**ОГЛАВЛЕНИЕ**

ВВЕДЕНИЕ……………………………………………………………………..3

ГЛАВА 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ………………….......5

1.1. Понятие «информационная безопасность»……………………..……..…5

1.2. Составляющие информационной безопасности…………………...…….7

1.3. Нормативно - правовые основы информационной безопасности в Российской Федерации………………………………………………………...9

1.4. Ответственность за нарушения в сфере информационной безопасности…………………………………………………………………..11

ГЛАВА 2. КИБЕРАТАКА И СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ…………………………..…….14

2.1. Понятие «кибератака»…………………………………..……..………....14

2.2. Типы кибератак ………………………………………………………….15

2.3. Данные об ущербе от кибератак ………………………………………..20

2.4. Компьютерные вирусы ………………………………………………….21

2.5. Типы вирусов……………………………………………………………..25

2.6. Признаки заражения…………………………………………………...…31

2.7. Современные методы и средства информационной безопасности…...32

2.8. Виды антивирусных программ…………………………………….…....34

ГЛАВА 3. ПРАКТИЧЕСКАЯ ЧАСТЬ………………………………….…....38

3.1. Анализ результатов олимпиады «Безопасный интернет»……………..38

ЗАКЛЮЧЕНИЕ……………………………………………………………….41

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ И ИСТОЧНИКОВ….....43

ПРИЛОЖЕНИЕ……………………………………………………………….45

**ВВЕДЕНИЕ**

Информационная безопасность является одной из проблем, с которой столкнулось современное общество и обусловлена она возрастающей ролью информации в общественной жизни.

Широкое распространение вычислительной техники как средства обработки информации привело к информатизации общества и появлению принципиально новых, так называемых, информационных технологий.

Информационные технологии - процессы, использующие совокупность средств и методов сбора, обработки, накопления и передачи данных для получения информации нового качества о состоянии объекта, процесса, явления, информационного продукта, а также распространения информации и способы осуществления таких процессов и методов. Появление любых новых технологий, как правило, имеет как положительные, так и отрицательные стороны.

Информационные технологии, также не являются исключением из этого правила, и поэтому следует заранее позаботиться о безопасности при разработке и использовании таких технологий.

Безопасность использования интернета, информационных и коммуникационных технологий одна из актуальнейших и важнейших тем современности.

Всё чаще поднимается проблема вопроса киберпреступности.

На сегодняшний день она достигла высокого уровня и продолжает развиваться. Это подтверждает статистика. Средний ущерб, нанесенный крупным компаниям РФ хакерами за период с июля 2022 года по июнь 2023 года, составил не менее 20 миллионов рублей, не учитывая репутационные потери.

Все чаще психологи констатируют негативные последствия взаимодействия людей с интернетом: отсутствие контроля над источниками информации, открытый доступ к личным данным, интернет - зависимость и прочее. Особенно страдают от этих последствий дети и подростки, которые очень активно осваивают просторы всемирной паутины.

**Объект исследования:** методы и средства информационной безопасности в сети Интернет.

**Предмет исследования:** информационная безопасность в сети Интернет.

**Цель:** на основании теоретического анализа и интерпретации данных изучить возможности использования методов и средств информационной безопасности в сети Интернет.

**Задачи:**

1. Проанализировать литературу и интернет - источники на данную тему.

2. Изучить методы и средства информационной безопасности в сети Интернет.

3. Разработать памятку по информационной безопасности в сети Интернет.

4. Обобщить материалы и оформить результаты.

В основу проекта положена **гипотеза** о том, что использование разнообразных методов и средств повышения уровня информационной культуры будет способствовать формированию информационной безопасности в сети Интернет.

**Методы исследования:**

* теоретический анализ литературы по данной теме;
* анализ результатов полученных в ходе участия обучающихся 8 - ых классов в олимпиаде «Безопасный интернет»;
* обобщение полученных результатов.

По структуре работа состоит из введения, трех глав, списка литературы и приложения.

Сроки проведения проекта: сентябрь 2023 г. - январь 2024 г.

**ГЛАВА 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

* 1. **Понятие «информационная безопасность»**

С понятием «информационная безопасность» связаны различные определения.

Так, в Законе РФ «Об участии в международном информационном обмене» информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Подобное же определение дается и в Доктрине информационной безопасности Российской Федерации, где указывается, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Оба эти определения рассматривают информационную безопасность в национальных масштабах и поэтому имеют очень широкое понятие [7, c. 136].

Наряду с этим характерно, что применительно к различным сферам деятельности, так или иначе связанным с информацией понятие «информационная безопасность» принимает более конкретные очертания.

Так, например, в «Концепции информационной безопасности сетей связи общего пользования Российской Федерации» даны такие определения этого понятия:

1. Информационная безопасность - это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

2. Информационная безопасность - свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя.

3. Информационная безопасность - это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации [16, c. 59].

Рассматривая информацию как товар можно сказать, что нанесение ущерба информации в целом приводит к материальным затратам.

Исходя из этого, отметим следующие важные выводы:

- задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;

- информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации - это принципиально более широкое понятие.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику, состоящую в том, что информационная безопасность есть составная часть информационных технологий - области, развивающейся беспрецедентно высокими темпами [4].

В области информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно - технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять [20].

Таким образом, можно сделать вывод о том, что информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни.

 Термин «информационная безопасность» и термин «компьютерная безопасность» тесно связаны и рассматриваются очень узко, поскольку компьютеры только одна из составляющих информационных систем.

* 1. **Составляющие информационной безопасности**

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

1. Обеспечением доступности информации.

2. Обеспечением целостности информации.

3. Обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности [6, c. 113].

Информационные системы создаются для получения определенных информационных услуг.

Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления - производством, транспортом и т. п.

Менее драматичные, но также весьма неприятные последствия - и материальные, и моральные - может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей, например, продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть Интернет и т. п. [5].

Доступность - это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени [2, c. 34].

Например, получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило.

Целостность информации условно подразделяется на статическую и динамическую.

Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации.

Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д.

Целостность - гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность - самый проработанный у нас в стране аспект информационной безопасности [12, c. 39].

К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями.

Во - первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках.

Во - вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы [12, c. 40].

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др.

Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Конфиденциальность - гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена [12, c. 42].

Можно сделать выводы о том, что нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом.

Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

* 1. **Нормативно - правовые основы информационной безопасности в Российской Федерации**

Правительство Российской Федерации придаёт высокий статус культуре информационной безопасности, утвердив Концепцию формирования и развития культуры информационной безопасности граждан Российской Федерации.

 Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

Работа по созданию нормативной базы предусматривает разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроль над исполнением указанных документов [16, c. 71].

Необходимо отметить, что такая работа в последнее время ведется практически непрерывно, поскольку сфера информационных технологий развивается стремительно, соответственно появляются новые формы информационных отношений, существование которых должно быть определено законодательно.

Законодательная база в сфере информационной безопасности включает пакет Федеральных законов, Указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов.

Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности [16, c. 83].

В Конституции РФ гарантируется «тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» (ст. 23, ч.2), а также «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (ст. 29, ч.4).

Кроме этого, Конституцией РФ «гарантируется свобода массовой информации» (ст. 29, ч.5), т. е. массовая информация должна быть доступна гражданам.

Концепция национальной безопасности РФ, введенная указом Президента РФ № 24 в январе 2000 г., определяет важнейшие задачи обеспечения информационной безопасности Российской Федерации:

- реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;

- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;

- противодействие угрозе развязывания противоборства в информационной сфере [21].

Таким образом, для обеспечения прав граждан в сфере информационных технологий и решения задач информационной безопасности, сформулированных в Концепции национальной безопасности РФ, разработаны и продолжают разрабатываться и совершенствоваться нормативные документы в сфере информационных технологий.

* 1. **Ответственность за нарушения в сфере информационной безопасности**

Немаловажная роль в системе правового регулирования информационных отношений отводится ответственности субъектов за нарушения в сфере информационной безопасности [8].

Основными документами в этом направлении являются:

1. Уголовный кодекс Российской Федерации.
2. Кодекс Российской Федерации об административных правонарушениях.

В Уголовном кодексе Российской Федерации, как наиболее сильнодействующем законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности, вопросам безопасности информации посвящены следующие главы и статьи:

1.Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

2.Статья 140. Отказ в предоставлении гражданину информации.

3.Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

4.Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей.

5.Статья 283. Разглашение государственной тайны.

6.Статья 284. Утрата документов, содержащих государственную тайну.

Особое внимание уделяется компьютерным преступлениям, ответственность за которые предусмотрена в специальной 28 главе кодекса «Преступления в сфере компьютерной информации» [21].

Глава 28 включает следующие статьи:

1. Статья 272. Неправомерный доступ к компьютерной информации.

Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или другого дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

2.Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ [21].

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, - наказывается лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

3. Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети [21].

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет [21].

**Глава 2. Кибератака и современные методы и средства информационной безопасности**

* 1. **Понятие «кибератака»**

Кибератаки стали неотъемлемой частью информационной реальности. Их число стремительно растёт, и если раньше мы слышали о десятках инцидентов в полугодие, то сегодня можно насчитать тысячи случаев всего за месяц.

Что же такое кибератака?

В источниках даются такие определения.

**Кибератака**  - это несанкционированное воздействие на информационную систему с целью повредить её, получить или ограничить к ней доступ, собрать конфиденциальные данные [21].

Кибератака  **-** это любой наступательный маневр, нацеленный на компьютерные информационные системы, компьютерные сети, инфраструктуры  или смартфоны [22].

В зависимости от контекста кибератаки могут быть частью кибервойны или кибертерроризма.

Кибератака может быть предпринята [суверенными государствами](https://en.wikipedia.org/wiki/Sovereign_state), отдельными лицами, группами, обществами или организациями и может исходить из анонимного источника.

Злоумышленник - это лицо или процесс, который пытается получить доступ к данным, функциям или другим ограниченным областям системы без авторизации, возможно, со злонамеренным умыслом [22].

Продукт, облегчающий кибератаку, иногда называют [кибероружием](https://en.wikipedia.org/wiki/Cyberweapon%22%20%5Co%20%22%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BE%D1%80%D1%83%D0%B6%D0%B8%D0%B5).

За последние несколько лет число кибератак увеличилось.

Сообщения о вирусах - шифровальщиках, атакующих компьютеры по всему миру, появляются на новостных лентах регулярно. И чем дальше, тем большие масштабы принимают кибератаки. Кибератаки становятся все более опасными и дорогостоящими в устранении [22].

* 1. **Типы кибератак**

Кибератаки могут классифицироваться по мотивам и целям, а могут - по типам воздействия. Рассмотрим оба варианта.

### Кибератаки по мотивам злоумышленников:

* финансовые мотивы, когда киберпреступники собираются украсть деньги или финансовую информацию, злоупотребить банковскими данными или провести мошеннические действия, например через фишинг или скимминг (технологии для обмана пользователя с целью получения его личных данных);
* политические или геополитические мотивы, когда кибергруппировки собирают разведывательную информацию о компании, которая по их мнению, не соответствует этическим представлениям;
* идеологические мотивы - хактивисты (активисты в сети) могут совершать кибератаки для поддержки своих убеждений или в целях привлечения внимания к определённым вопросам;
* коммерческие мотивы подразумевают взлом систем и сетей с целью кражи бизнес - секретов, клиентских данных или уклонения от налогов.

Кибератаки по типам воздействия:

* вирусы и черви (malware). Эти типы кибератак объединены общей целью - они могут передаваться между устройствами в качестве программ или скриптов и распространяются автономно и не всегда с участием человека;
* фишинг (phishing) включает в себя разные направления: атаки через электронную почту и фальшивые сайты. Их цель в том, чтобы обмануть пользователя и получить его личные данные, мимикрируя под реальный легальный ресурс;
* DDoS - атаки направлены на перегрузку серверов или сетей лишним трафиком, чтобы временно или полностью отключить доступ к сервисам;
* троянские программы (trojans). Эти вредоносные программы часто скрываются под видом полезного ПО, чтобы выполнить негативное действие после того, как пользователь установит его на компьютер;
* спуфинг (spoofing) - подделка идентификационных данных или адресов, чтобы обмануть пользователя и получить несанкционированный доступ к системе.

Кибератаки, использующие вредоносные программы, являются одними из наиболее распространённых и опасных.

Характерными типами атак на информационные системы являются:

1. Удаленное проникновение.

Тип информационных атак, которые позволяют реализовать удаленное управление компьютером пользователя информационных ресурсов системы по сети на базе удаленного доступа.

Примером такой программы является NetBus или BackOrifice.

1. Локальное проникновение.

 Атака, приводящая к получению несанкционированного доступа к узлу ИКСМ, на котором она запущена.

Примером такой программы является GetAdmin.

1. Удаленная - отказ в обслуживании.

Атаки, которые позволяют нарушить функционирование информационной системы по условиям реализации ее услуг или имеют возможность перезагрузки системы путем удаленного доступа.

Примером такой атаки является Teardrop или trin.

1. Локальная - отказ в обслуживании.

Атаки, позволяющие нарушить функционирование системы или перезагрузить систему, на которой они реализуются.

В качестве примера такой атаки, можно привести использование несанкционированных апплетов, которые загружают центральный процессор бесконечным циклом, что делает невозможным обработку запросов других приложений.

1. Сетевые сканеры.

Программы, которые анализируют топологию сети и обнаруживают сервисы, доступные для атаки.

Примером такой программы можно назвать систему nmap.

1. Сканеры уязвимостей.

Программы, осуществляющие поиск уязвимостей на узлах сети, могут быть использованы для реализации атак.

Примеры: система SATAN или Shadow Security Scanner.

1. Взломщики паролей.

Программы, которые подбирают пароли авторизованных пользователей информационных ресурсов системы и ее услуг.

Примером взломщика паролей может служить несанкционированное программное обеспечение: L0phtCrack для Windows или Crack для Unix.

1. Анализаторы протоколов.

Программы, которые «прослушивают» сетевой трафик.

С помощью этих программ можно автоматически найти такую информацию, как идентификаторы и пароли пользователей, информацию о кредитных картах и т.д. [13, c. 54]

Анализатором протоколов можно назвать программные продукты: Microsoft Network Monitor, NetXRay компании Network Associates или LanExplorer.

Приведём примеры:

1. WannaCry: глобальная атака в 2017 году, использующая вирус -вымогатель, который шифровал данные на компьютерах и требовал выкуп за их разблокировку.

2.Conficker: червь, который в 2008 году заразил миллионы компьютеров по всему миру. Отключая разные службы на компьютере, блокируя доступ к сайтам антивирусов, он запускал саморассылку на другие устройства.

3.NotPetya: вирус - вымогатель, который в 2017 году парализовал множество компьютерных систем и оказал серьёзный экономический ущерб.

4.Фишинг - это тип кибератаки, когда ресурсы злоумышленника пытаются выдать себя за доверенный источник, чтобы обмануть пользователей и получить доступ к личным данным или финансовой информации.

5. Почтовый фишинг - это отправка поддельных электронных писем, в которых авторы письма выдают себя за банковских работников или представителей налоговых организаций. Жертвы переходят по подставным ссылкам на фальшивый сайт и вводят личные данные, например номер банковской карты или ФИО.

Кибератаки с помощью фишинга обычно имеют финансовые мотивы, и их целью может быть кража банковских паролей, номеров карт или личных данных.

6. Ботнет - это сеть из устройств, которая заражена вредоносными программами и управляется удалённо. Сами эти устройства называются ботами и используются для выполнения различных задач: массовых атак, кибершпионажа и генерации спама.

Вот несколько примеров таких атак:

* Zeus Botnet - ботнет, заражающий компьютеры троянским скриптом Zeus для кражи финансовых данных.
* Mirai Botnet - ботнет, который нацелен на носимые устройства, например электронные часы или тонометры, и используется для организации масштабных DDoS - атак.
* Gameover Zeus - ботнет, который использовался для распространения вирусов - вымогателей, таких как Cryptolocker.

7. Брутфорс - атаки - это кибератаки, при которых злоумышленники пытаются взломать учётные записи или защищённые системы через методичный перебор паролей. С этой целью могут использоваться различные комбинации символов, слов и сервисов, которые позволяют подобрать верный пароль к учётным данным пользователя.

Приведём частые примеры таких атак:

* SSH-Brute-Force - получение доступа к удалённым серверам или устройствам через подбор паролей SSH. Атакующие могут использовать программы или сценарии для многократных попыток входа в учётные записи на сайтах или в приложениях, перебирая пароли.
* RDP-Brute-Force - взлом учётных записей RDP (Remote Desktop Protocol) для удалённого доступа к компьютерам.

Брутфорс - атаки могут использовать, чтобы получить доступ к системам, украсть данные или запустить другие кибератаки. Чтобы защититься от таких атак, нужно использовать сложные пароли и устанавливать системы ограничения доступа.

8.Man-in-the-Middle - это вид кибератаки, при которой злоумышленник пытается проникнуть между двумя устройствами или пользователями, подменяя данные и перехватывая конфиденциальную информацию, не будучи замеченным ни одной из сторон.

Приведём частые примеры таких атак:

* Wi - Fi MITM - создание фальшивой точки доступа Wi-Fi или перехват сигнала в открытых сетях Wi-Fi, чтобы подслушивать или модифицировать сетевой трафик пользователей.
* SSLStrip - удаление защищённого соединения SSL между пользователем и сайтом, что позволяет злоумышленнику читать и модифицировать передаваемые данные.
* ARP - spoofing - отправка фальшивых ARP-запросов, чтобы перенаправить сетевой трафик через свой компьютер и перехватывать данные.

Кибератаки с использованием вредоносных программ могут иметь разные цели, включая вымогательство выкупа, кражу конфиденциальных данных, разрушение систем и даже шпионаж.

Защита от таких атак требует актуальных антивирусных программ, регулярных обновлений и бережного обращения с прикреплёнными файлами и ссылками в электронной почте. Подобные атаки становятся всё более «безфайловыми», что усложняет их выявление традиционными методами, вроде антивирусных программ, которые анализируют вложения вредоносных файлов [11, c. 342].

### Данные об ущербе от кибератак

Кибербезопасность — это защита подключенных к Интернету систем, таких как оборудование, программное обеспечение и данные, от киберугроз. Эта практика используется отдельными лицами и предприятиями для предотвращения несанкционированного доступа к центрам обработки данных и другим компьютеризированным системам.

Целью внедрения кибербезопасности является обеспечение надежной защиты компьютеров, серверов, сетей, мобильных устройств и информации, хранящихся на этих устройствах, от злоумышленников.

Кибератаки могут быть предназначены для доступа, удаления или вымогательства конфиденциальных сведений организации или пользователя, делая кибербезопасность очень важной. Медицинские, государственные, корпоративные и финансовые организации могут хранить жизненно важную личную информацию, например, о человеке.

Кибербезопасность - это постоянно меняющаяся область, с развитием технологий, которые открывают новые возможности для кибератак. Кроме того, несмотря на то, что о серьезных нарушениях безопасности часто сообщается, небольшим организациям все равно приходится беспокоиться о нарушениях безопасности, поскольку они часто могут быть целью вирусов и фишинга [11, c. 347].

Согласно результатам исследования, каждую секунду 18 пользователей становятся жертвами киберпреступности, ежедневно это более полутора миллионов жертв киберпреступности в мире.

Средний ущерб от кибератаки на одного среднестатистического пользователя составляет 18100 руб.

За 2022 год примерно 556 миллионов пользователей во всем мире пострадали от киберпреступности [20].

Таким образом, можно сделать вывод, что проблема компьютерной грамотности и информационной безопасности в сети Интернет является довольно актуальной. Ведь большинство пользователей не прибегают к мерам предостороженности пока их устройства не начнут тормозить или сломаются. А общий ущерб от киберпреступности велик и продолжает расти по сегодняшний день.

Проблема защиты ресурсов информационно - коммуникационных систем, становится еще более актуальной в связи с развитием и распространением глобальных вычислительных сетей, территориально распределенных информационных комплексов и систем с удаленным управлением доступом к информационным ресурсам.

Таким образом, несмотря на разработку специальных программно - аппаратных средств защиты от воздействия угроз информационным ресурсам автоматизированных систем, количество новых методов реализации атак постоянно растет.

## Компьютерные вирусы

Компьютерные вирусы опасны неожиданным появлением и непредсказуемыми последствиями. Они уже всесторонне исследованы и изучены, но, несмотря на предпринимаемые усилия, полностью обезопасить программы и компьютеры от внедрения вирусов не удается.

Компьютерный вирус - специально созданная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии, внедрять их в файлы с целью нарушения работы других программ, порчи файлов и каталогов.

Компьютерный вирус - самовоспроизводящаяся программа, наносящая ущерб аппаратно - программному обеспечению компьютера, которая может внедрять свои клоны в файл, загрузочный сектор диска, драйверы устройств, сеть, оперативную память, прикладные программы и т.д.

Компьютерный вирус поражает данные, уменьшает объем свободного дискового пространства, блокирует работу системы, несанкционированно перезагружает компьютер и многое другое [1, c. 103].

К настоящему времени специалистами зарегистрировано свыше 25 тысяч разновидностей вирусных программ, и ежедневно появляются 6 - 8 новых.

Возникновение компьютерных вирусов связано с идеей создания

самовоспроизводящихся программ, которые исследовались еще в 1951 г. американским ученым Д. фон Нейманом.

Первые эксперименты в этом направлении проводились в 1962 г. при создании компьютерной игры Darwin.

В 1970 году была создана саморазмножающаяся программа Creeper для одной из первых компьютерных сетей ARPANET. Для борьбы с ней была создана программа Reaper.

Одновременно с появлением в 1977 г. первых персональных компьютеров Apple II и началом их массовой продажи появились и компьютерные вирусы.

В конце 1970 - х гг. стали бурно развиваться сети на базе коммутируемых телефонных линий.

С появлением BBS получил распространение новый вид компьютерного хулиганства - загрузка в сеть программ, уничтожающих данные на компьютерах пользователей.

Вначале 1980 - х гг. появился первый загрузочный вирус Elk Cloner для Apple II.

В истории компьютерных вирусов переломным стал 1984 г., когда итальянские программисты Р. Черути и М. Морокути подготовили теоретическую базу для практической реализации распространения на дискетах загрузочных вирусов. Они подробно изложили свои концепции широкой общественности и опубликовали спецификацию загрузочной (бутовой) вирусной программы. Несмотря на то, что Р. Черути и М. Морокути отказались от дальнейших практических исследований в этом направлении, их идеи были подхвачены и широко реализованы на практике [9, с. 546].

Еще одним исследователем в области реализации саморазмножающихся программ в 1984 г. стал сотрудник Лехайского университета Ф. Коэн, который провел ряд экспериментов на системе VAX 11/750, работавшей под управлением операционной системы UNIX. Опубликованные им статьи стали руководством для разработки вирусных программ.

Принято считать, что термин «компьютерный вирус» был впервые введен Ф. Коэном.

Первые попытки противодействия вирусным программам были предприняты в 1985 г. Т. Нельфом, который стал собирать список опасных загружаемых программ для MS DOS, получивший название «чертова дюжина».

В настоящее время этот список поддерживается Э. Ньюхаузом и его можно получить из сети Интернет, там же можно получить бюллетень WildList, автором которого является Д. Уэльс [9, с. 547].

В 1984 году американский программист Э. Хопкинс написал первые антивирусные программы.

Массовое распространение компьютеров нового семейства IBM PC со второй половины 1980 - х гг. стало вторым этапом в развитии вирусов, и именно в это время появились так называемые хакеры.

Хакеры - это специалисты, которые занимаются исследованием прикладных областей компьютерных технологий и разработкой небольших недокументированных программ. Эти программы, как правило, представляют собой модификации программного кода уже созданных программных продуктов [19, c. 96].

Таким образом, «кромсание» (hacker) чужих программ и соответствует понятию хакер.

Неформальный кодекс хакера запрещает создавать вирусные программы.

Кракеры - это специалисты, занимающиеся вопросами снятия защиты с программного продукта, изменения атрибутов защищенной программы.

Компьютерный взлом программ позволяет распространять в огромных количествах программные продукты без санкции разработчиков коммерческого программного обеспечения.

Кракеры проникают и в базы данных пользователей с конфиденциальной информацией, имеющие средства защиты от незаконного доступа и копирования.

Среди кракеров существуют «информационные путешественники», которые проникают по сети на удаленные компьютеры, извлекают из них коды и пароли и пользуются ими наравне с законными хозяевами.

На территорию бывшего СССР компьютерные вирусы стали проникать с момента освоения рынка персональных компьютеров, т. е. с 1988 г. [19, c. 97].

Первый компьютерный вирус (венский) был занесен в начале 1988 г. на компьютеры Переславль - Залесского института программных систем, в середине года этот вирус появился в Киеве.

В этом же году предпринята попытка создания отечественной антивирусной программы А.А. Чижовым.

Исторически появление компьютерных вирусов связано с идеей создания самовоспроизводящихся механизмов, в частности, программы, которая возникла в 1950 - х гг.

Первые случаи массового заражения вирусами ПК были отмечены в 1987 г. Сначала появился вирус, разработанный братьями Амджа - том и Базитом Алви (Пакистанский вирус). Этим они решили наказать американцев, покупавших дешевые незаконные копии программных продуктов в Пакистане; такие копии братья стали продавать, предварительно инфицировав их разработанным вирусом. В результате только в США он заразил более 18 тыс. компьютеров и, проделав поистине кругосветное путешествие, попал в тогдашний СССР.

Сейчас в мире существует свыше 40 тыс. вирусов (включая штаммы - варианты вируса одного типа), причем арсенал их постоянно увеличивается [19, c. 112].

Для понимания способов заражения и антивирусной защиты огромное множество вирусов достаточно разбить на несколько обобщенных групп по направленности своего действия, продолжительности действия, способам маскировки.

## 2.5. Типы вирусов

**Троянская программа (Троян, Троянский конь)** - эта программа полностью оправдывает свое название. Она проникает в другие программы и скрывается там до момента, когда программа - хозяин будет запущена.

До запуска хозяйской программы вирус не может нанести вред.

Чаще всего троянский конь используется для удаления, изменения или кражи данных. Самостоятельно размножаться троян не может.

**Программы шпионы -** эти Штирлицы занимаются сбором информации о пользователе и его действиях.

Чаще всего они воруют конфиденциальную информацию: пароли, адреса, номера карт - счетов и т. д.

Зомби - такое название вредоносные программы получили, оттого, что и в самом деле делают из компьютера «безвольную» машину, подчиняющуюся злоумышленникам.

Проще говоря, нехорошие люди могут управлять чьим - либо компьютером посредством этих вредоносных программ.

Чаще всего пользователь даже не знает, что его компьютер уже не только его.

**Программа - блокировщик (баннер)** - эти программы блокируют доступ к операционной системе.

При включении компьютера пользователь видит всплывающее окно, в котором обычно его в чем - то обвиняют: нарушении авторских прав или скачивании пиратского программного обеспечения.

Далее, следуют угрозы полного удаления всей информации с компьютера.

Для того чтобы этого избежать пользователь должен пополнить счет определенного телефона или отослать СМС. Только вот, даже если пользователь проделает все эти операции, баннер с угрозами никуда не денется.

**Загрузочные вирусы -** поражают загрузочный сектор винчестера (жесткого диска).

Их целью является существенное замедление процесса загрузки операционной системы. После длительного воздействия этих вирусов на компьютер существует большая вероятность не загрузить операционную систему совсем.

**Эксплойт -** это специальные программы, которые используются злоумышленниками для проникновения в операционную систему через ее уязвимые, незащищенные места с целью получения прав доступа к компьютеру.

Используются для проникновения программ, которые воруют информацию, необходимую для получения прав доступа к компьютеру.

**Фарминг -** вредоносная программа, осуществляющая контроль над браузером пользователя и направляющая его на фальшивые сайты злоумышленника.

Во «внутренности» браузера эти паразиты попадают при помощи троянов и червей. При этом будут отображаться только фальшивые сайты, даже если адрес был введен правильно.

**Руткит -** программные средства, которые позволяют злоумышленнику беспрепятственно проникать в программное обеспечение жертвы, а затем полностью скрыть все следы своего пребывания.

Полиморфные вирусы **-** вирусы, которые маскируются и перевоплощаются. Во время работы они могут менять собственный код. А посему их очень сложно обнаружить.

**Программный вирус  -** программа, которая прикрепляется к другим программам и нарушает их работу.

В отличие от трояна программный вирус может размножаться, и в отличие от червя для успешной работы ему нужна программа, к которой он может «прилипнуть».

**Сетевой червь -** разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные (Интернет) компьютерные сети.

## *Червь Морриса*

«Червь Морриса» был первым в истории развития вычислительной техники образцом вредоносного программного обеспечения, который использовал механизмы автоматического распространения по сети.

Для этого использовалось несколько уязвимостей сетевых сервисов, а так же некоторые слабые места компьютерных систем, обусловленные недостаточным вниманием к вопросам безопасности в то время.
По словам Роберта Морриса, червь был создан в исследовательских целях.

Его код не содержал в себе никакой «полезной» нагрузки (деструктивных функций). Тем не менее, из - за допущенных ошибок в алгоритмах работы, распространение червя спровоцировало так называемый «отказ в обслуживании», когда ЭВМ были заняты выполнением многочисленных копий червя и переставали реагировать на команды операторов.

«Червь Морриса» практически парализовал работу компьютеров в сети ARPANET на срок до пяти суток. Оценка простоя - минимум 8 миллионов часов и свыше 1 миллиона часов временных затрат на восстановление работоспособности систем.

Общие убытки в денежном эквиваленте оценивались в 98 миллионов долларов, они складывались их прямых и косвенных потерь.

Структурно червь состоял из трех частей - «головы» и двух «хвостов».

«Голова» представляла собой исходный текст на языке C (99 строк) и компилировалась непосредственно на удаленной машине.

«Хвосты» были идентичными, с точки зрения исходного кода и алгоритмов, бинарными файлами, но скомпилированными под разные типы архитектур [19, c. 140].

***Червь мессенджера****.*

Он распространяется в популярных программах, созданных для общения, таких как Теlegram, WhatsApp или Skype.

Этот зловред, классифицированный как троян - шпион для устройств на Android и получивший название CanesSpy, был обнаружен в модифицированных версиях мессенджера, которые распространялись посредством каналов в Telegram, WhatsApp или Skype.

В период с 5 по 31 октября 2023 года защитные системы «Лаборатории Касперского» блокировали более 340 тысяч попыток атак с применением данного трояна по всему миру, с основными случаями инфицирования, отмеченными в Азербайджане, Саудовской Аравии, Йемене, Турции и Египте. Российские пользователи также столкнулись с этой угрозой.

Зловред способен похищать конфиденциальную информацию со смартфона, включая список контактов, а также инициировать запись звука с микрофона устройства, когда телефон включается или подключается к зарядному устройству.

Активация шпионского программного обеспечения происходит в критические моменты использования устройства, увеличивая риск незаметного перехвата информации.

Преимущественно вредоносный файл распространяется через Telegram - каналы, насчитывающие в сумме до двух миллионов подписчиков.

Кроме того, отмечено, что подобные модификации мессенджера доступны и на различных интернет - ресурсах, предлагающих скачать альтернативные версии приложений для обмена сообщениями.

«Лаборатория Касперского» уже информировала администрацию Telegram, WhatsApp или Skype о распространении вредоносных программ в мессенджере, однако проблема всё ещё остаётся актуальной.

*Почтовый червь.*

Проникает на компьютер посредством почтовой рассылки.

Обычно это письмо, содержащее ссылку на файл или сам зараженный файл.

После того, как вы или запустите прикрепленный файл, или перейдете по ссылке и скачаете его, червь начинает свою вредоносную деятельность.

Затем он ищет другие почтовые адреса и начинает производить рассылку зараженных писем уже по ним.

Распространяется главным образом через компьютерные сети.

От других типов червей такой отличается тем, что ищет в локальной сети устройства, которые используют уязвимые программы. После обнаружения таковых, он посылает в сеть сформированный пакет, который содержит или весь код червя, или его часть. Если в сети есть незащищенная машина, то она принимает этот пакет и заражается.

Проникнув в компьютер, червь копирует недостающую часть своего кода и становится полностью активен [19, c. 141].

*Червь чата.*

Для распространения он использует интернет - чаты - системы для общения между собой в реальном времени.

Такой червь публикует в чате ссылку на файл со своей копией, либо же сам файл.

Заражение происходит после скачивания файла.

*Червь файлообменника.*

Для внедрения в файлообменную сеть, червь должен скопировать себя в каталог файлов на компьютере пользователя.

Сеть файлообменника отображает всю информацию о данном файле, поэтому пользователь легко может найти его в системе, загрузить и открыть, после чего заражение неминуемо.

Более продвинутые и сложные типы червей могут имитировать сетевой протокол определенной сети - они также положительно реагируют на запросы и предлагают зараженные файлы для загрузки.

*Другие черви.*

Сюда можно отнести вредоносное ПО, которое способно распространяться через сетевые ресурсы.

Оно может использовать функции операционной системы для поиска доступных сетевых папок, после чего подключается к устройствам в глобальной сети и пытается открыть их диски на полный доступ.

Главное отличие от сетевых червей - пользователь непременно должен открыть файл с копией вируса.

Также существуют черви, которые не обладают ни одним из вышеперечисленных признаков, и могут распространяться посредством мобильных телефонов, поражая их.

Термин «Вредоносная программа» является обобщенным для всех существующих вирусов [19, c. 142].

Стоит помнить, что программа, которая была поражена вирусом, уже не будет работать нормально. Поэтому ее нужно удалить, а затем установить заново.

**2.6. Признаки заражения**

Выделяют следующие признаки заражения:

* автоматическое открытие окон с незнакомым содержимым при запуске компьютера;
* блокировка доступа к официальным сайтам антивирусных компаний, или же к сайтам, оказывающим услуги по «лечению» компьютеров от вредоносных программ;
* появление новых неизвестных процессов в выводе диспетчера задач (например, окне «Процессы» диспетчера задач Windows);
* появление в ветках реестра, отвечающих за автозапуск, новых записей;
* запрет на изменение настроек компьютера в учётной записи администратора;
* невозможность запустить исполняемый файл (выдаётся сообщение об ошибке);
* появление всплывающих окон или системных сообщений с непривычным текстом, в том числе содержащих неизвестные веб - адреса и названия;
* перезапуск компьютера во время старта какой - либо программы;
* случайное и/или беспорядочное отключение компьютера;
* случайное аварийное завершение программ;
* снижение производительности при достаточном объёме памяти, вплоть до «зависаний» вкупе с аномальным перегреванием системного блока;
* появление неизвестных файлов и каталогов в файловой системе, которые обычно выдают ошибку удаления;
* шифрование или повреждение пользовательских файлов;
* неизвестные изменения в содержимом системных файлов при открытии их в текстовом редакторе;
* быстрая утечка памяти на жёстком диске [5].

Таким образом, при любых проявлениях признаков заражения следует воспользоваться современными методами и средствами безопасности.

**2.7. Современные методы и средства информационной безопасности**

Защита от кибератак требует комплексного подхода: начать можно с того, чтобы создавать и использовать сильные, уникальные пароли для каждого аккаунта, а также включить двухфакторную аутентификацию там, где это возможно.

Регулярное обновление операционных систем и программного обеспечения также играет ключевую роль в процессе предотвращения кибератаки.

Для защиты от проникновения вирусов необходимо проводить мероприятия, исключающие заражение программ и данных компьютерной системы.

Основными источниками проникновения вирусов являются:

* съемные носители (съемные винчестеры, флеш - память, компакт - диски CD и DVD), на которых находятся зараженные вирусом файлы;
* компьютерные сети и их сервисы, в том числе система электронной почты и World Wide Web;
* жесткие диски, на которые проник вирус в результате работы с зараженными программами;
* вирус, который остался в оперативной памяти после работы предшествующего пользователя с зараженными программами [8].

Каким бы ни был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от компьютерных вирусов необходимо использовать:

* общие средства защиты информации, которые полезны для защиты не только от вирусов, но и от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
* профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
* специализированные программы для защиты от вирусов [11, с. 69].

В качестве профилактических мер, предохраняющих от заражения компьютерными вирусами, рекомендуется:

1. Использовать современные операционные системы, имеющие более серьезный уровень защиты от вредоносных программ.
2. Своевременно устанавливать программы для устранения ошибок в операционной системе и прикладных программах, которые являются «лазейками» для вирусов.
3. Если имеется режим автоматического обновления операционной системы, то включить его для автоматической загрузки новых патчей.
4. Постоянно работать на компьютере исключительно с правами пользователя, а не администратора.
5. Использовать антивирусные программные продукты известных производителей с автоматическим обновлением антивирусных баз.
6. Использовать персональный сетевой экран, контролирующий выход с компьютера в сеть Интернет и защищающий от информационных атак извне.
7. Ограничить физический доступ к компьютеру посторонних лиц.
8. Использовать внешние носители информации, полученные только от проверенных лиц.
9. Не открывать компьютерные файлы, полученные из ненадежных источников (например, полученные в качестве вложения в письмо e - mail или скачанные из Интернета, без их предварительной проверки антивирусом).
10. Отключить автозапуск со сменных носителей, что не позволит запускаться вредоносным программам, которые без ведома пользователя были туда записаны при заражении этих носителей вирусами [12, с. 67].

Можно сделать вывод, о том, что стопроцентной защиты от всех вредоносных программ не существует, от них не застрахован никто, но перечисленные рекомендации, применение современных методов и средств, помогут значительно снизить риск потерь от воздействия компьютерных вирусов.

## 2.8. Виды антивирусных программ

Антивирусные программы предназначены для защиты компьютеров от большинства вирусов, червей и «троянских коней», которые могут удалять файлы, получать доступ к личным данным или использовать зараженную систему как средство атаки на другие компьютеры.

**Антивирусная программа (антивирус) -** это программа для обнаружения компьютерных вирусов и других вредоносных программ, лечения и восстановления инфицированных файлов, а также для профилактики (предотвращения) заражения файлов или операционной системы вредоносным кодом.

Антивирусные программы обычно используют два различных метода для выполнения следующих задач:

* сканирование (просмотр) файлов для поиска уже известных вирусов, для которых в вирусной базе (входящей в комплект антивирусной программы специальной базы данных) есть информация о характерных фрагментах вирусного программного кода (структурах вирусов);
* обнаружение подозрительного поведения любой программы, которое похоже на поведение зараженной программы.

Антивирусное программное обеспечение состоит из пакета программ, которые обнаруживают, предотвращают размножение и удаляют компьютерные вирусы и другие вредоносные программы [15, с. 318].

При выборе антивирусной программы необходимо учитывать следующие параметры, которым антивирус должен соответствовать:

1. Постоянство и надежность работы.

При стабильной работе антивирусной программы нет ощущения, что какие - то зараженные файлы остались незамеченными. Этот параметр является определяющим.

1. Большой объем и постоянное обновление вирусной базы.

Сюда же относится умение программы быстро опознавать виды вирусов, работать с файлами различных типов: архивами, документами и осуществлять автоматическую проверку всех новых файлов по мере их копирования.

1. Быстрота работы антивируса и дополнительные функции [14, с. 319].

К дополнительным функциям можно отнести наличие эвристического сканирования и возможность лечения зараженных файлов (когда вирусы из них удаляются, а файлы приводятся в исходное состояние, бывшее до их заражения).

1. Программная поддержка различных операционных систем.

При работе в сетевом варианте немаловажным является также наличие у антивирусной программы серверных модулей, предназначенных для администрирования, и наличие возможности работы на разных серверах [14, с. 320].

В настоящее время не существует единой классификации антивирусных средств защиты компьютеров, однако их можно разделить на пять основных типов:

1. Программы - детекторы (сканеры) обеспечивают поиск и обнаружение конкретных вирусов.

Основаны на сравнении специфической последовательности байтов, содержащихся в теле вируса с байтами проверяемых файлов.

Их недостатком является то, что они могут находить только вирусы, уже известные разработчикам таких программ.

Универсальные детекторы проверяют неизменность файлов путем подсчета и сравнения их контрольной суммы с эталоном.

1. Программы - доктора (фаги, дезинфекторы) не только находят файлы, зараженные вирусом, но и лечат их, удаляя из файлов тело вируса и возвращая файлы в исходное состояние.

Полифаги, программы - доктора, предназначенные для поиска и уничтожения большого количества разных видов вирусов.

1. Программы - ревизоры анализируют текущее состояние файлов и системных областей дисков и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора.

При этом проверяется состояние Boot - сектора, FAT, а также длина файлов, код циклического контроля (контрольная сумма файла), дата и время модификации, атрибуты и другие параметры файлов.

1. Программы - фильтры – резидентные программы, которые оповещают пользователя обо всех попытках какой - либо программы выполнить подозрительные действия, а пользователь сам принимает решение о разрешении или запрещении выполнения этих действий.

Фильтры контролируют обновление программных файлов и системной области дисков, форматирование диска, загрузку программ в ОЗУ. Однако они не способны обезвредить вирус, для этого нужно применять фаги.

1. Программы - иммунизаторы (вакцины) – резидентные программы, предотвращающие заражение файлов [14, с. 321].

Принцип их работы состоит в том, что в программу записываются признаки конкретного вируса так, что подобный вирус считает ее «уже зараженной» и не производит повторное инфицирование. Эти программы наименее эффективны и уже устарели.

Использование различных форм, методов и средств, при работе в сети Интернет, может существенно снизить риск заражения компьютера от различных компьютерных вирусов, а также снизит риск «утечки» личной информации о пользователе.

**Глава 3. Практическая часть**

**3.1. Анализ результатов олимпиады «Безопасный интернет»**

В период с 28 ноября по 25 декабря на учебной платформе «Учи. ру» проходила олимпиада «Безопасный интернет».

Олимпиада «Безопасный интернет»:

- учит разумному и безопасному поведения в сети;

- объясняет основные правила использования электронных средств с выходом в интернет;

- развивает навыки работы с информацией, логическое мышление и память;

- демонстрирует реалистичные ситуации, учит принимать взвешенные решения [22].

Мы обратились к обучающимся 8 – ых классов с просьбой принять активное участие в олимпиаде.

В олимпиаде приняли участие 32 восьмиклассника (8 «А» класс (16 человек) и 8 «Б» класс (16 человек)).

Ребятам предстояло решить 8 задач:

* 1. Научи его.
	2. Спам.
	3. Кто там?
	4. Ситуации.
	5. На связи.
	6. Переговоры.
	7. Искатель правды.
	8. Защити смартфон. (Приложение 1)

Ребята отвечали на вопросы:

1. Что такое искусственный интеллект.
2. Как обучается искусственный интеллект.
3. Что такое СПАМ, признаки.
4. Безопасный пароль и другие.

Результаты олимпиады.

8 «А» класс:

I место (Диплом победителя) - 6 чел. (37 %);

II место (Похвальная грамота) - 8 чел. (50 %);

Сертификат участника - 2 чел.(13 %). (Приложение 2)

8 «Б» класс:

I место (Диплом победителя) - 5 чел. (31 %);

II место (Похвальная грамота) - 9 чел. (56 %);

Сертификат участника - 2 чел. (13 %). (Приложение 3)

Общий результат:

I место (Диплом победителя) - 11 чел. (34 %);

II место (Похвальная грамота) - 17 чел. (53 %);

Сертификат участника - 4 чел. (13 %). (Приложение 4)

По результатам олимпиады можно сделать следующие выводы, что ребята владеют методами и средствами компьютерной безопасности, знают правила и используют их в повседневной жизни при использовании интернет – ресурсов, смартфонов и других гаджетов.

Интернет – это удивительный инструмент, где собраны миллионы развлечений и новой информации. Но, помимо полезного контента, удобных мессенджеров и интересных сайтов, в сети много опасностей.

Взрослый в силу своего опыта может оградить себя от них, а вот ребенок может о них и не знать.

В соответствии с целью и гипотезой исследования о том, что использование разнообразных методов и средств повышения уровня информационной культуры будет способствовать формированию информационной безопасности в сети Интернет, нами были разработаны правила безопасного поведения. (Приложение 5)

Но, также мы считаем, целесообразным формировать правила цифровой безопасности еще в младшем школьном возрасте, так как сейчас каждый ребенок пользуется смартфонами, компьютерами и другими гаджетами, поэтому для обучающихся 1 «А» класса мы провели беседу на тему «Безопасный интернет», показали видеоролик разработанный нами.

После беседы мы раздали ребятам памятки «Безопасность в сети Интернет», которые были нами разработаны на основе составленных правил. (Приложение 6)

**ЗАКЛЮЧЕНИЕ**

В заключении можно сделать следующие выводы о том, что информационная безопасность в сети Интернет является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни.

Использованиесети Интернет оказывает огромнейшее влияние на жизнь современного человека.

Несмотря на то, что сеть Интернет является важным инструментом, стоит понимать и осознавать все риски, связанные с выходом в сеть, а также знать о мерах безопасности и уметь применять их на практике.

Цель проекта как раз и состоит в том, чтобы разъяснить обучающимся важность осторожного обращения с информацией в сети Интернет.

В течение исследования были выявлены самые доступные, простые и часто используемые способы, которые каждый может начать применять уже сейчас. И всё же, стоит подчеркнуть, что самым доступным и надёжным способом является осведомлённость, так как большая часть преступлений совершаются именно из - за неосторожности пользователя.

Умение анализировать, подвергать сомнению входящую информацию является необходимым для современного человека, так как при анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий - области, развивающейся беспрецедентно высокими темпами.

В области информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно - технические средства), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.

Работа состоит из введения, двух теоретических глав и практической главы; заключения; списка литературы; приложения.

Во введение обосновывается актуальность выбранной темы, раскрывается предмет, объект, цели и задачи, выдвигается гипотеза.

В первой главе «Информационная безопасность» дается определение «информационная безопасность». Рассматриваются составляющие информационной безопасности; нормативно - правовые основы; ответственность за нарушения.

Во второй главе «Кибератака и современные методы и средства информационной безопасности» рассматриваются понятия «кибератака», «вирус», приведены их типы, а также современные методы и средства информационной безопасности.

В практической части анализ результатов олимпиады.

В заключении приводятся основные выводы по работе.

В списке литературы приведены библиографические данные.

Гипотеза, выдвинутая в начале, о том, что использование разнообразных методов и средств повышения уровня информационной культуры будет способствовать формированию информационной безопасности в сети Интернет нашла свое подтверждение.

Цели и задачи выполнены.

**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ И ИСТОЧНИКОВ**

1. Бабаш А. В., Баранова Е. К., Ларин Д. А. История защиты информации в России. - СПб.: Речь, 2016. - 210 с.
2. Блинов А. М. Информационная безопасность. Учебное пособие. Часть 1. - СПб.: Издательство СПбГУЭФ, 2010. - 96 с.
3. Бройдо В.Л. Вычислительные системы, сети телекоммуникации. - СПб.: Питер, 2015. - 568 с.
4. Дергунова О.К. Безопасность детей в Интернете. [Электронный ресурс] // Книга «Безопасность детей в Интернете» - 2006 - Режим доступа - www.ifap.ru/library/book099.pdf.
5. Добреля Т.В. Чего опасаться в Интернете [Электронный ресурс] / Тимофей  В. Добреля - 2013, Режим доступа - <http://tim-plus.ru/opasnost-v-internete-i-kak-ee-izbezhat.html>.
6. Информатика / под ред. проф. Ю. А. Романовой. - М.: Эксмо, 2015. - 322 с.
7. Курбатов В. А. Политики безопасности компании при работе в Интернет. - М.: Горячая линия - Телеком, 2014. - 248 с.
8. Левский Н.А. Чего опасаться в Интернете. Самые опасные сайты. Вредоносные программы. [Электронный ресурс] // Журнал ComputerBild - 2013, - Режим доступа -<http://www.windxp.com.ru/acpeg.htm>.
9. Леонтьев, В. А. Большая энциклопедия Microsoft Office / В. А. Леонтьев. - М.: ОЛМА - ПРЕСС, 2014. - 840 с.
10. Мелехин В.Ф. Вычислительные машины, системы и сети. - М.: Академия, 2015. - 560 с.
11. Назаров С.В. Администрирование локальных сетей Windows. -М.: Финансы и статистика, 2013. - 480 с.
12. Нестеров С. А. Основы информационной безопасности: Учебное пособие. - 3 - е изд., стер. - СПб.: Издательство «Лань», 2017. - 324 с.
13. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - СПб.: Питер, 2012. – 360 с.
14. Пятибратов А.П. Вычислительные системы, сети телекоммуникации. - М.: Финансы и статистика, 2014. - 470 с.
15. Петраков А.В. Основы практической защиты информации. - Москва : РадиоСофт, 2015. - 498 с.
16. Родичев Ю. Нормативная база и стандарты в области информационной безопасности. - СПб.: Питер, 2017. - 348 с.
17. Русско - английский толковый словарь по информационной безопасности» Э.М. Пройдаков, Л.А. Теплицкий, 2020. - 560 с.
18. Усманов А. Простые эффективные способы максимальной защиты компьютеров от вирусов. – М.: Стандарт, 2019. – 390 с.
19. Холмогоров В. PRO вирусы. - М.: Просто, 2020. - 208 с.
20. http://stopcrack.narod.ru/ - сайт посвящен всем тем, кто интересуется проблемами компьютерной безопасности в интернет.
21. http://www.compdoc.ru/secur/internet/securpolicy/glava5\_2.shtml - сайт посвящен Политике безопасности.
22. https://safenet.uchi.ru/closed

**ПРИЛОЖЕНИЕ**

**Приложение 1**

**Вопросы задач**

|  |  |
| --- | --- |
| **№****задачи** | **Наименование** |
| **1** | Научи его. |
| **2** | Спам. |
| **3** | Кто там? |
| **4** | Ситуации. |
| **5** | На связи. |
| **6** | Переговоры. |
| **7** | Искатель правды. |
| **8** | Защити смартфон. |

**Приложение 2**

**Результаты олимпиады**

**Приложение 3**

**Результаты олимпиады**

**Приложение 4**

**Общий результат олимпиады**

**Приложение 5**

**Правила безопасного поведения в интернете**

Важно помнить, что в Интернете есть свои правила и границы, свои «НЕЛЬЗЯ!», «ОСТОРОЖНО!», МОЖНО!»:

# НЕЛЬЗЯ!

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей).
2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя.
3. Грубить, придираться, оказывать давление - вести себя невежливо и агрессивно.
4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей.
5. Не встречайся с Интернет - знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

# ОСТОРОЖНО!

1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам.
2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха.
3. Незаконное копирование файлов в Интернете - воровство.
4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут.
5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

# МОЖНО!

1. Уважай других пользователей.
2. Пользуешься Интернет - источником - делай ссылку на него.
3. Открывай только те ссылки, в которых ты уверен.
4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут.

# БЕЗОПАСНОЕ ПОВЕДЕНИЕ В ИНТЕРНЕТЕ

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ.
2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его.
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере.
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз.
5. Ограничь физический доступ к компьютеру для посторонних лиц.
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников.
7. Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

**СОЦИАЛЬНЫЕ СЕТИ**

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.
4. Избегай групп и пользователей, говорящих на языке насилия и ненависти, призывающих к тем действиям, которые никогда бы не одобрили твои родители.
5. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее.
6. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение.
7. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.
8. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все

сразу.

**ЭЛЕКТРОННАЯ ПОЧТА**

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако, лучше доверять тем, кого знаешь и кто первый в рейтинге.
2. Не указывай в личной почте личную информацию.

Например, лучше выбрать «музыкальный\_фанат@» или «рок 2013» вместо «тема 13».

1. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.
2. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах.
3. Не открывай файлы, и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.
4. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

**ОНЛАЙН ИГРЫ**

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков.
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие - то доказательства в виде скринов.
3. Не указывай личную информацию в профайле игры.
4. Уважай других участников по игре.
5. Не устанавливай неофициальные патчи и моды.
6. Используй сложные и разные пароли.
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

**Приложение 6**

**Памятка**

**«Безопасность в сети Интернет»**

****