УДК 004.056.5
DOI: 10.21122/2309-4923-2023-3-48-54

ВАСИЛЬЕВ А.В.

ПРИЧИНЫ РОСТА КОЛИЧЕСТВА КИБЕРАТАК: АНАЛИЗ ТЕХНИЧЕСКИХ И НЕТЕХНИЧЕСКИХ ФАКТОРОВ

ЗАО «НАУЧСОФТ»
г. Минск, Республика Беларусь

Данная статья представляет анализ как технических, так и нетехнических факторов, способствующих нарастанию объема и разнообразия кибератак. Социальное взаимодействие в интернете способствует увеличению частоты кибератак и усугубляет разрушительные последствия, касающиеся не только технических аспектов, но и общественных и личных сфер. Ошибки и уязвимости в программном обеспечении, а также недостатки в сетевых протоколах, создают постоянную угрозу для безопасности, особенно в условиях растущего числа подключенных устройств и сложности управления критическими системами. Динамическая природа атак и постоянное развитие методов проникновения делают киберугрозы чрезвычайно адаптивными к условиям современной сетевой среды.

Дополнительно, расширенное использование социальных сетей и виртуализация социальной жизни с одной стороны приносят больше комфорта, но с другой стороны, создают плодотворную почву для кибератак, увеличивая объем доступной информации для потенциальных злоумышленников. Повышение технической грамотности злоумышленников предоставляет им новые инструменты для нарушения цифровой безопасности. Наряду с этим, недостаточное осведомление и небрежное поведение пользователей в интернете ставят под угрозу защиту персональных и конфиденциальных данных.

Данная работа доказывает, что киберриски увеличиваются как из-за постоянных технологических изменений в мире, так и из-за человеческих действий. Понимание динамики данных факторов становится критически важным для разработки более эффективных мер по защите цифровой среды.

Ключевые слова: *кибербезопасность; кибератаки; киберугрозы; сетевая безопасность*

В последние годы ежедневное использование Интернета стремительно возросло по всему миру. Этот рост привел к переносу повседневной жизни и в цифровой мир. Недавняя глобальная эпидемия COVID-19 лишь устрокила этот процесс. К примеру, люди теперь заводят дружеские отношения в социальных сетях, пользуются онлайн-банкингом и проводят встречи и семинары онлайн (рис. 1). Подобные условия создали идеальный фундамент для переноса преступной деятельности из визического мира в мир виртуальный.

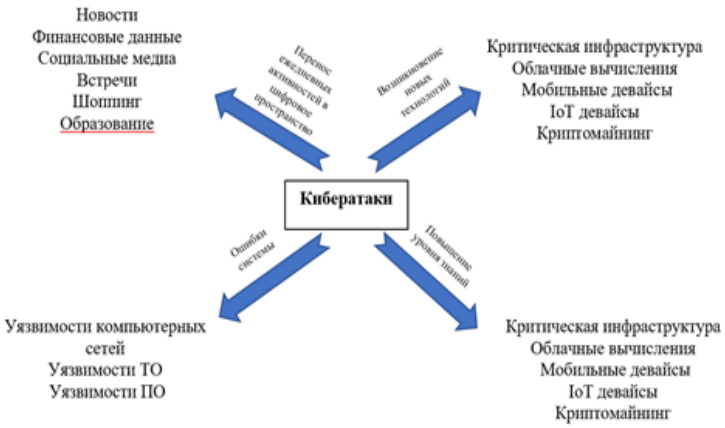


Рисунок 8. Временные параметры удержания контактов: размах T_H (*а*), $\mu(T_H)$ (*б*) и $c_v(T_H)$ (*в*)

Киберпреступления совершаются лицами или организованными группами, известными как хакеры. Хакеры обладают глубоким знанием операционных систем, могут быстро писать компьютерные программы и выявлять уязвимости других программ и систем в кротчайшие сроки. Развитие новых инструментов для кибератак, а также экономическая выгода постоянно мотивируют злоумышленников совсершать все новые преступления. Согласно последним исследованиям, ущерб, причиняемый кибератаками мировой экономике, измеряется сотнями миллиардов долларов и увеличивается ежегодно. Из-за упомянутых выше причин кибератаки учащаются с каждым днем. Прежде всего полезно рассмотреть

основные причины увеличивающие частотность кибератак. Основные причины кибератак можно перечислить следующим образом (рис. 1):

• причины, вызванные существующими ошибками системы;

• причины, обусловленные новыми технологиями;

• причины, вытекающие из увеличения уровня знаний;

• перенос повседневной жизни в цифровую среду;

• атаки не имеют географических границ, что затрудняет их выявление.

1.1. Причины, обусловленные существующими ошибками системы

Основной причиной для стремительного роста кибератак служит сама структура компьютерных систем и коммуникационных сетей. Уязвимости, дефекты и некорректные конфигурации в устройствах, программном обеспечении и компьютерных сетях становятся главной причиной для кибератак. Можно с уверенностью констатировать, что современные компьютерные системы стали практически беззащитны для кибератак из-за большим количества уязвимостей в программном обеспечении и дефектов в протоколах компьютерных сетей. Кроме того, пользователи, не обладающие базовыми знаниями о цифровой среде и способах использования компьютерных систем, также создают условия для увеличения количества кибератак. Причины, вытекающие из существующих ошибок системы, классифицируются на три группы: атаки, вызванные уязвимостями технических устройств, атаки, вызванные программными ошибками, и атаки, вызванные уязвимостями в компьютерных сетях.

• *Атаки, вызванные уязвимостью технических устройств.* Атаки, инициированные дефектами и ошибками технических устройств (hardware), сложнее предотвратить, потому что программные инструменты недостаточны для выявления и предотвращения подобных атак. Часто троянские конь является самым эффективным способом для осуществления кибератаки. Данный вредоносный вариант ПО приводит к чрезмерному использованию ресурсов компьютера, снижает производительность и может вызвать отключение системы путем потребления избыточного количества электроэнергии [1]. Более того, незаконное копирование аппаратных компонентов и приобретение ненадежных компонентов у нелицензированного провайдера создают дополнительные трудности для кибербезопасности.

Взаимосвязь аппаратных компонентов и сложности в архитектуре интегральных схем затрудняют обнаружение уязвимостей, связанных с техническими устройствами. Изменение всего лишь одной интегральной схемы может повлиять на множество компонентов и остаться незамеченным на протяжении длительного времени [2]. По этой причине обнаружение и реагирование на кибератаки, которая использует аппаратную уязвимость, является крайне сложной задачей. Использование устройств с встроенной защитой от вскрытия и нанесение водяных меток на устройства продолжает оставаться наиболее эффективными способы предотвращения подобных кибератак [3].

• *Атаки, вызванные ошибками программного обеспечения.* Большинство кибератак до сих пор вызваны ошибками, уязвимостями и дефектами в прикладном программном обеспечении (ПО). Количество подобных уязвимостей и ошибок увеличивается каждый день [4, 5]. Основные причины уязвимостей, связанных с программным обеспечением, можно перечислить следующим образом:

• ошибки валидации ввода;

• проблемы с контролем доступа пользователя;

• неполная или неправильная аутентификация;

• проблемы с каталогами миграций;

• переполнение буфера;

• проблемы с SQL;

• межсайтовые скрипты (XSS);

• использование компонентов с известными уязвимостями;

• проблемы с веб-сервисами и API;

• неправильное тестирование безопасности программного обеспечения.

Программное обеспечение разрабатывается стремительно, но проверок безопасности часто недостаточно как на этапе разработки, так и на этапе тестирования. Недостаток знаний команд разработчиков о безопасных процессах разработки ПО является дополнительным фактором для увеличения киберрисков. Использование приложений на разных платформах и устройствах также создают уязвимости, которые увеличивают риск нанесения программно-ориентированной атаки. Например, добавление в буфер большего объема данных может привести к несанкционированному доступу пользователей к системе или потере данных [6]. Внедрение SQL-кода может перегружать базы данных и приводить к краже имен пользователей, паролей и информации о кредитных картах.

Регулярное обновление программного обеспечения является наиболее рекомендуемым методом устранения ошибок и дефектов, но и оно не всегда способно помочь. Во время обновлений ПО ошибки и уязвимости не всегда устраняются; в некоторых случаях обновления могут стать причиной для появления новых уязвимостей. Самый эффективный способ минимизировать программно-ориентированные атаки заключается в разработке дизайна программы без ошибок (error-free program design) и формулирование четких требований перед написанием кода в жизненном цикле процесса разработки программного обеспечения. Крайне важно, чтобы разработчики ПО проходили обучение по безопасному процессу разработки. Создание ПО в кратчайшие сроки и попытка

позже исправить уязвимости безопасности — это не верный подход. По этой причине, угрозы безопасности следует учитывать с самого начала процесса разработки программного обеспечения, и весь код должен проходить ручное и автоматическое тестирование на каждом этапе. Для примера, Microsoft сделала использование этапов жизненного цикла разработки безопасности (Security Development Life Cycle, SDL) обязательным, что существенно уменьшило количество ошибок и уязвимостей в процессе разработки программного обеспечения. Операционная система Windows Vista, разработанная с применением SDL, содержит приблизительно на 45 % меньше ошибок и уязвимостей, чем Windows XP, написанная без использования SDL [7].

• *Атаки, вызванные уязвимостями компьютерных сетей.* Во время передачи данных онлайн хакеры могут получить доступ к данным и полностью их изменить. Основной причиной таких угроз является использование ранее созданных протоколов компьютерных сетей и устройств, в которых проблемы безопасности не учитывались вовсе. Подавляющее большинство атак на компьютерные сети возникают из-за уязвимостей в сетевых протоколах, таких как TCP, IP, ARP, DHCP и DNS. Например, так как при передаче пакетов по сети с использованием IP не предусмотрена структура для контроля точности и конфиденциальности пакетов, информация в пакетах может быть раскрыта и изменена в процессе передачи. Аналогично, поскольку DNS-ответы не проверяются, преступники могут создавать поддельные серверы, и пользователи могут подключаться к этим поддельным серверам вместо фактического сервера. Злоумышленники также могут отправлять избыточные запросы к DNS-серверам, делая их недоступными для законных пользователей. Кроме того, хакеры могут перехватывать информацию во время передачи данных из-за неполной или неправильной конфигурации сетевых устройств, включая коммутаторы, маршрутизаторы и беспроводные точки доступа. Уязвимости существующих протоколов должны быть исправлены, необходимо добавление новых протоколов, а также корректная и тщательная настройка сетевых устройств для защиты данных при их передвижении по компьютерной сети. Часто используемые методы кибербезопасности для минимизации атак на сеть могут быть перечислены следующим образом:

• использование шифрования;

• использование списков контроля доступа (ACL);

• использование виртуализации и виртуальных локальных сетей (VLAN);

• использование брандмауэра;

• использование систем обнаружения, предотвращения и защиты от вторжений (IDPS);

• использование устройств для веб-безопасности (WSA);

• использование устройств для защиты электронной почты (ESA);

• использование виртуальной частной сети (VPN);

• использование протоколов защиты транспортного уровня (TLS) и защищенного сокетного уровня (SSL).

Хотя с помощью этих методов и можно достичь определенной степени безопасности, нельзя сказать, что они способны гарантировать полную защиту.

1.2. Причины, вызванные развивающимися технологиями

С быстрым развитием технологий в интернет ежедневно добавляются новые устройства и приложения: смартфоны, планшеты, стационарные и портативные компьютеры, устройства Интернета вещей (IoT) и облачные технологии. Создание множества новых приложений за короткий промежуток времени и добавление новых устройств в компьютерные сети значительно увеличило количество кибератак. Кроме того, хранение информации, принадлежащей разным компаниям, в одной облачной среде, а также управление и обслуживание этих облачных решений силами сторонних организаций, также создает дополнительные бреши в системе безопасности. Причины, обусловленные развитием новых технологий, можно перечислить следующим образом:

• *Увеличение числа смартфонов.* Количество используемых смартфонов на сегодняшний день составляет приблизительно 6 миллиардов. Личные данные, хранящиеся на этих устройствах, постоянно растущее количество разработанных для них программных приложений и использование беспроводных сетей для доступа в Интернет делают эти устройства привлекательными целями для злоумышленников. Согласно отчетам о киберугрозах от компаний Symantec [8] и McAfee [9], количество вредоносного программного обеспечения, созданного для смартфонов, стремительно растет ежегодно. Также стоит отметить, что многие из вредоносных программ, изначально написанных для компьютеров, часто адаптируются и используются для атак на смартфоны.

• *Увеличение числа устройств IoT.* Умные устройства, такие как умные очки, смарт-часы и системы автоматизации, известные как Интернет вещей (IoT) становятся все более распространенными. Количество устройств, подключенных к Интернету на основе технологии IoT, предположительно в ближайшее время достигнет около 50 миллиардов. Большой объем данных, генерируемых этими устройствами, делает защиту компьютерных сетей чрезвычайно сложной задачей.

• *Увеличение использования облачных решений.* Облачные вычисления стали новой технологией, которая развилась относительно недавно. Такие компании как Amazon, IBM Cloud, Google, Rackspace, Microsoft и Salesforce предоставляют широкий

выбор облачных решений. Облачные решения легко использовать, они доступны на любых устройствах и в любых местоположениях, а тарифные планы гибки и масштабируемы в соответствии с потребностями конечных пользователей. Кроме того, обслуживание, ремонт и обновления осуществляются непосредственно поставщиками этих решений. Однако, подобные средства также часто сталкиваются с рисками кибератак. Такие проблемы обычно возникают по следующим причинам:

• компании и организации, использующие облачные решения, теряют прямой контроль над данными;

• использование одних и тех же физических ресурсов для разных компаний;

• технические трудности, вызванные использованием виртуальных машин;

• атаки происходят при передаче данных через компьютерную сеть.

В случае если данные хранятся в облачной среде, конечный пользователь полностью теряет прямой контроль над данными. Другими словами, пользователи не знают, где хранятся их данные и какие меры безопасности предприняты для их защиты. Так как несколько отдельных клиентов могут использовать одну и ту же инфраструктуру, пользователь может угрожать другому пользователю и получить доступ к его данным. С другой стороны, монитор виртуальных машин (VMM) – это своего рода промежуточное программное обеспечение, которое позволяет создавать несколько виртуальных машин на одних и тех же физических серверах. Возможные уязвимости были выявлены, например, во многих популярных VMM, таких как Xen, VMware и Microsoft Hyper-V. Например, уязвимость в Xen может позволить злоумышленнику запускать произвольный код с правами «root» [10]. Кроме того, VMM не может обеспечить полную изоляцию между виртуальными машинами. Поэтому выше упомянутая уязвимость продолжают представлять угрозу в облачной среде. Собственно, именно по этой причине и существует определенные сомнения в безопасности хранения данных в облаке.

• *Увеличение числа систем критической инфраструктуры.* Критическая инфраструктура является одной из наиболее важных систем, необходимых современному обществу для бесперебойной повседневной деятельности. К примерам подобных систем можно отнести производственные и распределительные системы энергии, финансовые услуги, систему здравоохранения, а также систему водоснабжения и канализации. Серьезные нарушения в этих системах способны кардинальным образом повлиять на общество и жизнь людей. Согласно проведенным исследованиям в последние годы, можно наблюдать существенный рост как числа, так и размера ущерба от кибератак направленных против систем критической инфраструктуры. Обеспечение безопасности систем критической инфраструктуры имеет серьезные трудности из-за структурной сложности, географического расположения и необходимости эффективной работы всех элементов системы с помощью интернета. Причины увеличения кибератак на системы критической инфраструктуры могут быть перечислены следующим образом:

• угрозы, вызванные характером систем критической инфраструктуры;

• угрозы, связанные с использованием компьютерных сетей при передаче данных;

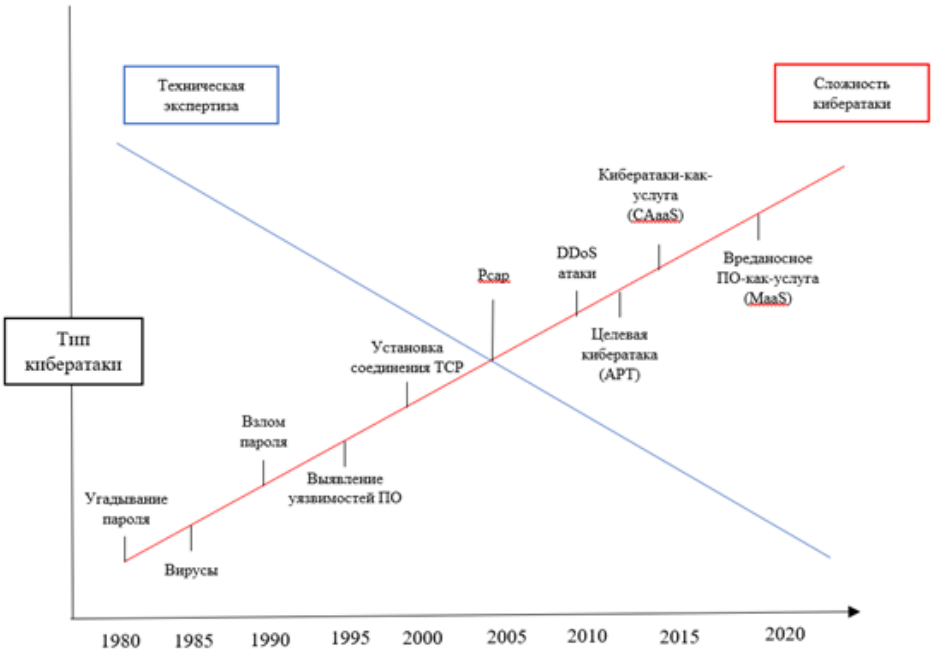
• угрозы, возникающие из-за протоколов связи, используемых в системах SCADA;

• угрозы, связанные с круглосуточной доступностью систем критической инфраструктуры.

Критическая инфраструктура имеют сложную структуру, состоящую из множества компонентов, не используемых в других системах. Эта сложность и уникальные характеристики приводят к угрозам безопасности, которых нет в других системах. Кибератаки на системы критической инфраструктуры нацелены на корпоративные сети, центры управления SCADA и удаленные подстанции. Атака на любую из этих систем может поставить под угрозу функционирование всей системы. Например, атака на датчики, расположенные на подстанциях, может сделать недоступными или полностью лишить контроля дистанционные терминальные устройства. Атака на центр SCADA может позволить третьим лицам взять всю систему под контроль. Кроме того, протоколы связи, такие как Modbus/TCP и DNP3, используемые в системах SCADA, уязвимы для новых типов кибератак. К примеру, передаваемые по этим протоколам данные не шифруются, что позволяет получить несанкционированный доступ к этим данным и изменить их [11].

1.3. Причины, обусловленные увеличением знаний

С увеличением знаний запуск атаки стал более доступным. В 1990-х и начале 2000-х годов было сложно осуществлять атаки на компьютерные системы. Только эксперты с обширными знаниями и опытом в данной области могли атаковать компьютеры. В последние несколько лет стало гораздо проще инициировать кибератаки из-за появления широкого набора инструментов для атак, быстрого распространения знаний и легкости обнаружения уязвимостей в программном обеспечении и сетевых протоколов. Сегодня даже обычные люди, которые не обладают большими знаниями о компьютерных системах, известные как "script kiddies" («скриптовые мальчики»), могут запускать атаки с использованием платформ для кибератак-как-сервис (Cyber Attack-as-a-service, CAaaS). Большинство из таких платформ доступны в Интернете. Рисунок 2 сравнивает сложность атаки с техническими знаниями атакующего [12,13]. Как показано на рисунке 2, сложность атак увеличивается, в то время как уровень технической экспертизы злоумышленников снижается.



1.4. Перенос повседневной жизни в цифровую среду

Социальная жизнь в последние годы все больше переходит в виртуальную среду, и пандемия COVID-19 лишь ускорила этот процесс. Сегодняшние люди всех возрастов проводят значительное количество времени в интернете, занимаясь свои повседневными активностями. Кроме того, многие начинают свой день со входа в интернет и продолжают проводить большую часть времени онлайн. Перенесенные на сегодняшний день в интернет-среду активности могут быть категоризированы следующим образом:

- Виртуализация социальных отношений в социальных медиа;
- финансовые данные и виртуализация денег;
- виртуализация деловых встреч;
- виртуализация образования;
- виртуализация новостей;
- виртуализация политики;
- виртуализация покупок;
- виртуализация военных конфликтов;
- виртуализация игр.

Использование социальных медиа, таких как Twitter, Facebook и Instagram, быстро распространяется по всему миру. Многие люди проводят значительную часть своей жизни в социальных медиа, которые хранят важную личную информацию о пользователях, включая их имя, фамилию, дату рождения, адрес и место жительства. Распространение изображений и видео о себе уже стало абсолютно привычным для пользователей. Владельцы социальных медиа хранят эти данные в больших центрах обработки данных, которые находятся под управлением сторонними компаниями. Однако, в то время как эти данные передаются по сети, они могут быть украдены из центров обработки данных или использоваться управляющими компаниями для своих целей.

Исследователи обнаружили, что многие пользователи социальных медиа получают нежелательные электронные письма (спам), и более 50 % крупных организаций сталкиваются с увеличением кибератак из-за избыточного распространения информации их сотрудниками в социальных медиа. Большинство вредоносных программ и вирусов в социальных медиа распространяются через новостную ленту, изображения или видео [14,15]. Кроме того, злоумышленники могут использовать неактивные учетные записи в социальных медиа для запуска новых атак.

Виртуализация финансовых операций также стремительно выросла за последние годы, во многом из-за широкого использования банковских карт и интернет-банкинга. Операции в банковской сфере в основном выполняются онлайн с использованием прикладных программ. Деньги на банковских счетах виртуальны, состоят из математических чисел, которые увеличиваются или уменьшаются во время онлайн-транзакций. Использование виртуальной валюты или криптовалют в онлайн-транзакциях также приводит к увеличению кибератак. Миллионы долларов каждый год похищаются киберпреступниками из-за технических сбоев и ошибок пользователей во время переводов денежных средств между счетами в виртуальных средах. Кибератаки на криптовалюты также происходят все чаще и приносят потери в размере сотен миллионов долларов ежегодно. Например, биржа криптовалют Coincheck была взломана, а ущерб от данной кибератаки составил около 550 миллионов долларов [16,17].

1.5. Отсутсвие четкого географического месторасположения как усложняющий фактор для обнаружения кибератак

Киберпреступники совершают атаки и попытки взлома круглосуточно из любого места в мире без каких-либо географических ограничений. Хакеры используют специфические техники, чтобы скрыть свое местоположение. Более того, отсутствие четких международных законов, которые бы удерживали страны от кибератак, лишь поощряет киберпреступников. Легкость проведения атак в интернете, отсутствие географических границ и отсутствие законодательства между странами относительно наказания киберпреступников также следует считать важными факторами для увеличения количества кибератак в мире.

Заключение

Данная статья обрисовывает широкий спектр технических и нетехнических факторов, стоящих за возрастающим количеством кибератак. Эволюция киберугроз демонстрирует их адаптивность и гибкость, что приводит к постоянным изменениям в способах атак и их целях, охватывая все уровни компьютерных систем и цифровой экосистемы интернета. Современная виртуализация социальных взаимодействий, а также активное использование социальных сетей, вносят новые грани в динамический портрет киберугроз.

Ошибки в программном обеспечении, уязвимости сетевых протоколов и растущее количество подключенных устройств усиливают постоянное нарастание рисков для кибербезопасности. Однако этот рост угроз также способствует и росту инноваций в области киберзащиты, мотивируя создание более надежных систем и более эффективных методов борьбы с кибератаками.

Следует подчеркнуть, что количество кибератак в мире, скорее всего, будет продолжать возрастать, по мере того как цифровой ландшафт будет и дальше расширяться. Данная проблема требует приложения дополнительных усилий в области кибербезопасности, развития новых технологий и методов, а также повышения осведомленности пользователей. Ответ на вызовы киберугроз потребуют от нас сотрудничества, дополнительного обучения и инвестиций, чтобы обеспечить безопасное и устойчивое цифровое будущее.

ЛИТЕРАТУРА / REFERENCES

1. **Karri, R.; Rajendran, J.; Rosenfeld, K.; Tehranipoor, M.** Trustworthy Hardware: Identifying and Classifying Hardware Trojans. Computer; 2010; 43, pp. 39-46. DOI: https://dx.doi.org/10.1109/MC.2010.299

2. **Weforum.** Available online: https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/ (accessed on 1 January 2023).

3. **Tehranipoor, M.; Wang, C.** Introduction to Hardware Security and Trust; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2011.

4. **McGraw, G.** Building secure software: Better than protecting bad software. IEEE Softw.; 2002; 19, pp. 57-58. DOI: https://dx.doi.org/10.1109/MS.2002.1049391

5. **Aslan, Ö.** How to decrease cyber threats by reducing software vulnerabilities and bugs. Proceedings of the 1st International Mediterranean Science and Engineering Congress, Çukurova University; Adana, Turkey, 26–28 October 2016; pp. 639-646.

6. **Aslan, O.; Samet, R.** Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs. Proceedings of the IEEE 2017 International Conference on Cyberworlds; Chester, UK, 20–22 September 2017; pp. 222-225. DOI: https://dx.doi.org/10.1109/cw.2017.22

7. **Techsurface.** Available online: http://techsurface.com/2010/01/microsoft-security-development-lifecycle-sdl.html (accessed on 1 January 2023).

8. **Broadcom.** Available online: https://docs.broadcom.com/docs/istr-21-2016-en/ (accessed on 1 January 2023).

9. **Mcafee.** Available online: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf (accessed on 1 January 2023).

10. **Padhy, R.P.; Manas, R.P.; Suresh, C.S.** Cloud computing: Security issues and research challenges. Int. J. Comput. Sci. Inf. Technol. Secur.; 2011; 1, pp. 136-146.

11. **Alcaraz, C.; Zeadally, S.** Critical infrastructure protection: Requirements and challenges for the 21st century. Int. J. Crit. Infrastruct. Prot.; 2015; 8, pp. 53-66. DOI: https://dx.doi.org/10.1016/j.ijcip.2014.12.002

12. **Lipso, H.F.** Tracking, and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues; Carnegie-Mellon University: Pittsburgh, PA, USA, 2002.

13. **Ramirez, J.H.P.** An Anomaly Behavior Analysis Methodology for the Internet of Things: Design, Analysis, and Evaluation. PhD Thesis; The University of Arizona: Tucson, AZ, USA, 2017.

14. **Trend Micro.** Available online: http://blog.trendmicro.com/trendlabs-security-intelligence/operation-woolen-goldfish-when-kittens-go-phishing/ (accessed on 1 January 2023).

15. **Info Security Group.** Available online: http://www.infosecurity-magazine.com/news/potao-trojan-served-up-by-russian/ (accessed on 1 January 2023).

16. **Litefinance.** Available online: https://www.litefinance.com/blog/for-professionals/cryptocurrency-exchange-hacks-history-causes-and-effects/ (accessed on 1 January 2023).

17. **BBC: News.** Available online: https://www.bbc.com/news/world-asia-42845505 (accessed on 1 January 2023).

ALEKSEY V. VASILYEV

REASONS FOR THE INCREASE IN CYBER ATTACKS: ANALYSIS OF TECHNICAL AND NON-TECHNICAL FACTORS

«SCIENCESOFT»
Minsk, Republic of Belarus

This article presents an analysis of both technical and non-technical factors contributing to the growth in volume and diversity of cyber attacks. Social interaction on the Internet contributes to the increased frequency of cyber attacks and exacerbates destructive consequences that extend beyond technical aspects, impacting societal and personal realms. Software errors, vulnerabilities, and deficiencies in network protocols pose a persistent security threat, particularly amidst the rising number of connected devices and the complexity of managing critical systems. The dynamic nature of attacks and evolving penetration methods make cyber threats highly adaptable to the conditions of the modern network environment.

Furthermore, the expanded use of social media and the virtualization of social life bring increased comfort but also provide fertile ground for cyber attacks, amplifying the volume of accessible information for potential malicious actors. The heightened technical proficiency of attackers equips them with new tools for breaching digital security. Concurrently, inadequate awareness and careless user behavior online jeopardize the protection of personal and confidential data.

This work demonstrates that cyber risks escalate due to both ongoing technological changes and human actions. Understanding the dynamics of these factors becomes critically important for developing more effective measures to safeguard the digital environment.

Keywords: *cybersecurity; cyber attacks; cyber threats; network security*

Васильев Алексей Викторович, ведущий специалист по продажам компании ЗАО «НАУЧСОФТ». Сфера научных интересов; вопросами кибербезопасности и разработки специализированных решений для корпоративного бизнеса.

Aleksey V. Vasilyev, Lead Solution Adviser at ScienceSoft company. Research interests: cybersecurity and custom software development for enterprises.

E-mail: alexey_vasilyev96@mail.ru