УДК 336.71

В. С. Протасова

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, e-mail: protasova_2.0@mail.ru

А. С. Ложечко

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, e-mail: aslozhechko@fa.ru

АНАЛИЗ DDOS-АТАК НА РОССИЙСКИЙ БАНКОВСКИЙ СЕКТОР И МЕХАНИЗМ ПРОТИВОДЕЙСТВИЯ ИМ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Ключевые слова: DDoS-атаки, банковский сектор, кибербезопасность, блокчейн, DDoS-Secure, мультивекторные атаки.

Данное исследование посвящено анализу ряда прикладных вопросов защитных механизмов российского банковского сектора против кибератак, таким как количественные и качественные характеристики DDoS-атак за 2022–2024 гг., ТОП атакуемых отраслей в рамках сервиса Anti-DDoS, последствия DDoS-атак на российские банки, а также механизмам противодействия таким атакам. В статье поводится анализ DDoS-атак, направленных на российский банковский сектор, включая характеристики, стратегии защиты от киберугроз и последствия для банковских учреждений. Целью исследования является оценка растущей угрозы DDoS-атак для российских банков и определение необходимых мер защиты, включая внедрение инновационных технологий. Для анализа использованы статистические данные о DDoS-атаках в 2022–2024 годах, в том числе информация о максимальной и средней мощностях атак в разных единицах измерения, их типах и распространенности. Кроме того, применен сравнительный анализ причин увеличения числа кибератак типа «отказ в обслуживании» и предложен способ их нейтрализации. Для снижения рисков и обеспечения безопасности автором рекомендуется внедрение DDoS-Secure – сервиса защиты на основе технологии блокчейн, который автоматически фильтрует трафик и блокирует аномалии, способствуя оптимизации защиты уязвимых ресурсов банковской инфраструктуры.

V. S. Protasova

Financial University under the Government of the Russian Federation, Moscow, e-mail: protasova_2.0@mail.ru

A. S. Lozhechko

Financial University under the Government of the Russian Federation, Moscow, e-mail: aslozhechko@fa.ru

ANALYSIS OF DDOS-ATTACKS ON THE RUSSIAN BANKING SECTOR AND A MECHANISM TO COUNTER THEM BASED ON BLOCKCHAIN TECHNOLOGY

Keywords: DDoS attacks, banking sector, cybersecurity, blockchain, DDoS-Secure, multivector attacks.

This study is devoted to the analysis of a number of applied issues of the protective mechanisms of the Russian banking sector against cyberattacks, such as quantitative and qualitative characteristics of DDoS attacks for 2022-2024, TOP attacked industries within the Anti-DDoS service, consequences of DDoS attacks on Russian banks, as well as mechanisms for countering such attacks. The article analyzes DDoS attacks aimed at the Russian banking sector, including characteristics, cyber threat protection strategies and consequences for banking institutions. The purpose of the study is to assess the growing threat of DDoS attacks for Russian banks and determine the necessary protection measures, including the introduction of innovative technologies. The analysis uses statistical data on DDoS attacks in 2022-2024, including information on the maximum and average attack power in different units of measurement, their types and prevalence. In addition, a comparative analysis of the reasons for the increase in the number of denial-of-service cyber attacks and suggestions of a way to neutralize them were applied. To reduce risks and ensure security, the author recommends the introduction of DDoS-Secure, a security service based on blockchain technologies that automatically filters traffic and blocks anomalies, helping to optimize the protection of vulnerable resources of the banking infrastructure.

Теоретические и практические вопросы DDoS-атак рассмотрены в работе У.Б. Кусаиновой, Ж. Сарсенбаевой, Д.В. Плескачева [4], на исследовании влияния DDoS-атак на финансовые учреждения, рассмотренного в работе А.М. Кипкеевой, С.А. Аслахановой [3], мощность DDoS-атак типа «отказ в обслуживании», рассмотренной в работах А.С. Белоусовой [1] и других работах.

Цифровизация банковского сектора, развитие банковских экосистем и онлайн-банкинга происходит параллельно с развитием киберпреступлений как на качественном уровне (злоумышленниками разрабатываются все новые и новые схемы мошенничеств), так и на количественном (растет число киберпреступлений и вызванные ими убытки) [6]. Так, по данным отчета StormWall о таком виде кибератак как DDoS-атаки, их число в России в 2024 году выросло на 45% по сравнению с 2023 годом, а мощность нападений на уровне приложений – сразу вдвое [10].

DDoS (Distributed Denial of Service) – распределенная атака типа «отказ в обслуживании» с одновременным использованием большого числа атакующих компьютеров, целью которой, как правило, является частичное нарушение штатного функционирования информационной инфраструктуры организации.

Целью подобной атаки является отключение или временная недоступность систем, сервисов и сетевой инфраструктуры путём их перегрузки постоянным потоком запросов. Атаки на банки отличаются высоким уровнем организации и широким охватом. В качестве сектора атаки используются ботнеты (компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным программным обеспечением [5]), которые генерируют масштабные объемы трафика, направленного на перегрузку серверов и сетевых ресурсов банка.

DDoS-атаки – нарастающая угроза кибербезопасности в России

Как показал 2024 год, банковские онлайн-ресурсы по-прежнему остаются одной из ключевых целей хакеров. При этом продолжительность DDoS-атак заметно снизилась. Во 2 квартале 2024 года количество DDoS-атак в целом по стране выросло до 215 тысяч, абсолютный прирост составляет 75 тысяч с 1 квартала 2024 года, что вступает в противоречие со статистикой 1-2 кварталов и 3-4 кварталов 2023 года, где прослеживается рост DDoS-атак на 21 тысячу (рисунок 1). Такой резкий рост может быть вызван ненадлежащей защитой организаций, что, в свою очередь, может послужить причиной для серьезных убытков бизнеса.

Частота атак представляет собой значимый показатель, благодаря которому можно определить уровень угрозы, с которой сталкивается бизнес, банк или государственный орган. В первой половине 2024 года частота ежедневных атак увеличилась более чем в четыре раза по сравнению с аналогичным периодом 2023 года. Резкое увеличение атак указывает на то, что злоумышленники активизировались и используют новые методы дестабилизации цифровой инфраструктуры компаний или адаптировались под современные антифрод системы, разрабатываемые отечественными IT-компаниями, Центральным банком Российской Федерации и банковским сектором в целом. Главная цель таких атак заключается в том, чтобы создать значительный сбой в работе организации, перегружая программное обеспечение (далее – ПО), нарушая важные бизнес-процессы, создавая трудности для целевой аудитории при использовании мобильного банкинга, что приводит к потерям доходов социально-значимых банков за счет недоверия и оттока клиентов [2].

Следует выделить следующие предпосылки роста числа DDoS-атак.

Во-первых, злоумышленники могут легко получить необходимые ресурсы для организации атак, накапливая огромные объемы трафика для перегрузки целевых систем. В то время как раньше для организации такого рода кибератак требовались серьезные технические знания и инвестиции, сейчас простота и доступность аренды вычислительных мощностей позволяют большому количеству людей реализовать создание ботнетов

Во-вторых, снизился «порог вхождения» в мир DDoS-атак за счет многочисленных бесплатных и недорогих инструментов, которые позволяют даже новичкам в кибербезопасности без особых усилий запустить атаку. Это «развязывает руки» большому количеству людей, и дает возможность действовать в рамках интересов своих компании, реализуя агрессивную политику по отношению к конкурентам.

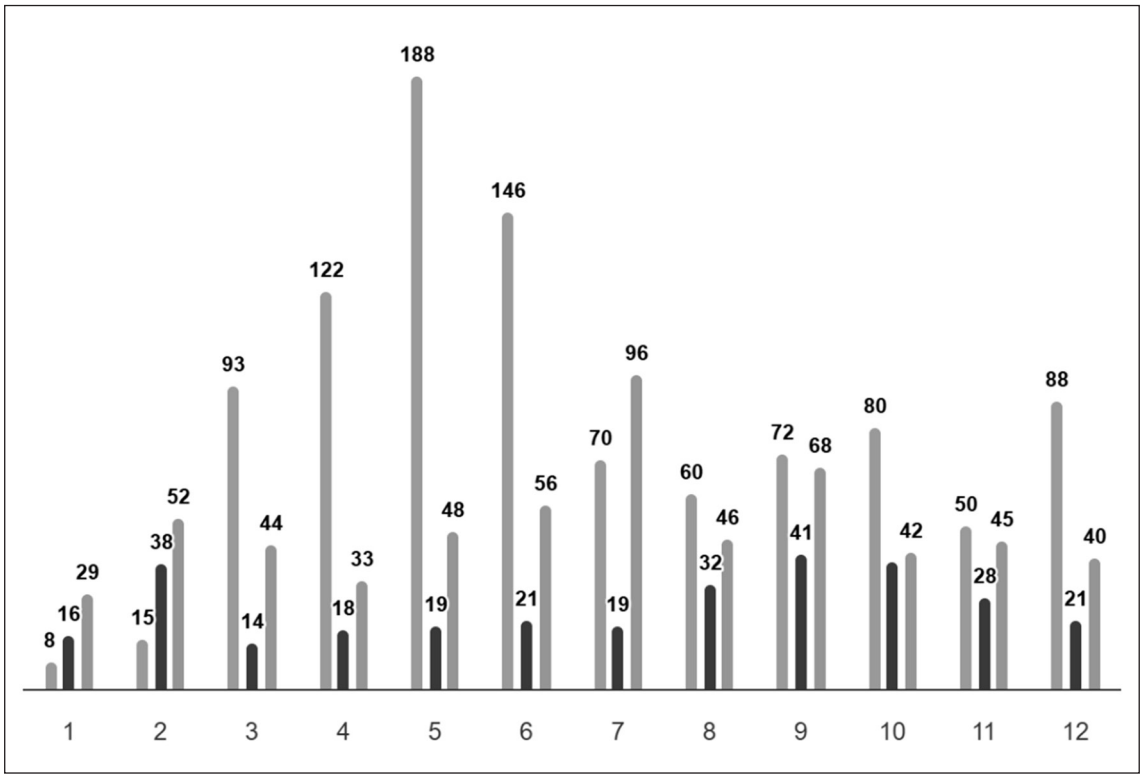

Рис. 1. Количество DDoS-атак помесячно в 2022, 2023 и 2024 гг. соответственно, тыс. ед. [9]

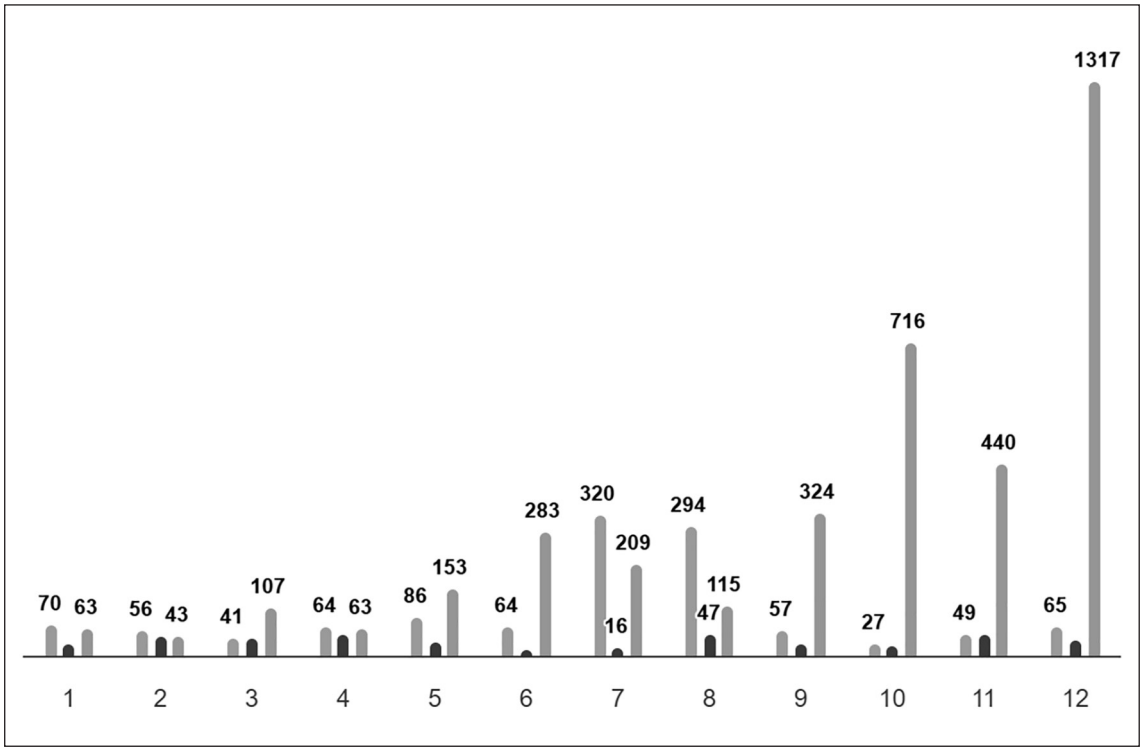

Рис. 2. Динамика мощности DDoS-атак помесячно в 2022, 2023 и 2024 гг. соответственно (Гбит/с) [9]

В первом полугодии 2023 года максимальная мощность зафиксированной DDoS-атаки составила 174 Гбит/с, что является внушительным показателем (рисунок 2), который может привести к значительным сбоям в работе целевых систем, особенно в тех случаях, как отмечалось ранее, они не защищены релевантными мерами безопасности.

Однако в первом полугодии 2024 года произошло резкое увеличение данного показателя: мощность самой крупной зарегистрированной атаки достигла 1,2 Тбит/с. Это увеличение в 6,7 по сравнению с аналогичным периодом прошлого года свидетельствует об использовании новых более мощных инструментов для реализации кибератак. В декабре 2024 года под одной из мощнейших атак за этот год оказались ключевые сектора, такие как телекоммуникации и информационные технологии [8].

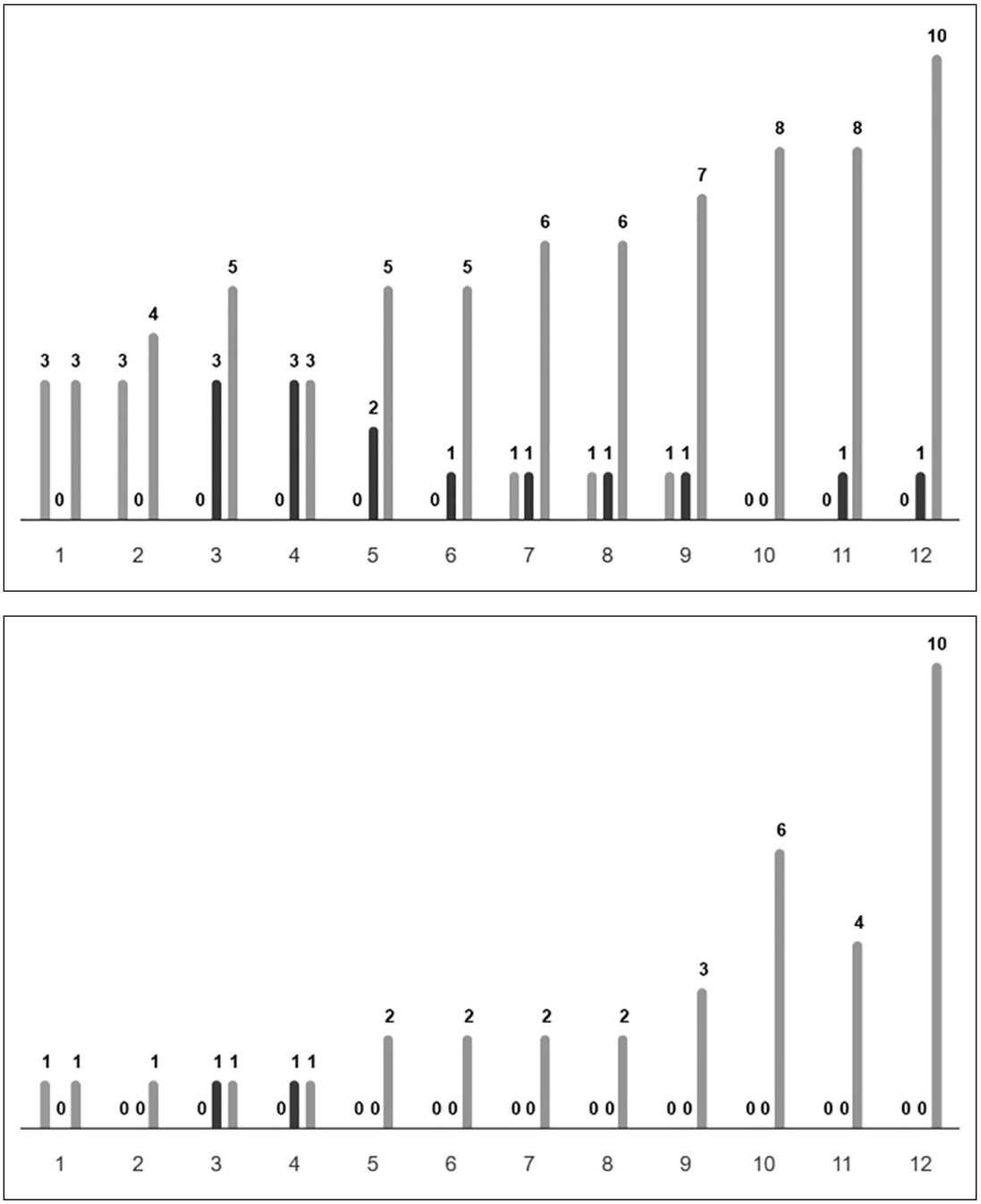

Рис. 3. Оценка средней мощности DDoS-атак помесячно в 2022, 2023 и 2024 гг. соответственно (Гбит/с и Mpps) [9]

Средняя мощность DDoS-атак в 2024 году также значительно выросла по сравнению с данными 2022 и 2023 годов (рисунок 3). Например, в феврале 2022 года мощность составляла 3,5 Гбит/с, а в марте 2023 года – 2,8 Гбит/с, что значительно меньше показателя 9,8 Гбит/с, который прослеживался в декабре 2024 года. Во втором квартале 2024 года средняя мощность атак начала постепенно увеличиваться и в апреле сравнялась с показателями аналогичного месяца 2023 года, а затем продолжала расти вплоть до декабря 2024 года. Рост связан все с тем же фактором, определяющим доступ к более мощным ботнетам.

Также стоит обратить внимание на то, что средняя мощность в Mpps (система измерения скорости, с которой коммутатор обрабатывает и пересылает пакеты) в 2024 году значительно превышает значения 2022 и 2023 года годов. В 2022 году она составила 0,17 Mpps, в 2023 году – 0,24 Mpps, а в 2024 году уже достигла 2,92 Mpps. Динамика в этом показателе указывает на совпадение первой половины 2024 года с 2023 годом, но во второй половине 2024 года наблюдается резкий рост [9].

Максимальная мощность DDoS-атак в Mpps в начале года оставалась на уровне 63 Mpps, который был отмечен в начале 2022 и 2023 годов, затем с мая 2024 года этот показатель взлетел до 1317 Mpps в декабре. Важно отметить, что атаки с одинаковым количеством пакетов в секунду могут иметь разную мощность в Гбит/с в зависимости от размера пакетов. Динамика значений в Гбит/с показала, что ожидаемые атаки в марте 2024 года, во время выборов Президента Российской Федерации, не стали самыми мощными в рассматриваемом году. Один из пиков активности кибератак пришелся на третий квартал 2024 года, когда под ударом оказалось множество ведущих организаций банковского сектора.

Таким образом, наблюдаемое резкое увеличение мощностей атак подчеркивает нарастающую угрозу и необходимость серьезных изменений в стратегиях защиты веб-сайтов банков и мобильного банкинга.

Банковский сектор – основная мишень DDoS-атак

Анализ динамики второй половины 2024 года показывает снижение доли организаций, подвергшимся DDoS-атакам, по сравнению с предыдущим годом. Тем не менее общая тенденция в количестве DDoS-атак остается стабильной. Примечательно, что среднее количество атак на одну организацию возросло до 132, что в 1,8 раза больше, чем в 2023 году, это свидетельствует о смене тактики злоумышленников: вместо массовых кибератак они стали применять более целевые стратегии, фокусируясь на наиболее привлекательных для себя отраслях. В середине 2024 года также фиксируется небольшой рост числа DDoS-атак на одну организацию, что особенно ярко проявилось в атаке на несколько системно значимых кредитных организаций одновременно. Пиковые значения наблюдались в третьем квартале 2024 года, что отличает текущее состояние от более равномерной динамики 2023 года, когда аналогичные всплески зарегистрированы в первых двух кварталах.

В целом в 2024 году большинство DDoS-атак пришлось на финансовый сектор, строительство и недвижимость, ИТ-сектор, государственный сектор и сектор телекоммуникаций [9]. При этом банки стали основными мишенями атак, с ростом «посягательств» на целевые структуры на 40% по сравнению с предыдущим годом. Особенно активные нападения произошли в июле, когда под удар попали крупнейшие финансовые учреждения России: ПАО «Банк ВТБ», АО «Россельхозбанк» и ПАО «Сбербанк», хотя к четвертому кварталу количество атак на банки снизилось. Причем ПАО «Банк ВТБ» является мишенью многократных попыток привести в неработоспособность веб-сайт банка и мобильного приложения с ресурсов как в России, так и из-за рубежа (2022 год).

К концу 2024 года банковский сектор демонстрировал одну из самых высоких уязвимостей к кибератакам, обусловленную необходимостью хранения и управления финансовыми ресурсами и конфиденциальными данными клиентов. Ярким примером обозначенной уязвимости стала масштабная DDoS-атака, которая произошла в декабре 2022 года и затронула банковский сектор, в частности ПАО «Банк ВТБ». Примечательно, что большая часть запросов поступала с зарубежных ресурсов, что подчеркивает сторонне привлечение информационной поддержки. Согласно открытым данным и новостным материалам, предположительно хакеры

применяли технику Flood HTTP-запросов, что инициировало дополнительную нагрузку на веб-сайты банка и ограничивало доступ клиентов к сервису «ВТБ Онлайн». Также могла быть использована технология SYN Flood, обеспечивающая усложнения в очереди соединений, что лишало банковских клиентов свободного доступа к приложению. Возможно, злоумышленники использовали утилиты типа LOIC (Low orbit ion cannon) или HOIC (High orbit ion cannon), которые работают на основе простого, но эффективного принципа – отправка постоянных запросов с целью перегрузки серверов. Также могли применяться «скрипты», созданные для генерации специфических типов графика, что усложняет их блокировку, или комбинирование этих методов для затруднения обнаружения и защиты.

В результате кибератаки любой банк может столкнуться с определенными последствиями. В первую очередь, прямые финансовые потери, включая снижение комиссионных доходов из-за технических работ, которые ограничивают функциональность мобильного банкинга и веб-сайтов банков, а также уменьшение объемов сделок, активов и депозитов при длительных или повторяющихся простоях в оказании услуг клиентам. Участие IP-адресов из Российской Федерации свидетельствует о том, что некоторые устройства могли быть связаны и заражены, что увеличивает риск последующих атак, направленных на кражу конфиденциальных данных [11]. Также стоит отметить, что потеря доверия клиентов, как правило, имеет долгосрочные последствия для формирования репутации и финансовых показателей банков.

В конце июля 2024 года ПАО «Сбербанк» столкнулся с самой масштабной DDoS-атакой в своей истории, которая продолжалась 13 часов. Рассматриваемая кибератака отличалась масштабностью за счет привлечения сторонних бот-сетей, состоящих из 62 тысяч устройств, свыше половины из которых располагались на территории Российской Федерации. Несмотря на мощность атаки, клиенты не пострадали от рук злоумышленников, более того хакеры не смогли преодолеть первый уровень защиты банка, который состоит из трех контуров. Инструментом для организации этой DDoS-атаки стало вредоносное письмо, содержавшее вирус. Кибератака затронула не только ПАО «Сбербанк», но и почти весь российский банковский сектор. Жертвами злоумышленников стали клиенты таких банков, как ПАО «Банк ВТБ», АО «Альфа-банк», АО «Газпромбанк», АО «Райффайзенбанк» и др. В ответ на эти события банки совместно с интернет-провайдерами и Центральным банком Российской Федерации принимают меры по снижению воздействия кибератак на свои операционные системы.

Вместе с тем, на основе детального анализа представленных инцидентов можно сделать вывод о том, что банковский сектор пока недостаточно инвестирует в современные методы кибербезопасности. Банковским и небанковским финансовым институтам усилить свои защитные механизмы, разработав и внедрив технологии, способные не только предотвращать кибератаки, но и минимизировать их последствия.

Механизм противодействия мультивекторным DDoS-атакам на основе технологии блокчейн

В первом полугодии 2024 года наиболее частыми и масштабными из DDoS-атак стали мультивекторные атаки, которые сочетают в себе различные методы нападения: SYN Flood, UDP Flood, ICMP [4]. Комбинирование нескольких типов атак одновременно усложняет обнаружение и попытки нейтрализации службами безопасности. Эти условия способствуют увеличению разрушительной силы атак, что актуализирует предположение о решении обозначенной проблемы. При этом, как отмечают специалисты [7], кибербезопасность (особенно в банковском секторе) не должна исходить только из парадигмы защищенности – в настоящее время ее должна дополнять парадигма развития систем безопасности, которая основывается на развитии собственных внутренних сил таких систем.

Актуальным способом снижения рисков при мультивекторных атаках является DDoS-Secure – сервис защиты банка на основе технологии блокчейн, обеспечивающий централизованную архитектуру, которая распределяет риски и ресурсы между участниками сети. Сервис предусматривает автоматическую фильтрацию входящего трафика за счет применения смарт-контрактов, а также выявление аномалий и блокировку подозрительных IP-адресов.

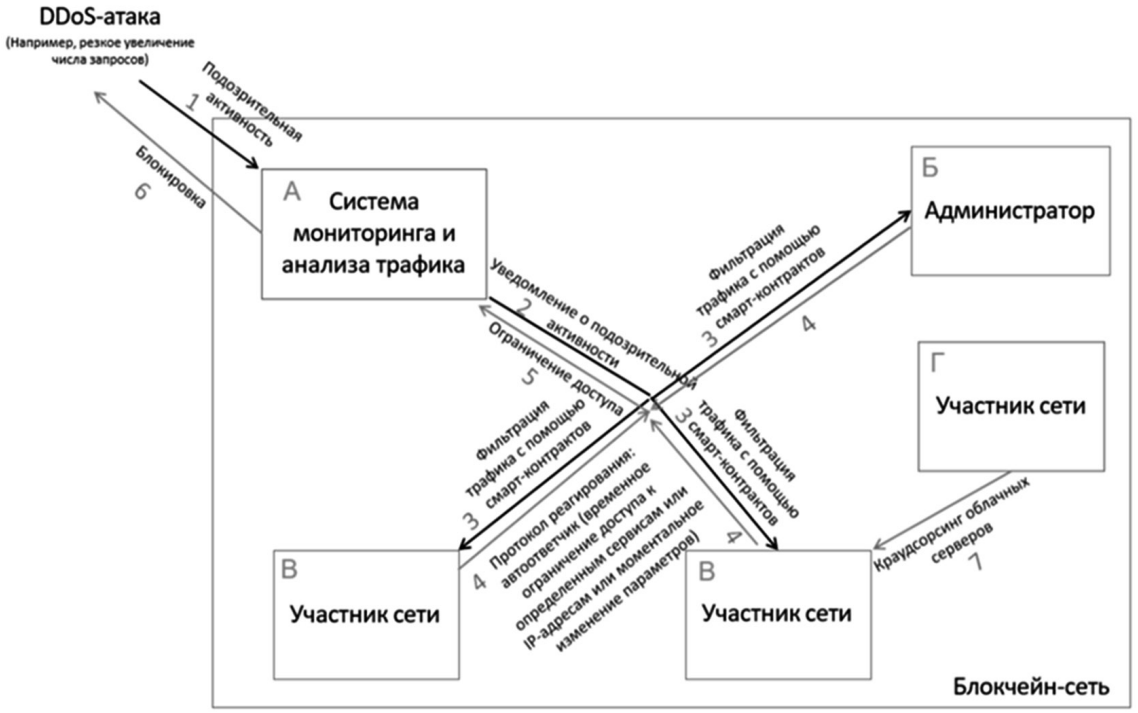

Рис. 4. Архитектура сервиса DDoS-Secure
Источник: составлено автором

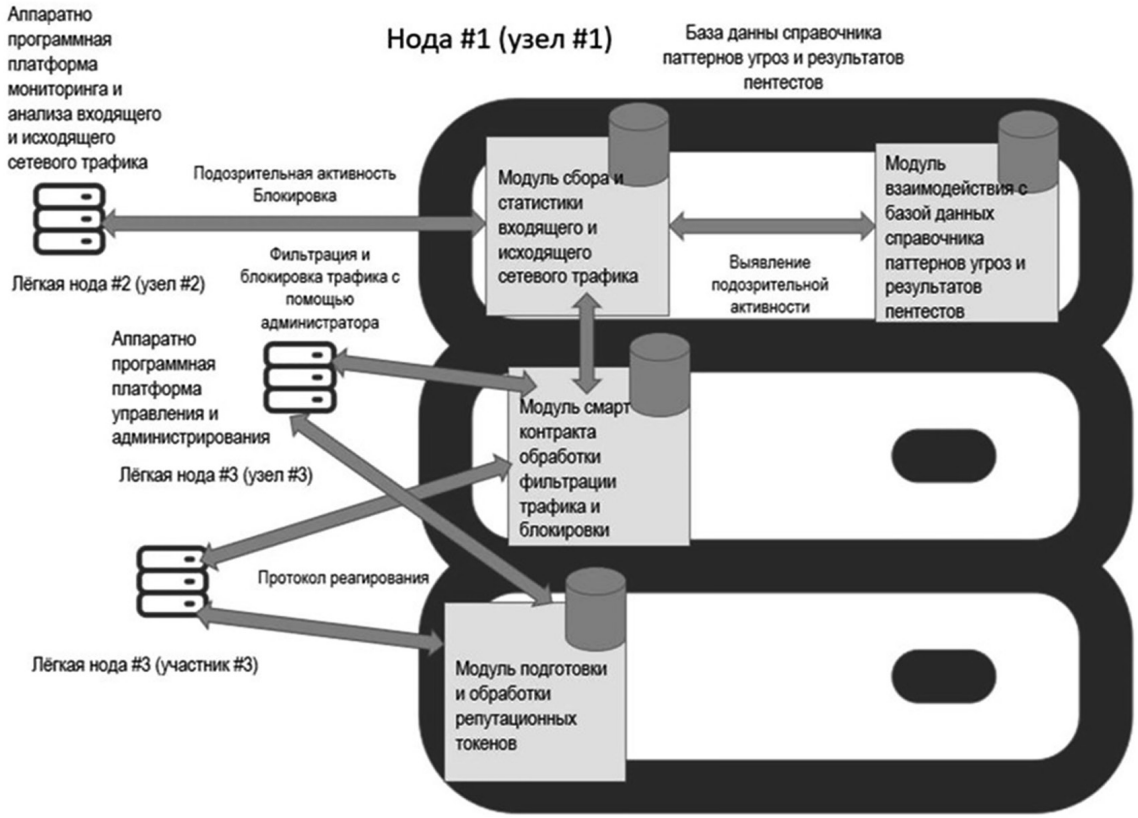

Рис. 5. Внутренняя схема сервиса DDoS-Secure
Источник: составлено автором

Процесс реализации механики DDoS-Secure предполагает прохождение следующих этапов обработки запросов: обнаружение атаки, фильтрация и блокировка трафика с помощью администратора, привлечение ресурсов участников сети, шифрование и анонимизация, завершение атаки, обновление отчетности, оценка и обновление репутации (рисунок 4).

Система непрерывно анализирует входящий трафик, используя заранее заданные алгоритмы для выявления аномалий и паттернов, характерных для мультивекторных DDoS-атак. В результате обнаружения аномалии система мониторинга автоматически выдает сигнал на платформе для администраторов от каждого участника сети. Администраторы получают уведомление о необходимости вмешаться в процесс воздействия атаки на банк. Так характеризуется первый этап – обнаружение атаки. На рисунке 5 представлена внутренняя схема сервиса.

Далее администраторы заходят на платформу управления смарт-контрактами, предоставляемые системой, на основе полученной информации о подозрительных IP-адресах и аномальном трафике вручную принимают решение о фильтрации. Администраторы блокируют идентифицированные подозрительные IP-адреса и, при необходимости, устанавливают дополнительные правила для фильтрации трафика.

В случае, если нагрузка на серверы банка возрастает из-за DDoS-атаки, администраторы вправе активировать пул ресурсов, которые включает в себя дополнительные сервера и вычислительные мощности, предоставляемые банками в рамках Open API. Распределение нагрузки среди участников сети позволит обеспечить стабильность работы банковских сервисов, а именно мобильного банкинга и web-версии банка, минимизирует риск простоя.

Вся информация, проходящая через систему, шифруется с использованием современных алгоритмов. Анонимизация поможет скрыть источники трафика, затрудняя злоумышленникам анализ структуры и содержания трафика. Администраторы в этот момент контролируют правильность шифрования и анонимизации данных для поддержания конфиденциальности клиентских данных.

После того как атака прекращена, система продолжает осуществлять мониторинг трафика для фиксации новых аномалий. Администраторы имеют возможность получить отчеты о том, какие действия были предприняты: какие участники сети предоставили доступ к дополнительным серверам, список заблокированных IP-адресов.

После инцидента атаки администраторы анализируют эффективность участников сети на основе отчетности об их действиях во время атаки. Участники, которые показали высокую активность и эффективность, награждаются репутационных токенами, что будет подтверждать их вклад в безопасность. Эти токены могут быть использованы банками для дальнейшей оценки надежности партнеров и повышения своего имиджа перед клиентами в качестве безопасного участника финансового рынка.

Такой подход представляет собой инновационное решение в контексте постоянно эволюционирующих киберугроз и масштабирования их сложности обнаружения. DDoS-Secure может стать неотъемлемой частью стратегии защиты для любого участника финансового рынка, стремящейся обеспечить стабильность работы своих серверов и защитить интересы клиентов. Предлагаемый сервис не только обеспечивает проактивность от DDoS-атак, но и способствует созданию системы коллективной ответственности и сотрудничества между финансовыми учреждениями.

В условиях роста угроз и последствий, связанных с DDoS-атаками, российский банковский сектор все больше сталкивается с новыми вызовами, требующими адаптации и усовершенствования стратегий защиты безопасности не только банков, финансовых учреждений, но и большинства отраслей в целом. Атаки, которые становятся более таргетировано адресными и мощными, наносят вред как самим компаниям, так и их клиентам, что значительно снижает их лояльность. Адаптация злоумышленников к методам защиты наглядно демонстрирует необходимость реализации инновационных решений, таких как DDoS-Secure, которые используют технологию блокчейн для создания централизованной усиленной инфраструктуры защиты. Интеграция финансовых учреждений внутри такой системы позволит значительно повысить устойчивость организаций к киберугрозам, минимизировав последствия атак и сохранив репутацию компаний. Такие механизмы защиты становятся все более актуальными не только для противостояния существующим угрозам, но и для обеспечения стабильности всей экономики в перспективе.

Библиографический список

1. Белоусова А.С. Оценка мощности атак типа «отказ в обслуживании» с использованием нечеткой логики // Вестник науки. 2023. Т. 4, № 7(64). С. 199-208.

2. Дауров, А. И. О некоторых путях повышения эффективности противодействия киберпреступности на современном этапе // Право и управление. 2023. № 2. С. 165-169.

3. Кипкеева А.М., Аслаханова С.А. Цифровизация финансового сектора экономики // Естественно-гуманитарные исследования. 2023. № 3(47). С. 302-304.

4. Кусаинова У.Б., Сарсенбаева Ж., Плескачев Д.В. Методы противодействия угрозам нарушения информационной безопасности при DDoS-атаках // Наука и реальность. 2020. № 4. С. 35-43.

5. Ревенков П.В., Бердюгин А.А. Расширение профиля операционного риска в банках при возрастании DDoS-угроз // Вопросы кибербезопасности. 2017. № 3(21). С. 16-23.

6. Федотова Г.В., Орлова Е.Р., Бочарова И.Е. Вопросы кибербезопасности цифровых финансовых сервисов // Информационные технологии и вычислительные системы. 2022. № 2. С. 37-45.

7. Фролов Д.Б., Ревенков П.В. Кибербезопасность в условиях применения систем электронного банкинга // Деньги и кредит. 2016. № 6. С. 9-12.

8. Атаки на онлайн-ресурсы российских компаний в I полугодии 2024 года // ГК «Солар». 2024. [Электронный ресурс]. URL: Otchet_ATAKI_NA_ROSSIYSKIE_KOMPANII_V_1_polugodii_2024.pdf (дата обращения: 16.02.2025).

9. Отчет о DDoS-атаках на онлайн-ресурсы российских компаний в 2024 году // ГК «Солар» [Электронный ресурс]. URL: https://rt-solar.ru/analytics/reports/5364/ (дата обращения: 16.02.2025).

10. Эксперты зафиксировали рост мощности DDoS-атак в России / Р. Кильдюшкин // Интернет-издание Газета.ру [Электронный ресурс]. URL: https://www.gazeta.ru/tech/news/2023/04/20/20254069.shtml (дата обращения: 11.02.2025).

11. OMNeT++ simulation system. [Электронный ресурс]. URL: http://omnetpp.org/ (дата обращения: 11.02.2025)