**Анализ опасностей сетевой безопасности в современном обществе и меры защиты**

***Ван Сиюань***

*Студент (бакалавр)*

*Московский государственный университет имени М.В.Ломоносова,*

*Институт русского языка и культуры, Москва, Россия*

*E-mail: wangxiyuan24@163.com*

С развитием общества Интернет становится всё более популярным. С момента появления бумажных рукописей до нынешней эры Интернета применение технологий помогало человечеству, упрощая не только быт, но и производственные процессы. В эпоху больших данных существует множество видов рисков компьютерной информационной безопасности, и их вред нельзя игнорировать, поэтому вопросам безопасности компьютерных сетей стало уделяться все больше внимания.

Прежде всего, самой распространенной угрозой для Интернета является распространение интернет-вирусов. Когда система предотвращения и контроля обнаруживает эти вирусы, во многих случаях большая часть данных оказывается украдена и незаконно присвоена [1]. Когда пользователи используют компьютеры, вирусы проникают в компьютер, вызывая потерю данных и позволяя преступникам получить большие объемы данных. Поэтому компьютерные вирусы являются одной из важных проблем информационных систем Интернета.

Поскольку число технических специалистов продолжает увеличиваться, появляются хакеры. Из «Карты мировых интернет-атак и защиты в реальном времени» Касперского видно, что безопасность Интернета находится под серьезной угрозой из-за таких высокочастотных сетевых атак [2]. Это показывает, что по мере развития технологий растет и уровень хакеров, которые будут получать файлы с самыми высокими разрешениями. Таким образом, хакеры также станут опасной частью сетевой безопасности.

Во-вторых, это рассылка спам-сообщений. В нашей повседневной жизни мы часто получаем спам-сообщения в мессенджерах или через почту. В то же время эта информация содержит вирусы, которые могут проникнуть в компьютеры и разрушить брандмауэры.

Наконец, cамое главное, люди имеют низкую осведомленность о сетевой безопасности. Многие люди потеряли деньги и личную информацию, открывая подобные сообщения.

Именно поэтому в эпоху развитого Интернета необходимо усилить защиту сетевой безопасности, чтобы сделать базу данных более конфиденциальной.

Системы безопасности являются одними из них. Уровень безопасности управления: этот уровень поддерживает операции, отвечающие за передачу данных об услугах или сетевых приложениях. Этот уровень обычно включает общесетевую межмашинную связь, которая часто включает в себя управляющие сообщения [3]. Это означает, что информация будет сегментирована и будут предоставлены только необходимые данные. Это также обеспечивает подлинность и уровень конфиденциальности, поэтому пользователи и системные администраторы получают разную информацию.

В компьютерах брандмауэры играют важную роль. Брандмауэры определяют, какие данные могут входить и выходить из системы, а какие нет [4]. Безопасные архитектуры, домены безопасности и связь можно регулировать путем правильной реализации и настройки межсетевых экранов [3]. Это показывает, что у него есть защитные меры. Аппаратные брандмауэры могут отслеживать сетевой трафик и обеспечивать передачу данных между сетью и Интернетом. В то же время администраторы могут вручную настроить коэффициент безопасности, что также повышает безопасность межсетевого экрана в сети.

Во-вторых, антивирусное программное обеспечение можно использовать для противодействия проникновению спам-информации, и в то же время оно также может уничтожать вирусы, содержащиеся в компьютере. Антивирусное программное обеспечение используется для обеспечения компьютерной безопасности и снижения вреда от вирусов. В то же время необходимо также повышать осведомленность людей о сетевой безопасности и улучшать понимание людьми закона.

Несмотря на то, что современные технологии делают нашу жизнь удобнее и технологичнее, мы должны помнить об опасностях, которые несет несовершенная система компьютерной безопасности, что может привести к потери информации и данных. Необходимо повышать осведомленность о правилах пользования Интернетом и соблюдать правила безопасности.

**Литература**

1.荆继武.我国网络信息安全发展的探讨[J].中国科学院院刊,2022,37(11): 1000-3045.20221103002.

2.黄炜,秦霖,刘晓欣,许诺,李岳峰.网络信息安全治理研究进展:基于国内外法治现状[J].情报杂志,2020,39(04):132-139+29.

3.D.Barrera, I.Molloy, and H.Huang “Standardizing IoT network security policy enforcement,” In: Workshop on Decentralized IoT Security and Standards (DISS). p 6, 2018.

4.H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, “A survey on software-defined wireless sensor networks: Challenges and design requirements.” IEEE access, vol. 5pp. 1872-1899, 2017.