УДК 004.056.57

# КИБЕРБЕЗОПАСНОСТЬ И МЕРЫ ПРЕДОСТОРОЖНОСТИ

*Винярская Ю.С., Копацкевич А.А.*

*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» филиал «Минский радиотехнический колледж», г. Минск, Республика Беларусь*

*Научный руководитель: Сальникова Е.А. - преподаватель первой категории, магистр*

**Аннотация**. Важность кибербезопасности в современной жизни, выявление основных угроз кибербезопасности, их виды и источники, а также меры безопасности по их предотвращению, виды вредоносного ПО.

**Ключевыя слова:** кибербезопасность, вирус, трояны, черви, атака на сеть, фишинг, защита информации, спам, антивирус.

***Введение.*** Кибербезопасность очень важна в нашей современной жизни, потому что все больше людей используют интернет и другие цифровые технологии для работы, шопинга, общения и других целей. Вместе с увеличением использования этих технологий, растет и риск нарушения безопасности данных и информации. Кибербезопасность помогает защитить наши личные данные, финансовую информацию, коммерческую тайну и другую конфиденциальную информацию от кражи, взлома или утечки. Нарушение кибербезопасности может иметь серьезные последствия для личной жизни, финансов и бизнеса, и даже для национальной безопасности. Поэтому понимание кибербезопасности и применение мер по ее защите являются необходимыми навыками для всех, кто использует цифровые технологии в своей жизни.

***Основная часть.*** К основным угрозам кибербезопасности относятся: вирусы, трояны и черви, атаки на сеть**.**

Вирусы, трояны и черви – это разновидности злонамеренного программного обеспечения, которые являются одной из основных угроз кибербезопасности. Вирусы – это программы, которые могут заражать другие файлы на вашем компьютере и распространяться на другие компьютеры через Интернет. Трояны – это программы, которые могут скрытно устанавливаться на компьютере, обычно вместе с другими программами, и выполнять злонамеренные функции, например, кражу личной информации. Черви – это программы, которые могут распространяться на другие компьютеры через локальную сеть или Интернет без участия пользователя [2].

Они могут появляться на устройствах из разных источников, включая:

1. Незащищенные сетевые подключения: Вирусы, трояны и черви могут попадать на компьютеры и другие устройства через незащищенные сетевые подключения. Например, когда пользователь подключается к открытой беспроводной сети Wi-Fi или к сети, защита которой легко взламывается.

2. Вредоносные веб-сайты: Вирусы, трояны и черви могут быть внедрены в веб-сайты, которые содержат вредоносный код. Пользователи могут случайно попасть на такие сайты, щелкнув по ссылке в электронном письме или на сайте низкого качества.

3. Электронные письма: Вирусы, трояны и черви могут быть отправлены в виде вложений в электронных письмах. Некоторые вирусы могут даже распространяться через адресную книгу пользователя, отправляя себя другим контактам пользователя.

4. Незащищенные внешние устройства: Некоторые вирусы, трояны и черви могут быть переданы на устройства через внешние носители данных, такие как флеш-накопители, CD- или DVD-диски.

Эти виды злонамеренного ПО могут привести к серьезным последствиям, таким как потеря данных, украденная личная информация, мошенничество и другие проблемы. Для защиты от этих угроз необходимо использовать программное обеспечение, которое может обнаруживать и удалять вирусы, трояны и черви. Также важно регулярно обновлять анти-

вирусное ПО, чтобы защита была максимально эффективной. Нужно избегать скачива-ния программ из недоверенных источников, не советуется также открывать вложения из непроверенных источников и переходить по ссылкам в подозрительных электронных письмах. Если обнаружено, что компьютер заражен вирусом, трояном или червем, следует немедленно обратиться к специалистам по компьютерной безопасности для помощи в решении проблемы.

Атаки на сеть – это угроза кибербезопасности, которая может привести к нарушению работы компьютерных систем и краже конфиденциальной информации. Атаки могут быть направлены на сеть компьютеров в офисе, на сервера, управляющие веб-сайтом, или на лич-ные компьютеры. Примеры атак на сеть включают в себя атаки на перегрузку (DDoS), в которых злоумышленники посылают большое количество запросов к серверу, чтобы пере-грузить его и вывести его из строя, и атаки на перехват информации, в которых злоумыш-ленники перехватывают данные, передаваемые по сети [1].

Для защиты от атак на сеть необходимо использовать средства защиты, такие как меж-сетевые экраны, которые позволяют управлять доступом к сети, и системы обнаружения вторжений, которые могут обнаружить несанкционированный доступ к компьютерной сис-теме [5]. Кроме того, необходимо убедиться, что программное обеспечение и операционная система на компьютерах обновляются регулярно, чтобы устранить известные уязвимости. Необходимо обучать пользователей сети, чтобы они знали, какие действия могут представ-лять угрозу для безопасности, и как их избежать. Регулярные резервные копии данных также могут помочь снизить ущерб от атак на сеть, если система все же будет скомпрометирована.

Меры по защите информации. Регулярное обновление программного обеспечения является одной из важных мер по защите информации и повышению кибербезопасности. Обновление программ позволяет исправлять уязвимости, которые могут быть использованы злоумышленниками для взлома системы или заражения вирусами [3].

Важно обновлять программы как можно скорее после того, как доступно новое обнов-ление. Многие злоумышленники стремятся использовать уязвимости в программном обеспечении, которые еще не были исправлены, поэтому обновление программ является необходимой мерой для защиты от кибератак.

Регулярное обновление программного обеспечения – это простой, но эффективный способ улучшения кибербезопасности. Он позволяет защитить компьютер и данные от многих видов угроз, связанных с уязвимостями программного обеспечения.[4]

Использование сложных паролей является одной из важных мер по защите инфор-мации и повышению кибербезопасности. Сильный пароль должен быть достаточно длинным и содержать комбинацию букв, цифр и символов.

Слабый пароль может быть легко угадан или подобран злоумышленником при помощи специальных программ, которые перебирают все возможные комбинации. Поэтому следует избегать использования простых паролей, таких как "123456" или "password".

Рекомендуется использовать отдельные пароли для каждого аккаунта и периодически их менять. Также не следует использовать личную информацию (например, даты рождения или имена) в качестве паролей.

Вот несколько примеров правильного использования сложных паролей:

1. Идеальным паролем считается длинный пароль, содержащий не менее 12 символов. Чем длиннее пароль, тем сложнее его подобрать взломщикам.

2. Хороший пароль должен содержать разнообразные символы, такие как заглавные и строчные буквы, цифры и специальные символы, такие как знаки пунктуации.

3. Избегайте использования личной информации, такой как имена, даты рождения, адреса или номера телефона в качестве пароля. Взломщики могут использовать эти данные для подбора пароля.

4. Используйте уникальные пароли для каждой учетной записи, чтобы обезопасить себя от взлома нескольких учетных записей одним паролем.

5. Используйте парольные менеджеры для создания и хранения сложных паролей. Эти приложения могут автоматически генерировать сложные пароли и хранить их в безопасном месте.

Например, хороший пароль может выглядеть так: "Hg#2^d@9L!4F". Он содержит разнообразные символы, длинный и не содержит личной информации. Используя такой пароль, вы значительно повышаете свою защиту от взлома учетной записи.

Также существует множество инструментов для создания сложных паролей, таких как генераторы паролей, которые могут помочь создать надежный пароль. Рекомендуется использовать двухфакторную аутентификацию, которая требует ввода кода, полученного на мобильный телефон или другое устройство, после ввода пароля.

Использование сложных паролей – это важная мера по защите информации и повышению кибербезопасности. Сильный пароль может помочь защитить ваши данные от несанкционированного доступа и предотвратить кибератаки.

Использование антивирусного программного обеспечения является важной мерой по защите компьютера от вирусов, троянов, червей и других вредоносных программ.

Ниже приведены некоторые примеры использования антивирусного программного обеспечения:

1. Сканирование на вирусы. Антивирус может сканировать компьютер или другое устройство на наличие вирусов, троянов, червей и других видов вредоносного ПО. При обнаружении вирусов, антивирус может помочь удалить их или поместить в карантин, чтобы предотвратить дальнейшее распространение.

2. Защита почты. Некоторые антивирусные программы могут обеспечить защиту от спам-писем, которые могут содержать вредоносные вложения или ссылки на вредоносные веб-сайты.

3. Защита от фишинга. Некоторые антивирусные программы могут предупреждать пользователей о подозрительных веб-сайтах, которые могут быть связаны с фишингом или другими мошенническими схемами.

4. Автоматические обновления. Антивирусные программы могут автоматически обновляться, чтобы быть защищенными от новых видов вредоносного ПО. Это обеспечивает более надежную защиту устройства в целом.

5. Удаление всплывающих окон. Некоторые антивирусные программы могут блокировать всплывающие окна, которые могут содержать вредоносный код или ссылки на вредоносные веб-сайты.

6. Оптимизация производительности. Некоторые антивирусные программы могут помочь оптимизировать производительность устройства, удаляя временные файлы и другие ненужные данные.[4]

Важно выбирать надежное и актуальное антивирусное ПО, которое будет регулярно обновляться и обеспечивать защиту от новых угроз. Рекомендуется использовать антивирусное ПО, которое имеет хорошую репутацию и отзывы от пользователей.

Использование антивирусного ПО – это важная мера по защите компьютера и данных от вредоносных программ. Однако необходимо помнить, что антивирусное ПО не является единственным средством защиты и его использование должно дополняться другими мерами по повышению кибербезопасности.

Проверка электронной почты на наличие спама и фишинга является важной мерой по защите информации и повышению кибербезопасности. Электронная почта – один из самых популярных способов общения и обмена информацией в интернете, который может быть использован злоумышленниками для распространения вирусов, троянов и фишинговых атак.

Спам – это нежелательные сообщения, которые могут содержать вредоносный код или ссылки на фишинговые сайты. Фишинг – это мошеннические попытки получить личную информацию, такие как пароли или данные кредитных карт, путем отправки фальшивых сообщений, которые выглядят как официальные.

Ниже приведены некоторые примеры того, как спам может появляться на электронной почте:

1. Рассылки от незнакомых отправителей. Спамеры могут отправлять миллионы электронных писем с рекламой или мошенническими предложениями от незнакомых отправителей. Эти письма могут содержать ссылки на вредоносные веб-сайты или вложения с вредоносным кодом.

2. Фишинговые письма. Спамеры могут использовать фишинговые письма, которые могут выглядеть как легитимные сообщения от банков, интернет-магазинов или других организаций. Эти письма могут содержать ссылки на поддельные веб-сайты, которые могут попросить вас ввести личную информацию, такую как номера кредитных карт или пароли.

3. Боты-рассыльщики. Спамеры могут использовать ботов-рассыльщиков для отправки множества электронных писем с рекламой или мошенническими предложениями. Эти письма могут содержать ссылки на вирусные веб-сайты или вирусные вложения.

4. Спам-фильтры. Спамеры могут использовать специальные программы, чтобы обойти спам-фильтры и доставлять свои сообщения в папку "Входящие" пользователя.

5. Подписки на рассылки. Спамеры могут добавить ваш адрес электронной почты в список рассылки без вашего согласия. Эти рассылки могут содержать рекламу или мошеннические предложения.[3]

Для защиты от спама и фишинга рекомендуется использовать фильтры спама, которые автоматически отсеивают нежелательные сообщения. Также не следует открывать вложения или переходить по ссылкам, если вы не уверены в надежности отправителя.

Проверка электронной почты на наличие спама и фишинга – это важная мера по защите информации и повышению кибербезопасности. Она помогает защитить ваши данные от кибератак и предотвратить утечку личной информации.

***Заключение.*** В данной статье были рассмотрены основные угрозы кибербезопасности, а также меры по их предотвращению. Были изучены виды вредоносного ПО, виды атак на сеть, фишинг и распространение личной информации. Были рассмотрены меры по защите информации, такие как использование сложных паролей, регулярное обновление программного обеспечения, использование антивирусного ПО и проверка электронной почты на наличие спама и фишинга.

В целом, кибербезопасность является крайне важной темой в нашей современной цифровой эпохе. Необходимо принимать меры по защите программных устройств и информации.

### *Список литературы*

*1. Алешин Л. И. Информационные технологии / Л. И. Алешин. - М.: , 2014. - 384 с.*
*2. Гохберг Г. С. Информационные технологии / Г. С. Гохберг, А. В. Зафиевский, А. А. Короткин. - М.: Академия, 2014. - 208 с.*
*3. Елочкин М. Е. Информационные технологии / М. Е. Елочкин, Ю. С. Брановский, И. Д. Николаенко. - М.: Оникс, 2016. - 256 с.*
*4. Информационные технологии / Под редакцией В. В. Трофимова. - М.: Юрайт, 2014. - 632 с.*
*5. Мельников В. П. Информационные технологии / В. П. Мельников. - М.: Академия, 2015. - 432 с.*

UDC 004.056.57

## CYBERSECURITY AND PRECAUTIONS

*Vinyarskaya Y.S., Kopatskevich A.A.*

*Educational institution "Belarusian State University of Informatics and Radioelectronics" branch "Minsk Radio Engineering College", Minsk, Republic of Belarus*

*Scientific supervisor Salnikova E.A. - teacher of the first category, master*

**Abstract**. The importance of cybersecurity in the modern world, identifying the main threats to the life of cybersecurity, their types and sources, as well as security measures to prevent them, types of malware.

**Keywords:** cybersecurity, virus, trojans, worms, network attack, phishing, information protection, spam, antivirus.