Муниципальное автономное общеобразовательное учреждение

«Гимназия №25 г. Благовещенска»

Итоговый индивидуальный проект

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Автор:ученик 11Б класса

МАОУ гимназии №25

Новицкий Г.С.

Руководитель:Гражданцев А.В.

Учитель информатики

2021-2022 учебный год

**Паспорт проекта**

|  |  |
| --- | --- |
| Автор материала(ФИ) | Новицкий Георгий |
| Руководитель | Учитель информатики  Гражданцев Александр Викторович |
| Образовательное учреждение | МАОУ «Гимназия №25 г. Благовещенска» |
| Название материала | Презентация по теме: Информационная безопасность |
| Класс(возраст) | 11 класс, 17 лет |
| Учебный предмет | Информатика |
| Сроки и основные этапы выполнения проекта | 1. Подготовительный этап  май-июнь 2021  2. Основной этап  сентябрь-ноябрь 2021  3. Заключительный этап  ноябрь-декабрь 2021 |
| Методы, используемые в проекте | Изучение литературы, анализ статистических и анкетных данных |
| Вид ресурса(презентация, текстовый документ) | Презентация, текстовый документ |
| Техническое оснащение(интерактивная доска, компьютер и другое) | Компьютер, проектор |
| Цель | Выработать методы и средства информационной безопасности. |

**ВВЕДЕНИЕ**

Быстрый рост глобальной сети Интернет и стремительное развитие информационных технологий привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности.

Развитие современного общества напрямую связано с ростом производства, потребления и накопления информации во всех отраслях человеческой деятельности. Информационные потоки в обществе увеличиваются с каждым днем, и этот процесс носит лавинообразный характер. По своему значению для развития общества информация приравнивается к важнейшим ресурсам наряду с сырьем и энергией. В развитых странах большинство работающих заняты не в сфере производства, а в той или иной степени занимаются обработкой информации.

Несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей, к сожалению, не уменьшается. Средства взлома компьютерных систем и хищения информации развиваются так же быстро, как и все высокотехнологичные компьютерные отрасли. Не материальные ценности, а чистая информация становится объектом хищения. Это обстоятельство подчеркивает, насколько важной является информация для современного общества.

Несмотря на серьезные затраты, вкладываемые в обеспечение безопасности, количество и многообразие преступлений, совершаемых с использованием компьютерных технологий, возрастает с каждым годом.

В столь широком распространении киберпреступлений некоторые специалисты склонны винить пользователей, не всегда соблюдающих обыкновенные правила компьютерной безопасности. В современном мире утечка конфиденциальной информации может повлечь серьезные последствия, но при этом многие пользователи используют для хранения файлов и совместной работы над ними средства, которые не всегда защищены достаточно надежно.

К сожалению, большинство пользователей персональных компьютеров и Интернета сами позволяют похищать/использовать свои личные данные злоумышленникам или просто подкованным в техническом плане третьим лицам. И ущерб от таких противоправных действий колеблется от незначительного до катастрофического.

**Цель:** Изучить вопрос обеспечения информационной безопасности. Определить основные методы и средства информационной безопасности.

**Задачи:** 1. Познакомиться с литературой и интернет - источниками на данную тему;

2. Отработать и выстроить нужный материал, провести его анализ;

3. Выяснить, существенна ли проблема информационной безопасности, проведя анкетирование и проанализировав его результаты;

4. Разработать рекомендации по безопасной работе с компьютером;

5. Обобщить материал и оформить результаты.

**План по реализации проекта**

|  |  |  |  |
| --- | --- | --- | --- |
| **п/п** | **Мероприятия** | **Дата** | **Исполнители** |
| **I. Подготовительный этап** | | | |
| 1. | Изучение литературы | май 2021 | Новицкий Г.С. |
| 2. | Создание команды | май 2021 | Новицкий Г.С. |
| 3. | Составление плана работы | июнь 2021 | Новицкий Г.С. |
| **II. Реализация проекта** | | | |
| 1. | Изучение статистики преступлений в сфере информационно-телекоммуникационных технологий за 2020-2021 годы | октябрь 2021 | Новицкий Г.С. |
| 2. | Классификация киберпреступлений | октябрь 2021 | Новицкий Г.С. |
| 3. | Исследование знания основных правил информационной безопасности | ноябрь 2021 | Новицкий Г.С. |
| 4. | Разработка рекомендаций по безопасной работе с компьютером | ноябрь 2021 | Новицкий Г.С. |
| **III. Заключительный этап** | | | |
| 1. | Защита проекта | декабрь 2021 | Новицкий Г.С. |

**I. Подготовительный этап**

1.Изучение литературы

2. Создание команды

Директор проекта: Намаконова Е.А.

Автор проекта: Новицкий Г.С.

Координатор проекта: Гражданцев А.В.

Волонтеры: учащиеся 11-х классов МАОУ «Гимназия № 25 г. Благовещенска»

3. Составление плана работы

**II. Реализация проекта**

**1. ИЗУЧЕНИЕ СТАТИСТИКИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ЗА 2018-2019 ГОД**

Согласно статистике о состоянии преступности, приведенной Генпрокуратурой более 461 тыс. киберпреступлений зафиксировано в России за 11 месяцев 2020 года, на них приходится почти четверть всех преступлений, совершенных в стране.

Вместе с тем в Генпрокуратуре сообщили, что темпы роста количества киберпреступлений в сравнении с итогами первого полугодия 2020 года замедлились с 91,7% до 76,6%.

В этом году более 70% всех мошенничеств совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Всего их зафиксировано свыше 215 тыс., что на 76,1% больше, чем годом ранее. "При совершении 25,5 тыс. мошенничеств использовались электронные средства платежа. Заметное увеличение [числа] таких деяний зафиксировано в большинстве регионов", - сообщили в Генпрокуратуре.

В целом, как и прежде, на состояние преступности в значительной мере влияют деяния против собственности, на которые приходится более половины всех выявленных уголовно наказуемых деяний. Среди них наибольшие темпы прироста (на 30%) отмечаются у различного рода мошенничеств. В результате в структуре преступности их доля увеличилась с 12,6% до 16,2%.

Последние шесть лет киберпреступность, согласно статистике, демонстрирует десятикратный рост (в 2013 году подобных преступлений было 11 тыс., в 2014 году - 44 тыс., в 2016 году - 66 тыс.). Ранее в Генпрокуратуре сообщали, что только с 2015 по 2016 год в шесть раз выросло число мошенничеств (с 2,2 тыс. до 13,4 тыс.) и более чем в три раза - краж (с 2,3 тыс. до 8,5 тыс.) с использованием интернета и иных коммуникационных ресурсов, в 5,5 раза (с 995 до 5,5 тыс.) выросло количество преступлений, связанных с хищением, удалением, блокировкой компьютерной информации с целью мошенничества (ст. 159.6 УК РФ).

1.1 *К крупным киберпреступлениям, произошедшим в 2018-19 годах в России и мире относятся:*

1. Утечка персональных данных сотрудников РЖД:

Основатель и технический директор компании DeviceLock, специализирующейся на предотвращении утечек данных с корпоративных компьютеров, Ашот Оганесян во вторник, 27 августа, сообщил в своем Telegram-канале «Утечки информации» и блоге на сайте Habr.com, что неизвестные выложили в свободный доступ персональные данные 703 тыс. человек. При этом злоумышленники добавили к публикации примечание: «Спасибо ОАО «РЖД» за предоставленную информацию путем бережного обращения с персональными данными своих сотрудников».

Данные работников РЖД были опубликованы на сайте «Инфач» под заголовком «Рабы РЖД». Около 14:00 мск администратор сайта закрыл к нему доступ — при попытке зайти на сайт выдается ошибка 403, «доступ запрещен». Домен infach.me был зарегистрирован в феврале 2018 года, он позволял пользователям анонимно публиковать персональные данные других людей. Среди данных сотрудников РЖД, опубликованных на сайте, были их имена, номера телефонов, должности, фотографии в форме и снимки СНИЛС.

«Откуда произошла утечка — неизвестно, но есть предположение, что это база данных службы безопасности. Судя по формату фотографий, это снимки на пропуска», — отметил Оганесян в своем блоге. Он предполагает, что даже блокировка сайта уже не поможет предотвратить дальнейшее распространение оказавшихся в открытом доступе сведений.

2. Утечка персональных данных клиентов Сбербанка:

Персональные данные клиентов Сбербанка оказались на черном рынке. Продавцы уверяют, что владеют данными о 60 млн кредитных карт, как действующих, так и закрытых (у банка сейчас около 18 млн активных карт). Утечка могла произойти в конце августа. Эксперты, ознакомившиеся с данными, считают их подлинными и называют утечку самой крупной в российском банковском секторе.

3. Утечка паспортных данных жителей Индии:

В январе 2018 года группа неизвестных в WhatsApp начала рассылать индийским пользователям сообщения, в которых за 500 рупий предлагалось получить доступ к базе данных Aadhaar. Так называется индийский электронный паспорт — что-то вроде нашей УЭК. IT-компания, обслуживающая базу, организовала брешь в защите базы данных, в результате чего паспортные данные более чем 1,1 млрд. жителей страны стали доступны любому желающему. А надо сказать, что номер электронного ID — это дверь ко всей информации о человеке, включая личные и финансовые данные. Так что под угрозой оказалось практически 98% населения Индии.

## 4. Криптомайнинг через порталы госуслуг:

В феврале 2018 года исследователи Иэн Торнтон-Трамп (Ian Thornton-Trump) и Скотт Хельме (Scott Helme) забили тревогу: официальный сайт правительства Великобритании оказался заражен криптомайнером — вирусом, который «крадет» ресурсы процессоров посетителей сайта, чтобы «майнить» криптовалюту. Дело в том, что по всем правилам европейской толерантности и инклюзивности, сайт был снабжен плагином Browsealoud, который зачитывает его контент для слабовидящих. Вот в этом плагине и оказался вирус.

Безопасники всех стран бросились проверять: оказалось, что зараженный плагин стоит на более чем 4 000 сайтов государственных услуг — не только в Великобритании, но и в Австралии и США. Сколько злоумышленникам удалось «намайнить» на обычных гражданах, пришедших за госуслугами — неизвестно.

1.2 *Крупнейшие кибератаки за всю историю Всемирной Паутины:*

1. Вирус Stuxnet:

В конце сентября 2010г. стало известно, что вирус Stuxnet нанес серьезный урон иранской ядерной программе. Используя уязвимости операционной системы и пресловутый «человеческий фактор», Stuxnet успешно поразил 1368 из 5000 центрифуг на заводе по обогащению урана в Натанзе, а также сорвал сроки запуска ядерной АЭС в Бушере. Заказчик – неизвестен. Исполнитель – нерадивый сотрудник Siemens, вставивший инфицированный флэш-накопитель в рабочую станцию. Ущерб, нанесенный ядерным объектам Ирана, сопоставим с ущербом от атаки израильских ВВС.

Создание подобного проекта требует огромных интеллектуальных и финансовых инвестиций, а значит, под силу лишь структурам масштаба государственных. Все эксперты сходятся во мнении, что вирус не является плодом усилий «группы энтузиастов». Лоран Эсло, руководитель отдела систем безопасности Symantec предполагает, что над созданием Stuxnet работали, как минимум, от шести до десяти человек на протяжении шести-девяти месяцев. Франк Ригер (Frank Rieger), технический директор GSMK поддерживает своего коллегу — по его словам, вирус создавала команда из десяти опытных программистов, а разработка заняла около полугода. Ригер называет и ориентировочную сумму создания Stuxnet: она составляет не менее $3 млн.

2. Вирус WannaCry:

Другое крупное происшествие, связанное с киберпреступлениями, связано с уязвимостью операционной системы.

В 2017 году 12 мая по всему миру прокатилась волна заражения компьютеров вирусом-шифровальщиком WannaCry. Жертвами вируса стали около полумиллиона компьютеров. Вирус распространился с такой скоростью из-за уязвимости в операционной системе Windows — с её помощью можно было получить удалённый доступ к компьютеру и установить на него программу-шифровальщик.

После проникновения в систему шифровальщик начинает распространяться по локальной сети на другие компьютеры, используя те же алгоритмы, которые применяют компьютерные черви. Именно поэтому больше всего от вируса пострадали крупные корпорации — зловред, попав в локальную сеть, быстро распространился на остальные компьютеры.

Внутри системы WannaCry начинает шифровать данные. В первую очередь, конечно же, вирус интересуют документы, фотографии, фильмы, архивы, видео и другие форматы файлов, которые скорее всего содержат важную информацию. После завершения шифрования пользователь получает сообщение о том, что для получения кода дешифровки необходимо заплатить выкуп. Стоимость выкупа варьировалась от $300 до $600, при это кибермошенники не давали никакой гарантии того, что за эти деньги пострадавшие действительно получат код дешифровки.

Распространение вируса удалось остановить достаточно простым и неожиданным способом: с помощью регистрации домена, к которому некоторые версии вируса обращались за разрешением на запуск процесса шифрования данных. Позже ещё несколько похожих вирусов атаковали компьютеры по всему миру, но наибольший ущерб нанёс всё же WannaCry.

**2. КЛАССИФИКАЦИЯ КИБЕРПРЕСТУПЛЕНИЙ**

Прежде, чем приступить к рассмотрению вопросов непосредственно организации IT-безопасности, пожалуй, есть смысл разобраться, что же это такое — киберугрозы, какие они бывают, какую опасность несут, как и с помощью чего можно им наиболее эффективно противодействовать. Это, во-первых, даст понимание — защита от каких именно рисков наиболее важна в данной конкретной компании, и, во-вторых, позволит определиться с тем, какие средства для этого потребуются. Дело в том, что защита, что называется, по максимуму, это вещь, конечно, хорошая, но всегда ли она требуется? В каких-то случаях достаточно установки самых обычных антивирусов на пару-тройку имеющихся в наличии компьютеров, а где-то нельзя использовать даже Windows в качестве операционной системы, а то и необходимы специальные меры по дополнительному электромагнитному экранированию системных блоков и мониторов для снижения вероятности дистанционного считывания конфиденциальной информации.

Киберугрозы сегодня принято подразделять на внешние, источники и причины которых находятся вне ваших компьютеров и вашей компании, обычно — в глобальной сети, и внутренние, зависящие, в первую очередь, не от каких-то абстрактных злоумышленников из интернета, а от вашего собственного персонала, оборудования и программного обеспечения.

*2.1 Внешние угрозы*

1. Вирусы

К внешним киберугрозам относятся всевозможные компьютерные вирусы, так называемые «черви», троянские программы и тому подобное вредоносное программное обеспечение, скрытно проникающее в компьютерные системы. Именно вирусы на сегодня являются главной угрозой — с ними сталкиваются более 70% российских компаний, поскольку «подцепить» их в отсутствие эффективной защиты проще простого. Для того чтобы они проникли на ваш компьютер, может оказаться достаточным, например, открыть вложение в электронном письме (причём совсем не обязательно, чтобы это письмо было от неизвестного адресата — вирус вам может прислать и хорошо известный партнёр, если его ПК оказался заражён раньше вашего). Некоторым вредоносным программам достаточно уже одного того, что ваш ПК просто подключен к той же локальной сети, что и уже заражённый ПК! Огромное число подобного ПО используют для своего распространения «флешки», оптические носители и мобильные жёсткие диски. Словом, способов, которыми вирусы могут проникнуть в вашу сеть и на ваши ПК — великое множество. Вредоносы уничтожают файлы, нарушают работоспособность программ и компьютеров, используют в своих целях каналы связи, пожирая трафик, рассылают спам и так далее. Самая же опасная категория программного обеспечения подобного рода, появившаяся буквально совсем недавно — кибероружие, направленное, порой, на уничтожение целой промышленной инфраструктуры. Создание таких программ, как нашумевшие Stuxnet, Duqu, Flame, Gauss, обошлось, возможно, во многие миллионы долларов. И это уже не поделки студентов-недоучек, за ними стоят весьма серьёзные профессионалы и организации — известно, что «хакеры на госслужбе» уже работают в кибервойсках США, Израиля, Китая, Германии. Первые образцы кибероружия были направлены против далёкого от нас Ирана и его ядерных центрифуг, но кто знает, что будет дальше?..

2. Спам

Второй по важности тип внешних киберугроз — уже много лет вызывающий всеобщее раздражение спам. Доля спама среди всей электронной корреспонденции сегодня может достигать 70%! Мусорная электронная почта, призывающая вас купить таблетки от похудения или записаться на курсы английского языка, расходует интернет-трафик, забивает каналы связи, отвлекает от работы, вынуждая персонал выявлять среди гор рекламы действительно важную корреспонденцию, которую при таком положении дел несложно и потерять (особенно если используются некачественные бесплатные спам-фильтры с большим процентом ложных срабатываний). Всё это в конечном итоге ведёт к финансовым потерям. Кроме того, спам — это ещё один из распространённых каналов внедрения вирусных и троянских программ.

3. Удалённый взлом

Крайне опасен удалённый взлом компьютеров, благодаря которому злоумышленник, находящийся, возможно, на другом конце земли, а может — в офисе конкурента, получает возможность читать и редактировать хранящиеся на ваших ПК и файл-серверах документы, уничтожать их по своему желанию, внедрять в вашу сеть какие-то свои программы, следящие за вашими действиями или собирающие какую-то иную информацию.

4. Фишинг

Чрезвычайно опасны так называемые фишинговые атаки, при которых пользователь ПК «попадается на крючок» поддельного веб-сайта, полностью имитирующего, скажем, сайт банка, в котором он держит свой депозит. В этом случае злоумышленники, получив все его реквизиты и пароли, могут запросто лишить бедолагу всех его накоплений. Забрасывается же такой «крючок» обычно с помощью всё того же спама, уязвимостей в веб-браузере, а иногда — и таргетированных атак, при которых письма со ссылками на поддельный банк не просто рассылаются «кому бог пошлёт», а отправляются конкретным людям, конкретным организациям, причём с осмысленным текстом, адресованным именно им и не вызывающим, на первый взгляд, никаких особенных подозрений.

5. DoS/DDoS-атаки

Организациям, имеющим свои интернет-сайты и другие типы видимых из интернета серверов, представляют нешуточную угрозу DoS/DDoS-атаки, то есть специальным образом организованные массированные сетевые запросы, полностью или частично нарушающие работоспособность веб-сайта, почтового сервера или, скажем, интернет-магазина. Порой, чтобы избавиться от конкурента, достаточно, чтобы до его интернет-магазина всего лишь несколько дней не могли «достучаться» потенциальные покупатели.

6. Хищение мобильных устройств

В последнее время всё актуальнее становится защита и от такого типа внешних угроз, как хищение мобильных устройств, в памяти которых может в открытом виде храниться важнейшая корпоративная информация — финансовая документация, персональные данные сотрудников и клиентов, интеллектуальная собственность, электронная переписка, различные идентификационные данные и пароли.

7. Другие внешние угрозы

Этим список внешних угроз, к сожалению, не исчерпывается, и если выйти за рамки угроз, защита от которых производится, главным образом, на уровне соответствующего программного обеспечения, то можно вспомнить, например, о промышленном шпионаже, краже аппаратного обеспечения других типов или преднамеренном причинении ущерба, но об этом, возможно, как-нибудь в другой раз.

*2.2 Внутренние угрозы*

1. Уязвимости ПО

Из внутренних же угроз наибольшую опасность сегодня представляют уязвимости в программном обеспечении. Программы пишут люди, а людям, как это ни банально звучит, свойственно ошибаться. Ошибки и недоработки в популярных программах, которые впоследствии выявляются наиболее опытными хакерами, и ложатся в основу многих и многих «вредоносов» — вирусов, червей, троянских программ, проникающих на ПК пользователей через эти лазейки. Причём поиск лазеек ведётся практически целенаправленно, с акцентом на ПО, установленное и работающее почти без перерыва на подавляющем большинстве компьютеров. Некоторые такие программы устанавливаются одновременно с операционной системой (в Windows это Media Player, Internet Explorer), без других почти невозможно обойтись ни в одном офисе (например, привычный Microsoft Office, Adobe Reader), что-то приходится устанавливать для полноценной работы в интернете (Java-плагин для веб-браузеров, а также альтернативные браузеры, такие как Opera, Firefox). И, разумеется, не лишена уязвимостей и сама операционная система — Windows, Linux, FreeBSD, iOS — никто не застрахован от ошибок. В результате, чем больше программ используется в вашем офисе, тем выше вероятность того, что через какую-то из них в вашу систему проникнет вирус. Если же используемое ПО и сама ОС обновляется нерегулярно, от случая к случаю, то вероятность поражения системы возрастает просто катастрофически. Всё-таки надо отдать должное ведущим разработчикам программного обеспечения — выявленные ошибки в своих программах они стремятся исправлять как можно оперативнее. Однако, чтобы своевременно устанавливать все эти обновления на весь парк имеющихся компьютеров, требуются некоторые усилия и со стороны IT-персонала. Каждый лишний день с незакрытой «дырой» в системе — неоправданный риск. Разумеется, использование бесплатных программ (поддержка которых со стороны производителя, как правило, почти на нулевом уровне), а тем более нелицензионного ПО также сыграет в этом вопросе только против вас.

2. Утечки данных

Плакат советских времен «Болтун — находка для шпиона», к сожалению, всё ещё не утратил своего значения. Случайная утечка/распространение конфиденциальных данных стоит на втором месте по опасности. Тем более, что современные средства связи этому всячески способствуют. ICQ, Skype, «ВКонтакте», «Одноклассники», просто электронная почта: всё это — каналы утечки информации, которая может стоить очень дорого. Плюс телефоны, планшеты, ноутбуки, «флешки» и мобильные жёсткие диски, которые регулярно теряются и крадутся даже у сотрудников спецслужб, о чем нас периодически извещают новостные ленты. К тому же утечка конфиденциальных данных может быть и не совсем случайной, а вовсе даже преднамеренной, с соответствующими мероприятиями по сокрытию самого факта утечки.

**3. ИССЛЕДОВАНИЕ НА ТЕМУ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

*3.1 Проведение анкетирования*

В проведении анкетирования приняли участники 11 классов МАОУ «Гимназия № 25 г. Благовещенска.

**Анкета содержала следующие вопросы:**

1. Знаком ли ты с понятием информационная безопасность?

а) Да

б) Нет

2. Как ты считаешь, если опасность в Интернете?

а) Да

б) Нет

в) Может быть

г) Не знаю

3. Делишься ли ты в интернете информацией о своей семье, школе, адресе, телефоне?

а) Да

б) Нет

4. Часто ли ты получаешь подозрительные письма на электронную почту?

а) Да

б) Нет

5. Ты пользуешься антивирусной программой?

а) Да

б) Нет

в) Не знаю

6. Как часто ты выполняешь резервное копирование?

а) Раз в неделю

б) Раз в месяц

в) Никогда

г) Что это?

7. При регистрации в социальных сетях ты пользуешься настоящим или вымышленным именем; называешь личные данные?

а) Да, подлинные данные

б) Нет, имя и данные вымышленные

в) Когда как

8. Делишься ли ты в Интернете с малознакомыми людьми информацией? (возможны несколько вариантов ответов)

а) О своей семье

б) О своей школе

в) О своем адресе и телефоне

г) Нет, не делюсь

9.Что ты делаешь, когда приходит предложение зарегистрироваться в «друзьях» от незнакомых людей?

а) Удаляю информацию

б) Добавляю в «друзья»

в) Пытаюсь сначала что-либо узнать о них

г) Другое

10. Как ты реагируешь на получение спамов, рекламных роликов, различных сообщений, содержащих неприятную информацию, оскорбления, запугивания и др.; приглашений на участие в лотереях, конкурсах, азартных играх?

а) Сразу удаляю

б) Пытаюсь найти для себя что-то интересное

в) Мне это неинтересно

г) Меня это раздражает

11. Знаком ли ты с правилами безопасного поведения в Интернете?

а) Да, знакомили в школе

б) Да, рассказали родители

в) Да, прочитал(а) на специальных сайтах в Интернете

г) Нет никаких правил, Интернет - это свободное пространство, в котором можно все

*3.2 Анализ анкетных данных*

Для анализа анкетных данных была разработана специальная бальная система, в которой положительные ответы оценивались высшим балом и далее уменьшались. Результаты анкетирования показывают, что 40% опрошенных имеют достаточно знаний для безопасного пользования компьютером. Однако 60% опрошенных эти правила знакомы плохо или не знакомы совсем. Эта статистика подтверждает актуальность проблематики проекта на сегодняшний день и выявляет необходимость пропаганды главных правил пользования электронными устройствами с доступом к Интернету. Составление памятки, содержащей эти правила и станет следующим этапом моей работы.

Рис. 1. Результаты анкетирования

**4. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО БЕЗОПАСНОМУ ПОЛЬЗОВАНИЮ КОМПЬЮТЕРОМ;**

**Главные правила пользования компьютером:**

* Никому не передавайте конфиденциальные данные для входа в приложения или на сайты (логин, пароль), в том числе родственникам, коллегам. Если у вас есть подозрение, что ваши логин и пароль украдены, как можно быстрее смените их. Сейчас большая часть Интернет-ресурсов предоставляет возможность смены входных данных.
* Используйте сложные пароли, состоящие из букв, цифр и специальных символов, которые вы сможете запомнить, не записывая.
* Для работы в системе используйте защищенный паролем персональный компьютер. Вход в систему с чужого компьютера, а также с компьютеров в интернет-кафе не является безопасным.
* Регулярно меняйте пароли
* На компьютере должно быть установлено лицензионное антивирусное программное обеспечение. Установленное антивирусное программное обеспечение, и антивирусные базы данных должны регулярно обновляться. Кроме того, на этот компьютер необходимо регулярно устанавливать обновления безопасности
* Соединение установлено в безопасном режиме, т.е. адресная строка в браузере начинается с https:// (а не http://). В этом случае в адресной строке вашего веб-браузера должен быть изображен значок закрытого замка (справа или слева, в зависимости от браузера)
* Не используйте функцию автозаполнения в установках вашего браузера. Это поможет не сохранять данные (пароль пользователя, имя пользователя и др.) в памяти браузера, что, в свою очередь, предотвратит использование данных сторонними лицами.
* Включите систему фильтрации ложных web-узлов (антифишинг) в своем браузере; если браузер ее не имеет — обновите браузер.
* Не открывайте электронные почтовые сообщения и сообщения систем мгновенного обмена сообщениями (например, ICQ), поступающие от неизвестных отправителей, не открывайте файлы, вложенные в эти сообщения, сразу же удаляйте эти сообщения.
* Регулярно делайте резервное копирование важных данных на внешний носитель.

**5. ЗАКЛЮЧЕНИЕ**

В ходе своего исследования мне удалось глубоко изучить вопрос обеспечения информационной безопасности и лишний раз убедиться в актуальности проблемы проекта на сегодняшний день. Так же при работе над проектом я выяснил, что достаточное количество подростков плохо знакомы с правилами пользования компьютером. Мною были подробно изучены статистические данные по кибератакам за все время существования Всемирной Паутины, определены основные рекомендации по пользованию Интернетом и компьютером в целом.

В ходе работы была составлена специальная памятка основных правил безопасного пользования компьютером, что стало заключительным этапом моей работы.

**СПИСОК ЛИТЕРАТУРЫ**

1) http://www.kaspersky.ru – антивирус «Лаборатория Касперского»;

2) http://www.onlandia.org - безопасная web-зона;

3) http://www.interneshka.net – международный онлайн-конкурс по

безопасному использованию Интернета;

4) http://www.saferinternet.ru – портал Российского Оргкомитета по

безопасному использованию Интернета;

5) http://content-filtering.ru – Интернет СМИ «Ваш личный Интернет»;

6) http://www.rgdb.ru – Российская государственная детская библиотека.

7) Башлы П.Н., Бабаш А.В., Баранова Е. - Информационная безопасность. Учебное пособие (2015)

8) Камский В.А. - Защита личной информации в интернете, смартфоне и компьютере-Наука, и Техника (2017)

9) Масалков А.С. - Особенности киберпреступлений. Инструменты нападения и защита информации. (2018)

10) Халявин В. - Бесплатная защита компьютера от хакеров, вирусов и «блондинов»-Мартин (2014)

11) Шаньгин В.Ф. - Информационная безопасность-Издательство \_ДМК Пресс\_ (2014)