о каком — либо событии на основе непроверенных слухов?
- В чем же основное отличие ресурсов, относящихся к разным зонам?

Ресурсы «белой» зоны содержат официальную, проверенную информацию. Такая информация может быть использована в качестве первоисточников. Информация, полученная из источников в «серой» зоне, всегда требует проверки. Необходимо изучить хотя бы три ресурса подобной тематики, для выяснения истинности полученной информации. Ресурсы «темной» зоны содержат зачастую контент, нарушающий законодательство.

Программное обеспечение. Вредоносное программное обеспечение

Компьютер без программного обеспечения — набор дорогой, высокотехнологичной, но абсолютно бесполезной электроники. Первое программное обеспечение появилось вместе с первыми вычислительными машинами.

Как гласит статья 1261 Гражданского Кодекса РФ — «Программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата». Иными словами, **программное обеспечение** — это совокупность всех программ, размещенных на компьютере.

Для повторного использования программа и данные должны как-то храниться. Для этого в вычислительной технике используются **носители информации** — любые материальные объекты, способные без использования дополнительных устройств достаточно длительное время сохранять зафиксированную на них информацию. История развития информационных носителей — важный фактор развития программного обеспечения как такового. Рассмотрим некоторые из них.

Первыми носителями такой информации стали **перфокарты** — прямоугольные листы тонкого картона с выбитыми на них отверстиями. При помощи считывающего устройства, определялось наличие или отсутствие отверстий в определенных местах и на основе этого формировались команды.

Ответьте на вопрос:

— Давайте постараемся вспомнить, где еще применяется схожий принцип хранения информации?

Впервые перфокарты начали применяться в ткацких станках Жаккарда в начале XIX века. В первой половине XX века наиболее распространенными были перфокарты «формат IBM», размером 187,325 на 82,55 мм. и толщиной 0,178 мм. На ней содержалось 12 строк и 80 колонок. Для хранения 1 Гб информации потребовалось бы приблизительно 22 тонны перфокарт (приблизительно 17м³).

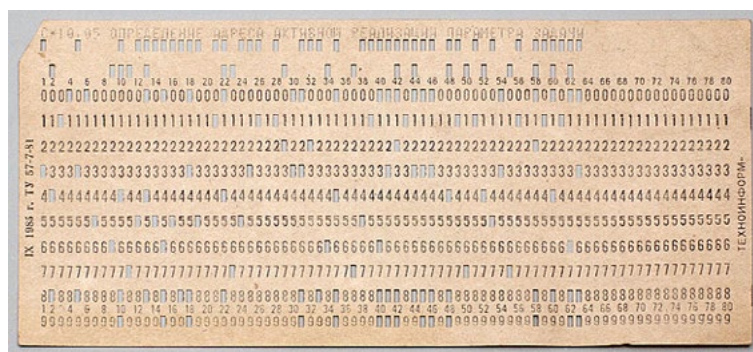


Рис. 11. Перфокарта

Но прогресс не стоял на месте, параллельно развитию самих вычислительных средств, развивались и носители информации. Размеры носителей уменьшались, а скорость доступа и объем сохраняемой информации повышались. Устаревшие носители информации, такие как перфокарты, перфоленты, магнитофонные кассеты, дискеты постепенно исчезали из обращения. На текущий момент на рынке цифровых носителей информации

осталось не так много популярных типов: CD/DVD/BluRay диски, жесткие и твердотельные диски, USB-флешки и SD-карточки. На текущий момент для этих типов, кроме CD/DVD/BluRay дисков, дальнейшее развитие заключается в увеличении объема. Принципиально новых форматов хранения на физических носителях, которые могли бы стать популярными, пока не возникает. Но в середине 2000-х стала набирать обороты принципиально новая концепция хранения данных — облачные хранилища.

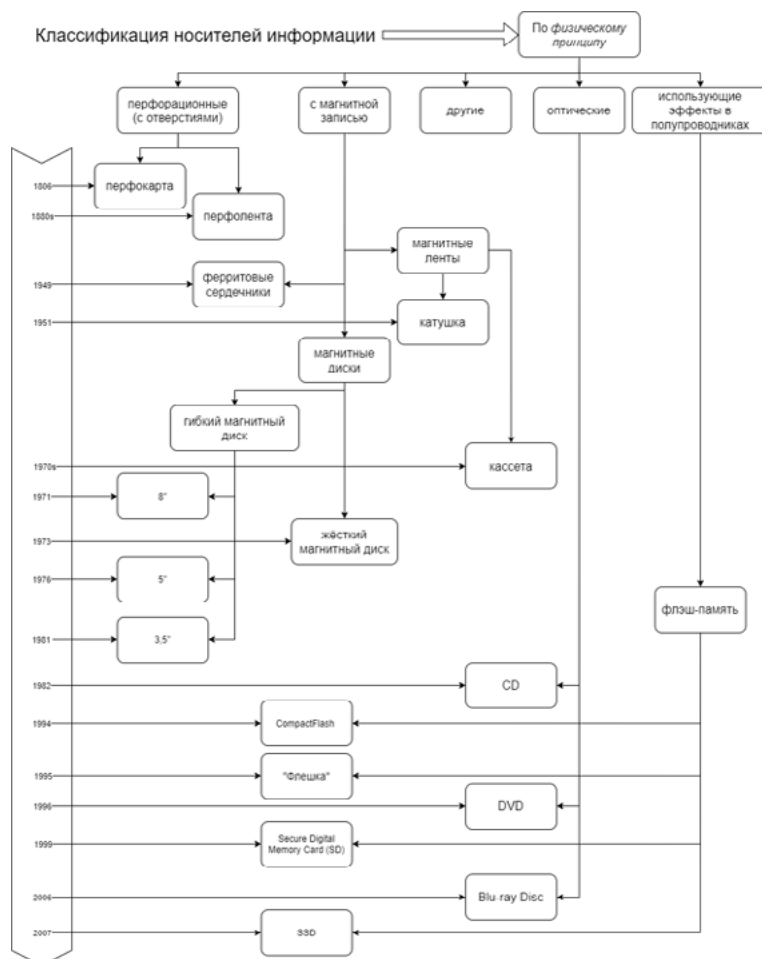
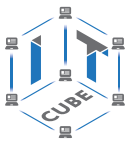


Рис. 12. Классификация носителей информации

Облачные хранилища не являются устройствами в полном смысле этого слова, они представляют собой самый новый и гибкий тип хранилищ данных для компьютеров. Облако — это не место и не объект, а огромное количество серверов, расположенных в центрах обработки данных по всему миру. Когда вы храните документ в облаке, вы храните его на этих серверах. Поскольку все хранится онлайн, облачное хранилище не предусматривает использования локальных накопителей вашего компьютера, что позволяет сэкономить место на них. Информация становится доступной всегда и из любого места, где есть подключение к Интернету. Одновременно с этим бурно развивались и другие интернет-технологии, что позволило в конечном итоге создавать полнофункциональные приложения, работающие целиком в браузере, без необходимости установки на компьютер. Также большую популярность получили мобильные приложения. Тем самым, понятие программного обеспечения компьютера за последнее десятилетие сильно трансформировалось. При этом весьма схожая концепция удаленного запуска программ была до появления персональных компьютеров, когда программное обеспече-



ние запускалось на мощных компьютерах — мейнфреймах, а человек через терминал удаленного доступа получал возможность взаимодействовать с этим программным обеспечением.

Но в разговоре о программном обеспечении нельзя не упомянуть отдельную категорию — вредоносное программное обеспечение (те программы, которые так или иначе наносят пользователям компьютеров ущерб).

Первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Первые вирусные эпидемии относятся к 1986-1989 годам, наиболее крупные из них:

- Brain — вирус распространялся в загрузочных секторах дискет
- Jerusalem — уничтожал программы при их запуске
- червь Морриса — этим червем по сети было заражено свыше 6200 компьютеров, что парализовало сеть
- DATACRIME — поразил около 100 тысяч ПЭВМ на территории Нидерландов.

Тогда же оформились основные классы двоичных вирусов:

- 1987 — сетевые черви (червь Морриса)
- 1989 — «троянские кони» (AIDS)
- 1990 — полиморфные вирусы (Chameleon)
- 1990 — стелс-вирусы (Frodo, Whale).

В 1996 году появился первый вирус для Windows 95 — Win95.Boza, а в декабре того же года — первый резидентный вирус для неё — Win95.Punch.

С распространением сетей и Интернета файловые вирусы всё больше ориентируются на них как на основной канал работы, например, появившийся в 1999 макровирус и сетевой червь Melissa, побивший все рекорды по скорости распространения. Эру расцвета «троянских коней» открывает утилита скрытого удаленного администрирования BackOrifice (1998) и последовавшие за ней аналоги (NetBus, Phase).

В конце 1990-х — начале 2000-х годов с усложнением ПО и системного окружения, закреплением сетей как основного канала обмена данными, а также успехами антивирусных технологий, вирусы стали всё больше заменять внедрение в файлы на внедрение в операционную систему (необычный автозапуск, руткиты) и подменять полиморфизм (единообразная обработка разнотипных данных) огромным количеством видов.

Вместе с тем обнаружение в Windows и другом распространенном ПО многочисленных уязвимостей открыло дорогу червям-эксплоитам. Кроме того, монолитные вирусы в значительной мере уступают место комплексам вредоносного ПО с разделением ролей и вспомогательными средствами (троянские программы, загрузчики/дропперы, фишинговые сайты, спам-боты и пауки). Также расцветают социальные технологии — спам и фишинг — как средство заражения в обход механизмов защиты ПО.

На основе троянских программ, а с развитием технологий p2p-сетей — и самостоятельно — набирает обороты самый современный вид вирусов — черви-ботнеты (Rustock, 2006, ок. 150 тыс. ботов; Conficker, 2008—2009, более 7 млн ботов; Kraken, 2009, ок. 500 тыс. ботов). Вирусы в числе прочего вредоносного ПО окончательно оформляются как средство киберпреступности.

Вредоносных программ существует огромное количество. У каждого из типов есть свои особенности, о которых можно догадаться из названия:

Вирус — это самовоспроизводящийся программный код, который внедряется в установленные программы. Название этого типа вредоносного ПО пришло из биологии — в природе вирусы действуют схожим образом, заражая клетку и заставляя ее воспроизводить их. Заразить компьютер вирусом можно различными способами: от нажатия вредоносной ссылки или запуска файла из письма до заражения во время посещения вредо-



носного сайта. Вирус может выполнять множество разных задач, направленных в первую очередь на нанесение вреда операционной системе.

Червь — программа, которая саморазмножается также, как и вирус, но, в отличие от вирусов, находясь в системе отдельным файлом, ищет уязвимости для дальнейшего распространения.

Троян — это противоположность вирусам и червям. Принцип его действия станет понятен, если вспомнить миф о Троянском коне. Эта программа проникает в систему под видом полезной утилиты и в некоторых случаях даже выполняет свои функции, но вместе с этим скрытно ведет и разрушающую деятельность. Трояны не воспроизводят и не распространяют сами себя, тем не менее сегодня его очень легко подцепить в Интернете.

Руткит — программа или набор программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения.

На текущий момент вредоносные программы чаще всего совмещают в себе признаки и функционал разных типов, например, руткита (маскировать свое присутствие) и червя (самораспространяться).

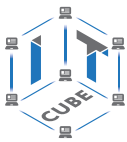
Какие еще угрозы может нести вредоносное ПО? **Кейлогеры** — программы считывающие нажатия клавиатуры и передающие их в сеть для последующего анализа. Такие программы позволяют перехватывать пароли от аккаунтов, номера кредитных карт и их коды, а также иную важную информацию. **Программы-вымогатели** — тип зловредного программного обеспечения, предназначенный для вымогательства, блокирующий доступ к компьютерной системе или предотвращающий считывание записанных в нём данных (часто с помощью методов шифрования), а затем требующий от жертвы выкуп для восстановления исходного состояния. С появлением криптовалют возник отдельный класс программ для нелегального майнинга без ведома владельца вычислительной системы.

Как противостоять таким угрозам? Во-первых, не посещать сомнительные сайты, с которых через уязвимости браузеров может быть установлено зловредное программное. Во-вторых, не устанавливать сомнительное программное обеспечение, код которого может содержать элементы вредоносных программ. В-третьих, не использовать в сетевом программном обеспечении настройки и пароли по умолчанию, либо такие, которое возможно подобрать. Ну и самое очевидное — использовать антивирусное программное обеспечение и сетевые фильтры. Эти, казалось бы, простые правила позволяют минимизировать риск заражения компьютера зловредным программным кодом.

Финансовая деятельность. Электронные платежи

За последнее десятилетие использование безналичных платежей стало доминировать над наличным расчетом. Факторов, повлиявших на это несколько: понижение возраста доступности банковских продуктов, увеличение количества электронных услуг и услуг, предоставляемых через Интернет, появление недорогих устройств, которые можно использовать как инструмент оплаты. Дополнительным фактором можно считать появление криптовалют и игровых валют разного характера. Немаловажную роль сыграло и государство, стимулируя безналичные расчеты на законодательном уровне и инициировав создание национальной платежной системы. На начало 2021 года доля безналичных расчетов составляла около 70 %.

Нет сомнения в том, что отказ от наличности несет повышение комфорта, но с другой стороны, безналичные платежи требуют понимания процессов и повышенного внимания, (отслеживать и контролировать нематериальные вещи сложнее).



Оплата банковскими картами — это, пожалуй, самый распространенный, на данный момент, способ безналичных расчетов. С момента своего появления технология оплаты банковскими картами претерпела много изменений — от оффлайн-использования, заверенного подписью, до бесконтактных технологий. На данный момент, за фактом оплаты картой всегда стоит большое количество процессов, для проведения которых основной средой являются компьютерные сети и сетевые технологии. Год за годом повышается безопасность транзакций, но тем не менее для компьютерных преступников банковские карты остаются лакомым куском, ключом в «квартиру, где деньги лежат». Как можно минимизировать риск потерять средства? Карта — это набор данных, на основе которых предоставляется доступ к счету: номер карты, срок действия, владелец, код проверки, подлинности, пин-код. И если в некоторых случаях мы вынуждены раскрывать номер карты, например для того, чтобы нам могли перевести средства, то все остальные данные, а особенно код проверки подлинности (CCV2) и пин-код необходимо хранить в тайне!

У взрослого человека зачастую в бумажнике есть несколько различных банковских карт. С появлением технологии NFC и платежных систем Google Pay и Apple Pay, смартфон способен заменить их все, предоставляя удобный цифровой инструмент управления платежными средствами.

Интернет-банкинг и банковские приложения также призваны повысить уровень комфорта в сфере банковских услуг, предоставляя возможность совершать оплату услуг и перевод денежных средств без необходимости посещения отделения банка, используя современные сетевые технологии.

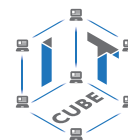
Поэтому возникает необходимость блокировать несанкционированный доступ к устройству, с которого вы совершаете банковские операции: авторизация по паролю, биометрии, сложные пароли для аккаунтов. Но этого порой бывает недостаточно — есть иные способы получить контроль над вашим устройством, а соответственно над вашими деньгами.

Сейчас мы подошли к тому, чтобы узнать — каким образом компьютерные злоумышленники или хакеры могут взять под контроль ваш компьютер или телефон, так как именно с этого начинается подавляющее число компьютерных преступлений. Для этого нужно, чтобы вредоносное программное обеспечение было загружено на ваше устройство. Способов заполучить на свое устройство вредоносное ПО много: перейти по ссылке, ведущей на автоматическую загрузку и установку программного кода; посетить сайт, на котором присутствуют вредоносные скрипты; запустить программу из письма от неизвестного адресата и др.

Теперь разберёмся, что же может натворить такая злобная программа на вашем устройстве. Уже давно прошло то время, когда вирусы создавались ради забавы, чтобы подшутить над знакомыми или незнакомыми людьми. К настоящему моменту злоумышленники пишут трояны, черви и руткиты с конкретной целью — получить выгоду, похищая конфиденциальную информацию обычных пользователей.

Итак, попав на ваше устройство, вредоносная программа уже нарушает конфиденциальность. В общем случае итог ее работы таков: все интересующие злоумышленника данные, которые есть на зараженном устройстве, отправляются злоумышленнику.

Давайте представим такую ситуацию: вы решили зайти в свою почту — вводите логин/пароль и... мошенник получает доступ ко всем вашим письмам. Происходит это потому, что специальная программа фиксирует пароль в момент входа. Многие скажут, что пароль обычно не отображается открыто, а заменяется на точки или звездочки. Сейчас и это не помеха для мошенников — разработанные ими вредоносные программы умеют считывать и записывать нажатия на клавиатуру или перехватывать введенный пароль в



памяти зараженного устройства. По такому же принципу, работая на зараженной машине, можно «подарить» мошеннику данные для входа в личный кабинет банка.

Теперь представьте, что вы часто делаете покупки в интернет-магазине, который ни разу вас не обманывал и заслужил доверие не только ваше, но и многих других пользователей. В этот раз вы снова заходите на привычный сайт, оформляете заказ, вводите информацию со своей карты, чтобы расплатиться... И снова мошенник получил то, что хотел — все о вашей карте. Как же так получилось? Все очень просто — в момент, когда вы заходили на сайт этого проверенного магазина, злобная программа «подсунула» вам сайт, как две капли воды похожий на этот магазин и вы добровольно ввели там все, о чем вас попросили.

Бывает, что мошенники создают такие условия, при которых пользователи сами добровольно и охотно готовы предоставлять им свои сбережения. Такой вот «взлом» сознания и психологии людей называется «социальной инженерией», и те, кто ей владеют, могут с легкостью усыплять бдительность, входить в доверие и незаметно управлять теми, кого они сделали своей целью. Наиболее яркий пример социальной инженерии сегодня — это фишинг.

Те, кто знаком с английским, подумают, что это название можно перевести как «рыбалка», и на самом деле так и есть — мошенники «забрасывают удочку» с приманкой, а затем им остается немного подождать, пока кто-нибудь не «клюнет» на их привлекательные предложения. И вот тогда-то можно выудить из попавшегося простофили всё необходимое — конфиденциальную информацию и/или деньги.

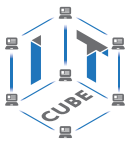
Злоумышленники понимают, что человек в любой ситуации в первую очередь ищет выгоду для себя — ведь согласитесь, вряд ли кто-нибудь будет покупать дорогую вещь в первом попавшемся магазине, если в соседнем она продается ощутимо дешевле. Но иногда поиск выгоды активизирует другую природную черту человека — жадность, отключая при этом здравый смысл и логику. И именно этим человеческим свойством пользуются мошенники, используя в роли «приманки» в своих схемах предложения, невероятно выгодные и потому очень привлекательные.

Схема их работы проста — вам дают несложное задание (например, ответить на несколько вопросов, посмотреть несколько роликов, попробовать что-нибудь угадать и тому подобное) — этим мошенники пытаются создать у вас ощущение какой-то деятельности. В результате после всех операций на вашем как бы «счете», который просто является картинкой на сайте, появляется некая сумма, порой внушительная. Затем становится активной кнопка, отвечающая за вывод средств на ваш кошелек, и после попытки их забрать происходит то, что отличает фишинговые сайты от других — под любыми предложениями из вас начинают вытягивать деньги. Это может быть оплата комиссии за перевод средств, оплата открытия вашего счета, оплата залога и еще множество причин, почему вам надо перевести деньги на указанные счета. Чтобы завоевать ваше доверие, мошенники постараются продемонстрировать работоспособность рекламируемого сайта и то, что деньги с него действительно будут вам перечислены.

Однако большинство фишинговых сайтов работают более аккуратно, и выявить их тяжелее. Например, это может быть сервис по переводу средств с карты одного банка на карту другого, интернет-магазин, сервис покупки билетов, ресурс несуществующего банка или поддельная страница кредитной организации, где вы обслуживаетесь. В таком случае должно насторожить несколько факторов — если это сервис, то цены на услуги или товары могут быть очень низкими и сильно отличаться от рыночных.

Также, с большой вероятностью, фишинговыми окажутся такие сайты:

- сайты, которые при предложении произвести оплату онлайн вас не перенаправляют на страницу банка с защищенным подключением «https://» (буква «s» означает secure — безопасное соединение);



- на странице оплаты отсутствуют логотипы программ MasterCard SecureCode и Verified by Visa, которые с помощью технологии 3D-Secure дополнительно защищают вас во время покупок в Интернете. Если онлайн-магазин поддерживает эту технологию, после ввода реквизитов карты он перенаправит вас на безопасную интернет-страницу банка. Для подтверждения покупки банк должен отправить смс с одноразовым паролем на мобильный номер, привязанный к карте или счету;
- если на сайте отсутствуют сведения о регистрации организации (адрес, регистрационный номер, контактные данные), или такие данные не соответствуют действительности;
- если банк, на сайте которого вы находитесь, отсутствует в справочнике по кредитным организациям Центрального Банка РФ.

Но методы социальной инженерии не ограничиваются этим, теперь представьте, что вам звонит оператор, представляется сотрудником вашего банка и сообщает, что по вашей карте осуществляется подозрительная или мошенническая операция, и чтобы ее остановить, требуется назвать номер карты, пин-код или CVV\CVC код и последнюю операцию, которую вы совершали. Тот, кто положит трубку, поступит правильно. Почему? Да потому что это тоже пример фишинга. Во-первых, сотрудники банка не имеют права узнавать у вас такую информацию о карте, как ПИН-код или CVV\CVC код. Во-вторых, сегодня на вооружении у банков стоят автоматизированные системы, которые анализируют все операции клиентов. Такая система называется «антифрод». При выявлении подозрительных операций, система автоматически блокирует карту, а уже потом клиенту приходит уведомление, что его карта заблокирована в связи с возможными мошенническими операциями по ней. Поэтому будьте бдительны и хорошо подумайте, прежде чем отдавать свои персональные данные в чужие руки, даже если человек выглядит и представляется официально.

Никогда не поддавайтесь своим эмоциям, и даже если вам в социальной сети пишет лучший друг с просьбой перевести небольшую сумму на какой-то счет, потому что он попал в сложную ситуацию, не бросайтесь делать перевод. Лучше позвоните ему и лично узнайте, действительно ли он, а не мошенник, писавший от его имени, нуждается в деньгах.

Резюмируя, перечислим правила, которые нужно помнить:

- не переходить по неизвестным ссылкам, не перезванивать по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверять адреса с доменными именами официальных сайтов организаций, а номера проверять в официальных справочниках,
- не сообщать персональные данные, а уж тем более пароли и коды, никому. Сотрудникам банка они не нужны, а мошенникам откроют доступ к вашим деньгам. Если кто-либо пытается узнать их у вас — это мошенник. Те же правила для интернет-кошельков: никогда не сообщать логин и пароль от своего аккаунта,
- Не хранить данные карт на компьютере или в смартфоне. Не использовать чужие устройства,
- Проверять информацию. Если вам говорят, будто вы что-то выиграли или с вашей карты «случайно» списали деньги и нужно назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне вашей карты,
- Если вам сообщают, что родственники или друзья попали в беду, постарайтесь связаться с ними напрямую,
- Обязательно поставить и регулярно обновлять антивирус на всех своих устройствах, включая мобильные. Хороший антивирусный пакет всегда включает защиту от фишинга и вирусных программ. Не забывать про своих пожилых родственников, которым очень нужна в этом ваша помощь.



Трансформация понятия частной собственности

Конъюнктура современного рынка формирует новые модели потребления товаров и услуг, прежние же понятия собственности и владения чем-либо также трансформируются и обретают иные черты. Для начала рассмотрим пример владения программным обеспечением. С появлением индустрии платного программного обеспечения модель взаимодействия пользователя и автора ничем не отличалась от любого другого рынка — у автора есть товар, который пользователь покупает для персонального владения. Оплатив единой разовой, пользователь неограниченно во времени мог пользоваться всем функционалом приобретенного программного продукта. В начале XXI века появилась новая система, когда пользователь не покупает программный продукт, а оплачивает возможность использования функционала этого продукта в течении времени подписки. Соответственно, чем больше время единоразовой подписки, тем ниже стоимость владения. С появлением облачных сервисов данная модель успешно прижилась и в этой сфере: онлайн-овые хранилища, вычислительные ресурсы и т. д.

Подписка на сервисы и услуги или аренда чего-либо — изобретение не XXI века, до того, как такая модель появилась в цифровом мире она успешно существовала в мире реальном. Появление и развитие мобильной связи создало прекрасный плацдарм для того, чтобы данная модель прижилась в массах, но именно возможности цифровизации этой модели открыли широкие горизонты по ее применению. При этом нивелируется психологический барьер, возникающий в контексте того, что любой цифровой объект не имеет материального воплощения. Суть явления заключается в том, что сложно платить за нематериальный объект, за «ничто» и «ничто». И это, в свою очередь, породило волну пиратства — незаконного использования цифровых ресурсов. В подписной модели пользователь не покупает набор «нулей и единиц», он покупает вполне определенный и понятный функционал: отсутствие рекламы при просмотре видео, прослушивание музыки в фоне, дополнительное дисковое пространство для хранения фотографий, функции обработки фотографий на основе машинного обучения и т. д. И даже избыточность сервисов в подписке (1 000 000 песен и столько же фильмов) не является останавливающим фактором, а наоборот выдается за преимущество и вызывает фиктивное чувство свободы, а незначительные месячные платежи за подписку не вызывает финансового дискомфорта. За последние 10—15 лет система подписок проникла практически во все сферы цифровой жизни, а с развитием технологий постоянно раздвигает рамки применения. На текущий момент можно сказать, что на массовом рынке аренда и подписки вытеснили непосредственное владение: раньше фильмы, музыку, ПО покупали на носителях, теперь подписка на стриминговые сервисы позволяет получить любой контент в любое время.

Несомненно, цифровой способ применения подписок и аренды сильно трансформировал саму идею в принципе, что позволило совершить данной модели обратный переход в реальный мир, например, в виде каршеринга, который уже сейчас во многих случаях становится дешевле по стоимости владения чем персональный автомобиль.

Но и это не предел того, как можно использовать данную модель в реальном мире сейчас, некоторые производители пытаются применять ее на стыке физических объектов и цифровой составляющей. Например, принтеры компании HP, не печатающие без оформленной подписки на сервисы производителя или автомобили марки BMW, имеющие единую техническую конфигурацию в рамках модельного ряда, но с возможностью включить определенный функционал только по подписке (зимний пакет, ассистенты водителя и т. п.).

Общение в сети. Социальные сети и системы обмена сообщениями.

Самым первым способом общения в сети была электронная почта. Она по составу элементов и принципу работы практически повторяет систему обычной бумажной почты, заимствуя как термины (почта, письмо, конверт, вложение, ящик, доставка и другие), так и характерные особенности — простоту использования, задержки передачи сообщений, достаточную надёжность и, в то же время, отсутствие гарантии доставки.

Появление электронной почты можно отнести к 1965 году, когда сотрудники Массачусетского технологического института Ноэль Моррис и Том Ван Влек написали программу «mail» для операционной системы CTSS (Compatible Time-Sharing System), установленную на компьютере IBM 7090/7094.



Рис. 13. IBM 7090/7094

```

user@server ~$ mail
mail version 5.1 5/9/95. type / for help.
~/var/mail/user*.0 messages
?
Mail Commands
t message list      type messages
a                    auto and type next message
e message list     edit messages
f message list     give head lines of messages
d message list     delete messages
o message list file append messages to file
u message list     undelete messages
r message list     reply to message headers
@ message list     apply to message headers and all recipients
p message list     make messages go back to /var/mail
s <user list>      mail to special users
q                    quit, saving unresolved messages in mbox
Q                    quit, do not remove system mailbox
k                    print out active message headers
!                    shell escape
!d [directory]     cd dir to directory or home if none given
?
t message list consists of integers, ranges of same, or user names separated
by spaces. If omitted, Mail uses the last message typed.
o <user list> consists of user names or aliases separated by spaces.
Aliases are defined in /mail in your home directory.

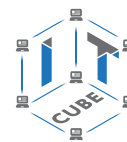
```

Рис. 14. Интерфейс программы «mail»

Развитие электронной почты шло через развитие взаимодействия пользователей на многопользовательских системах. Они могли, используя программу «mail» или её эквивалент, пересылать друг другу сообщения в пределах одного мейнфрейма. После возникновения локальных сетей появилась возможность переслать сообщения пользователю на другой машине — для этого также использовалось указание имени машины и имени пользователя на машине. Адрес мог записываться в виде «jack!beanstalk» (пользователь jack на компьютере beanstalk).

В 1971 году Рэй Томлинсон разработал почтовую программу для пересылки сообщений по распределенной сети, за основу были использованы две другие — почтовая программа для интрасети и экспериментальная программа пересылки файлов. К марту 1972 года он модернизировал свою программу для использования в сети ARPANET. Именно в это время в адресах электронной почты стал использоваться символ @. На телетайпном аппарате «модель 33», который был в распоряжении Рэя Томлинсона, эта клавиша использовалась для пунктуации и обозначения английского предлога «at» (на). Таким образом, электронный адрес вида <имя_пользователя>@<имя_сервера> обозначает не что иное, как «пользователь с таким-то именем на таком-то сервере».

Адрес электронной почты — запись, установленная по RFC 5322, однозначно идентифицирующая почтовый ящик, в который следует доставить сообщение электронной почты. Адрес состоит из двух частей, разделенных символом «@». Левая часть указывает имя почтового ящика, часто оно совпадает с логином пользователя. Правая часть адреса указывает доменное имя того сервера, на котором расположен почтовый ящик.



Ответьте на вопросы:

- Где и как ещё сейчас используется символ «@» при общении в сети?
- Знаете ли вы, что раньше можно было передавать логин и пароль через URL сервиса и эту возможность заблокировали по соображениям безопасности?

В июле 1972 года Ларри Робертс написал первую почтовый клиент — программу, которая позволяла создавать и сортировать списки писем, выбирать и читать требуемое сообщение, сохранять послание в файле, а также пересылать электронные письма на другой адрес или автоматически отвечать на полученное послание. Эта программа позволяла даже неспециалистам легко управляться с электронной почтой и поэтому за короткий срок программа завоевала огромную популярность.

По исследованию ARPA в 1973 году 75% всего трафика сети ARPANET приходилось на электронную почту.

В 1975 году появилась первая почтовая рассылка. Ее основателем стал Стив Уолкер, а модератором, а по сути дела редактором, и человеком, ответственным за выход рассылки, стал Эйнар Стефферуд. Первая почтовая рассылка не была автоматизирована, всё делалось вручную.

В 1984 году была разработана система доменных имён (Domain Name System, DNS), что позволило обращаться к узлам сети удобным для человека способом, а адреса электронной почты получили тот вид, в котором мы знаем их сейчас — jack@beanstalk.org.

В 1988 году был разработан протокол Internet Relay Chat (IRC), благодаря чему в Интернете стало возможно общение в реальном времени (чат). IRC предоставлял возможность как группового, так и частного общения. Для группового общения было предусмотрено два различных варианта. Первый, когда сообщение отправлялось списку пользователей, при этом на сервер IRC отправлялся список, сервер выделял из него отдельных пользователей и отправлял копию сообщения каждому из них. Второй, более эффективный, использование каналов. В этом случае сообщение отправлялось непосредственно серверу, а сервер отправлял его всем пользователям в канале.

Ответьте на вопрос:

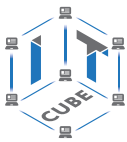
- Какие аналогии с современными средствами общения в сети вы видите?

В 1994 в сети появился новый тип программ — интернет-пейджер. Первым, вопреки общественному мнению, был PowWow, разработанный компанией Tribal Voice, основанной Джоном Макафи. А в 1996 появляется мессенджер ICQ от компании Mirabilis, название сервиса — сокращенная аббревиатура от англоязычной фразы «I seek you» — Я тебя ищу. Именно с этого момента сервисы мгновенного обмена сообщениями начинают набирать популярность.

В 1995 году Рэнди Конрадом была создана первая социальная сеть в современном понимании — Classmates.com. Концепция оказалась очень востребованной, и с этого года начинается бурное развитие социальных сетей в Интернете.

4 июля 1996 год запускается в коммерческую эксплуатацию почтовый сервис Hotmail — эта дата символизировала освобождение от интернет-провайдеров, так как почтовые сервисы до этого времени были только под их управлением.

8 марта 1997 год компания Yahoo!, один из интернет-лидеров того времени, приобретает портал RocketMail — один из первых бесплатных почтовых сервисов, и создает на его основе сервис Yahoo! Mail.



15 октября 1998 год заработала бесплатная электронная почта от Mail.ru. 26 июня 2000 год запущена Яндекс.Почта.

18 марта 1999 года американский программист Брэд Фицпатрик запускает сервис LiveJournal. LiveJournal или Живой Журнал блог-платформа для ведения онлайн-дневников (блогов), а также отдельный персональный блог, размещенный на этой платформе. Предоставляет возможность публиковать свои и комментировать чужие записи, вести коллективные блоги («сообщества»), добавлять в друзья («френдить») других пользователей и следить за их записями в «ленте друзей» («френдленте»).

В феврале 2004 появляется Facebook, который за несколько лет становится самой популярной в мире социальной сетью.

1 апреля 2004 год компания Google запускает собственный бесплатный почтовый сервис Gmail, отличительной особенностью которого был огромный по тем временам размер почтового ящика для хранения почты — 1Гб! А в 2005 году сервис получает интеграцию с сервисом мгновенного обмена сообщениями GTalk, построенном на базе протокола XMPP.

26 марта 2006 года был основан проект «Одноклассники» — российский аналог Classmates.com.

Также в марте 2006 года началась история сервиса Twitter — социальной сети для публичного обмена сообщениями при помощи веб-интерфейса, SMS, средств мгновенного обмена сообщениями.

В октябре 2006 года появилась российская социальная сеть ВКонтакте, которая во многом копировала Facebook.

В 2009 вышла первая версия мессенджера WhatsApp. 19 февраля 2014 года компания Facebook Inc. объявила о приобретении WhatsApp.

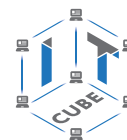
В октябре 2010 появился сервис Instagram — приложение для обмена фотографиями и видеозаписями с элементами социальной сети.

14 августа 2013 года представлен первый клиент Telegram.

Эти вехи сформировали современную систему общения в сети в том виде, в котором мы знаем ее сейчас. И несомненное благо иметь возможность общаться в режиме реального времени с собеседниками во всех уголках мира, но, к сожалению, доступность такого общения несет в себе и отрицательные стороны.

Первой проблемой, которая возникла в сетевом общении, стала проблема назойливой рекламы — спам. Первоначально слово «SPAM» появилось в 1937 году. Оно расшифровывалось как «Spiced ham» (острая ветчина), а также «Shoulder of pork and ham» (свинные лопатки и окорока) и было товарным знаком для мясных консервов компании Hormel Foods Corporation. После Второй мировой войны остались огромные запасы этих консервов, изготовленные для снабжения во время войны не только американских солдат, но и солдат союзников. Для того, чтобы сбыть свою продукцию не первой свежести, компания Hormel Foods провела первую в своем роде рекламную кампанию. Слово «SPAM» бросалось в глаза на каждом углу, с витрин всех дешёвых магазинов, оно было написано на бортах автобусов и трамваев. Это слово можно было прочесть на фасадах домов и в газетах. Реклама консервов «SPAM» непрерывно транслировалась по радио. Всемирную известность в применении к назойливой рекламе термин «SPAM» получил благодаря знаменитому скетчу «Спам» из известного телевизионного шоу «Летающий цирк Монти Пайтона».

В 1986 году в конференциях Usenet появилось множество одинаковых сообщений от некоего Дэйва Родеса, который рекламировал новую финансовую пирамиду. Заголовок гласил: «Заработай кучу денег», а в письмах содержалась инструкция, как это сделать. Автор с завидным упорством продолжал дублировать свои тексты, и они настолько прие-



лись подписчикам, что их стали сравнивать с рекламируемыми в скетче консервами. Так за словом «спам» закрепилось новое значение, позднее перешедшее в компьютерную терминологию для обозначения назойливых рекламных рассылок.

Приблизительно в то же время, благодаря распространению электронной почты, появились так называемые «Нигерийские письма» — вид мошенничества, типа писем счастья, в которых мошенники просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются все более крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, и т. п.

Ответьте на вопрос:

— Какие современные виды подобного мошенничества вы знаете?

В начале 2000-х набрали популярность сервисы сокращения URL, помогающие создавать более короткие адреса, но так как изначально по такому короткому адресу не было видно конечной точки перехода, этим стали пользоваться мошенники и преступники, рассылая сообщения с заманчивыми предложениями и короткими адресами, ведущими на собственные сайты фишингового характера или содержащие вредоносное программное обеспечение.

Ответьте на вопрос:

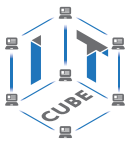
— Как вы поступите, если от меня в личку во ВКонтакте придет сообщение: «Нужно срочно выполнить тест на оценку! Тест по адресу <https://is.gd/xCEzgL>? («Не верь глазам своим»)

Иная потенциальная угроза лежит в самой плоскости интернет-общения. Во-первых, анонимность пользователей сервисов общения, даже в социальных сетях реальные личности зачастую скрываются за вымышленными псевдонимами. Во-вторых, трансформация понятия «друг» — интернет-друзья порой даже не знакомы лично, не говоря уже о том, что такие знакомства поверхностны и основываются на каких-либо общих интересах и увлечениях. И принцип «Не разговаривай с незнакомцем» в цифровом мире не работает! Учитывая огромную популярность и влияние социальных сетей на жизнь людей в современном мире, это влечет за собой весомые проблемы. И формирование норм поведения и потребления в социальных сетях, этических норм сетевой активности, так называемого сетевого этикета, является важной задачей.

Понятие сетевого этикета зародилось еще в середине 80-х годов XX века и включает в себя правила поведения, общения в Сети, традиции и культуры интернет-сообщества, которых придерживается большинство. Эти правила не являются всеобщими и жестко регламентированным, но их соблюдение позволяет минимизировать потенциальные проблемы в общении:

— Перед тем, как становиться активным участником сетевого сообщества, желательно в течение определённого времени посещать его, оставляя минимум собственных комментариев, чтобы привыкнуть к правилам сообщества, а также узнать о некоторых его традициях.

— Прежде чем задать вопрос, воспользуйтесь поиском — быть может, этот вопрос уже задавали и на него дан ответ. На уместное поднятие старой темы обсуждения реакция обычно благосклонная, в то время как возобновление темы сначала обычно не приветствуется.



— Старайтесь делать свои записи удобочитаемыми. Если запись трудно прочитать, её скорее всего либо проигнорируют, либо отнесутся к ней отрицательно. Несоблюдение языковых норм также нередко приводит к предвзятому отношению.

— Уважительно относитесь ко всем участникам сообщества, так же как это происходит и при реальном общении.

— Во многих сообществах не поощряется написание сообщений, имеющих единственную цель — привлечение внимания к своей персоне. Распространённая ошибка новичков: написание сразу после регистрации «приветствия», не имеющего никакой смысловой нагрузки.

— Дурным тоном считается игнорирование корректного личного обращения либо некорректная обратная реакция.

Также иногда возникают ситуации, которые трактуются в зависимости от правил конкретного сообщества.

Разберём некоторые устоявшиеся названия сетевого общения.

Флейм — это неожиданно возникшее бурное обсуждение, во время которого участники обычно забывают о первоначальной теме, переходят на личности и не могут остановиться. Это тот самый вид спора, в котором истина не рождается. Если случилось так, что вы стали невольным участником флейма, наиболее разумное поведение в этой ситуации — один раз максимально четко, конструктивно и доброжелательно выразить свою позицию, и больше в дискуссию не вступать.

Флуд — это сообщения в интернет-форумах и чатах, не несущие никакой полезной информации.

Оффтоп или **оффтопик** — сетевое сообщение, выходящее за рамки заранее установленной темы общения. Оффтопик рассматривается как нарушение сетевого этикета, так как затрудняет поиск важной информации. Наиболее нежелательной формой оффтопика являются рекламные сообщения.

Спам — сообщения рекламного характера. К спамерам часто применяются более жёсткие меры, чем к пишущим оффтопик.

Если в доцифровую эпоху социализация подрастающего поколения происходила посредством прямого личного общения, то сейчас социализация виртуализировалась. А проистекающая из анонимности и трансформации ключевых понятий мнимая вседозволенность приводит к новым формам отрицательного воздействия, таким как троллинг, пранки, интернет-травля. Защита от этого, в первую очередь, совершенствование знаний и понимания в области современных цифровых технологий родителей, педагогов и воспитателей, а также самих детей. Необходимо воспитать в ребенке четкое понимание того, что при возникновении сложных ситуаций при общении в Интернете, необходимо незамедлительно обращаться за помощью ко взрослым, которые, в свою очередь, должны информировать о этом школу и, при необходимости, полицию, выступить в качестве посредника в разрешении конфликта.

В последние годы тема информационной безопасности и приватности в социальных сетях становится очень актуальной. Этому есть ряд причин: как уже говорилось выше, влияние социальных сетей на повседневную жизнь возрастает, возникают случаи утечки личных данных, аккаунты пользователей постоянно подвергаются попыткам взлома, а у владельцев сетей есть доступ к любой информации о пользователях. Но это далеко не полная картина потенциальных угроз для личных данных.

Самым безобидным, на первый взгляд, вариантом использования личных данных без разрешения пользователя можно считать внутренние механизмы социальных сетей для показа таргетированной рекламы, подбора потенциальных знакомых или отбора потенциально интересного контента.



Больше проблем пользователям создает утечка личных данных по вине сети, что неоднократно случалось в разных проектах. Ещё более серьезные проблемы может вызвать взлом отдельных аккаунтов и получение доступа ко всей личной информации отдельного пользователя. Не стоит забывать о вирусах и фишинге, при помощи которых могут незаметно для пользователя воровать логины и пароли и после использовать их для незаконных действий (например, автоматическая рассылка спама от лица пользователя).

Ответьте на вопрос:

— Какие еще проблемы с персональной информацией из социальных вы можете вспомнить?

Важно помнить, что то, что попало в Интернет, остаётся в нем навсегда, и очень важно размещать информацию в социальных сетях вдумчиво, с оглядкой на перспективу.

Цифровой портрет. Социальный рейтинг.

С появлением концепции «Web 2.0» большая часть содержимого интернет-ресурсов появилась благодаря обычным пользователям. С каждым годом объемы такого контента растут, и при этом существует негласное правило «Что попало в Интернет навсегда осталось в нем». Так или иначе, но цифровой след всё равно остается и при должном желании и усердии в Интернете можно отыскать практически любую информацию.

Для «белой» части сети существует специальный сервис, который регулярно делает «снимки» текущего состояния сайтов. Называется он «Wayback Machine — Internet Archive» и появился он в 24 января 1996 года. Историю развития любого крупного интернет-ресурса с тех пор можно проследить по шагам и датам.



Welcome to Google

[Google Search Engine Prototype](#)
[Might-work-some-of-the-time-prototype-that-is-much-more-up-to-date](#)

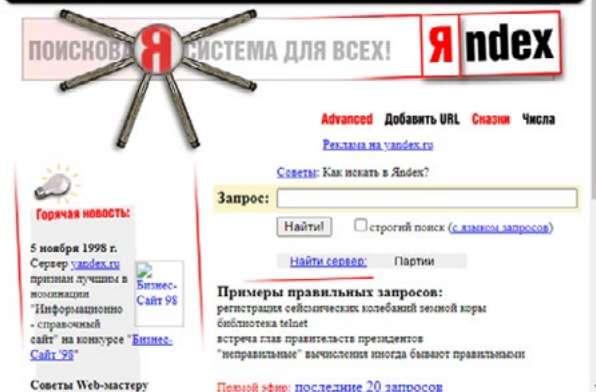
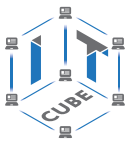


Рис. 15. Первая страница Google в 1998 году

Рис. 16. Первая страница Яндекс в 1998 году

Пользователи также часто сохраняют страницы и отдельные элементы, например, графические файлы или скриншоты частей страниц, которые впоследствии могут стать достоянием общественности. Бывают случаи, когда пользователи выносят в открытый доступ содержимое закрытых сообществ. Все это означает только одно — тот контент, который размещается в Сети, должен быть предварительно оценён с точки зрения последующих действий и событий. Это касается не только графических изображений, но текстовых сообщений. Необдуманная пересылка чужих сообщений тоже может негатив-



но влиять на цифровой портрет. Поэтому осознанное формирование цифровой чистоплотности с первых шагов в Интернете является важнейшей задачей на начальном этапе для родителей, а в последующем, и для педагогов.

Цифровые технологии развиваются с каждым днём. Все больше и больше информации о каждом конкретном человеке сохраняется различными сервисами: история поиска, история посещений интернет-ресурсов, история перемещений, частота пульса, физическая активность и параметры сна, публичные элементы общения в Интернете, предпочитаемые товары и многое другое — совокупность всех этих данных формирует цифровой портрет человека.

Сейчас эти данные не используются повсеместно в совокупности, хотя существуют попытки строить на базе этого рейтинг человека и в зависимости от него предоставлять или запрещать доступ человека к определенным благам. Как пример, можно привести кредитный скоринг (система оценки кредитоспособности (кредитных рисков) лица, основанная на численных статистических методах) или китайскую систему социального кредита.

Цифровая безопасность вне дома.

Современные цифровые технологии присутствуют рядом с человеком на каждом его шагу. Персональные или общественные, каждую секунду они фиксируют различные параметры жизнедеятельности. С действием некоторых сервисов человек соглашается добровольно, другие действуют вне его воли. Большинство подобных технологий призвано улучшить качество человеческой жизни, но это не означает, что они не могут оказывать и негативного воздействия. Рассмотрим несколько таких современных технологий.

Системы безналичного расчета. Банковские карты появились уже достаточно давно, интернет-платежи тоже. Но с появлением технологии NFC и систем бесконтактной оплаты безналичные платежи вышли на новый уровень.

Ответьте на вопрос:

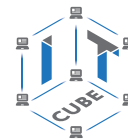
— Вы пользуетесь Google Pay или Apple Pay?

Технология NFC. Технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров. Наличие чипа NFC в мобильном устройстве позволяет комфортно пользоваться банковскими услугами.

Технология отслеживания местоположения на основе GPS. До появления мобильных карт, люди пользовались бумажными картами и атласами, что было неудобно, но других вариантов не было. Первые картографические сервисы появились в Интернете в середине 90-х годов XX века, но популярность они обрели только с появлением мобильных устройств iPhone и Android, а также доступного мобильного Интернета.

Помимо уже ставших привычной геолокации и навигации у данной технологии существуют и дополнительные полезные функции, например возможность поделиться своим местоположением разово или в режиме реального времени. Данная функция может быть полезна родителям для того, чтобы знать где в данный момент находится ребенок.

Современные системы видеонаблюдения и функции на основе машинного обучения. На российских дорогах камеры видеонаблюдения появились в 2008 году. Сейчас уже никого не удивляет автоматическая фиксация нарушений ПДД. С развитием компьютерного зрения и систем машинного обучения стали появляться точные системы



распознавания лиц. На базе подобных систем стали появляться системы оплаты проезда, взаимодействия с банкоматами, оплаты покупок.

Совокупность этих и других современных технологий позволяет достичь повышенного комфорта в повседневной жизни, но с очевидными плюсами возникают и потенциальные угрозы, связанные с подобными сервисами.

Ответьте на вопросы:

- Какие возможные сценарии правонарушений с использованием данных технологий вы можете назвать?
- Какие есть способы минимизации рисков?

Настройка оборудования

С каждым днем человека окружает все больше устройств, называемых умными, устройств, подключенных к сети, умеющих собирать данные, передавать их в Сеть и т. п. Чаще всего данные устройства подключаются к каким-либо аккаунтам в сети или же имеют авторизацию для доступа к своему функционалу.

Для того, чтобы злоумышленник не получил доступ к вашему устройству, нужно научиться придумывать надежные пароли.

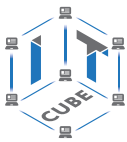
Что представляет собой надежный пароль? Надежный пароль — это пароль, который будет трудно подобрать человеку, а также трудно взломать с помощью компьютерных программ, предназначенных для получения несанкционированного доступа. **Случайный пароль — это золотой стандарт в информационной безопасности.** Он по определению лучше, чем любой пароль, придуманный человеком.

Лучше всего хранить пароли в уме. Туда хакерам точно не добраться. Записать пароль на бумажке или сохранить в заметках смартфона способ ненадежный. Но доступ к вашему паролю злоумышленник может получить также, используя и другие методы:

- перебор по словарю: использование программы, которая автоматически комбинирует распространенные слова из словаря, используя их часто встречающиеся сочетания;
- данные из социальных сетей и другая раскрытая вами личная информация также могут оказаться полезными злоумышленникам. Пользователи часто используют для составления паролей имена и дни рождения, клички домашних животных и даже названия любимых спортивных команд;
- при брутфорс-атаках используются автоматические программы, перебирающие все возможные сочетания символов до тех пор, пока не найдется ваш пароль;
- фишинг — это попытка заставить вас самостоятельно отдать мошеннику деньги или важную информацию;
- утечки данных — это еще одна опасность, угрожающая и паролям, и другой важной информации. Утечки данных представляют особенно большую угрозу, если используется один и тот же пароль в разных местах.

Новый пароль всегда трудно запомнить. Лучший способ это сделать — **первое время не сохранять пароль, а вводить его вручную.** После нескольких десятков попыток выработается механическая память, и вы начнете вводить пароль рефлексивно.

Труднее запоминать много паролей одновременно, а это необходимо, так как у человека есть доступ к большому количеству сервисов и для каждого желательно иметь уникальный пароль. Для таких случаев есть менеджеры паролей, например, KeePass. Это



программы, которые запоминают и хранят пароли за вас. Вам нужно только придумать и запомнить главный пароль — для входа в программу.

Существует несколько паролей, которые обязательно должны быть сильными и которые необходимо помнить:

- пароль от вашего устройства;
- пароль для шифрования/расшифровки (например, жесткого диска);
- мастер-пароль или парольная фраза для менеджера паролей;
- пароль от E-mail.

Чтобы защититься от новейших методов взлома, нужны сверхнадежные пароли. Для определения стойкости пароля можно воспользоваться следующим списком:

- **ваш пароль длинный?** (длина пароля должна быть минимум 10—12 символов);
- **ваш пароль трудно угадать?** (следует избегать простых последовательностей («12345», «qwerty») — такие пароли подбираются за очень быстро. По той же причине следует избегать распространенных слов («password1»));
- **разнообразен ли состав символов в вашем пароле?** (чем больше в пароле разнотипных символов, тем он менее предсказуем);
- **есть ли в вашем очевидные подстановки символов?** (например, ноль вместо буквы «О»);
- **есть ли в вашем пароле необычные сочетания слов?** (кодовые фразы надежнее, если слова в них идут в неожиданном порядке);
- **сможете ли вы запомнить свой пароль?** (составляйте пароль так, чтобы он был понятен вам, но труден для машинного подбора);
- **пользовались ли вы этим паролем раньше?** (каждый пароль должен быть уникальным)

Как же можно придумать надежный пароль, который легко запомнить? Для этого существуют различные методы.

Метод «Diceware» заключается в том, что человек бросает игральные кости, чтобы случайным образом выбрать несколько слов из списка. Выбранные слова образуют парольную фразу. Это отличный способ сгенерировать последовательность, потому что такой метод действительно гарантирует вам случайную комбинацию слов. К тому же, образованную фразу будет легко запомнить. Можно усовершенствовать данный метод, используя отрывок литературного произведения, которое вы помните наизусть. Для выбора слова можно воспользоваться приложением, имитирующим броски игровых кубиков. А полученную комбинацию цифр можно хранить даже в открытом доступе, при условии, что контрольную фразу знаете только вы.

Метод **«Ключевого слова»** состоит в выборе контрольного слова, на основе которого генерируются все пароли следующим образом:

- пароли вводятся латиницей, поэтому необходимо выбрать одно английское слово (не собственное имя, не название аккаунта и т. п.). Например, **Firefox**;
- следующая часть пароля должна отличаться от сервиса к сервису. И ей может стать название сервиса. Например, **yandex** для аккаунта на Яндекс или **mail**, соответственно, для mail.ru;
- многие сайты просят использовать и буквы, и цифры. На этот случай нам понадобится еще одна часть пароля — цифровая. В качестве цифры можно использовать, например, количество букв в предыдущей части (названии сервиса). То есть для Яндекса это 6, для mail.ru это 4. Как вариант — количество гласных или согласных. **yandex6**;
- сервисы могут попросить использовать и строчные, и заглавные буквы. Поэтому необходимо использовать общее правило написания пароля. Например, каждая часть

пишется с большой буквы. Дополнительно можно добавить в конце какой-нибудь символ — например, «!». Использование символов тоже может быть требованием сервиса. **FirefoxYandex6!;**

Мало придумать надёжный пароль — нужно еще соблюдать осторожность, чтобы не раскрыть его для посторонних. Запоминать пароли — это только первый шаг, но этого мало, так как пароли могут быть перехвачены в момент ввода. Чтобы сохранить свои пароли в тайне, необходимо:

- создать новый пароль для каждого важного сервиса;
- включить двухфакторную аутентификацию везде, где есть эта опция;
- не сохранять пароли в браузере;
- не вводить пароли на сайтах без SSL-сертификата;
- никому не доверять и не называть пароль (ни друзьям, ни родителям, **никому!**);
- менять пароль каждый раз, когда кажется, что его могли украсть (в остальных случаях менять пароль не реже, чем раз в 6 месяцев).

Поиск и обработка данных. Основные принципы.

Когда мы начинаем изучать незнакомую нам тему, мы всегда ищем наиболее простую точку входа. В рамках школьной программы нам ее обычно обеспечивает учебное пособие. Дополнительные материалы расширяют круг наших знаний. Объяснения учителя помогают разобраться во всех деталях, понять и научиться использовать полученную информацию. Но в реальной жизни не всегда предоставляется возможность столь простого сценария, да и темы порой возникают сложные и неоднозначные.

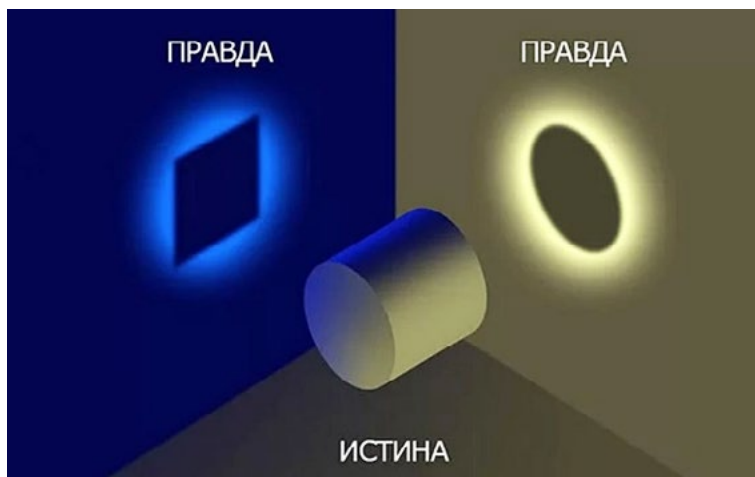
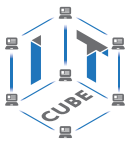


Рис. 17. Различные точки зрения

Умение абстрагироваться и взглянуть на рассматриваемую тему с разных сторон предоставляет возможность получать наиболее качественную информацию, на основе которой будут формироваться знания. Информация нас окружает повсюду. Информация нематериальна, но всеобъемлюща. В литературе можно найти достаточно много определенных терминов «информация», отражающих различные подходы к толкованию этого понятия.

«Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, технологиях и о защите информации» дает следующее толкование термина: **«информация** — сведения (сообщения, данные) независимо от формы их представления».



А вот толковый словарь русского языка Ожегова содержит уже 2 определения слова «информация»:

— Сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством.

— Сообщения, осведомляющие о положении дел, о состоянии чего-нибудь (научно-техническая и газетная информации, средства массовой информации — печать, радио, телевидение, кино).

В информатике наиболее часто используется следующее определение этого термина: **информация** — осознанные сведения об окружающем мире, которые являются объектом хранения, преобразования, передачи и использования. **Сведения** — это знания, выраженные в сигналах, сообщениях, известиях, уведомлениях и т. д.

Информация содержится везде. Стремление зафиксировать, сохранить надолго свое восприятие информации было всегда свойственно человеку. Мозг человека хранит множество информации и использует для хранения её свои способы, основа которых — двоичный код, как и у компьютеров. Человек всегда стремился иметь возможность поделиться своей информацией с другими людьми и найти надежные средства для её передачи и долговременного хранения. Для этого в настоящее время изобретено множество способов хранения информации на внешних носителях и её передачи на огромные расстояния.

То, как информация представлена, как она кодируется и хранится, даёт возможность её классифицировать следующим образом:

- **графическая** — первый вид, для которого был реализован способ хранения информации об окружающем мире в виде наскальных рисунков, а позднее в виде картин, фотографий, схем, чертежей на бумаге и др.;
- **звуковая** — мир вокруг нас полон звуков и задача их хранения и тиражирования была решена с изобретением звукозаписывающих устройств в 1877 г.;
- **текстовая** — способ кодирования речи человека специальными символами — буквами, особенно большое значение этот способ приобрел после изобретения бумаги и книгопечатания;
- **числовая** — количественная мера объектов и их свойств в окружающем мире; особенно большое значение приобрела с развитием торговли, экономики и денежного обмена; аналогично текстовой информации для ее отображения используется метод кодирования специальными символами — цифрами, причем системы кодирования (счисления) могут быть разными;
- **видеоинформация** — способ сохранения динамических картин окружающего мира, появившийся с изобретением кино.

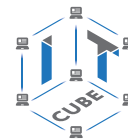
Существуют также виды информации, для которых пока ещё не изобретено способов их кодирования и хранения — это **тактильная** информация, передаваемая ощущениями; **органолептическая**, передаваемая запахами и вкусами и др.

С точки зрения информатики, как науки, изучающей информацию и все что с ней связано, наиболее важными можно считать следующие качественные свойства: достоверность, полноту, точность, актуальность, полезность, ценность, своевременность, понятность, доступность, краткость и пр.

Что же подразумевается, когда мы говорим про качественные свойства информации?

Объективность информации означает, что она отражает объективную действительность и не зависит от субъективного восприятия.

Информация **достоверна**, если она отражает истинное положение дел. Достоверная информация помогает принять нам правильное решение. Недостоверной информация может быть по следующим причинам:



- преднамеренное искажение (дезинформация) или непреднамеренное искажение субъективного свойства;
- искажение в результате воздействия помех («испорченный телефон») и недостаточно точных средств ее фиксации.

Информацию можно назвать **полной**, если её достаточно для понимания и принятия решений. Неполная информация может привести к ошибочному выводу или решению.

Точность информации определяется степенью её близости к реальному состоянию объекта, процесса, явления и т. п.

Актуальность информации — важность данной информации для настоящего времени. Только вовремя полученная информация может быть полезна.

Полезность может быть оценена применительно к нуждам конкретных ее потребителей и оценивается по тем задачам, которые можно решить с ее помощью.

Самая ценная информация — **полезная**. При этом следует учитывать, что и недостоверная информация (например, художественная литература), имеет большую значимость для человека. В художественной литературе полезная информация представлена неявным образом.

С течением времени количество информации растёт, информация накапливается, происходит ее систематизация, оценка и обобщение. Это свойство назвали ростом и аккумуляцией информации. Старение информации заключается в уменьшении ее ценности с течением времени. Старит информацию не время, а появление новой информации, которая уточняет, дополняет или отвергает полностью, или частично более раннюю. Научно-техническая информация стареет быстрее, эстетическая (произведения искусства) — медленнее.

По результатам проведённых исследований современный человек за две недели получает объём информации больший, чем человек средневековья за всю жизнь. Информационные процессы ускоряются, объёмы увеличиваются. Изменяются способы хранения и обработки информации. В этом современному человеку помогают компьютеры. Особой средой можно считать информацию, представленную в глобальной сети Интернет. Здесь используются особые приёмы хранения, обработки, поиска и передачи распределённой информации больших объёмов и особые способы работы с различными видами информации. Постоянно совершенствуется программное обеспечение, обеспечивающее коллективную работу с информацией всех видов.

Аналитический подход к информации. Структурирование информации.

Ради получения и сохранения знаний, повышения удобства в последующим их использовании человечество на протяжении всей своей истории старалось отыскать наиболее простые, но в то же время эффективные способы управления информацией. XX век принес человечеству информатизацию, а вместе с этим и ускорение информационных процессов, и увеличение объёмов потребляемой информации, что, в свою очередь, породило разнообразные методологии, помогающие человеку с этим справиться. Об одной из них — интеллект-картах — пойдёт речь ниже.

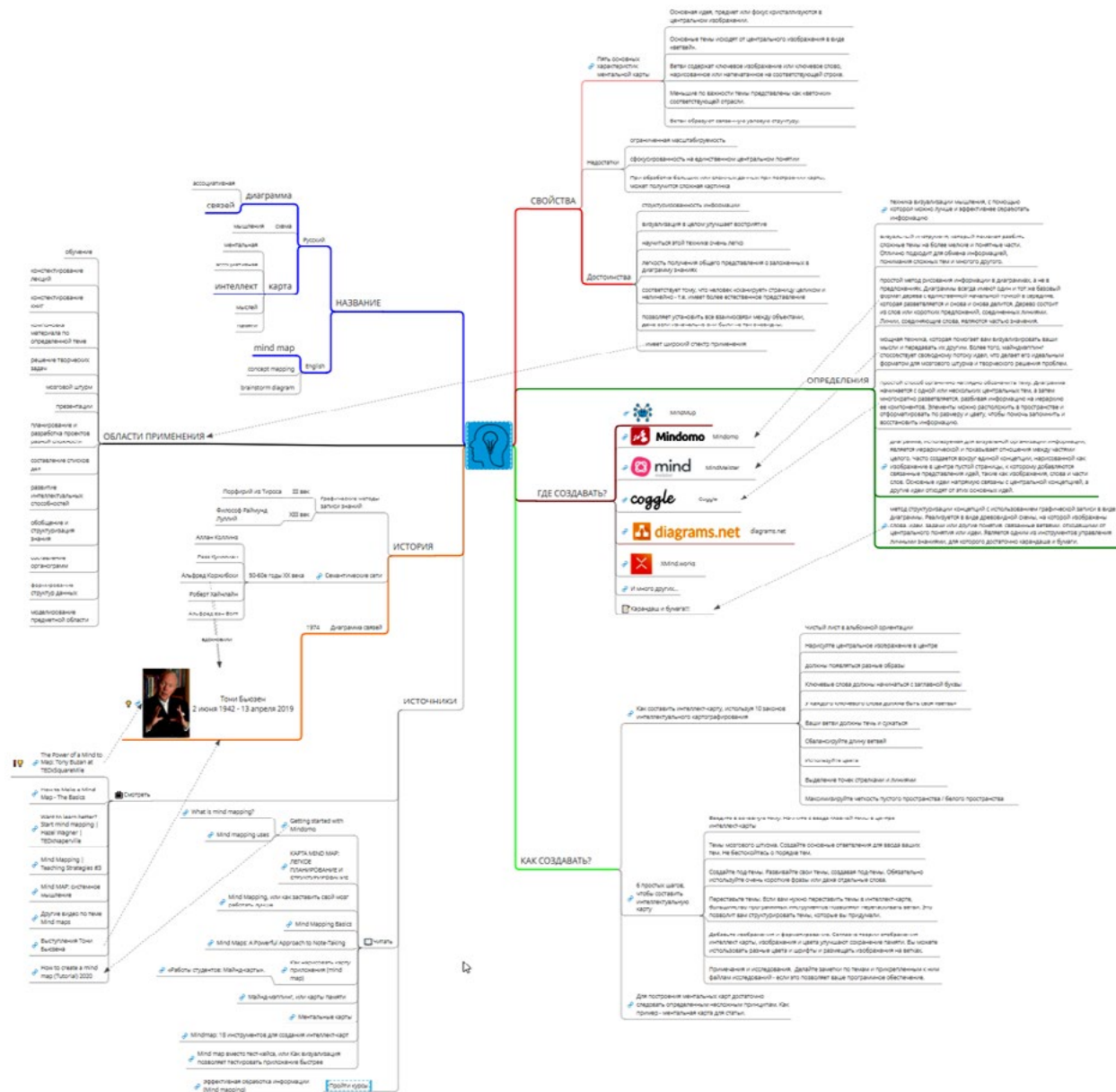


Рис. 18. Интеллект-карта

На первый взгляд может показаться, что перед нами паутина, сплетенная пауком, или схема метрополитена. Много всего и ничего не понятно. Но на самом деле всё не так. Давайте попробуем разобраться и ответить на следующие вопросы:

- что же такое интеллект-карты?
- как они появились?
- какие у них есть особенности и положительные черты?
- как и при помощи чего их создавать и использовать?

Что же такое интеллект-карты? Для начала необходимо разобраться с терминологией и названиями. В английском языке существует устоявшийся термин «Mind map». Кроме него иногда употребляются названия «concept mapping» и «brainstorm diagram», отражающие определённые аспекты применения данного метода. В русском языке, к сожалению, полного согласия нет. Чаще всего используются названия «диаграмма связей» и «интеллект-карта». Помимо этого, встречаются следующие варианты: карта мыслей, ас-



социативная карта, карта памяти, ментальная карта, ассоциативная диаграмма, схема мышления. Мы будем придерживаться термина «интеллект-карта».



Рис. 19. Ветвь «Название»

Точно также, как и с названием, дело обстоит и с определением, что же такое интеллект-карта. Приведем некоторые из них:

- диаграмма, используемая для визуальной организации информации, является иерархической и показывает отношения между частями целого. Часто создается вокруг единой концепции, нарисованной как изображение в центре пустой страницы, к которому добавляются связанные представления идей, такие как изображения, слова и части слов. Основные идеи напрямую связаны с центральной концепцией, а другие идеи отходят от этих основных идей;
- метод структуризации концепций с использованием графической записи в виде диаграммы. Реализуется в виде древовидной схемы, на которой изображены слова, идеи, задачи или другие понятия, связанные ветвями, отходящими от центрального понятия или идеи. Является одним из инструментов управления личными знаниями, для которого достаточно карандаша и бумаги;
- техника визуализации мышления, с помощью которой можно лучше и эффективнее обработать информацию;
- визуальный инструмент, который поможет разбить сложные темы на более мелкие и понятные части. Отлично подходит для обмена информацией, понимания сложных тем и многого другого;
- простой метод рисования информации в диаграммах, а не в предложениях. Диаграммы всегда имеют один и тот же базовый формат дерева с единственной начальной точкой в середине, которая разветвляется и снова и снова делится. Дерево со-

стоит из слов или коротких предложений, соединенных линиями. Линии, соединяющие слова, являются частью значения;

- мощная техника, которая помогает вам визуализировать ваши мысли и передавать их другим. Более того, майндмэппинг способствует свободному потоку идей, что делает его идеальным форматом для мозгового штурма и творческого решения проблем;
- простой способ органично и наглядно обозначить тему. Диаграмма начинается с одной или нескольких центральных тем, а затем многократно разветвляется, разбивая информацию на иерархию ее компонентов. Элементы можно расположить в пространстве и отформатировать по размеру и цвету, чтобы помочь запомнить и восстановить информацию.

Все определения сходятся в одном, что это визуальный инструмент, иерархическая диаграмма, позволяющая просто и эффективно обеспечивать информационные процессы — обработки, сохранения и передачи информации.

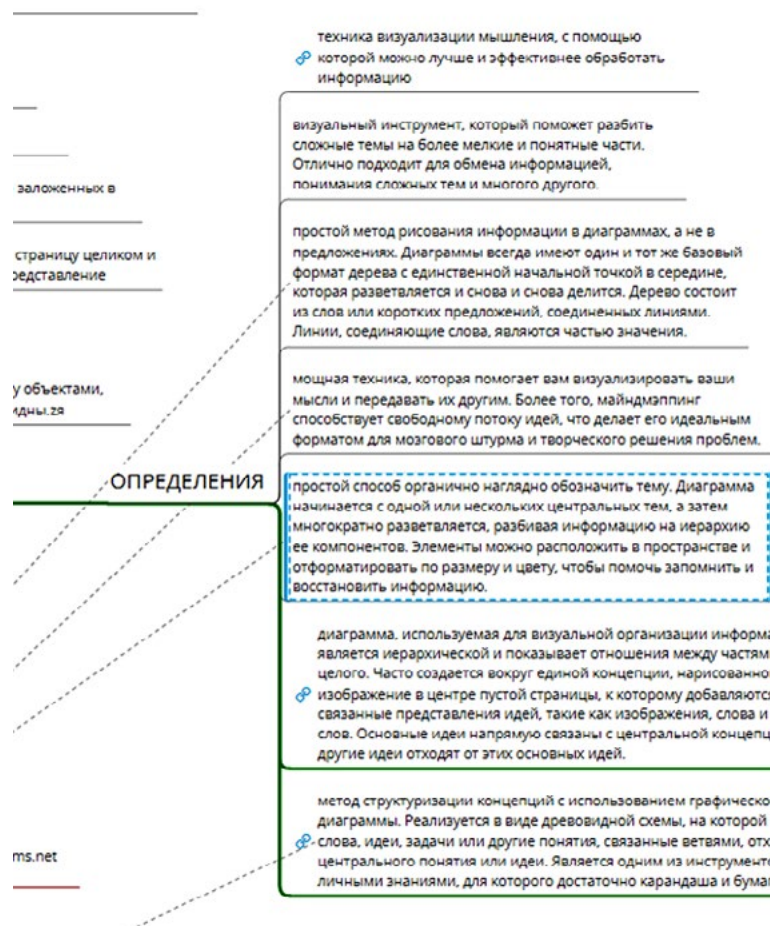


Рис. 20. Ветвь «Определения»

Графические способы записи знаний на протяжении веков использовались человеком в различных областях его деятельности. Тут стоит вспомнить и наскальные рисунки, отражающие жизнь и быт древних людей, и пиктографические письма первых цивилизаций. Но наиболее близким по духу и одним из самых ранних примеров графических записей, подобных рассматриваемой нами, будут изображения концепции категорий философии Аристотеля, сделанные в III веке философом Порфирием из Тираса.

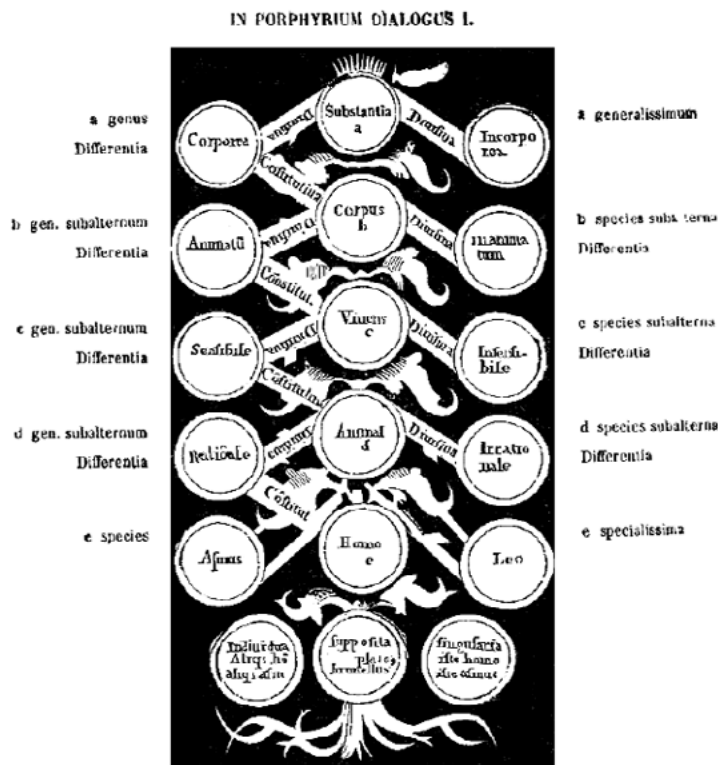
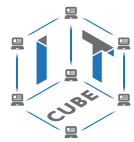


Рис. 21, 22. Изображение концепции категорий философии Аристотеля. Порфирий из Тироса

Также подобной методикой пользовался философ Раймунд Луллий в XIII веке при иллюстрации схемы разумной связи, в его знаменитых «кругах» (в XIII веке Раймунд Луллий создал логическую машину в виде бумажных кругов, построенных по троичной логике).

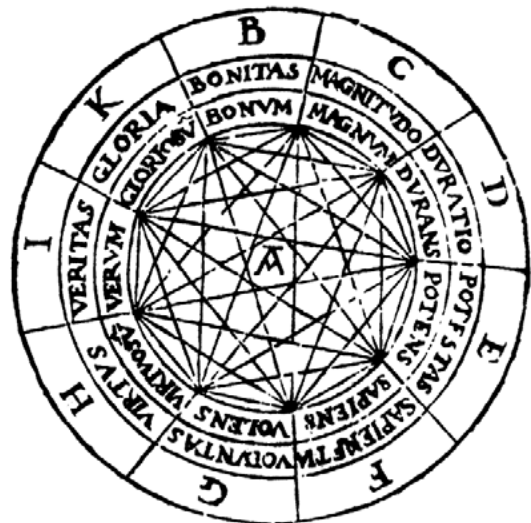


Рис. 23, 24. Раймунд Луллий. Иллюстрации схемы разумной связи.

Этот логический механизм, изображаемый в сочинениях Луллия соответствующими фигурами, состоял из нескольких подвижных концентрических кругов, разделенных поперечными линиями на отделения («камеры»), в которых в известном порядке обозначались общие понятия или основные категории всего существующего; вследствие концен-

тричности кругов, подразделения каждого из них занимали определенное положение относительно тех или других подразделений прочих кругов, а вращая их так или иначе, можно было получать множество новых, более или менее сложных комбинаций.

В конце 50-х годов XX века была сформирована теория семантической сети, как информационной модели предметной области. Графическое представление семантической сети имеет вид ориентированного графа, у которого вершины соответствуют объектам предметной области, таким как понятия, события, свойства, процессы, а дуги (рёбра) задают отношения между ними. В начале 60-х эта теория получила свое дальнейшее развитие благодаря работам Аллана Коллинза и Росса Куиллиана. А идеи Альфреда Коржибски из области общей семантики, поляризованной в научно-фантастических романах Роберта Хайнлайна и Альфреда ван Вогта в свою очередь послужили вдохновением и подтолкнули Тони Бьюзена, британского писателя, автора книг по популярной психологии, сформулировать методику интеллект-карт в том виде, в котором мы сейчас ими пользуемся, иначе говоря, он является изобретателем современного вида интеллект-карт.

Какие особенности и положительные черты есть у интеллект-карт? В первую очередь хотелось бы озвучить пять основных характеристик интеллект-карт:

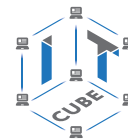
- основная идея, предмет или фокус кристаллизуются в центральном изображении;
- основные темы исходят от центрального изображения в виде «ветвей»;
- ветви содержат ключевое изображение или ключевое слово, нарисованное или написанное на соответствующей строке;
- меньшие по важности темы представлены как «веточки» соответствующей отрасли;
- ветви образуют связанную узловую структуру.

Из этих характеристик явно проглядываются основные положительные аспекты влияния интеллект-карт на информационные процессы:

- структурированность информации;
- визуализация, улучшающая восприятие;
- низкий порог вхождения при изучении данного метода и, как следствие, «быстрый старт»;
- легкость получения общего представления о заложенных в диаграмму знаниях;
- позволяет установить все взаимосвязи между объектами, даже если изначально они были не так очевидны;
- более естественное представление, позволяющее воспринимать информацию нелинейно;
- широкий спектр применения.

Если попытаться расширить последний пункт, то мы получим довольно внушительный список тех областей человеческой деятельности в которой могут найти применение интеллект-карты: обучение, конспектирование лекций, конспектирование книг, компоновка материала по определенной теме, решение творческих задач, мозговой штурм, презентации, планирование и разработка проектов разной сложности, составление списков дел, развитие интеллектуальных способностей, обобщение и структуризация знания, составление органограмм (документ, схематически отражающий состав и иерархию подразделений какого-либо предприятия и т. п.), формирование структур данных, моделирование предметной области. И это далеко не полный список. Всё это нам говорит о том, что универсальность метода позволяет использовать его практически в любой области деятельности!

Из вышесказанного очевидно просматриваются положительные достоинства интеллект-карт, но во избежание односторонней оценки, стоит упомянуть и о потенциально негативных свойствах, таких как ограниченная масштабируемость, сфокусированность на единственном центральном понятии и, как следствие из этого, возможность получения сложной и запутанной диаграммы при обработке больших или сложных данных.



Как уже было замечено выше, процесс создания интеллект-карт не сложен. Обучиться данному методу можно очень быстро, даже не имея никаких способностей к рисованию, что позволяет при наличии листа бумаги и карандаша осуществить «быстрый старт» и практически сразу создать свою первую интеллект-карту. Для того, чтобы первая диаграмма не «вышла комом», следует соблюдать несложные правила.

Как составить интеллект-карту, используя 10 законов интеллектуального картографирования:

1. Чистый лист в альбомной ориентации (альбомная ориентация важна, потому что мы видим мир горизонтально, а не вертикально. Периферическое зрение влево-вправо свободнее, чем вверх и вниз).
2. Нарисуйте основное изображение в центре (изображение должно выражать вашу основную цель/идею).
3. Должны появляться разные образы (стоит использовать разные размеры и образы, например, нарисовать некоторые ключевые слова «объемными»).
4. Ключевые слова должны начинаться с заглавной буквы.
5. У каждого ключевого слова должна быть своя «ветвь».
6. Ваши ветви должны изгибаться и сужаться.
7. Сбалансируйте длину ветвей.
8. Используйте цвета.
9. Соединяйте разные ветви стрелками и линиями, организуя вторичные связи.
10. Максимизируйте четкость пустого / белого пространства. Это предполагает использование пустого места для ясности. Другими словами, вы должны позволить вашим интеллектуальным картам дышать.

И еще 6 простых шагов, чтобы составить интеллектуальную карту:

1. Введите в основную тему (начните с ввода главной темы в центре интеллект-карты).
2. Темы мозгового штурма (создайте основные ответвления для ввода ваших тем. Не беспокойтесь о порядке тем).
3. Создайте подтемы (развивайте свои темы, создавая подтемы. Обязательно используйте очень короткие фразы или даже отдельные слова).
4. Переставьте темы. (если вам нужно переставить темы в интеллект-карте, большинство программных инструментов позволяют перетаскивать ветви. Это позволит вам структурировать темы, которые вы придумали).
5. Добавьте изображения и форматирование (согласно теории отображения интеллект-карты изображения и цвета улучшают сохранение в памяти. Вы можете использовать разные цвета и шрифты и размещать изображения на ветках).
6. Примечания и исследования (делайте заметки по темам и прикрепленным к ним файлам исследований — если это позволяет ваше программное обеспечение).

Как мы в очередной раз убедились, все правила просты и очевидны, но большая часть из них не догматична, для достижения хорошего результата достаточно будет соблюдать первые, касающиеся поля карты, расположения основного понятия, его составляющих и соответствующих иерархических связей.

Если воспользоваться современными технологиями, создавать интеллект-карты становится еще проще! Популярность метода повлияла на появление большого количества приложений для создания интеллект-карт. А развитие интернет-технологий позволило сделать их доступным из любой точки планеты, где есть подключение к Сети. Ниже перечислены веб-сервисы наиболее полно соответствующие определенным критериям:

- современный дизайн;
- удобство создание карт;
- грамотная навигация;

- условия для естественного выполнения вышеприведенных правил создания интеллект-карт;
- дополнительные возможности при создании карт;
- возможность интеграции с облачными решениями (Гугл-диск);
- возможность экспорта в графические форматы;
- полностью или частично бесплатное использование без ощутимой потери функциональности

В данный список включены только веб-сервисы, хотя некоторые из них имеют и десктопное исполнение:

- MindMup <https://www.mindmup.com/>
- Mindomo <https://www.mindomo.com/ru/>
- MindMeister <https://www.mindmeister.com/ru>
- Coggle <https://coggle.it/>
- diagrams.net <https://www.diagrams.net/>
- XMind.works <https://xmind.works/>



Рис. 25. Ветка «Где создавать?»

Также существует расширенный список программного обеспечения для создания интеллект-карт, находящийся по адресу https://en.wikipedia.org/wiki/List_of_concept_and_mind-mapping_software. Для создания интеллект-карты, иллюстрирующей данный материал, использовалось программное обеспечение MindMup, выбранное по совокупности субъективно более удобного интерфейса и функционала по созданию и оформлению интеллект-карт в бесплатной версии.

Правонарушения в сфере компьютерной информации.

Хотя чёткого определения компьютерного преступления не существует, их условно можно подразделить на две большие категории:

- преступления, связанные с вмешательством в работу компьютеров;
- преступления, использующие компьютеры как необходимые технические средства.



Вывод: компьютерное преступление есть противоправные действия, направленные на достижение доступа к хранимой на компьютере информации, имеющей ограниченные права доступа. При этом компьютер может быть, как объектом преступления, так и в качестве инструмента преступной деятельности.

Составы компьютерных преступлений (т. е. перечень признаков, характеризующих общественно опасное деяние как конкретное преступление) приведены в 28 главе УК, которая называется “Преступления в сфере компьютерной информации” и содержит три статьи:

- ст. 272 “Неправомерный доступ к компьютерной информации”;
- ст. 273 “Создание, использование и распространение вредоносных программ для ЭВМ”;
- ст. 274 “Нарушение правил эксплуатации ЭВМ, Системы ЭВМ или их сети”.

Соответственно юридически рассматриваются следующие понятия:

Объект — безопасность компьютерной информации как разновидности общественной информации.

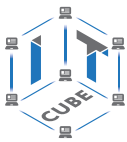
Объективная сторона может характеризоваться деянием как в форме действия (ст. ст. 272-273 УК РФ), так и в форме как действия или бездействия (ст. 274 УК РФ).

Субъект — общий (ст. ст. 272-273 УК РФ) и специальный (ч. 2 ст. 272, ч. 2 ст. 273, ст. 274 УК РФ).

Субъективная сторона по ст. 272 УК РФ характеризуется виной в форме умысла как прямого, так и косвенного: ст. 273 УК РФ — только прямым умыслом; ст. 274 УК РФ — как умышленной, так и неосторожной виной.

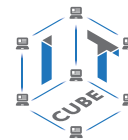
В мировой практике термин “киберпреступность” впервые появился во второй половине XX века. Первые подобные преступления были связаны с проникновением в компьютерные системы путем их повреждения и хищением данных. С течением времени, и, как следствие, развития компьютерных и телекоммуникационных технологий, понятие “киберпреступность” изменялось, включая в себя все новые и новые преступления. Традиционные формы компьютерных преступлений переходили в новые, такие как: компьютерное мошенничество, несанкционированный доступ к личным данным, незаконное использование программного обеспечения.

Современные тенденции развития киберпреступности продолжаются и в XXI веке. Общедоступность глобальной сети Интернет, простота в использовании, анонимность и высокая скорость передачи данных превратила локальные киберпреступления в транснациональную киберпреступность. В зарубежной литературе и во многих официальных документах кроме/вместо «computer crime» также часто употребляется термин «cybercrime» — киберпреступность, киберпреступление. Определения этого термина разные, существуют широкие и узкие трактовки. Некоторыми исследователями киберпреступность связывается с преступлениями, совершаемыми в различных информационных сетях. Высказана также точка зрения, согласно которой киберпреступность относят к преступлениям, совершаемым посредством компьютерной техники против различных прав и благ человека. Под преступлениями в сфере компьютерной информации следует понимать общественно опасные деяния (предусмотренные главой 28 Раздела IX УК РФ), которые посягают на сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Термин же «компьютерные преступления» несколько шире, чем «преступления в сфере компьютерной информации». Он охватывает и те преступления, где компьютерная техника, программы, компьютерная информация и цифровые каналы связи являются орудиями совершения преступления (понятно, что из разряда компьютерных преступлений мы исключаем такие преступления, в которых компьютерная техника используется лишь как



материальная ценность) или объектом посягательства. К таким преступлениям относятся: мошенничество с применением банковских карт (кардинг), мошенничество с выманиванием персональных данных (фишинг), незаконное пользование услугами связи и иной обман в области услуг связи, промышленный и иной шпионаж, когда объектом являются информационные системы, и т. д.

Хотелось бы подчеркнуть, что никакие аппаратные, программные и любые другие решения никогда не смогут дать стопроцентные гарантии на абсолютную надежность и безопасность данных в компьютерных сетях. Но в то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности, не забывая об осторожности.



Планы учебных занятий

Тема урока «Человек в цифровом пространстве»

Тип урока: открытия новых знаний

Цель урока: ознакомление с современным положением человека информационном пространстве.

Планируемые результаты

Предметные: получение знаний о том, что такое персональные данные, способах их обработки, законодательно-правовых аспектах.

Метапредметные: способность ставить и формулировать для себя цели действий, прогнозировать результаты, анализировать их (причём как положительные, так и отрицательные), умение соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности, определять способы действий в рамках предложенных условий, корректировать свои действия в соответствии с изменяющейся ситуацией.

Личностные: готовность и способность обучающихся к саморазвитию и личностному самоопределению; сформированность их мотивации к обучению и целенаправленной познавательной деятельности.

Время реализации: 1 академический час

Оборудование и материалы: компьютер, проектор.

Ход урока

I. Мотивационный этап — 5 мин.

Деятельность учителя: сообщает учащимся о том, что огромное количество информации о людях являются персональными данными, эти данные описывают человека в информационном пространстве. Некоторые из таких данных являются конфиденциальными.

Деятельность учеников: приводят примеры из своей жизнедеятельности.

Дидактические и методические материалы: дидактические материалы пособия «Человек в цифровом пространстве».

II. Этап актуализации знаний по предложенной теме и осуществление первого пробного действия — 8 мин.

Деятельность учителя: рассказывает ученикам о том, что такое персональные данные с точки зрения закона, озвучивает соответствующие определения.

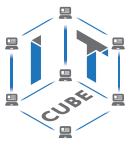
Деятельность учеников: описывают понятия на основе собственного опыта и уровня знаний.

Дидактические и методические материалы: дидактические материалы пособия «Человек в цифровом пространстве».

III. Этап изучения нового материала — 16 мин.

Деятельность учителя: конкретизирует и объясняет озвученные понятия, приводит актуальные примеры. Акцентирует внимание учеников на важной информации — необходимо запомнить самое главное:

- информация, содержащая любые персональные данные, не принадлежит никому кроме нас;



- если кто-то хочет ее получить, он должен обосновать это желание и получить наше разрешение либо иметь на обработку законные основания;
- этот человек (или компания) должен обеспечить безопасность этой информации;

Деятельность учеников: фиксируют ключевые мысли лекции в письменной форме.

Деятельность учителя: предлагает классифицировать персональные данные по степени их важности:

1. Критические персональные данные:
 - a. СНИЛС
 - b. Паспортные данные
 - c. Биометрические данные
 - d. Номер телефона
2. Не критические
 - a. Регион проживания
 - b. Электронная почта
3. Зависящие от условий предоставления
 - a. Местожителство
 - b. Семейные условия
 - c. Личные фотографии

Действие учеников: на основе информации, полученной от учителя, пытаются классифицировать типы личных данных по их степени важности. Записывают итоговую классификацию.

IV. Этап проверки понимания и первичного закрепления — 8 мин.

Деятельность учителя: предлагает учащимся ответить на следующий вопрос и выполнить задание.

— Часто вы полностью и внимательно читаете пользовательское соглашение?

— Прочитайте внимательно пользовательское соглашение компании Яндекс. Оно находится по адресу <https://yandex.ru/legal/rules/> или можно воспользоваться QR кодом для перехода:



Деятельность учеников: отвечают на поставленный вопрос и выполняют задачу, предложенную учителем.

Дидактические и методические материалы: дидактические материалы пособия «Человек в цифровом пространстве».

V. Этап контроля усвоения и коррекции ошибок — 4 мин.

Деятельность учителя: предлагает ответить учащимся на следующие вопросы:

- 1) Что такое персональные данные?
- 2) Приведите примеры персональных данных.
- 3) Какие персональные данные являются конфиденциальными?

Деятельность учеников: отвечают на вопросы учителя.

Дидактические и методические материалы: дидактические материалы пособия «Человек в цифровом пространстве».

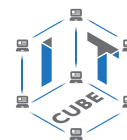
VI. Информация о домашнем задании, инструктаж по его выполнению — 2 мин.

Деятельность учителя: сообщает учащимся домашнее задание. Прочитать соглашение пользователя почтового сервиса, которым чаще всего пользуется ученик. Выписать, какую персональную информацию собирает сервис и на каких условиях.

VII. Этап рефлексии деятельности на уроке — время 2 мин.

Деятельность учителя: для оценки своей деятельности учащимся предлагается ответить на следующие вопросы:

- 1) Сегодня на уроке я узнал...
- 2) Буду ли я в дальнейшем подробно знакомиться с пользовательским соглашением?



Тема урока «Интернет. История развития»

Тип урока: открытия новых знаний

Цель урока: Ознакомление с историей возникновения вычислительных сетей и Интернета.

Планируемые результаты

Предметные: получение знаний о том, что такое вычислительные сети, какова история возникновения вычислительных сетей и их трансформации в глобальную сеть Интернет.

Личностные: готовность и способность обучающихся к саморазвитию и личностному самоопределению; сформированность их мотивации к обучению и целенаправленной познавательной деятельности.

Время реализации: 1 академический час

Оборудование и материалы: компьютер, проектор.

Ход урока

I. Мотивационный этап — 5 мин.

Деятельность учителя: сообщает о том, что для современного человека Интернет вполне естественная среда. При этом история его возникновения и развития уходит в 60-е годы XX века.

Дидактические и методические материалы: дидактические материалы пособия «Интернет. История развития и современное состояние».

II. Этап актуализации знаний по предложенной теме и осуществление первого пробного действия — 8 мин.

Деятельность учителя: на текущий момент Интернет и сетевые технологии пронизывают все сферы человеческой жизни. Порой наличие сетевого взаимодействия настолько прозрачно, что на первый взгляд кажется, что его и вовсе нет.

Деятельность учеников: называют неочевидные примеры использования сетевых технологий на основе собственного опыта.

Дидактические и методические материалы: дидактические материалы пособия «Интернет. История развития и современное состояние».

III. Этап изучения нового материала — 16 мин.

Деятельность учителя: рассказывает о появлении сети ARPANET, предшественницы современного Интернета. О том, что изначально сеть связывала Университет Юты с тремя исследовательскими центрами в Калифорнии.



The ARPANET in December 1969

Рис. 28. Карта ARPANET, 1969 год

Рассказывает о том, что проект ARPANET был тестовой площадкой для новой технологии — коммутации пакетов, позволяющей разбивать данные на небольшие «пакеты», чтобы их можно было эффективно передавать по сети, о практической значимости проекта и первых сетевых сервисах.

На примерах показывает динамику развития сети в первые годы.

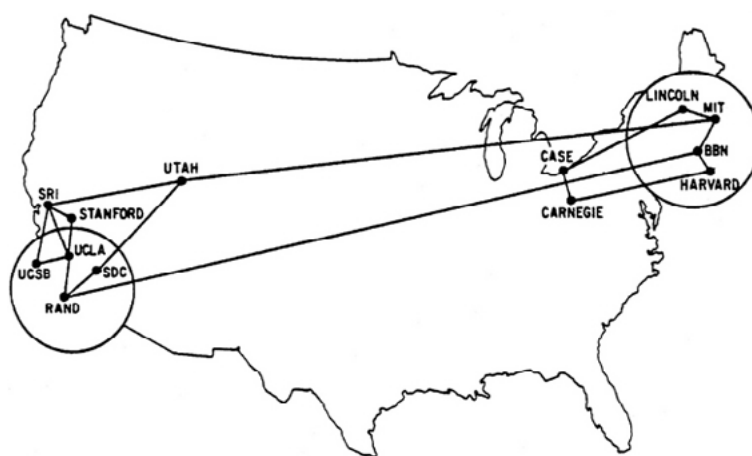


Рис. 29. Карта ARPANET, 1970 год

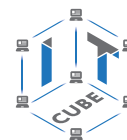
Рассказывает о возникновении электронной почты и первых программах для работы с ней. Рассказывает про переход на протокол TCP/IP и появление системы доменных имен.

Деятельность учеников: фиксируют ключевые даты и определения в письменной форме.

Дидактические и методические материалы: дидактические материалы пособия «Интернет. История развития и современное состояние», «Общение в сети. Социальные сети и системы обмена сообщениями».

IV. Этап проверки понимания и первичного закрепления — 8 мин.

Деятельность учителя: предлагает учащимся ответить на следующий вопрос и выполнить задание.



- Как вы думаете, сколько всего было компьютеров на момент появления ARPANET?
- Компьютеры какого поколения объединялись в первые вычислительные сети?
- Как выглядели эти компьютеры?

Деятельность учеников: отвечают на поставленные вопросы.

Дидактические и методические материалы: дидактические материалы пособия «Интернет. История развития и современное состояние».

V. Этап контроля усвоения и коррекции ошибок — 4 мин.

Деятельность учителя: предлагает ответить учащимся на следующие вопросы:

1. Что такое вычислительная сеть?
2. Когда появился проект ARPANET?
3. Когда появился сервис электронной почты?
4. Когда был осуществлен переход на протокол TCP/IP?
5. Когда появилась система DNS?

Деятельность учеников: отвечают на вопросы учителя.

Дидактические и методические материалы: дидактические материалы пособия «Интернет. История развития и современное состояние», «Общение в сети. Социальные сети и системы обмена сообщениями».

VI. Информация о домашнем задании, инструктаж по его выполнению — 2 мин.

Деятельность учителя: сообщает учащимся домашнее задание.

Изучить историю возникновения вычислительных сетей в СССР.

VII. Этап рефлексии деятельности на уроке — время 2 мин.

Деятельность учителя: для оценки своей деятельности учащимся предлагается ответить на следующие вопросы:

1. Сегодня на уроке я узнал...
2. Что представляет собой система DNS и почему она удобна для адресации ресурсов?
3. Какие домены верхнего уровня появились в первую очередь и что они означали?

Тема урока «Создание надёжного пароля»

Тип урока: открытия новых знаний

Цель урока: Ознакомление с критериями надёжности пароля и методами его создания.

Планируемые результаты

Предметные: получение знаний о необходимости формирования определенных правил при создании, хранении и использовании паролей.

Личностные: готовность и способность обучающихся к саморазвитию и личностному самоопределению; сформированность их мотивации к обучению и целенаправленной познавательной деятельности.

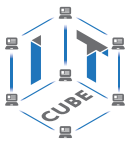
Время реализации: 1 академический час

Оборудование и материалы: компьютер, проектор.

Ход урока

I. Мотивационный этап — 5 мин.

Деятельность учителя: сообщает о том, человека окружает огромное количество устройств, подключенных к сети, использующих различные аккаунты и сервисы, защищенные паролем.



Деятельность учеников: приводят примеры на основе собственного опыта.

Дидактические и методические материалы: дидактические материалы пособия «Настройка оборудования».

II. Этап актуализации знаний по предложенной теме и осуществление первого пробного действия — 8 мин.

Деятельность учителя: для того чтобы злоумышленник не получил доступ к вашему устройству нужно научиться придумывать надежные пароли.

Деятельность учеников: называют критерии надежного пароля на основе собственного опыта.

Дидактические и методические материалы: дидактические материалы пособия «Настройка оборудования».

III. Этап изучения нового материала — 16 мин.

Деятельность учителя: сообщает о том, что случайный пароль — это золотой стандарт в информационной безопасности. Он по определению лучше, чем любой пароль, придуманный человеком. Но возникают сложности с его запоминанием.

Рассказывает о том, как злоумышленники могут получить доступ к паролю злоумышленник: перебор по словарю, личные данные из открытых источников, брутфорс-атаки, фишинг, утечки данных.

Рассказывает о программах для сохранения паролей.

Обращает внимание на то, что существует несколько паролей, которые обязательно должны быть сильными и которые необходимо помнить:

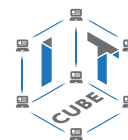
- пароль от вашего устройства;
- пароль для шифрования/расшифровки (например, жесткого диска);
- мастер-пароль или парольная фраза для менеджера паролей;
- пароль от E-mail;

Приводит чек-лист для проверки стойкости пароля ко взлому:

- ваш пароль длинный? Длина пароля должна быть минимум 10—12 символов;
- ваш пароль трудно угадать? Следует избегать простых последовательностей («12345», «qwerty») — такие пароли подбираются за очень быстро. По той же причине следует избегать распространенных слов («password1»);
- разнообразен ли состав символов в вашем пароле? Чем больше в пароле разнотипных символов, тем он менее предсказуем;
- есть ли в вашем пароле очевидные подстановки символов? Например, ноль вместо буквы «О»;
- есть ли в вашем пароле необычные сочетания слов? Кодовые фразы надежнее, если слова в них идут в неожиданном порядке;
- сможете ли вы запомнить свой пароль? Составляйте пароль так, чтобы он был понятен вам, но труден для машинного подбора;
- пользовались ли вы этим паролем раньше? Каждый пароль должен быть уникальным.

Рассказывает о двух методах генерации надежных паролей, которые легко запоминать:

Метод «Diceware» заключается в том, что человек бросает игральные кости, чтобы случайным образом выбрать несколько слов из списка. Выбранные слова образуют парольную фразу. Это отличный способ сгенерировать последовательность, потому что такой метод действительно гарантирует вам случайную комбинацию слов. К тому же, образованную фразу будет легко запомнить. Можно усовершенствовать данный метод, используя отрывок литературного произведения, которое вы помните наизусть. Для выбора слова можно воспользоваться приложением, имитирующим броски игровых кубиков.



А полученную комбинацию цифр можно хранить даже в открытом доступе, при условии, что контрольную фразу знаете только вы.

Метод «**Ключевого слова**» состоит в выборе контрольного слова, на основе которого генерируются все пароли следующим образом:

- пароли вводятся латиницей, поэтому необходимо выбрать одно английское слово (не собственное имя, не название аккаунта и т. п.). Например, **Firefox**;
- следующая часть пароля должна отличаться от сервиса к сервису. И ей может стать название сервиса. Например, **yandex** для аккаунта на Яндекс или **mail**, соответственно, для mail.ru;
- многие сайты просят использовать и буквы, и цифры. На этот случай нам понадобится еще одна часть пароля — цифровая. В качестве цифры можно использовать, например, количество букв в предыдущей части (названии сервиса). То есть для Яндекса это 6, для mail.ru это 4 или вариант — количество гласных или согласных. **yandex6**;
- сервисы могут попросить использовать и строчные, и заглавные буквы. Поэтому необходимо использовать общее правило написания пароля. Например, каждая часть пишется с большой буквы. Дополнительно можно добавить в конце какой-нибудь символ — например, «!». Использование символов тоже может быть требованием сервиса. **FirefoxYandex6!**

Рассказывает основные правила, с помощью которых возможно сохранить свои пароли в тайне:

- создать новый пароль для каждого важного сервиса;
- включить двухфакторную аутентификацию везде, где есть эта опция;
- не сохранять пароли в браузере;
- не вводить пароли на сайтах без SSL-сертификата;
- никому не доверять и не называть пароль. Даже друзьям. Даже родителям;
- менять пароль каждый раз, когда кажется, что его могли украсть. В остальных случаях менять пароль не реже, чем раз в 6 месяцев.

Деятельность учеников: фиксируют ключевую информацию в письменной форме.

Дидактические и методические материалы: дидактические материалы пособия «Настройка оборудования».

IV. Этап проверки понимания и первичного закрепления — 8 мин.

Деятельность учителя: предлагает учащимся ответить на следующий вопрос и выполнить задание.

- что такое надежный пароль?
- как часто желательно менять пароли?
- нужно ли включать двухфакторную авторизацию и почему?

Деятельность учеников: отвечают на поставленные вопросы.

Дидактические и методические материалы: дидактические материалы пособия «Настройка оборудования».

V. Этап контроля усвоения и коррекции ошибок — 4 мин.

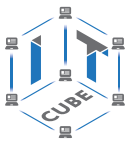
Деятельность учителя: предлагает ответить учащимся на следующие вопросы:

- какой длины должен быть надежный пароль?
- какие символы можно и нужно использовать при создании пароля?
- может ли быть один пароль у нескольких сервисов и почему это опасно?

Деятельность учеников: отвечают на вопросы учителя.

Дидактические и методические материалы: дидактические материалы пособия «Настройка оборудования».

VI. Информация о домашнем задании, инструктаж по его выполнению — 2 мин.



Деятельность учителя: сообщает учащимся домашнее задание — *сформировать пароли на основе предложенных методов и потренироваться в их запоминании.*

VII. Этап рефлексии деятельности на уроке — время 2 мин.

Деятельность учителя: для оценки своей деятельности учащимся предлагается ответить на следующие вопросы:

- сегодня на уроке я узнал...;
- почему опасно иметь одинаковые пароли от разных сервисов?
- я буду создавать надежные пароли и стараться регулярно их обновлять в будущем?

Тема урока «Поиск и обработка информации»

Тип урока: открытия новых знаний

Цель урока: Ознакомление с свойствами и типами информации, способами ее получения, проверки и обработки.

Планируемые результаты

Предметные: получение знаний о свойствах информации, способах работы с информационными источниками, способах анализа и систематизации информации.

Личностные: готовность и способность обучающихся к саморазвитию и личностному самоопределению; сформированность их мотивации к обучению и целенаправленной познавательной деятельности.

Время реализации: 1 академический час

Оборудование и материалы: компьютер, проектор.

Ход урока

I. Мотивационный этап — 5 мин.

Деятельность учителя: Информация нас окружает повсюду. Информация нематериальна, но всеобъемлюща и когда мы начинаем изучать незнакомую нам тему, мы всегда ищем наиболее простую точку входа. В рамках школьной программы нам ее обычно обеспечивает учебное пособие. Дополнительные материалы расширяют круг наших знаний. Объяснения учителя помогают разобраться во всех деталях, понять и научиться использовать полученную информацию. Но в реальной жизни не всегда предоставляется возможность столь простого сценария, да и темы порой возникают сложные и неоднозначные.

Деятельность учеников: приводят примеры информационных процессов на основе собственного опыта.

Дидактические и методические материалы: дидактические материалы пособия «Поиск и обработка данных. Основные принципы».

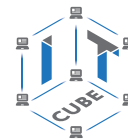
II. Этап актуализации знаний по предложенной теме и осуществление первого пробного действия — 8 мин.

Деятельность учителя: озвучивает определения термина «информация». Предлагает учениками сформулировать определение термина собственными словами.

Деятельность учеников: формулируют определение.

Дидактические и методические материалы: дидактические материалы пособия «Поиск и обработка данных. Основные принципы».

III. Этап изучения нового материала — 16 мин.



Деятельность учителя: рассказывает о способах хранения и передачи информации, почему это важно для человека. Стремление зафиксировать, сохранить надолго свое восприятие информации было всегда свойственно человеку. Мозг человека хранит множество информации и использует для хранения её свои способы, основа которых — двоичный код, как и у компьютеров. Человек всегда стремился иметь возможность поделиться своей информацией с другими людьми и найти надежные средства для её передачи и долговременного хранения. Для этого в настоящее время изобретено множество способов хранения информации на внешних носителях и её передачи на огромные расстояния.

То, как информация представлена, как она кодируется и хранится, даёт возможность её классифицировать следующим образом:

- **графическая** — первый вид, для которого был реализован способ хранения информации об окружающем мире в виде наскальных рисунков, а позднее в виде картин, фотографий, схем, чертежей на бумаге и др.;
- **звуковая** — мир вокруг нас полон звуков и задача их хранения и тиражирования была решена с изобретением звукозаписывающих устройств в 1877 г.;
- **текстовая** — способ кодирования речи человека специальными символами — буквами, особенно большое значение этот способ приобрел после изобретения бумаги и книгопечатания;
- **числовая** — количественная мера объектов и их свойств в окружающем мире; особенно большое значение приобрела с развитием торговли, экономики и денежного обмена; аналогично текстовой информации для её отображения используется метод кодирования специальными символами — цифрами, причем системы кодирования (счисления) могут быть разными;
- **видеоинформация** — способ сохранения динамических картин окружающего мира, появившийся с изобретением кино.

Существуют также виды информации, для которых пока еще не изобретено способов их кодирования и хранения — это **тактильная** информация, передаваемая ощущениями, **органолептическая**, передаваемая запахами и вкусами и др.

Основные свойства информации с точки зрения информатики:

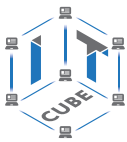
- объективность информации означает, что она отражает объективную действительность и не зависит от субъективного восприятия;
- информация достоверна, если она отражает истинное положение дел. Достоверная информация помогает принять нам правильное решение;
- информацию можно назвать полной, если ее достаточно для понимания и принятия решений;
- точность информации определяется степенью ее близости к реальному состоянию объекта, процесса, явления и т. п.;
- актуальность информации — важность информации для настоящего времени. Только вовремя полученная информация может быть полезна;
- полезность может быть оценена применительно к нуждам конкретных ее потребителей и оценивается по тем задачам, которые можно решить с ее помощью.

Деятельность учеников: фиксируют ключевую информацию и приведенные классификации в письменной форме.

Дидактические и методические материалы: дидактические материалы пособия «Поиск и обработка данных. Основные принципы».

IV. Этап проверки понимания и первичного закрепления — 8 мин.

Деятельность учителя: предлагает учащимся ответить на следующий вопрос и выполнить задание.



- что такое информация?
- как информация может быть представлена?
- перечислите свойства информации?

Деятельность учеников: отвечают на поставленные вопросы.

Дидактические и методические материалы: дидактические материалы пособия «Поиск и обработка данных. Основные принципы».

V. Этап контроля усвоения и коррекции ошибок — 4 мин.

Деятельность учителя: предлагает ответить учащимся на следующие вопросы:

- перечислите свойства информации по мере их важности?
- чем отличается точность и объективность?
- может ли недостоверная информация быть полезна?

Деятельность учеников: отвечают на вопросы учителя.

Дидактические и методические материалы: дидактические материалы пособия «Поиск и обработка данных. Основные принципы».

VI. Информация о домашнем задании, инструктаж по его выполнению — 2 мин.

Деятельность учителя: сообщает учащимся домашнее задание — *подобрать два примера того, как один и тот же объект или процесс описывается с полярных точек зрения.*

VII. Этап рефлексии деятельности на уроке — время 2 мин.

Деятельность учителя: для оценки своей деятельности учащимся предлагается ответить на следующие вопросы:

- сегодня на уроке я узнал...;
- почему важно, чтобы при оценке качества информации учитывались все ее свойства?
- всем ли источникам информации можно доверять?

Тема урока «Создание интеллект-карт»

Тип урока: открытия новых знаний

Цель урока: Ознакомление с одним из способов систематизации знаний.

Планируемые результаты

Предметные: получение знаний о способе структурирования, систематизации, классификации информации по определенной области знаний.

Личностные: готовность и способность обучающихся к саморазвитию и личностному самоопределению; сформированность их мотивации к обучению и целенаправленной познавательной деятельности.

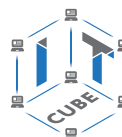
Время реализации: 1 академический час.

Оборудование и материалы: компьютер, проектор.

Ход урока

I. Мотивационный этап — 5 мин.

Деятельность учителя: ради получения и сохранения знаний, повышения удобства в последующим их использовании человечество на протяжении всей своей истории старалось отыскать наиболее простые, но в то же время эффективные способы управления информацией. XX век принес человечеству информатизацию, а вместе с этим ускорение



информационных процессов и увеличение объемов потребляемой информации, что в свою очередь породило разнообразные методологии, помогающие человеку с этим справиться.

Деятельность учеников: на основе собственного опыта приводят примеры информационных процессов, в которые они вовлечены.

Дидактические и методические материалы: дидактические материалы пособия «Аналитический подход к информации. Структурирование информации».

II. Этап актуализации знаний по предложенной теме и осуществление первого пробного действия — 8 мин.

Деятельность учителя: приводит пример интеллект-карты.

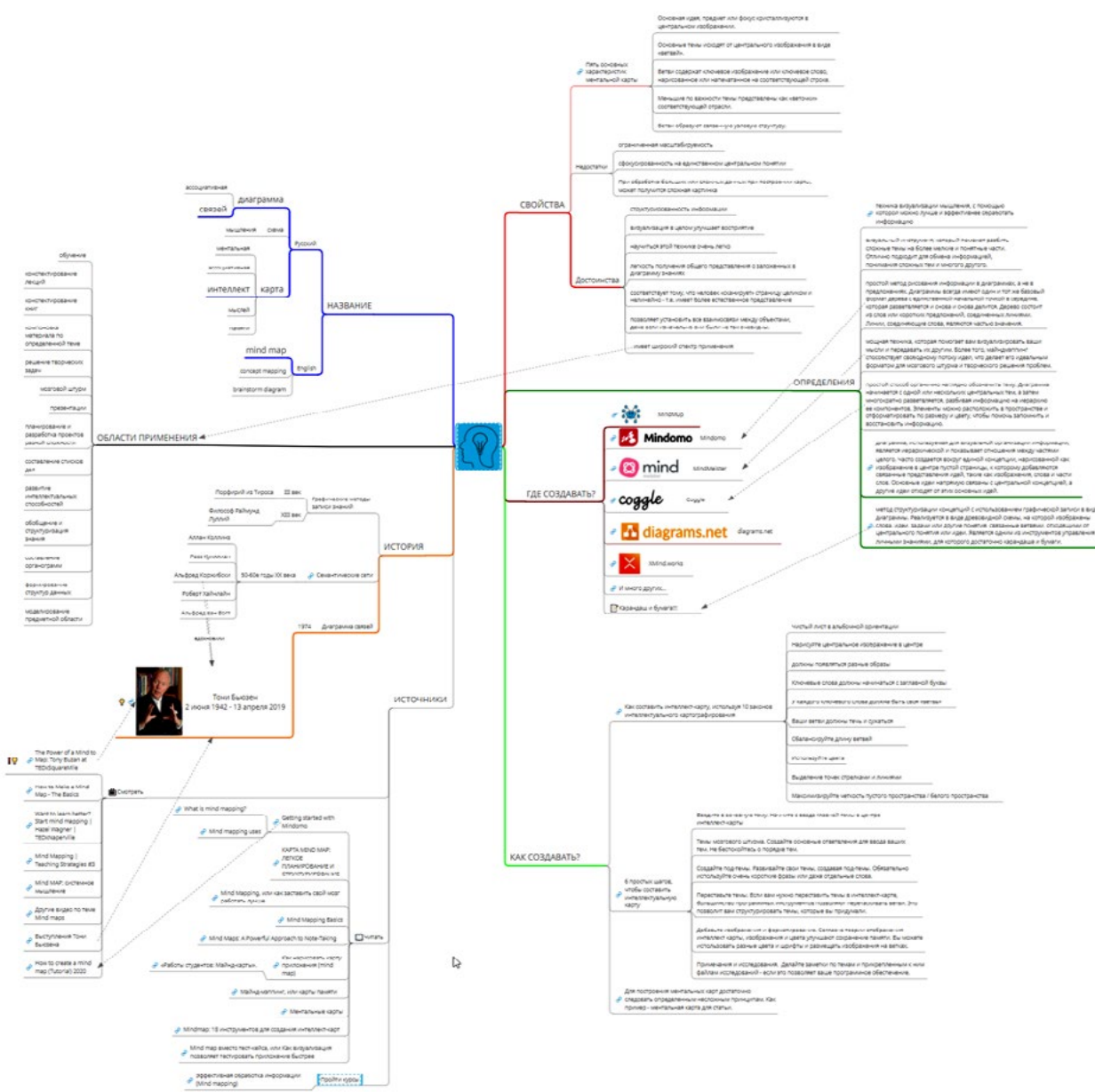


Рис. 30. Интеллект-карта

Кратко рассказывает, что же такое интеллект-карты с точки зрения терминологии. В английском языке существует устоявшийся термин «Mind map». Кроме него иногда употребляются названия «concept mapping» и «brainstorm diagram», отражающие опреде-

ленные аспекты применения данного метода. В русском языке, к сожалению, полного согласия нет. Чаще всего используются названия «диаграмма связей» и «интеллект-карта». Помимо этого, встречаются следующие варианты: карта мыслей, ассоциативная карта, карта памяти, ментальная карта, ассоциативная диаграмма, схема мышления. Мы будем придерживаться термина интеллект-карта.



Рис. 31. Ветвь «Название»

Деятельность учеников: письменно фиксируют возможные названия.

Дидактические и методические материалы: дидактические материалы пособия «Аналитический подход к информации. Структурирование информации».

III. Этап изучения нового материала — 16 мин.

Деятельность учителя: приводит несколько определений понятия «интеллект-карта».

Проводит исторический экскурс по тому, как, когда и почему возникали графические способы записи знаний. Как возникла методология интеллект-карт.

Озвучивает какие особенности и положительные черты есть у данной методологии, акцентируя внимание на пяти основных характеристиках интеллект-карт.

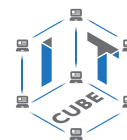
Озвучивает правила создания интеллект-карт (10 законов и 6 шагов).

Деятельность учеников: фиксируют полученную информацию в письменном или графическом виде.

Деятельность учителя: рассказывает о том, что использование современных технологий и соответствующего программного обеспечения позволяет создавать и работать с интеллект-картами намного эффективнее.

Приводит примеры программного обеспечения.

Дидактические и методические материалы: дидактические материалы пособия «Аналитический подход к информации. Структурирование информации».



IV. Этап проверки понимания и первичного закрепления — 8 мин.

Деятельность учителя: предлагает учащимся ответить на следующий вопрос и выполнить задание.

- что такое графические способы записи знаний?
- на что похожа интеллект-карта?
- может ли быть у интеллект-карты несколько корневых понятий?

Деятельность учеников: отвечают на поставленные вопросы.

Дидактические и методические материалы: дидактические материалы пособия «Аналитический подход к информации. Структурирование информации».

V. Этап контроля усвоения и коррекции ошибок — 4 мин.

Деятельность учителя: предлагает ответить учащимся на следующие вопросы:

- где на карте должно находиться основное понятие?
- как много может быть подтем у основного понятия?
- чем отличается каждый уровень ветки от предыдущего?

Деятельность учеников: отвечают на вопросы учителя.

Дидактические и методические материалы: дидактические материалы пособия «Аналитический подход к информации. Структурирование информации».

VI. Информация о домашнем задании, инструктаж по его выполнению — 2 мин.

Деятельность учителя: сообщает учащимся домашнее задание -создать интеллект-карту для понятия «Хлеб».

VII. Этап рефлексии деятельности на уроке — время 2 мин.

Деятельность учителя: Для оценки своей деятельности учащимся предлагается ответить на следующие вопросы:

- сегодня на уроке я узнал...
- как я могу применять интеллект-карты в процессе обучения?

Описание лабораторных работ

Лабораторная работа 1. Выбор и установка антивирусного ПО.

Теоретическая часть

В целях обеспечения конфиденциальности информации, хранящейся на персональных компьютерах, возникают следующие вопросы: какой антивирус выбрать, какие плюсы или минусы имеет тот или иной антивирусный продукт. Для того, чтобы провести сравнительный анализ можно воспользоваться бесплатными версиями антивирусных программ, некоторые из которых обеспечивают уровень защиты, практически не уступающий их платным версиям.

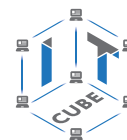
Цель работы: познакомиться с антивирусным программным обеспечением, оценить удобство настройки и использования.

Ход лабораторной работы

1. Выполнить поиск в Интернете по запросу «бесплатный антивирус».
2. Из результатов поиска выбрать 5 антивирусных продуктов.
3. Проанализировать доступную информацию о продуктах: описания на сайтах производителей, имеющаяся документация по продуктам.
4. Занести соответствующую полученную информацию в контрольную таблицу 1.
5. На основе полученной информации выбрать конкретный программный продукт
6. Скачать с официального сайта и установить выбранное антивирусное программное обеспечение.
7. Настроить и проверить работоспособность антивируса.

Таблица 1. Сравнительный анализ антивирусного ПО

Название антивируса					
1. Общая информация					
Веб-сайт					
Версия продукта					
Русифицированный интерфейс					
2. Сравнение возможностей					
Антивирусный монитор					
Поведенческий анализ					
Антируткит (приложение, позволяющее обнаруживать и удалять скрытые угрозы — руткиты)					
Эвристический анализ					
Различные варианты сканирования					
Сканирование при загрузке ПК					
Система репутации файлов					
Песочница					



Продолжение

Название антивируса					
3. Защита при работе в Интернете					
Веб-антивирус					
Черный список URL					
Репутация ссылок и веб-сайтов					
Антибаннер					
Антифишинг					
Почтовый экран					
4. Дополнительные возможности					
Оптимизация работы Windows					
Защита настроек антивируса паролем					
Облачное сканирование подозрительных файлов					
Пассивный режим					
5. Суммарный балл					

Лабораторная работа 2. Создание надежных паролей.

Теоретическая часть

Устанавливать один и тот же пароль на несколько аккаунтов небезопасно. Запомнить несколько десятков разных паролей невозможно. Существует всего несколько паролей, которые должны быть сильными и которые необходимо запомнить:

- пароль от устройства;
- пароль для шифрования/расшифровки (например, жесткого диска);
- мастер-пароль или парольная фраза для менеджера паролей;
- пароль от E-mail.

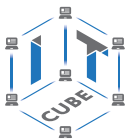
Случайный пароль — это золотой стандарт в информационной безопасности. Он по определению лучше, чем любой пароль, придуманный человеком. Но помнить наизусть такой пароль сложно. Поэтому возникает необходимость уметь создавать надежные пароли, которые возможно запомнить.

Цель работы: освоить базовые принципы создания надежных паролей.

Ход лабораторной работы

1. Изучить критерии определения надежности пароля: длина, наборы используемых символов и т. д.

2. На основе критериев сформировать запоминающийся пароль без использования дополнительного ПО или сложных методик. Пример: XzSaWq21@!

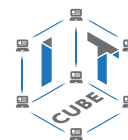


3. Проверить его:
 - На скорость подбора при помощи сервиса <https://2ip.ru/passcheck/>
 - На уникальность и наличие в базах раскрытых паролей <https://haveibeenpwned.com/Passwords>
 - При помощи сервиса <https://password.kaspersky.com/ru/>
4. Провести процедуру регистрации с использованием полученного пароля на любом массовом почтовом сервисе. Получить оценку системы регистрации о надежности пароля и соответствии требованиям системы.
5. Выбрать отрывок любого литературного произведения, которое ученик помнит наизусть (пример — «Однажды в студеную зимнюю пору я из лесу вышел был сильный мороз.»).
6. Воспользоваться методом **Diceware** для создания фразового пароля на основе этого отрывка. Для имитации бросков кубика можно воспользоваться соответствующими мобильными приложениями или сервисом <https://www.random.org/dice/> **Пример:**
10 — был 5 — пору 4 — зимнюю 8 — лесу 7 — из
7. Набрать полученные слова используя английскую раскладку клавиатуры (пример — skgjhepbvy.ktcebp).
8. Комбинацию полученных чисел (10 5 4 8 7) можно записать. Контрольный отрывок не должен быть известен никому.
9. Проверить полученный пароль:
 - На скорость подбора при помощи сервиса <https://2ip.ru/passcheck/>
 - На уникальность и наличие в базах раскрытых паролей <https://haveibeenpwned.com/Passwords>
 - При помощи сервиса <https://password.kaspersky.com/ru/>
10. Провести процедуру регистрации с использованием полученного пароля на любом массовом почтовом сервисе. Получить оценку системы регистрации о надежности пароля и соответствии требованиям системы.
11. Воспользоваться методом «ключевого слова» для создания пароля на его основе.
12. Проверить полученный пароль:
 - На скорость подбора при помощи сервиса <https://2ip.ru/passcheck/>
 - На уникальность и наличие в базах раскрытых паролей <https://haveibeenpwned.com/Passwords>
 - При помощи сервиса <https://password.kaspersky.com/ru/>
13. Провести процедуру регистрации с использованием полученного пароля на любом массовом почтовом сервисе. Получить оценку системы регистрации о надежности пароля и соответствии требованиям системы.
- 14.* Разбиться по парам. Чередуясь между собой попробовать определить и запомнить вводимые символы придуманных паролей без использования технических средств.

Лабораторная работа 3. Настройка Wi-Fi роутера.

Теоретическая часть

Wi-Fi роутер один из основных сетевых компонентов современного цифрового пространства. Wi-Fi роутер позволяет объединить беспроводные устройства в одну сеть и подключить их к Интернету. Он открывает пользователям свободный доступ в Интернет, но может также и послужить лазейкой для злоумышленников в ваше личное простран-



ство. Как быстро начать раздавать Интернет на телефон, телевизор или ноутбук, но при этом обезопасить себя от вторжения?

Цель работы: освоить принципы установки и настройки беспроводного сетевого оборудования создания надежных паролей.

Ход лабораторной работы

1. Выбрать модель роутера из предоставленных.
2. Найти в Интернете инструкцию к соответствующей модели.
3. Изучить способы сброса роутера в исходное состояние, этапы первоначальной настройки, методы блокировки доступа.
4. Провести первоначальную установку устройства (создать Сеть, установить надежные пароли на доступ к Сети и к интерфейсу управления, отключить лишние и не надежные сервисы).
5. Проверить подключение к Интернету.
6. В качестве контроля выполнения лабораторной работы пригласить преподавателя.
7. Сообщить информацию, необходимую для подключения к Сети.
8. После того как преподаватель подключится к Сети и проверит наличие доступа в Интернет (выполнение на оценку «4»), по сигналу необходимо заблокировать доступ в Интернет для устройства, с которого он подключился, и отключить это устройство от Сети без возможности повторного подключения (на основе mac адреса) — выполнение на оценку «5».
9. При оценивании качества настройки учитываются безопасность устройства (стойкость паролей, наличие WPS) и скорость выполняемых действий.

Лабораторная работа 4. Поиск и обработка информации

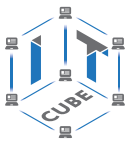
Теоретическая часть

Умение быстро находить нужную и достоверную информацию, а также обрабатывать ее соответствующим образом, является одним из ключевых навыков современного человека.

Цель работы: закрепить способы поиска достоверной информации, работы с различными источниками, формирования на основе этого обзорного доклада.

Ход лабораторной работы

1. Обучающийся выбирает одну из предложенных тем:
 - 1.1. История компании NeXT Computer, Inc. и операционной системы NeXTSTEP.
 - 1.2. Be Incorporated, ее компьютеры и ОС.
 - 1.3. Palm Inc., ее компьютеры и ОС.
 - 1.4. Первый web-сервер и возникновение WWW.
 - 1.5. Появление ПК Macintosh и ОС Mac OS.
 - 1.6. История ПК ZX Spectrum
 - 1.7. История компьютеров Amiga и AMIGA OS
 - 1.8. Компания Atari и ее компьютеры
 - 1.9. Xerox Alto и его операционная система



- 1.10. Первый ПК IBM PC
- 1.11. Носители информации: от перфокарты до облака.
- 1.12. История Windows.
- 1.13. История развития MacOS
- 1.14. История UNIX и Linux
2. На основе открытых источников собирается информация по выбранной теме (минимум 3 источника)
3. По отобранной информации формируется доклад.
4. Для подкрепления доклада создается простая презентация, содержащая графические изображения и ключевые элементы доклада.
5. Доклад и презентация сдаются в конце занятия в электронном виде.
6. Критерии оценивания:
 - 6.1. Доклад длительностью не более 5-ти минут.
 - 6.2. Полное раскрытие темы.
 - 6.3. Презентация должна соответствовать докладу.
 - 6.4. Презентация не должна полностью дублировать текст доклада, а содержать только ключевые мысли.
 - 6.5. Наличие титульного и финального слайда в презентации **обязательно**.
 - 6.6. В тексте не должно быть форматирования, ссылок, сносок и т. п. элементов использованных источников.
 - 6.7. В презентации должны быть сохранены правильные пропорции изображений.

Лабораторная работа 5. Анализ предметной области «Музыкальный сервис»

Теоретическая часть

Предметную область можно определить как сферу человеческой деятельности, выделенную и описанную согласно установленным критериям. В описываемое понятие должны входить сведения об ее элементах, явлениях, отношениях и процессах. Предметную область можно определить как объект или систему со всем комплексом понятий и знаний о ее функционировании.

Цель работы: познакомиться с методологией декомпозиции и анализа предметной области.

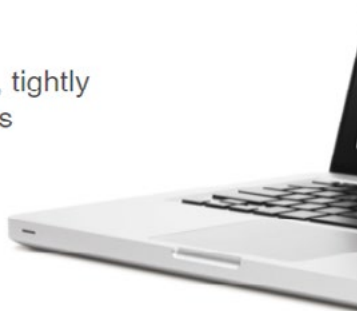
Ход лабораторной работы

1. Выбрать любой из популярных музыкальных стриминговых сервисов (Apple Music, YouTube Music, VK (Boom), Яндекс.Музыка, Spotify, SoundCloud, Deezer).
2. Создать новую интеллект-карту при помощи сервиса <https://drive.mindmup.com/>



MindMup 2

Zero-friction mind mapping, tightly
integrated with Google Apps



Store unlimited mind maps for free on Google Drive, share and collaborate using online mindmapping. Based i

MindMup 2.0 is connected to your Google Drive but not set-up to open files on double-click. [Enabl](#)

CREATE A NEW MAP

OPEN FROM GOOGLE DRIVE

Рис. 32. Титульная страница сервиса MindMup 2

3. В качестве центрального понятия ввести название выбранного сервиса и добавить соответствующее изображение.



Рис. 33. Центральное понятие

4. На основе имеющихся знаний, функционала сервиса постараться выделить ключевые элементы, из которых состоит сервис и отразить их на диаграмме.



Рис. 34. Первый уровень

5. Последовательно разделить понятия первого уровня на составляющие их настолько, насколько это возможно.

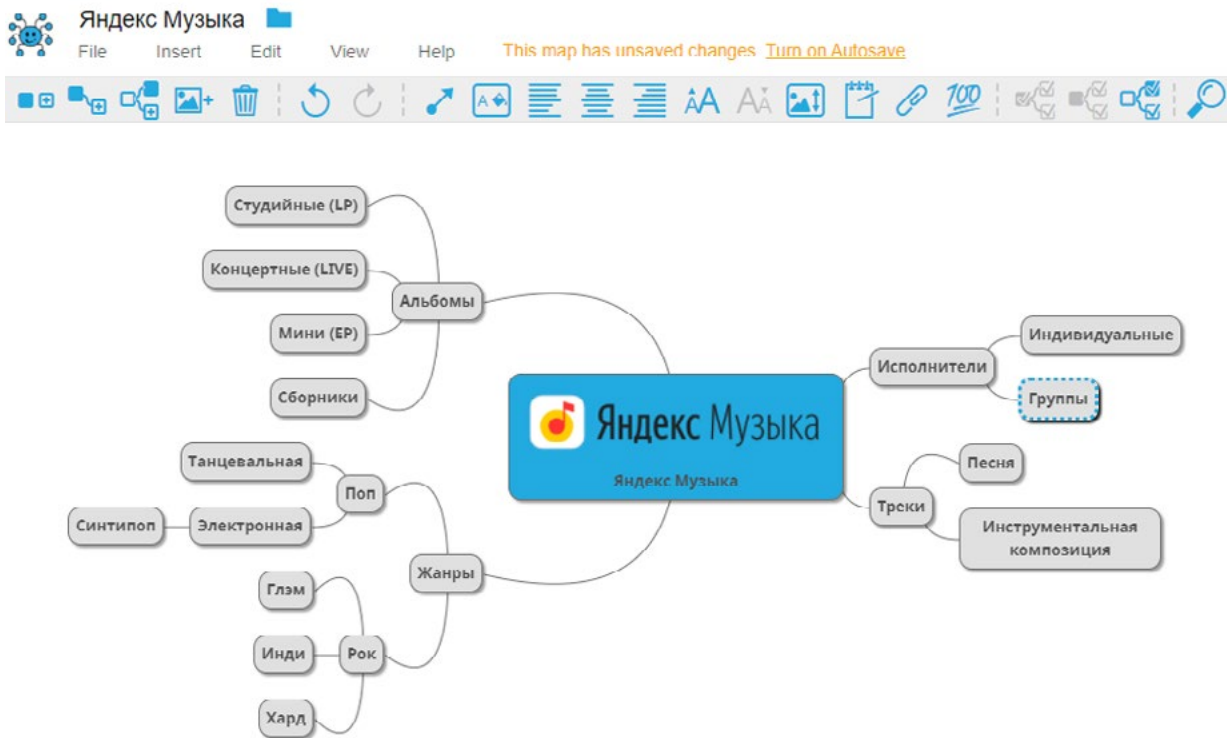


Рис. 35. Структуризация

6. На основе полученной первоначальной схемы провести уточнение полученных веток понятий.

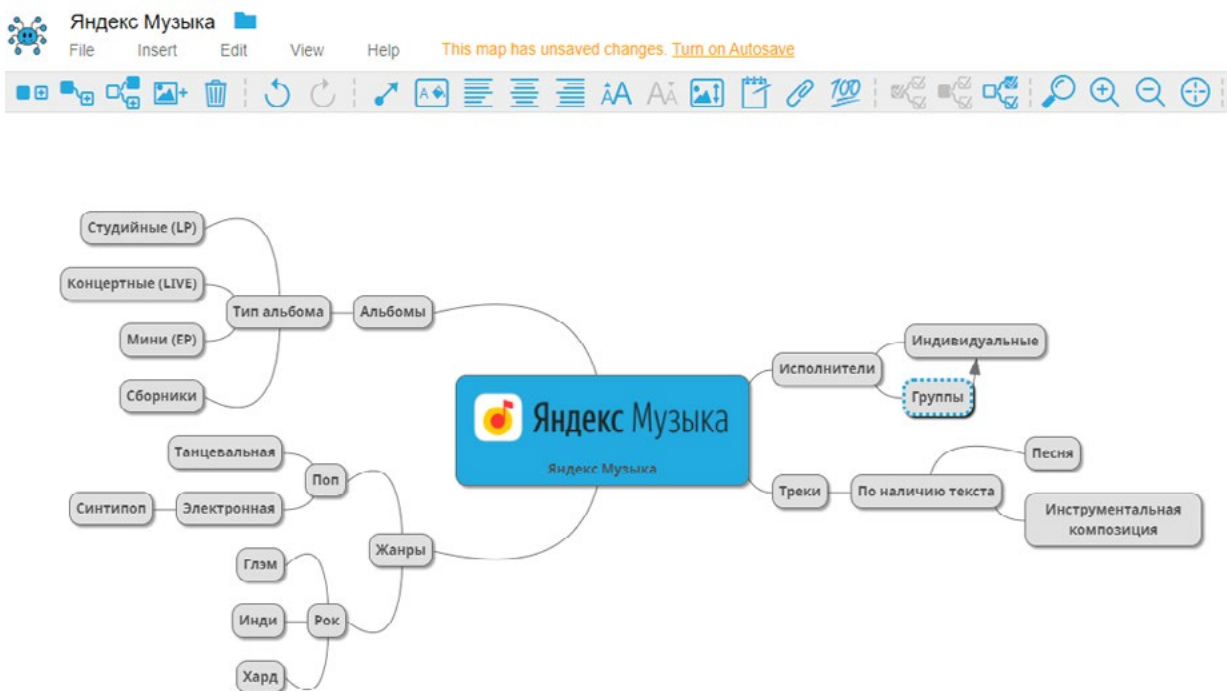
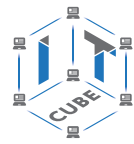


Рис. 36. Введение промежуточных понятий



7. Дополнить схему необходимыми свойствами.

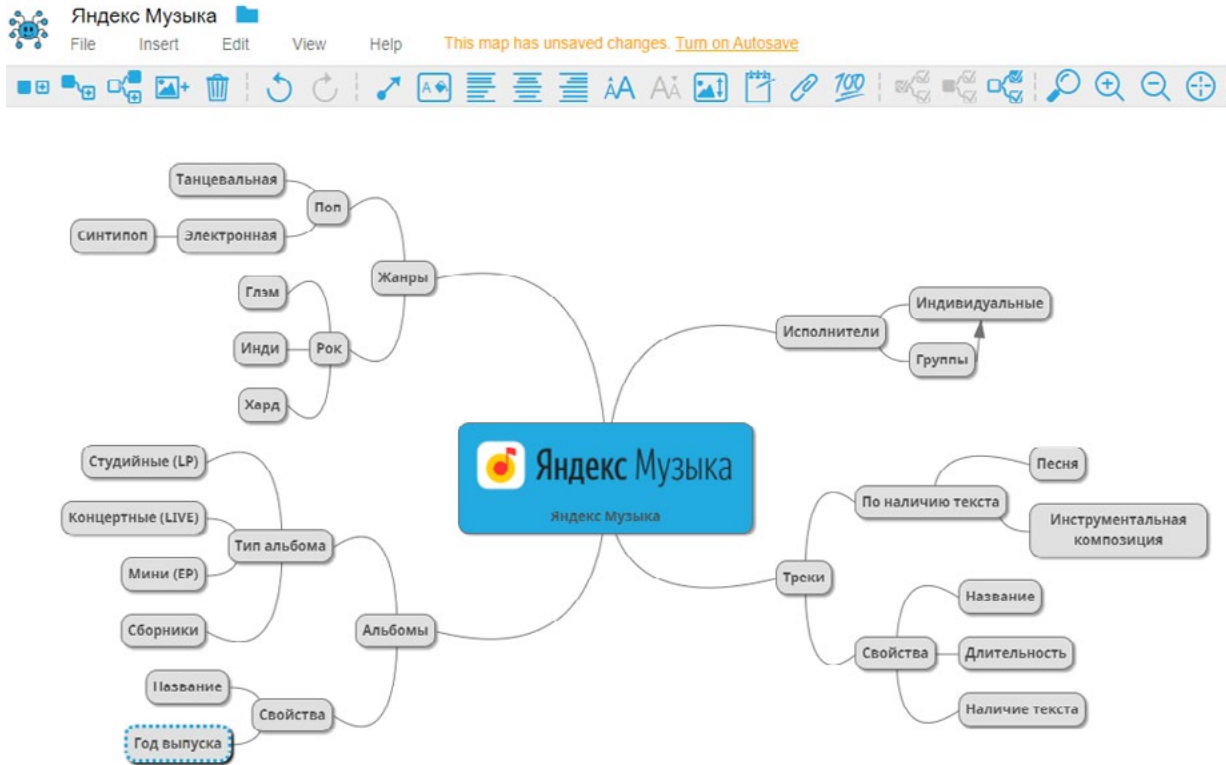


Рис. 37. Добавление свойств

8. Восстановить дополнительные связи между понятиями.

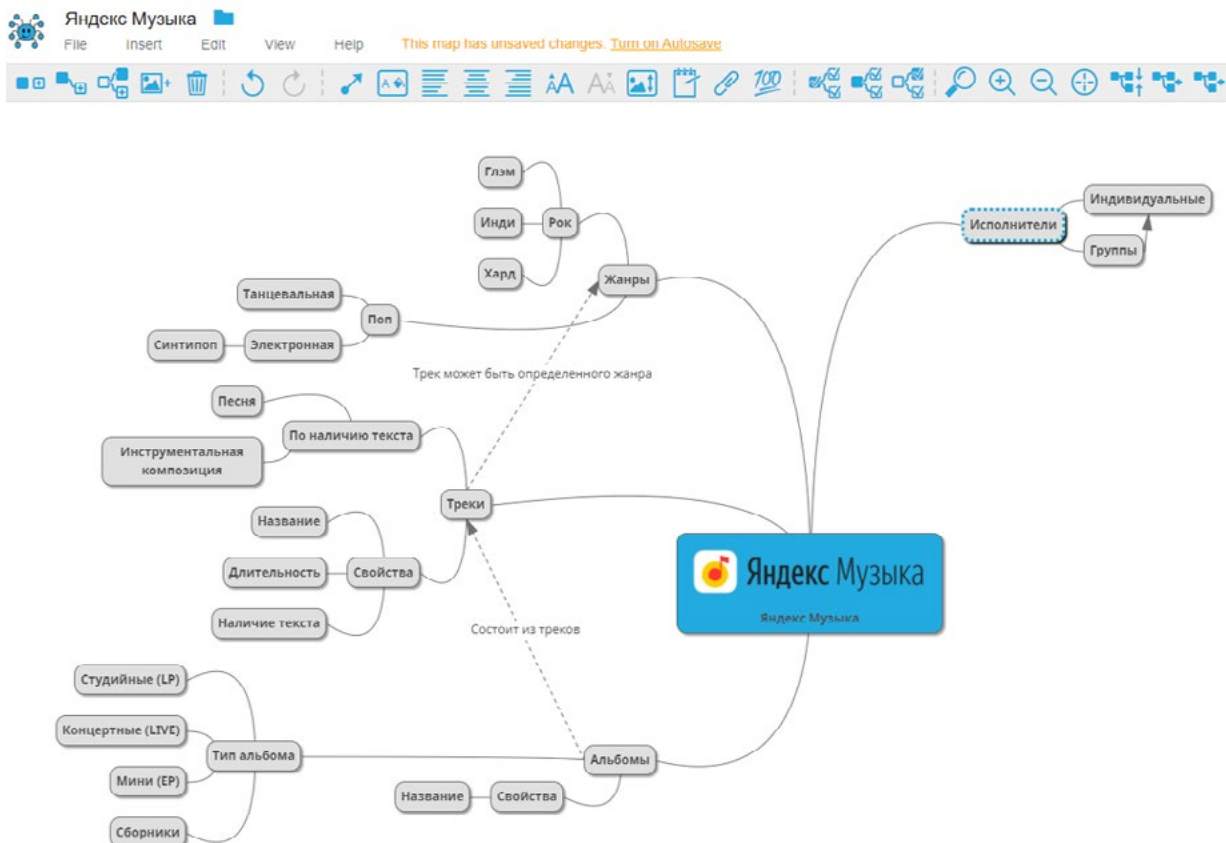
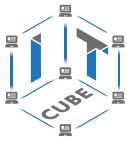
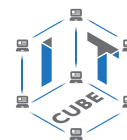


Рис. 38. Создание дополнительных связей



9. Проанализировать полученную схему.

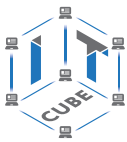
10. Выбрать пару из учеников группы. Сравнить полученные схемы. Проанализировать схожие и различные элементы. При необходимости внести изменения в свою схему.



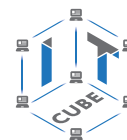
Список доступных источников

Источники приведены в алфавитном порядке.

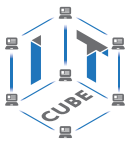
1. Архив Интернета — [Электронный ресурс] URL:https://ru.wikipedia.org/wiki/%D0%90%D1%80%D1%85%D0%B8%D0%B2_%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0 (дата обращения: 10.04.2021)
2. Виды запоминающих устройств — [Электронный ресурс] URL:<https://www.dropbox.com/ru/business/resources/storage-devices> (дата обращения: 10.04.2021)
3. Выступления Тони Бьюзена — [Электронный ресурс] URL:https://www.youtube.com/results?search_query=Tony+Buzan (дата обращения: 10.04.2021)
4. ГРАЖДАНСКИЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ. ЧАСТЬ ЧЕТВЕРТАЯ. (с изменениями на 30 декабря 2020 года) (редакция, действующая с 17 января 2021 года) — [Электронный ресурс] URL:<https://docs.cntd.ru/document/902019731?marker=8PC0LS> (дата обращения: 10.04.2021)
5. Диаграмма связей — [Электронный ресурс] URL:https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%B0%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0_%D1%81%D0%B2%D1%8F%D0%B7%D0%B5%D0%B9 (дата обращения: 10.04.2021)
6. Другие видео по теме Mind maps — [Электронный ресурс] URL:https://www.youtube.com/results?search_query=mind+map (дата обращения: 10.04.2021)
7. Законодательство в области борьбы с преступлениями против несовершеннолетних Выдержки из уголовного кодекса — [Электронный ресурс] URL:<http://www.ligainternet.ru/encyclopedia-of-security/citizens/%D1%81itizens-detail.php?ID=433> (дата обращения: 10.04.2021)
8. Запоминающее устройство — [Электронный ресурс] URL:https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BF%D0%BE%D0%BC%D0%B8%D0%BD%D0%B0%D1%8E%D1%89%D0%B5%D0%B5_%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%BE (дата обращения: 10.04.2021)
9. История компьютерных вирусов — [Электронный ресурс] URL:https://ru.wikipedia.org/wiki/%D0%98%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%8F_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D1%85_%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BE%D0%B2 (дата обращения: 10.04.2021)
10. Как нарисовать карту приложения (mind map) — [Электронный ресурс] URL:<http://okiseleva.blogspot.com/2020/01/mind-map.html> (дата обращения: 10.04.2021)
11. Как появилась электронная почта: история с соб@чкой — [Электронный ресурс] URL:https://gb.ru/posts/at_symbol_history (дата обращения: 10.04.2021)
12. Карта mind map: легкое планирование и структурирование — [Электронный ресурс] URL:<https://blog.checkiant.com/ru/blog-o-produktivnosti/166-tekhnologiya-mind-mapping> (дата обращения: 10.04.2021)
13. Краткая история Интернета — [Электронный ресурс] URL:<https://www.youtube.com/watch?v=rQPBT2dimSg> (дата обращения: 10.04.2021)
14. Кредитный скоринг — [Электронный ресурс] URL:https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B5%D0%B4%D0%B8%D1%82%D0%BD%D1%8B%D0%B9_%D1%81%D0%BA%D0%BE%D1%80%D0%B8%D0%BD%D0%B3 (дата обращения: 10.04.2021)
15. Майнд-мэппинг, или карты памяти — [Электронный ресурс] URL:<https://web.archive.org/web/20100611215537/http://perevodik.net/ru/posts/31/> (дата обращения: 10.04.2021)



16. Майндмэппинг — Ментальные карты онлайн — MindMeister — [Электронный ресурс] URL:<https://www.mindmeister.com/ru> (дата обращения: 10.04.2021)
17. Ментальные карты — [Электронный ресурс] URL:<https://kolesnik.ru/2005/mindmapping/> (дата обращения: 10.04.2021)
18. Основы сетей передачи данных. Модель OSI и стек протоколов TCP IP. Основы Ethernet. [GeekBrains] — [Электронный ресурс] URL:https://www.youtube.com/watch?v=Z-a7MNStFQs&t=754s&ab_channel=GeekBrains (дата обращения: 10.04.2021)
19. Персональные данные — [Электронный ресурс] URL:https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5 (дата обращения: 10.04.2021)
20. Перфокарта — [Электронный ресурс] URL:<https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%84%D0%BE%D0%BA%D0%B0%D1%80%D1%82%D0%B0> (дата обращения: 10.04.2021)
21. Работы студентов: Майнд-карты — [Электронный ресурс] URL:<https://testbase.atlassian.net/wiki/spaces/STUDENTS/pages/436109314/> (дата обращения: 10.04.2021)
22. Система социального кредита — [Электронный ресурс] URL:https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BA%D1%80%D0%B5%D0%B4%D0%B8%D1%82%D0%B0 (дата обращения: 10.04.2021)
23. Федеральный закон “О внесении изменений в Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию” и отдельные законодательные акты Российской Федерации” 139-ФЗ — [Электронный ресурс] URL:<http://www.ligainternet.ru/encyclopedia-of-security/citizens/%D1%81itizens-detail.php?ID=444> (дата обращения: 10.04.2021)
24. Федеральный закон о защите детей от информации, причиняющей вред их здоровью и развитию 436-ФЗ в ред. Федерального закона от 28.07.2012 N 139-ФЗ — [Электронный ресурс] URL:<http://www.ligainternet.ru/encyclopedia-of-security/citizens/%D1%81itizens-detail.php?ID=445> (дата обращения: 10.04.2021)
25. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 30.12.2020) “О персональных данных” (с изм. и доп., вступ. в силу с 01.03.2021) — [Электронный ресурс] URL:<https://docs.cntd.ru/document/901990046> (дата обращения: 10.04.2021)
26. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, технологиях и о защите информации — [Электронный ресурс] URL:<http://www.rg.ru/2006/07/29/informacia-dok.html> (дата обращения: 10.04.2021)
27. Эффективная обработка информации (Mind mapping) — [Электронный ресурс] URL:<https://intuit.ru/studies/courses/647/503/info> (дата обращения: 10.04.2021)
28. Coggle — [Электронный ресурс] URL:<https://coggle.it/> (дата обращения: 10.04.2021)
29. Evolution Of The Desk — [Электронный ресурс] URL:https://www.youtube.com/watch?v=r5IC_jyZKJg (дата обращения: 10.04.2021)
30. Getting started with Mindomo — [Электронный ресурс] URL:<https://help.mindomo.com/> (дата обращения: 10.04.2021)
31. History of Most Popular Websites (1997-2020) — [Электронный ресурс] URL:https://www.youtube.com/watch?v=1tUB7ltoYx4&list=PL_EZXeYDybfSxfVDmrNqaoeZJZID07Y-A&index=7&ab_channel=DatalsBeautiful (дата обращения: 10.04.2021)
32. How to create a mind map (Tutorial) 2020 — [Электронный ресурс] URL:https://www.youtube.com/watch?v=RNErLu8BMiw&ab_channel=Mindomo (дата обращения: 10.04.2021)



33. How to Make a Mind Map — The Basics — [Электронный ресурс] URL:https://www.youtube.com/watch?v=wLWV0XN7K1g&ab_channel=SusanGregory (дата обращения: 10.04.2021)
34. IBM 7090 — [Электронный ресурс] URL:https://ru.wikipedia.org/wiki/IBM_7090 (дата обращения: 10.04.2021)
35. IBM 7094 Data Processing System — [Электронный ресурс] URL:https://www.ibm.com/ibm/history/exhibits/mainframe/mainframe_PP7094.html (дата обращения: 10.04.2021)
36. Mind map — [Электронный ресурс] URL:https://en.wikipedia.org/wiki/Mind_map (дата обращения: 10.04.2021)
37. Mind map вместо тест-кейса, или Как визуализация позволяет тестировать приложение быстрее — [Электронный ресурс] URL:<https://habr.com/ru/company/badoo/blog/418353/> (дата обращения: 10.04.2021)
38. Mind Map Mastery: 10 Tony Buzan Mind Mapping Laws You Should Follow — [Электронный ресурс] URL:<https://www.magneticmemorymethod.com/tony-buzan-mind-map-mastery/> (дата обращения: 10.04.2021)
39. Mind MAP: системное мышление — [Электронный ресурс] URL:https://www.youtube.com/watch?v=vB6wl9y1_Vs (дата обращения: 10.04.2021)
40. Mind Mapping | Teaching Strategies #3 — [Электронный ресурс] URL:https://www.youtube.com/watch?v=xCujFipyRE&ab_channel=TeachingsinEducation (дата обращения: 10.04.2021)
41. Mind Mapping Basics — [Электронный ресурс] URL:<https://simplemind.eu/how-to-mind-map/basics/> (дата обращения: 10.04.2021)
42. Mind mapping uses — [Электронный ресурс] URL:<https://help.mindomo.com/mind-mapping/mind-mapping-uses/> (дата обращения: 10.04.2021)
43. Mind Mapping, или как заставить свой мозг работать лучше — [Электронный ресурс] URL:<https://habr.com/ru/company/devexpress/blog/291028/#What> (дата обращения: 10.04.2021)
44. Mind Maps: A Powerful Approach to Note-Taking — [Электронный ресурс] URL:https://www.mindtools.com/pages/article/newISS_01.htm (дата обращения: 10.04.2021)
45. Mindmap: 18 инструментов для создания интеллект-карт — [Электронный ресурс] URL:<https://texterra.ru/blog/obzor-15-besplatnykh-programm-dlya-sozdaniya-intellekt-kart.html> (дата обращения: 10.04.2021)
46. Mindomo — [Электронный ресурс] URL:<https://www.mindomo.com/ru/> (дата обращения: 10.04.2021)
47. Most Popular Instant Messaging Apps (2000-2020) — [Электронный ресурс] URL:https://www.youtube.com/watch?v=pdZ179PmCPk&list=PL_EZXeYDybfSxfVDmrNqaoeZJZID07Y-A&index=6&ab_channel=DatalsBeautiful (дата обращения: 10.04.2021)
48. Most Popular Instant Messengers 1995 — 2020 — [Электронный ресурс] URL:https://www.youtube.com/watch?v=yJ3TTV0II4o&list=PL_EZXeYDybfQW9ry5U7H6zd8xXPPY8cwS&index=4&t=114s&ab_channel=CaptainGizmo (дата обращения: 10.04.2021)
49. Most Popular Internet Browsers (1994-2020) — [Электронный ресурс] URL:https://www.youtube.com/watch?v=th6ipORQaOY&list=PL_EZXeYDybfSxfVDmrNqaoeZJZID07Y-A&index=4&t=3s&ab_channel=DatalsBeautiful (дата обращения: 10.04.2021)
50. Most Popular Web Browsers 1993 — 2020 — [Электронный ресурс] URL:https://www.youtube.com/watch?v=W4wWdmfOibY&list=PL_EZXeYDybfQW9ry5U7H6zd8xXPPY8cwS&index=3&t=3s&ab_channel=CaptainGizmo (дата обращения: 10.04.2021)
51. Most Sold Mobile Phones (1994-2020) — [Электронный ресурс] URL:<https://www.youtube.com/watch?v=nuqvbh56VyM> (дата обращения: 10.04.2021)



52. PowWow (chat program) — [Электронный ресурс] URL:[https://en.wikipedia.org/wiki/PowWow_\(chat_program\)](https://en.wikipedia.org/wiki/PowWow_(chat_program)) (дата обращения: 10.04.2021)
53. RFC 5322 — Internet Message Format — [Электронный ресурс] URL:<https://tools.ietf.org/html/rfc5322> (дата обращения: 10.04.2021)
54. RFC 822 — Standard for the format of arpa internet text messages — [Электронный ресурс] URL:<https://tools.ietf.org/html/rfc822> (дата обращения: 10.04.2021)
55. The Power of a Mind to Map: Tony Buzan at TEDxSquareMile — [Электронный ресурс] URL:https://www.youtube.com/watch?v=nMZCghZ1hB4&ab_channel=TEDxTalks (дата обращения: 10.04.2021)
56. Theory Behind Mind Maps — [Электронный ресурс] URL:<https://www.mindmapping.com/mind-map#mindmap-theory> (дата обращения: 10.04.2021)
57. Want to learn better? Start mind mapping | Hazel Wagner | TEDxNaperville — [Электронный ресурс] URL:https://www.youtube.com/watch?v=5nTuScU70As&ab_channel=TEDxTalks (дата обращения: 10.04.2021)
58. What is mind mapping? — [Электронный ресурс] URL:<https://help.mindomo.com/mind-mapping/what-is-mind-mapping/> (дата обращения: 10.04.2021)
59. Wikipedia List of concept- and mind-mapping software — [Электронный ресурс] URL:https://en.wikipedia.org/wiki/List_of_concept-_and_mind-mapping_software (дата обращения: 10.04.2021)
60. XMPP — [Электронный ресурс] URL:<https://ru.wikipedia.org/wiki/XMPP> (дата обращения: 10.04.2021)



Материалы для организации и проведения учебно-исследовательской и проектной деятельности

Примерные темы по развитию учебно-исследовательских и проектных навыков

1. Инструментарий современного специалиста по большим данным.
2. Методологии информационного моделирования.
3. Современные программы для моделирования информационных систем и бизнес-процессов.
4. Использование Excel для обработки больших данных.
5. Инструментарий языка Python по обработке и анализу информации.
6. Поиск в открытом доступе наборов данных для обучения нейронных сетей.
7. Большие данные большого города.
8. Перспективы развития цифровых технологий и критерии их безопасности.
9. Проблемы безопасности в современном мире и их зависимость от цифровых технологий.
10. Методы получения доступа к конфиденциальной информации.

Данный перечень тем является далеко не полным. На основе данных тем можно проводить как обзорные занятия, поверхностно погружающие в проблематику вопроса, так и формировать цикл занятий, на основе детализации выбранной темы. Также данные темы могут помочь обучающимся при выборе направления учебно-исследовательских проектов. Все темы являются на текущий момент актуальными для современного общества и не потеряют своей актуальности в ближайшей перспективе.



Григорьев Сергей Георгиевич
Львов Алексей Юрьевич
Старостина Екатерина Вячеславовна

**Реализация дополнительной общеобразовательной программы
по тематическому направлению «Кибергигиена и работа
с большими данными» с использованием оборудования
центра цифрового образования детей «IT-куб»**

Методическое пособие

Под ред. Григорьева С. Г.

Центр естественно-научного и математического образования
Руководитель центра *З. Г. Гапонюк*
Ответственный за выпуск *Е. С. Карауш*
Редактор *Е. С. Карауш*
Художественное оформление *С. И. Ситникова*
Компьютерная вёрстка и техническое редактирование *Э. В. Алексеева*
Корректор *Г. И. Мосякина*