СОВРЕМЕННЫЕ УГРОЗЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

Калмуратов М.Т.
преподаватель Нукусского филиала Ташкентского университета информационных технологий имени Мухаммеда аль-Хорезми
https://doi.org/10.5281/zenodo.10648827

Аннотация. Современный мир стал невероятно зависимым от интернета и компьютерных сетей, что делает сетевую безопасность критически важной для защиты частных данных, бизнес-информации, государственных систем и многих других аспектов жизни. Однако, с развитием технологий появляются и новые угрозы, которые могут привести к серьезным последствиям. В этой статье мы рассмотрим современные угрозы сетевой безопасности, с которыми сталкиваются организации и обычные пользователи, и обсудим способы защиты от них.

Ключевые слова: кибербезопасность, киберугрозы, социальная инженерия, вредоносное ПО, безопасность информации, дистанционная работа, защита от DDoS-атак, мобильная безопасность, аутентификация, уязвимости ПО, защищенные сети, защита конфиденциальности.

Сетевая безопасность - это область информационной безопасности, которая занимается защитой компьютерных сетей, систем и данных от несанкционированного доступа, изменений или уничтожения. Она включает в себя различные методы, технологии и процессы, направленные на обеспечение конфиденциальности, целостности и доступности информации, а также защиту от киберугроз, включая вредоносное программное обеспечение, хакерские атаки, кибершпионаж, кибертерроризм и другие формы киберпреступности. Сетевая безопасность также включает в себя разработку и соблюдение политик безопасности, обучение пользователей, мониторинг сетей и реагирование на инциденты [4].

Современная цифровая среда имеет множество потенциальных угроз для сетевой безопасности, которые могут повлиять на организации и частных пользователей. Некоторые из наиболее распространенных угроз включают в себя кибератаки, вредоносное программное обеспечение, кражу личной информации, социальную инженерию, DDoS-атаки, фишинг и многие другие. Введение общих угроз сетевой безопасности необходимо для понимания потенциальных рисков и разработки мер по их предотвращению.

Кибератаки представляют собой различные виды нападений на компьютерные системы, сети и данные с использованием технологий

информационной и коммуникационной безопасности. Ниже приведено описание некоторых типов кибератак:

1. Вирусы: Вирусы являются вредоносными программами, которые могут распространяться через зараженные файлы и программы. Они могут наносить ущерб компьютерам, изменять данные и даже украсть личные сведения.

2. Вредоносное программное обеспечение: К этой категории относятся различные виды вредоносных программ, такие как черви, троянские кони, шпионское ПО и рекламное ПО (adware), которые могут незаконно получать доступ к данным и управлять компьютером без ведома пользователя.

3. DDoS-атаки: Атаки отказа в обслуживании (DDoS) направлены на перегрузку сети или серверов большим количеством запросов, что приводит к временной недоступности ресурса для легальных пользователей.

4. Фишинг: Киберпреступники используют фишинг для мошеннической передачи личных данных, таких как пароли или информация о банковских счетах, путем маскировки под официальные и доверенные источники.

5. Мальва и Рэмпэм: Эти атаки включают в себя захват компьютера или сервера и шифрование данных с требованием выкупа для их восстановления, форма атаки, известная как вымогательство.

6. Социальная инженерия: Это метод манипулирования людьми путем обмана и манипуляции для получения конфиденциальной информации или выполнения действий, которые могут привести к компрометации безопасности [2].

Защита личных данных является критически важной, особенно в цифровую эпоху. Вот несколько методов, которые могут помочь вам защитить свою личную информацию:

1. Сильные пароли: Используйте уникальные и сложные пароли для своих онлайн-аккаунтов, избегая использования одного и того же пароля для нескольких сервисов. Многие эксперты рекомендуют использовать фразы паролей.

2. Двухфакторная аутентификация: Включите функцию двухфакторной аутентификации для своих онлайн-аккаунтов, чтобы добавить дополнительный уровень защиты.

3. Обновления программного обеспечения: Регулярно обновляйте операционные системы, приложения и антивирусное программное обеспечение на своих устройствах, чтобы защитить их от уязвимостей.

4. Осторожность в сети: Будьте осторожны при открытии вложений в электронных письмах, переходах по подозрительным ссылкам и передаче личной информации через интернет.

5. Безопасное подключение к сети: Используйте защищенные сети Wi-Fi и виртуальные частные сети (VPN) при работе с чувствительными данными через интернет.

6. Мониторинг кредитной истории: Регулярно проверяйте свою кредитную историю, чтобы быстро обнаруживать любые подозрительные транзакции или кредитные запросы.

7. Осознанное использование социальных сетей: Будьте осторожны с информацией, которую вы публикуете в социальных сетях, чтобы избежать разглашения личной информации.

8. Шифрование данных: Используйте шифрование для хранения и передачи чувствительных данных [1].

9. Образование и информирование: Образование в области кибербезопасности, а также постоянное информирование о последних методах мошенничества и угрозах помогут вам быть более осторожными в сети.

Соблюдение этих практик поможет защитить вас от кражи личной информации и уменьшить риск стать жертвой киберпреступности.

Заключение. В цифровую эпоху кибербезопасность становится все более важной, поскольку социальная инженерия и другие виды кибератак становятся все более изощренными. Необходимо осознавать, что атаки на основе социальной инженерии могут привести к серьезным последствиям, включая утечку конфиденциальной информации, финансовые потери и нарушение репутации. Поэтому важно обучать и информировать сотрудников и пользователей о методах социальной инженерии, соблюдать строгие политики безопасности, обновлять программное обеспечение и постоянно следить за новыми угрозами. Только путем всестороннего подхода и постоянного осознания рисков можно обеспечить надежную защиту от атак на базе социальной инженерии.

Использованная литература:

1. Алиева М.Ф. Информационная безопасность как элемент информационной культуры // Вестник Адыгейского государственного

университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2012. №4. С.104.
2. Боршевников А.Е. Сетевые атаки. Виды. Способы борьбы. Современные тенденции технических наук: материалы Междунар. науч. конф. — Уфа, 2011. — С. 8-13. — URL: moluch.ru/conf/tech/archive/5/1115/
3. Калмуратова, И. (2023). The role of rubrics and checklists in validation of speaking skill. Ренессанс в парадигме новаций образования и технологий в XXI веке, 1(1), 384–386. https://doi.org/10.47689/XXIA-TTIPR-vol1-iss1-pp384-386
4. Ланецкая А.Ю., & Александрова Е.Н. (2022). СОВРЕМЕННЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Международный журнал гуманитарных и естественных наук, (7-2), 192-195. doi: 10.24412/2500-1000-2022-7-2-192-195
5. Менциев А.У., & Чебиева Х.С. (2019). Современные угрозы безопасности в сети интернет и контрмеры (обзор). Инженерный вестник Дона, (3 (54)), 16.
6. Inkar, K., & Kamola, M. (2022). THE VALIDITY OF SPEAKING TESTS. Journal of new century innovations, 18(5), 199-202.
7. Kalmuratova, A., & Kalmuratova, I. (2023). THE IMPORTANCE OF VALIDATION SYSTEM IN SPEAKING TESTS. Евразийский журнал академических исследований, 3(3 Part 3), 62-64.
8. Kalmuratova, I., & Arepov, J. (2023). QARAQALPAQ HÁM INGLIS TILLERINDE ATLÍQTÍŃ KÓPLIK KATEGORIYASÍNÍŃ AŃLATÍLÍW ÓZGESHELIKLERI. Бюллетень педагогов нового Узбекистана, 1(12), 11-13.
9. Makhsetovna, K. I., & Shamuratovna, K. A. (2023). TYPES OF VALIDITY IN SPEAKING TESTS. American Journal Of Philological Sciences, 3(03), 18-21.