ИНТЕГРАЦИЯ ОБЛАЧНОГО СЕРВИСА CLOUDFLARE КАК ЭЛЕМЕНТА ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ DDOS-АТАК

Бодров Д.А., магистрант гр. 567001

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бойправ О.В. – канд. тех. наук, доцент,
заведующий кафедрой защиты информации

Аннотация. В статье рассматриваются организационно-технические аспекты интеграции облачного сервиса Cloudflare в систему защиты информационной системы от DDoS-атак. На основе анализа учебной и научной литературы раскрыта сущность распределенных атак отказа в обслуживании, охарактеризованы их разновидности и последствия для доступности цифровых ресурсов. Обоснована необходимость многоуровневой защиты, сочетающей локальные и облачные средства фильтрации трафика. Показаны основные направления интеграции Cloudflare, включая изменение DNS-маршрутизации, использование HTTPS, применение защитных правил и режимов усиленной проверки трафика. Сделан вывод о целесообразности использования Cloudflare как внешнего уровня защиты информационной системы, дополняющего традиционные средства обеспечения информационной безопасности.

Ключевые слова. Информационная система, DDoS-атака, Cloudflare, информационная безопасность, облачная защита, фильтрация трафика, HTTPS, DNS.

В современных условиях развития цифровой среды устойчивое функционирование информационных систем становится одной из предпосылок надежной работы организаций, предприятий, учреждений и различных сетевых сервисов. Информационные системы представляют собой совокупность средств, методов и персонала, обеспечивающих хранение, обработку, передачу и предоставление данных, поддерживают взаимодействие пользователей, функционирование веб-приложений, доступ к корпоративным ресурсам и выполнение повседневных управленческих, производственных и сервисных процессов [1]. По мере роста числа цифровых услуг и усиления зависимости организаций от сетевой инфраструктуры проблема обеспечения доступности ресурсов приобретает особую значимость. Нарушение стабильности работы информационной системы даже на короткий промежуток времени способно вызвать организационные сбои, финансовые потери, снижение качества обслуживания и ухудшение репутации владельца ресурса [2, с. 215].

Одной из наиболее опасных угроз доступности информационных систем остаются DDoS-атаки. Согласно определению А.А. Головина, DDoS-атака (распределенная атака отказа в обслуживании) представляет собой целенаправленное воздействие на информационную систему, осуществляемое с большого количества распределенных источников, с целью исчерпания ее вычислительных или сетевых ресурсов и, как следствие, нарушения доступности предоставляемых сервисов для легитимных пользователей [3, с. 128]. В отличие от обычной атаки отказа в обслуживании, распределенный характер DDoS-воздействия усложняет его отражение, вредоносный поток поступает сразу из множества источников и может имитировать обычную пользовательскую активность [3, 4].

Сложность защиты от DDoS-атак связана также с тем, что они могут реализовываться на различных уровнях эталонной модели взаимодействия открытых систем (OSI). На сетевом и транспортном уровнях широко распространены flood-атаки, основанные на генерации большого количества ICMP-, UDP- или SYN-запросов. Их цель состоит в перегрузке пропускной способности канала связи, сетевых буферов, таблиц соединений либо других инфраструктурных механизмов обработки трафика. На прикладном уровне атака может принимать форму многократных HTTP- или HTTPS-запросов, внешне похожих на обращения обычных пользователей. Как подчеркнул С.И. Макаренко, такие атаки являются особенно опасными, поскольку они затрудняют четкое разграничение между вредоносной и легитимной активностью и могут оставаться незамеченными на протяжении длительного времени [4, с. 87]. Дополнительные сложности возникают при использовании шифрованного трафика, так как он увеличивает нагрузку на серверные ресурсы и одновременно усложняет глубинный анализ содержимого запросов.

Последствия DDoS-атак для информационной системы имеют многоплановый характер. А.Б. Грушо и Е.А. Линева выделяются три основных уровня проявления последствий: технический, организационный и экономический [5, с. 156]. На техническом уровне они проявляются в снижении производительности серверов, отказе веб-приложений, перегрузке сетевого оборудования и нарушении доступа к цифровым сервисам. На организационном уровне атака может привести к дестабилизации внутренних процессов, невозможности выполнения пользователями своих функций, нарушению обмена данными между подразделениями и временной остановке критически значимых сервисов. На экономическом уровне последствия выражаются в прямых потерях, связанных с простоем, необходимостью восстановления работоспособности, привлечением дополнительных ресурсов и усилением защитной инфраструктуры.

Кроме того, для систем, ориентированных на обслуживание клиентов, важную роль играют репутационные риски.

Традиционная система защиты информационной инфраструктуры, подробно описанная в учебных изданиях, предполагает использование набора локальных средств безопасности, размещенных внутри собственного контура организации [5, 6]. К ним относятся межсетевые экраны, средства контроля доступа, системы обнаружения и предотвращения вторжений (IDS/IPS), балансировщики нагрузки, механизмы сегментации сети и организационные меры реагирования на инциденты. Межсетевые экраны позволяют контролировать входящий и исходящий трафик и применять к нему правила фильтрации, основанные на адресах, портах, типах соединений и других параметрах. IDS и IPS предназначены для выявления аномального поведения, фиксации признаков известных атак и автоматического блокирования подозрительного трафика [6, с. 302]. Дополнительно могут применяться ограничения частоты запросов, резервирование серверных ресурсов, распределение нагрузки и аудит защищенности. Однако возможностей локальной инфраструктуры оказывается недостаточно при отражении массированных распределенных атак. Причина состоит в том, что вредоносный трафик уже достигает защищаемой системы и начинает потреблять ее собственные сетевые и вычислительные ресурсы [4, с. 112]. Даже если часть запросов впоследствии будет отфильтрована, сама необходимость их приема, анализа и обработки может привести к дополнительной нагрузке на серверы и оборудование.

В современных концепциях информационной безопасности все большее значение приобретает использование внешних распределенных платформ фильтрации трафика, которые способны анализировать и отсекать значительную долю вредоносного потока до его поступления к целевой информационной системе. Одним из наиболее известных решений такого типа, является облачный сервис Cloudflare. Его применение позволяет организовать внешний уровень защиты, расположенный между пользователем и исходным сервером. В общем виде принцип работы заключается в том, что запросы к защищаемому ресурсу перенаправляются через распределенную сеть узлов Cloudflare, где осуществляется их маршрутизация, анализ, проверка и фильтрация. После этого только очищенный или допустимый трафик передается на исходный сервер [7]. За счет подобной архитектуры уменьшается нагрузка на локальную инфраструктуру, снижается вероятность ее перегрузки и повышается доступность ресурса для легитимных пользователей.

Интеграция Cloudflare в информационную систему может рассматриваться как одно из направлений реализации принципа многоуровневой (эшелонированной) защиты, который является основополагающим в современной теории информационной безопасности. Данный принцип предполагает создание нескольких последовательных рубежей обороны, что позволяет затруднить преодоление защиты злоумышленником и повысить общую устойчивость системы [3, с. 95]. Такой подход не отменяет использование локальных средств безопасности, а дополняет их внешним облачным уровнем фильтрации и востребован прежде всего в ситуациях, когда информационная система предполагает публичную доступность веб-ресурсов, взаимодействие с удаленными пользователями либо подвержена существенным и трудно-прогнозируемым колебаниям сетевой нагрузки.

Интеграция Cloudflare начинается с изменения логики сетевого взаимодействия. Основное действие состоит в перенастройке DNS-записей домена таким образом, чтобы запросы направлялись не на исходный сервер организации, а в инфраструктуру Cloudflare. Тем самым формируется промежуточный узел обработки трафика, который принимает на себя значительную часть защитных функций. Фильтрация начинает выполняться до того, как пакеты достигают локальной сети. Без этого этапа применение большинства анти-DDoS-механизмов Cloudflare становится невозможным, а последующая настройка защиты теряет смысл. Следующий этап заключается в построении защищенного канала связи. Для современных информационных систем использование HTTPS и корректная настройка SSL/TLS являются базовым требованием. Криптографическая защита каналов связи остается одним из основных средств обеспечения конфиденциальности и целостности данных при передаче по открытым сетям [5, с. 210]. При интеграции Cloudflare задача организации защищенного соединения усложняется, поскольку шифрование должно быть корректно настроено одновременно на двух участках сетевого взаимодействия, между пользователем и облачным сервисом, а также между Cloudflare и исходным сервером. Данная схема может обеспечить безопасную передачу данных, сохранив при этом возможности фильтрации трафика, кэширования и контроля сетевой активности.

Cloudflare позволяет ограничивать частоту запросов, применять сетевую и поведенческую фильтрацию, различать типы трафика и выявлять признаки аномальной активности. Эти механизмы особенно значимы в тех случаях, когда вредоносные обращения внешне не отличаются от обычных пользовательских запросов. На прикладном уровне атаки нередко направляются на наиболее уязвимые и ресурсоемкие элементы веб-приложения, формы аутентификации, API-интерфейсы, динамически формируемые страницы, поисковые модули. В подобных условиях стандартной фильтрации по IP-адресам и портам недостаточно, поскольку для эффективного противодействия требуется учитывать характер и модель поведения входящих запросов.

Особое место занимает режим усиленной проверки трафика Under Attack mode. Его применение позволяет ввести дополнительный этап проверки обращений к ресурсу и тем самым затруднить доступ автоматизированных скриптов и иных источников подозрительной активности. Для пользователей доступ

к ресурсу сохраняется, однако осуществляется через промежуточную процедуру подтверждения. Наиболее оправдано использование данного режима в ситуациях, когда обычных правил фильтрации уже недостаточно для поддержания стабильной работы веб-приложения, прежде всего при атаках прикладного уровня, ориентированных на перегрузку сервера потоком формально корректных запросов.

Сервис Cloudflare используется также для защиты DNS-инфраструктуры, ускорения доставки контента, перераспределения нагрузки в периоды ее резкого роста, функционирования межсетевого экрана веб-приложений и общей оптимизации сетевого взаимодействия. Благодаря этому Cloudflare целесообразно рассматривать не как отдельный инструмент защиты, а как один из элементов архитектуры, обеспечивающей доступность, устойчивость и отказоустойчивость информационной системы. Для организаций это означает, что выбор решения должен учитывать не только угрозу атак, но и повседневные требования к стабильности цифровых сервисов.

Внутренние межсетевые экраны, IDS и IPS, безопасная конфигурация серверов, актуализация программного обеспечения, контроль уязвимостей, резервирование ресурсов и разработка регламентов реагирования сохраняют свое фундаментальное значение [3, 5]. Облачная фильтрация трафика в таком случае выступает как внешний рубеж защиты, который уменьшает объем вредоносного потока и повышает устойчивость системы, но не отменяет необходимости поддержания внутренней безопасности на должном уровне.

Особое значение многоуровневого подхода проявляется в том, что разные механизмы защиты решают различные задачи. Локальные средства позволяют контролировать внутреннюю инфраструктуру, разграничивать доступ, фиксировать инциденты и реагировать на угрозы в пределах собственного контура. Облачный сервис, напротив, наиболее эффективен на этапе предварительной фильтрации и распределения нагрузки. Сочетание данных уровней позволяет добиться заметного эффекта при отражении сложных распределенных атак [6, с. 345]. Cloudflare не подменяет традиционные средства защиты, а дополняет их, усиливая внешний уровень противодействия сетевым угрозам. Его применение оправдано в тех случаях, когда собственных ресурсов информационной системы недостаточно для устойчивого отражения интенсивного потока вредоносного трафика.

Интеграция Cloudflare в защитный контур информационной системы позволяет повысить ее устойчивость за счет переноса части защитных функций во внешнюю распределенную инфраструктуру. При такой организации снижается зависимость доступности ресурса от состояния одного канала связи или производительности отдельного сервера. Даже при значительной нагрузке часть вредоносного трафика задерживается еще до поступления на защищаемый ресурс, что создает более благоприятные условия для сохранения его работоспособности. Для систем, функционирующих в открытой сети, обслуживающих большое количество пользователей и ориентированных на постоянную доступность, это имеет важное значение.

Таким образом, высокая опасность DDoS-атак определяется тем, что их объектом выступает именно доступность информационного ресурса. Вследствие этого последствия подобных воздействий выходят за пределы технических нарушений и затрагивают организационную деятельность, стабильность предоставления сервисов и экономические показатели. Базовые локальные средства защиты формируют необходимую основу безопасности, однако при массированных распределенных атаках их возможности оказываются ограниченными. Это связано с тем, что вредоносный трафик уже достигает инфраструктуры организации, а его обработка и последующая фильтрация сами по себе создают дополнительную нагрузку на оборудование и каналы связи.

Использование Cloudflare позволяет вынести первичную фильтрацию на внешний уровень. За счет этого значительная часть подозрительного и вредоносного трафика анализируется и блокируется до его поступления к серверной инфраструктуре. В результате уменьшается нагрузка на вычислительные ресурсы и сетевые каналы, а сама информационная система получает более высокий запас устойчивости в условиях атаки. Наиболее эффективным такой подход является в составе многоуровневой защиты, где облачная фильтрация сочетается с внутренними средствами сетевой и прикладной безопасности, корректной настройкой инфраструктуры и заранее определенными процедурами реагирования на инциденты. Именно такое сочетание мер в наибольшей степени соответствует современным требованиям к защите информационных систем от DDoS-атак.

Список использованных источников:

1. Информационные системы и технологии : учебник / под ред. В.В. Трофимова. – М. : Юрайт, 2021. – 549 с.

2. Баранова, Е.К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова. – М. : РИОР, 2020. – 256 с.

3. Головин, А.А. Информационная безопасность : учебное пособие / А.А. Головин. – М. : Форум, 2020. – 352 с.

4. Макаренко, С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями : монография / С.И. Макаренко. – СПб. : Наукоемкие технологии, 2018. – 122 с.

5. Грушо, А.Б. Защита информации в компьютерных системах и сетях / А.Б. Грушо, Е.А. Линев. – М. : Горячая линия – Телеком, 2018. – 342 с.

6. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М. : ДМК Пресс, 2019. – 592 с.