Цечоев М.Х., Шарыпова Т.Н. Киберугрозы и меры их предотвращения на предприятии // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 5–8

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

# КИБЕРУГРОЗЫ И МЕРЫ ИХ ПРЕДОТВРАЩЕНИЯ НА ПРЕДПРИЯТИИ

**[1]Цечоев М.Х., Шарыпова Т.Н**.
*Ростовский государственный экономический университет (РИНХ), Ростов-на-Дону, Россия (344000, г. Ростов-на-Дону, пер. Островского, 62), e-mail: [1]tcechoev02@inbox.ru*

**Статья представляет собой обзор основных видов киберугроз, которые могут стать причиной серьезных проблем для компаний и частных лиц. В статье рассматриваются такие типы киберугроз, как вредоносный код, фишинг, DDoS-атаки, вредоносное ПО. Кроме того, в статье предлагается ряд мер по защите от киберугроз, включая использование антивирусных программ, установку брандмауэров, регулярное обновление программного обеспечения и обучение сотрудников правилам безопасности в сети. Также в статье подробно рассматриваются киберугрозы, связанные с облачными хранилищами и устройствами Интернета вещей (IoT).**

Ключевые слова: киберугрозы, вредоносный код, вредоносное ПО, DDoS-атаки, фишинг, меры по защите от киберугроз.

# CYBER THREATS AND MEASURES TO PREVENT THEM AT THE ENTERPRISE

**[1]Tsechoev M.H., Sharypova T.N.**
*Rostov State University of Economics (RINH), Rostov-on-Don, Russia (344000, Rostov-on-Don, lane. Ostrovsky, 62), e-mail: [1]tcechoev02@inbox.ru*

**The article is an overview of the main types of cyber threats that can cause serious problems for companies and individuals. The article discusses such types of cyber threats as malicious code, phishing, DDoS attacks, malware. In addition, the article suggests a number of measures to protect against cyber threats, including the use of antivirus programs, the installation of firewalls, regular software updates and training of employees in network security rules. The article also discusses in detail the cyber threats associated with cloud storage and Internet of Things (IoT) devices.**

Keywords: cyber threats, malicious code, malware, DDoS attacks, phishing, measures to protect against cyber threats.

Киберпреступность представляет собой серьезную угрозу для организаций и отдельных лиц в 21 веке. Киберугрозы — это злоумышленные действия, которые используют компьютерные системы и сети, часто применяя вредоносное или другое вредоносное программное обеспечение для получения несанкционированного доступа или контроля над системой, что приводит к повреждению или нарушению работы данных, служб или сетей. За последние пять лет количество кибератак увеличилось более чем на 200%. В 2022 году из-за утечки данных было раскрыто более 4,1 миллиарда записей[1].

В кибератаках используются различные методы и приемы, в том числе вредоносный код, фишинг, вредоносное ПО, программы-вымогатели, социальная инженерия и атаки типа «отказ в обслуживании» (DoS) [2]:

1. Вредоносный код — это код, предназначенный для выполнения вредоносных действий, таких как кража конфиденциальной информации или отключение компьютерных систем.

2. Фишинг — это форма социальной инженерии, при которой злоумышленники рассылают электронные письма, пытаясь обманом заставить пользователей раскрыть конфиденциальную информацию.

3. Вредоносное ПО — это тип вредоносного программного обеспечения, предназначенного для проникновения в компьютерные системы и их повреждения.

4. Программа-вымогатель — это тип вредоносного ПО, которое шифрует файлы и требует оплаты в обмен на их разблокировку. Социальная инженерия — это использование обмана и манипуляций для получения конфиденциальной информации.

5. DoS-атака — это атака, при которой компьютер жертвы переполняется трафиком, лишая его возможности отвечать на законные запросы.

По мере того, как технологии становятся все более неотъемлемой частью ведения любого бизнеса, компании все чаще сталкиваются с рисками, связанными с киберугрозами. Киберпреступность вызывает все большую озабоченность у предприятий любого размера и может привести к разрушительным потерям денег, данных, лояльности клиентов и репутации. Компании должны предпринимать упреждающие действия, чтобы защитить свои системы и данные от злоумышленников.

Организациям необходимо начать с внедрения надежных мер безопасности, таких как надежные брандмауэры, антивирусное программное обеспечение и шифрование данных. Они также должны убедиться, что их сотрудники обучены передовым методам кибербезопасности, таким как избегание подозрительных электронных писем и веб-сайтов, а также понимание того, как выявлять потенциальные угрозы. Компании также должны использовать двухфакторную аутентификацию и регулярно обновлять свои исправления безопасности, чтобы обеспечить актуальность своих систем [5].

В дополнение к этим основным мерам организациям следует проводить регулярные аудиты безопасности и сканирование для обнаружения любых потенциальных уязвимостей. Им также следует рассмотреть возможность использования системы мониторинга и реагирования для постоянного мониторинга своих систем и быстрого реагирования на любые потенциальные угрозы. Компании также должны создать политику кибербезопасности, подробно описав шаги, которые они предпримут для защиты своих систем и данных, а также последствия любых нарушений.

В конечном счете предотвращение киберугроз требует сочетания упреждающих мер, обучения сотрудников и систем реагирования. Компании должны проявлять бдительность в своих усилиях по защите своих систем, данных и информации о клиентах от злоумышленников.

Рассмотрим подробнее киберугрозы, связанные с облачными хранилищами и устройствами Интернета вещей (IoT), которые представляют собой все более сложную среду кибербезопасности из-за большого количества потенциальных точек входа. По мере роста использования облачных хранилищ и устройств Интернета вещей в компаниях увеличивается вероятность того, что злоумышленники получат доступ к данным и устройствам [4].

Одной из основных киберугроз, связанных с облачными хранилищами и устройствами IoT, является утечка данных, которая происходит, когда неавторизованные пользователи

получают доступ к конфиденциальным данным, хранящимся в облаке. Утечка данных может быть вызвана различными злоумышленниками, включая хакеров, мошеннических инсайдеров, вредоносное ПО и незащищённые API. Доступ к данным в облаке через незащищённую конечную точку также может привести к раскрытию данных для злоумышленника.

Ещё одна проблема безопасности — использование ненадёжных паролей пользователями, которые получают доступ к облачным хранилищам и устройствам IoT. Слабый пароль можно легко угадать или подобрать методом грубой силы, что позволяет злоумышленникам получить доступ к данным. Кроме того, пользователи, которые непреднамеренно или злонамеренно повторно используют пароли для нескольких учетных записей, могут непреднамеренно предоставить злоумышленникам доступ к нескольким ресурсам.

Вредоносное ПО — это еще один тип киберугроз, которые можно использовать для нападения на облачные хранилища и устройства IoT[3]. Вредоносное ПО может заражать машины, предоставляя злоумышленникам доступ к данным, хранящимся на устройстве, или возможность удаленного управления устройством. Вредоносное ПО также может использоваться для создания бэкдоров в системе, позволяя злоумышленникам вернуться позже и получить доступ к данным.

Наконец, отсутствие исправлений может представлять значительный риск для облачных хранилищ и устройств IoT. По мере выявления новых уязвимостей к устройствам необходимо применять исправления, чтобы обеспечить безопасность системы. Отсутствие исправления для устройства может привести к нарушению безопасности, поскольку злоумышленники могут воспользоваться неисправленной уязвимостью.

Из проведенного исследования видно, что киберугрозы являются реальной проблемой и могут иметь серьезные последствия для отдельных лиц и предприятий. Для защиты от этих угроз важно использовать лучшие практики, такие как внедрение надежных мер аутентификации, регулярное обновление программного обеспечения, использование безопасных сетей и обучение персонала осведомленности о кибербезопасности. Кроме того, организации должны быть в курсе последних угроз и использовать соответствующие контрмеры.

**Список литературы**

1. Пустовая Е.И., Шарыпова Т.Н. Кибербезопасность в наше время. Инновация. Наука. Образования. 2020. № 24.
2. Лыженкова А.Н., Шарыпова Т.Н. Киберпреступления: понятие, классификация, юридическая ответственность, основные правила компьютерной безопасности.Инновация. Наука. Образования. 2021. № 26.
3. Евкина И.Е., Шарыпова Т.Н. Киберпреступность как угроза информационной безопасности. Инновации. Наука. Образование. 2021. № 36.
4. Решетова Виктория Александровна, Шарыпова Татьяна Николаевна. Вопросы противодействия киберпреступности. Инновации. Наука. Образование. 2022. №56. С. 60-64.
5. Шарыпова Т.Н., Селиванов С.А. Анализ угроз информационной безопасности и способы ее защиты. Наукосфера. 2021. № 1-1. С. 242-245.

**References**

1. Pustovaya E.I., Sharypova T.N. Cybersecurity in our time. Innovation. The science. Education. 2020. № 24.
2. Lyzhenkova A.N., Sharypova T.N. Cybercrime: concept, classification, legal responsibility, basic rules of computer security.Innovation. The science. Education. 2021. № 26.
3. Ivkina I.E., Sharypova T.N. Cybercrime as a threat to information security. Innovation. The science. Education. 2021. № 36.
4. Reshetova Victoria Alexandrovna, Sharypova Tatiana Nikolaevna.Issues of countering cybercrime. Innovation. The science. Education. 2022. No. 56. pp. 60-64.
5. Sharypova T.N., Selivanov S.A. ANALYSIS OF THREATS TO INFORMATION SECURITY AND WAYS TO PROTECT IT. The sciencosphere. 2021. No. 1-1. pp. 242-245.