УДК 004.056
DOI 10.26118/2782-4586.2024.78.32.143

Асянова Светлана Рифовна
Стерлитамакский филиал Уфимского университета науки и технологий
Жигалова Яна Ивановна
Стерлитамакский филиал Уфимского университета науки и технологий

Спуфинг как угроза кибербезопасности: понятие, виды, меры противодействия

Аннотация. В данной статье подробно рассматриваются различные виды спуфинга, включая IP-спуфинг, email-спуфинг, DNS-спуфинг, VoIP-спуфинг, ARP-спуфинг и GPS-спуфинг. Каждый из этих методов анализируется с точки зрения механизмов реализации, а также потенциальных последствий для пользователей и организаций. Приведены примеры из реальной жизни, которые иллюстрируют, как злоумышленники используют эти техники для скрытия своей идентичности и осуществления мошеннических действий. Статья подчеркивает важность осведомленности о спуфинге и необходимости внедрения эффективных мер защиты для минимизации рисков, связанных с киберугрозами, а также предлагает рекомендации по повышению безопасности в цифровом пространстве.

Ключевые слова: спуфинг, IP-спуфинг, Email-спуфинг, DNS-спуфинг, VoIP-спуфинг, ARP-спуфинг, GPS-спуфинг, киберугрозы, защита данных, мошенничество.

Asyanova Svetlana Rifovna
Sterlitamak branch of Ufa University of Science and Technology
Zhigalova Yana Ivanovna
Sterlitamak branch of Ufa University of Science and Technology

Spoofing as a threat to cybersecurity: concept, types, countermeasures

Abstract. The article provides a detailed examination of various types of spoofing, including IP spoofing, email spoofing, DNS spoofing, VoIP spoofing, ARP spoofing, and GPS spoofing. Each of these methods is analyzed in terms of implementation mechanisms and potential consequences for users and organizations. Real-life examples are provided to illustrate how attackers use these techniques to conceal their identities and carry out fraudulent activities. The article emphasizes the importance of awareness regarding spoofing and the necessity of implementing effective protective measures to minimize risks associated with cyber threats, as well as offering recommendations for enhancing security in the digital space.

Key words: spoofing, IP spoofing, email spoofing, DNS spoofing, VoIP spoofing, ARP spoofing, GPS spoofing, cyber threats, data protection, fraud.

В настоящее время количество методов обмана систем и пользователей с целью получения несанкционированного доступа, распространения ложной информации или манипуляции данными, используемых телефонными мошенниками, растет с каждым днем. В последние годы такое явление как спуфинг стало одной из серьезных угроз в области информационной безопасности, затрагивающей как индивидуальных пользователей, так и организации.

Спуфинг (от англ. “spoof” – обманывать) включает в себя подделку идентификационной информации с целью обмана системы или пользователя, например, подделку IP-адресов, адресов электронной почты, веб-сайтов и даже голосовых вызовов. Спуфинг может использоваться для различных целей, включая кражу данных, распространение вредоносного ПО и финансовые мошенничества.

Существует много разновидностей данного мошенничества. IP-спуфинг – это метод, при котором злоумышленник подделывает IP-адрес отправителя пакета данных, чтобы скрыть свою настоящую личность или обойти механизмы безопасности. Этот метод часто используется в атаках типа «отказ в обслуживании» (DoS) и других формах сетевых атак. Email-спуфинг заключается в подделке адреса отправителя в электронном письме для распространения фишинговых писем, которые выглядят как сообщения от доверенных источников, чтобы обманом заставить пользователей предоставить личные данные. DNS-спуфинг (или DNS-кампинг) подразумевает подмену записей DNS, чтобы перенаправить пользователей на фальшивые веб-сайты для кражи учетных данных или распространения вредоносного ПО. VoIP-спуфинг позволяет злоумышленникам подделывать номера телефонов в голосовых вызовах, что используется для мошенничества или запугивания жертв.

Рассмотрим подробнее основные виды спуфинга. При реализации IP-спуфинга злоумышленник использует специальное программное обеспечение, чтобы изменить свой исходный IP-адрес (это может быть достигнуто с помощью утилит, таких как hping, nmap или scapy). Например, при DDoS-атаке злоумышленник может отправить пакеты на сервер, подделывая IP-адреса жертв, чтобы скрыть свое местоположение.

Злоумышленники, использующие Email-спуфинг, взаимодействуют с SMTP-серверами для отправки электронных писем с поддельным адресом отправителя. С помощью утилит вроде sendmail или специальных фишинговых инструментов они могут настроить заголовки писем так, чтобы они выглядели как отправленные от известного источника. Пример, часто встречающийся в реальной жизни: человек получает письмо от «своего друга», который говорит, что он попал в какую-либо трудную финансовую ситуацию и нуждается в деньгах. Письмо выглядит очень правдоподобно, но на самом деле это мошенник, который подделал адрес и воспользовался стилем общения близкого человека. В настоящее время этот вид мошенничества чаще реализуется через мессенджеры и социальные сети, нежели email-сервисы.

Мошенники могут использовать вредоносное ПО или эксплойты для изменения DNS-записей на целевом сервере или маршрутизаторе. Это достигается через «слабые», менее защищенные места в программном обеспечении, в таком случае можно получить доступ к учетной записи администратора. Например, при попытке зайти на сайт банка, вместо этого можно попасть на поддельный сайт, созданный злоумышленником: DNS-записи маршрутизатора изменены, чтобы перенаправить абоненты на фальшивую страницу, которая выглядит как настоящая. При вводе учетных данных, они попадают к мошеннику.

Часто встречается использование VoIP-систем и специальных приложений для изменения номера телефона, который отображается на экране жертвы. Это можно сделать с помощью программного обеспечения вроде Caller ID Spoofing, которое позволяет вводить любой номер телефона в качестве идентификатора вызывающего абонента. На данный момент наиболее распространена схема, когда звонит человек, представляющийся службой безопасности вашего банка, и говорит, что данные были скомпрометированы и просит подтвердить личность. На самом деле это мошенник, который использует VoIP-спуфинг, чтобы скрыть свое истинное местоположение и номер телефона. Если предоставить ему персональные данные, он сможет получить доступ к финансам.

Некоторые злоумышленники отправляют ложные ARP-ответы в локальную сеть, связывая свой MAC-адрес с IP-адресом другого устройства (например, маршрутизатора), с целью перехватить трафик между устройствами в сети. Так можно увидеть все передаваемые данные, включая пароли и конфиденциальную информацию, что ставит под угрозу безопасность всей сети. Кроме этого, мошенники нередко используют специальные устройства или программное обеспечение для передачи ложных сигналов GPS с помощью радиочастотного оборудования или программных решений, которые имитируют GPS-сигналы. Например, во время работы с навигационным приложением в повседневной жизни

злоумышленник может перенаправить устройство на неправильный маршрут или даже в небезопасное место, что может вызвать путаницу и потенциально привести к ситуациям, угрожающим здоровью.

Приведенные примеры показывают разнообразие методов реализации спуфинга и их потенциальные последствия в реальной жизни. Спуфинг может иметь серьезные последствия как для отдельных пользователей, так и для организаций. Во-первых, это кража данных, утечка конфиденциальной информации, такой как пароли, номера кредитных карт и личные данные. Во-вторых, значительные финансовые потери. В-третьих, наносимый ущерб репутации организации или отдельному человеку, вследствие чего доверие клиентов и деловых партнеров может быть подорвано. Наконец, речь идет о правовых последствиях – уголовная ответственность и судебные разбирательства. Спуфинг представляет собой серьезную угрозу в современном цифровом мире. Понимание его механизмов и методов реализации является ключевым для разработки эффективных стратегий защиты. Комплексный подход к информационной безопасности, включающий технические меры и обучение пользователей, может значительно снизить риски, связанные со спуфингом, и защитить как индивидуальных пользователей, так и организации от потенциальных угроз.

Для предотвращения спуфинга используются различные меры безопасности – от двухфакторного подключения и шифрования до обучения пользователей методам распознавания фишинговых атак и других форм спуфинга. Безусловно, необходимо применять комплексный подход. Использование методов аутентификации, таких как SPF (Sender Policy Framework) и DKIM (DomainKeys Identified Mail), может остановить email-спуфинг, шифрование данных также помогает защитить информацию от перехвата. Обучение граждан основам информационной безопасности может значительно снизить риск успешных атак. Пользователи должны быть осведомлены о методах социальной инженерии и фишинга, а регулярный мониторинг сетевого трафика поможет выявить подозрительные активности и предотвратить атаки до того, как они нанесут ущерб. Своевременное обновление программного обеспечения и систем безопасности помогает устранить уязвимости, которые могут быть использованы злоумышленниками для спуфинга.

Спуфинг представляет опасность для людей всех возрастов, но последствия и уязвимость могут варьироваться в зависимости от возрастной группы. Рассмотрим, как спуфинг может повлиять на разные возрастные категории. Дети и подростки, мало осведомленные о киберугрозах, являются одной из наиболее уязвимых групп населения. Мошенники пользуются наивным восприятием мира подростков и создают ложные аккаунты в социальных сетях, чтобы завести дружбу и получить личную информацию, а затем манипулировать или даже шантажировать. Нередко это доходит до кибербуллинга и маниакального преследования детей, что приводит к психологическим травмам. Молодые люди и взрослые, активно использующие приложения онлайн-банков и электронные денежные переводы, становятся жертвами финансовых мошенничеств через подделку адресов электронной почты или веб-сайтов. Часто молодые профессионалы могут столкнуться с проблемами в карьере из-за подделки их личных данных или репутации в интернете. Пожилые люди, легко подвергаемые психологическим манипуляциям, менее знакомы с инновационными технологиями и киберугрозами, что делает их более уязвимыми к спуфингу и мошенничеству. Ежедневно спуфинг приводит к значительным финансовым потерям, особенно если пожилые люди доверяют поддельным звонкам или письмам от «банков» или «государственных учреждений». Жертвы спуфинга могут испытывать стресс, тревогу и страх за себя и безопасность близких людей, что может негативно сказаться на их общем состоянии здоровья. Спуфинг подрывает доверие пользователей к онлайн-сервисам, что влияет на их желание использовать цифровые технологии. В некоторых случаях жертвы могут стать невольными участниками преступлений, если их данные будут использованы злоумышленниками. Спуфинг представляет собой большую угрозу для всех возрастных групп, но особенно уязвимыми

являются дети, пожилые люди и те, кто недостаточно осведомлен о киберугрозах. В связи с этим профилактика спуфинга на бытовом уровне, несомненно, обретает все большую значимость. Приведем несколько эффективных форм профилактики:

- Обучение. Изучение и информирование окружающих о различных формах спуфинга (например, фишинг, вишинг, смс-фишинг) и способах их распознавания. Обсуждение с членами семьи потенциальных угроз и способы их предотвращения.
- Использование надежных паролей. Создание уникальных и сложных паролей для каждого аккаунта: использование комбинаций букв, цифр и специальных символов, менеджеров паролей для хранения и генерации безопасных паролей.
- Двухфакторная аутентификация (2FA). Активация двухфакторной аутентификации на всех поддерживаемых сервисах, что добавляет дополнительный уровень защиты, требуя подтверждения входа через SMS или приложение.
- Проверка источников. Проверка адреса электронной почты и ссылки на соответствие официальным доменам перед тем, как кликнуть на них. В случае подозрительных сообщений или звонков, рекомендуется перезвонить на официальный номер компании для подтверждения.
- Защита личной информации. Ограничение количества личной информации, которая публикуется в социальных сетях и на других платформах. Постоянный контроль настроек конфиденциальности на личных аккаунтах и изменение их для повышения безопасности.
- Использование антивирусного программного обеспечения. Защита от вредоносных программ и фишинговых атак путем регулярного обновления операционной системы и программ для защиты от распространенных кибератак.
- Осторожность при открытии вложений. Максимальная бдительность при работе с файлами, полученными по электронной почте или через мессенджеры, особенно если они поступили от незнакомых отправителей.
- Регулярный мониторинг аккаунтов. Периодическая проверка личных аккаунтов на наличие подозрительной активности или несанкционированных входов.

В последние годы наблюдается рост числа киберпреступлений в России, включая фишинг, спуфинг, атаки на банковские системы и утечки данных. По данным различных исследований, киберпреступления могут наносить значительный ущерб как частным лицам, так и организациям. Процентное соотношение различных типов киберпреступлений может варьироваться, однако на основе данных до 2023 года, можно выделить следующие общие категории киберпреступлений и их примерное соотношение:

1. Фишинг: 30-50% всех кибератак (атаки, направленные на получение конфиденциальной информации, такой как пароли и данные кредитных карт). По данным отчета APWG (Anti-Phishing Working Group), в 2022 году было зафиксировано более 1,5 миллиона фишинговых атак [CNews].
2. Вредоносное ПО (Malware): 20-30% всех кибератак (вирусы, трояны, шпионские программы и другие виды вредоносного программного обеспечения). Согласно отчету SonicWall, в 2022 году было обнаружено более 10 миллиардов атак вредоносного [clickfraud].
3. Атаки на систему (Hacking): 10-20% всех кибератак (несанкционированный доступ к системам и данным). В отчете Verizon о нарушениях безопасности (DBIR) за 2022 год было указано, что около 15% инцидентов связаны с несанкционированным доступом [Каспарьянц, 2021].
4. DDoS-атаки (Distributed Denial of Service): 5-10% всех кибератак (перегрузка серверов и сетей, что приводит к недоступности сервисов). По данным Cloudflare, в 2022 году было зафиксировано более 10 миллионов DDoS-атак, что на 50% больше по сравнению с предыдущим годом. Кроме этого, в том же году было зафиксировано несколько крупных DDoS-атак на российские ресурсы [Информационная безопасность, 2024].

5. Кража данных: 5-10% всех кибератак (утечки и кража личной информации пользователей и организаций). В отчете IBM о стоимости утечек данных за 2022 год указано, что средняя стоимость утечки данных составила $4,35 миллиона, при этом большинство инцидентов связано с кражей личной информации [Тейт, 2023].

6. Спуфинг: 2-5% всех кибератак (подмена идентификаторов для обмана пользователей или систем). Согласно различным отчетам, подобные атаки составляют меньшую часть от общего числа инцидентов.

Сравнительная таблица, рис. 1.

Вид киберпреступления	Мировые показатели (%)	Российские показатели (%)
Фишинг	30-50	40-60
Вредоносное ПО	20-30	25-35
Атаки на систему	10-20	10-15
DDoS-атаки	5-10	5-10
Кража данных	5-10	5-10
Спуфинг	2-5	2-5

В Российской Федерации ответственность за спуфинг, который подразумевает подмену адреса отправителя или иного обмана с целью получения доступа к информации или совершения мошеннических действий, может быть предусмотрена несколькими статьями Уголовного кодекса РФ и другими нормативными актами:

- Статья 159. Мошенничество;
- Статья 272. Неправомерный доступ к компьютерной информации;
- Статья 273. Создание, использование и распространение вредоносных программ [УК РФ].

Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных Административного кодекса Российской Федерации может применяться в случае нарушения правил использования средств связи, включая методы спуфинга [КоАП РФ].

Таким образом, за спуфинг в России предусмотрена уголовная и административная ответственность, которая зависит от конкретных обстоятельств дела и последствий действий правонарушителя. Защиту персональных данных от несанкционированного доступа к ним регулирует Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [Собрание законодательства России].

Стоит обратить внимание на то, что ответственность родителей за действия несовершеннолетних, в том числе за совершение преступлений, таких как спуфинг, регулируется несколькими статьями Уголовного кодекса и Гражданского кодекса России. Согласно статье 20 Уголовного кодекса РФ, уголовная ответственность наступает с 16 лет, а для некоторых преступлений – с 14 лет. Если несовершеннолетний совершил преступление, например, спуфинг (который может быть квалифицирован как мошенничество или другое преступление), он может быть привлечен к уголовной ответственности [УК РФ]. Согласно статье 1073 Гражданского кодекса РФ, родители или законные представители несут ответственность за вред, причиненный их детьми, если не смогут доказать, что они не могли предотвратить это действие. В случае, если несовершеннолетний совершил преступление, родители могут быть привлечены к гражданской ответственности за ущерб, причиненный третьим лицам [ГК РФ]. Также следует учитывать, что родители обязаны воспитывать своих детей и контролировать их поведение. Если будет установлено, что родители не исполняли свои обязанности должным образом, это может повлечь за собой дополнительные меры со стороны органов опеки и попечительства.

В заключение отметим, что основная идея спуфинга заключается в том, чтобы выдать себя за другого человека или устройство, чтобы получить доступ к защищенной информации, обойти меры безопасности или совершить мошеннические действия. Спуфинг, как один из видов киберпреступлений, включает подмену адресов электронной

почты, IP-адресов и других идентификаторов для обмана пользователей или систем. Хотя точные данные о проценте спуфинга в общем объеме киберпреступлений могут варьироваться, по оценкам экспертов, фишинговые атаки (которые часто используют спуфинг) составляют значительную долю от общего числа кибератак. Образование и осведомленность о методах защиты являются ключевыми факторами в снижении рисков, связанных со спуфингом.

Список источников

1. APWG. Anti-Phishing Working Group (Антифишинговая рабочая группа. Рабочая группа по борьбе с фишингом). – Текст: электронный // Индексная книга (каталог) CNews. URL: clck.ru/3F83u2 (дата обращения: 09.12.2024)
2. Cloudflare подверглась сильным DDoS-атакам в сентября. – Текст: электронный // Информационная безопасность. – 2024. URL: https://www.itsec.ru/news/cloudflare-podverglas-silnim-ddos-atakam-v-sentiabria (дата обращения: 09.12.2024)
3. Вирусы-вымогатели (шифровальщики) Ransomware. – Текст: электронный // TADVISER. URL: https://clck.ru/3F83va (дата обращения: 09.12.2024)
4. Гражданский кодекс Российской Федерации (часть первая): от 30.11.1994 № 51-ФЗ (ред. от 16.12.2019) // Собрание законодательства РФ. – 05.12.1994. – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.
5. Каспарьянц Д. Обзор ежегодного отчета компании VERIZON по результатам расследования утечки данных и первого отчета по кибершпионажу. – Текст: электронный // Научно-технический центр ФГУП «ГРЧЦ». – 2021. – URL: https://rdc.grfc.ru/2021/07/verizon-report/ (дата обращения: 09.12.2024)
6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 02.08.2019) // Собрание законодательства РФ. – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.
7. О персональных данных: федеральный закон от 27 июля 2006 г. N 152-ФЗ // Собрание законодательства Российской Федерации. — 2006. — № 31 (часть I). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.
8. Статистика вредоносных программ 2023. – Текст: электронный // lickfraud. URL: https://clickfraud.ru/statistika-vredonosnyh-programm-2023/ (дата обращения: 09.12.2024)
9. Стоимость утечки данных. – Текст: электронный // IPBurger. – 2022. URL: https://www.ipburger.com/ru/blog/the-cost-of-a-data-breach-2022/ (дата обращения: 09.12.2024)
10. Уголовный кодекс Российской Федерации [Текст]: от 13.06.1996 № 63-ФЗ (ред. от 07.04.2020) // Собрание законодательства РФ. – 17.06.1996. – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

Информация об авторах

Асянова Светлана Рифовна, канд. пед. наук, Стерлитамакский филиал Уфимского университета науки и технологий, г. Стерлитамак, Россия.
Жигалова Яна Ивановна, магистрант, Стерлитамакский филиал Уфимского университета науки и технологий, г. Стерлитамак, Россия.

Information about the authors

Asyanova Svetlana Rifovna, Candidate of Pedagogical Sciences, Sterlitamak Branch of Ufa University of Science and Technology, Sterlitamak, Russia.
Zhigalova Yana Ivanovna, Master's student, Sterlitamak Branch of Ufa University of Science and Technology, Sterlitamak, Russia.