ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
И ЗАЩИТА ИНФОРМАЦИИ

DOI 10.21672/2074-1707.2021.53.1.063-074
УДК 004.051

ИССЛЕДОВАНИЕ ВОПРОСОВ СОВЕРШЕНСТВОВАНИЯ СИСТЕМ ЗАЩИТЫ ОТ DDOS-АТАК НА ОСНОВЕ КОМПЛЕКСНОГО АНАЛИЗА СОВРЕМЕННЫХ МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ

Статья поступила в редакцию 25.01.2021, в окончательном варианте – 30.01.2021.

Бачманов Дмитрий Андреевич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID:0000-0003-3474-6831, e-mail: bachmanov.dm@gmail.com
Очередько Андрей Романович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID: 0000-0002-1451-995X, e-mail: andrewlisten@mail.ru
Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com
Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru

В статье представлены результаты анализа роста развития ботнет-сетей и новых киберугроз при их использовании злоумышленниками. Проведен обзор и сравнение моделей реализации ботнет-сетей, в результате которого основными являются два их вида. Выделены и классифицированы основные виды атак, реализуемых при помощи использования инфраструктуры распределенных компьютерных сетей, сформированных в 7 основных группах с учетом актуальности, распространенности и величины нанесенного ущерба. По результатам анализа было определено, что наиболее распространенной и актуальной является тип атаки «Отказ в Обслуживании». Представлена классификация сервисов, предоставляющих услуги обеспечения защиты сетевых ресурсов от распределенных атак по типу «Отказ в обслуживании», по типу развертывания, уровню защищённости и видам предоставляемых сервисов. Приведены критерии сравнения с учетом их инфраструктуры, наличия технической поддержки и тестового периода, доступных типов защиты, возможностей, дополнительных опций, оповещения и отчетности, а также лицензирования. Практически реализован и показан способ интеграции сервиса DDoS-Guard Protection с дополнительным модулем на уровне приложения, который позволил расширить методы защиты от DDoS-атак. Различные модификации совместного применения модуля и модифицируемой системы позволяют повысить ожидаемый уровень выявления и предотвращения кибератак.

Ключевые слова: кибербезопасность, защита информации, ботнет, DDoS, распределенные компьютерные сети, отказ в обслуживании, киберугрозы, модель OSI

RESEARCH OF THE ISSUES OF IMPROVEMENT OF PROTECTION SYSTEMS AGAINST DDOS-ATTACKS BASED ON THE COMPREHENSIVE ANALYSIS OF MODERN INTERACTION MECHANISMS

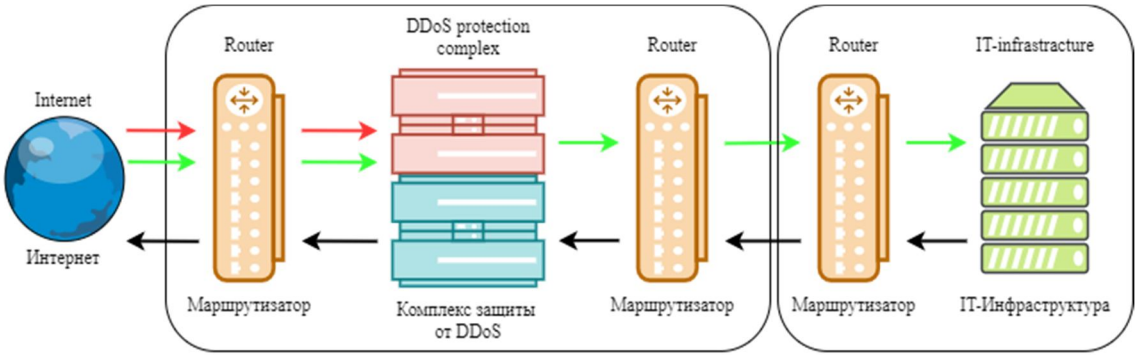
The article was received by the editorial board on 25.01.2021, in the final version – 30.01.2021.

Bachmanov Dmitriy A., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
postgraduate, ORCID: 0000-0003-3474-6831, e-mail: bachmanov.dm@gmail.com
Ocheredko Andrey R., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
postgraduate, ORCID: 0000-0002-1451-995X, e-mail: andrewlisten@mail.ru
Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru

The article presents the results of an analysis of the growth in the development of botnet networks and new cyber threats when they are used by cybercriminals. A review and comparison of the models for the implementation of botnet networks is carried out, as a result of which there are two main types. The main types of attacks carried out using the infrastructure of distributed computer networks are identified and classified, formed into 7 main groups, taking into account the relevance, prevalence and amount of damage. Based on the results of the analysis, it was determined that the most widespread and relevant type of attack is “Denial of Service”. The article presents a classification of services that provide services to ensure the protection of network resources from distributed attacks by the "Denial of Service" type, by the type of deployment, the level of security and the types of services provided. The comparison criteria are given taking into account their infrastructure, availability of technical support and a test period, available types of protection, capabilities, additional options, notification and reporting, as well as licensing. Practically implemented and shown a way to integrate the DDoS-Guard Protection service with an additional module at the application level, which made it possible to expand the methods of protection against DDoS attacks. Various modifications of the combined use of the module and the modified system make it possible to increase the expected level of detection and prevention of cyber-attacks.

Keywords: cybersecurity, information security, botnet, DDoS, distributed computer networks, denial of service, cyber threats, OSI model

Graphical annotation (Графическая аннотация)



Введение. Современные возможности связи из любой точки планеты при помощи интернета и подключенных к ней устройств не только значительно расширили наши возможности, но и открыли неограниченное число реализаций для таких угроз, как вирусы, спам, кибератаки и многие другие варианты атак для киберпреступников. В отчетах по количеству атак типа «Отказ в обслуживании» (DDoS) при помощи распределенных компьютерных сетей аналитики склоняются к выводу, что угроза, которая зародилась в 1999 г., до сих пор является одной из самых актуальных, и количество подобных инцидентов стремительно растет [1, 2, 3, 4, 5]. К примеру, за 2-й и 3-й кварталы 2020 года общее количество DDoS-атак на киберпространства, по сравнению с аналогичным периодом прошлого года, увеличилось в полтора раза [6]. Опасность и распространённость использования распределенных сетей ботнет в качестве основного средства совершения кибератак отмечается в исследованиях и прогнозах ведущих аналитиков [7]. Кроме того, об этом говорит и анализ областей, которые подвергаются данным атакам (рис. 1).

Исследователи «Лаборатории Касперского» в своих отчетах отмечают, что, помимо приведенных отраслей, большое количество атак также приходилось на сетевые ресурсы силовых, образовательных и административных ведомств [8, 9]. По оценке специалистов McAfee и Центра стратегических и международных исследований, общая сумма денежных потерь в 2020 году из-за атак киберпреступников превысила 1 000 000 млн долларов, что составляет 1 % от мирового ВВП [10]. В рамках современных исследований в области кибербезопасности [11] защита от таких видов атак на киберпространство занимает одно из важнейших мест в структуре адаптивных распределенных интеллектуальных систем защиты информации [12].

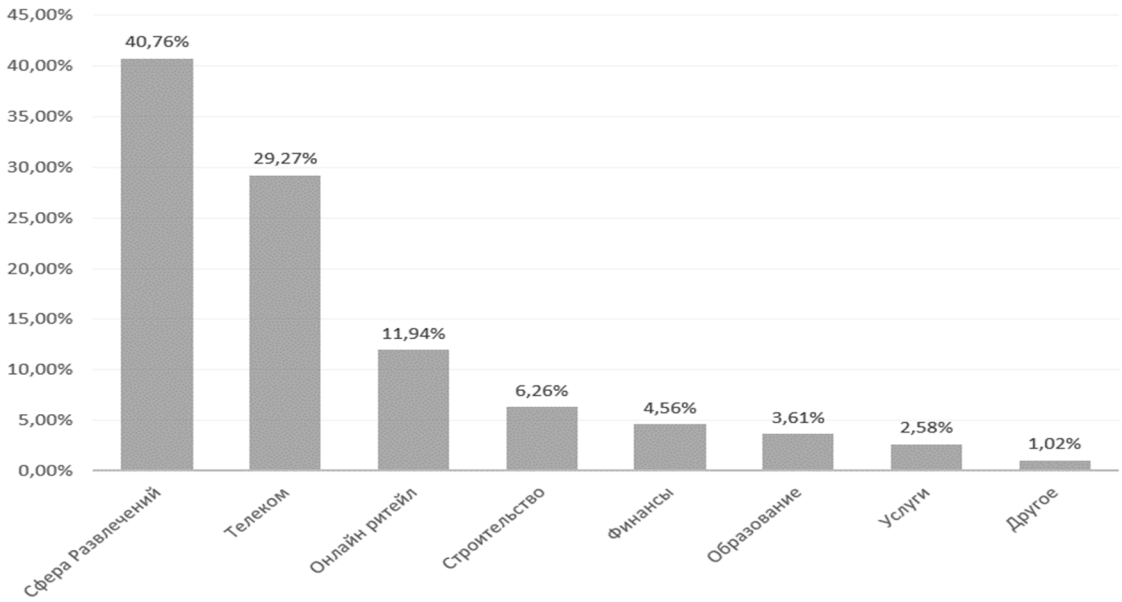


Рисунок 1 – Разделение областей, которые подвергаются атакам типа «Отказ в обслуживании» с применением распределенных компьютерных сетей

Характеристика ботнетов. Существует 2 модели реализации ботнетов (рис. 2). Реализация любой из них начинается с загрузки особого программного обеспечения со встроенным вредоносным кодом. После загрузки и установки устройство подключается к удаленному серверу, который был настроен как система управления сети (ботмастер). Используя систему управления, злоумышленник может периодически внедрять новый вредоносный код в установленную на устройство ботнета программу.

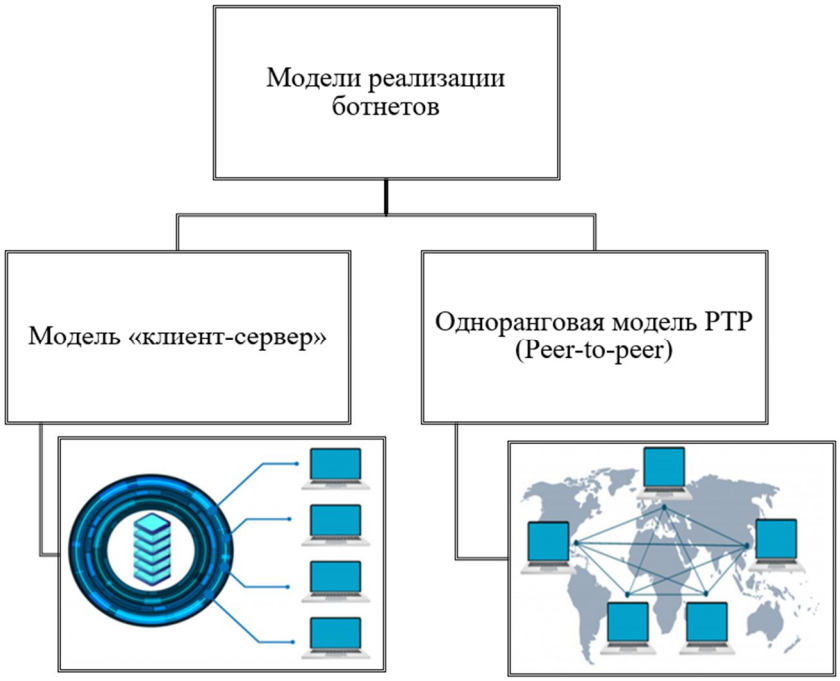


Рисунок 2 – Модели реализации ботнетов

Проведем сравнение моделей реализации ботнетов для выяснения их достоинств и недостатков (табл. 1).

Таблица 1 – Сравнение моделей реализации ботнетов

Название	Краткое описание	Достоинства	Недостатки
Модель «клиент – сервер»	Базовая сеть, в которой один сервер выступает в роли ботмастера, который посылает команды клиентам	Простота реализации и сохранение постоянного контроля над клиентскими устройствами	Легкость обнаружения и наличие одной контрольной точки, в отсутствии которой вся сеть перестает функционировать
Одноранговая модель PTP (peer-to-peer, P2P)	Каждое подключенное устройство работает независимо и как клиент, и как сервер. Координация и передача информации происходит между собой	Отсутствие централизованного управления и, вытекающая из этого, сложность детектирования	Не обнаружено

После построения ботнет-сети киберпреступник переходит к планированию, организации и реализации атак. Проведем сравнение основных типов ботнет-атак (табл. 2).

Таблица 2 – Сравнение основных типов ботнет-атак

Название атаки	Краткое описание	Сложность реализации	Уровень угрозы
Распределенные атаки типа «Отказ в обслуживании» (DDoS)	Лавинная посылка пакетов на целевую систему с целью исчерпания ресурсов и превышения полосы пропускания каналов связи	Низкая	Высокий
Применение шпионских программ и вредоносного ПО	Автоматическая установка программного обеспечения на устройствах входящих в распределенную компьютерную сеть	Высокая	Средний
Хищение персональной информации	Хищение персональной информации с зараженных устройств входящих в состав ботнета	Высокая	Высокий
Применение средств навязывания рекламы	Вредоносный код на зараженном компьютере может автоматически загружать, устанавливать и отображать всплывающие окна с рекламой или регулярно открывать в браузере определенные web-сайты	Средняя	Низкий
Рассылка спама	Отправка нежелательных сообщений по электронной почте	Средняя	Низкий
«Накручивание» кликов	Накрутка рекламной сети с оплатой за каждый клик с целью заставить платить определенного рекламодателя	Средняя	Средний
Фишинг	Поиск уязвимых серверов для размещения фишинговых сайтов с целью хищения персональных данных	Высокая	Высокий

В результате сравнения можно сделать вывод, что распределенные одноранговые P2P ботнет-модели являются сложно детектируемым средством совершения киберпреступлений с высоким уровнем угрозы реализуемых атак. Наиболее распространенной и требующей особого внимания являются распределенные атаки типа «Отказ в обслуживании» (DDoS), так как имеют относительно небольшую сложность реализации и высокую степень наносимого ущерба.

Классификация DDoS-атак. Обобщенная структура реализации такого вида атаки может быть представлена в виде структурированных объединенных групп-участников продолжительного по времени процесса (рис. 3).

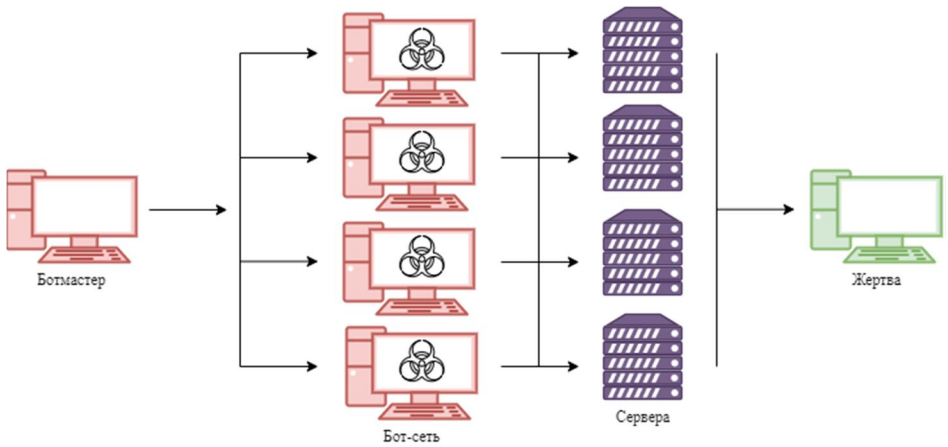


Рисунок 3 – Схема базовой DDoS-атаки

Опираясь на анализ способов реализации DDoS-атак, можно выделить основные виды (рис. 4) [13].

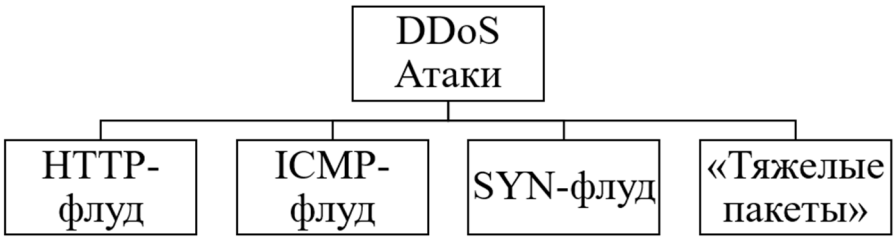


Рисунок 4 – Виды DDoS-атак

HTTP-флуд. Является самым распространённым типом DDoS-атаки. В специально сформированном запросе к серверу злоумышленник заменяет свой IP-адрес на сетевой идентификатор устройства внутри сети-жертвы, ожидая, что сервер на него ответит гораздо более емким ответом.

ICMP-флуд. Целью этого типа является перегрузка сетевого канала. Заключается в отправке ICMP-пакета усиливающей сети, либо через отправку UDP-пакетов. IP-адрес атакующего заменяется целевым, и на атакуемый сервер приходит ответ на команду, увеличенный во столько раз, сколько устройств подключено к усиливающей сети.

SYN-флуд. Так как компьютерам для совершения обмена информацией необходима установка соединения, при этом на само соединение выделяются компьютерные ресурсы – именно на их исчерпание направлена данная атака, отправляя ложные запросы на открытие соединений, которые не могут быть завершены до истечения тайм-аута.

«Тяжелые пакеты». Для реализации этого метода атаки злоумышленник с помощью ботнета отправляет серверу трудные для обработки пакеты данных, которые не переполняют канал связи, но отнимают ресурсы процессора, что может привести к его перегреву или перегрузке.

Из-за различия типов возникает проблема корректной и своевременной идентификации данных инцидентов информационной безопасности. Защита от слабых DDoS-атак организуется обобщенными процедурами настройки лимита подключений к серверу, ограничениями UDP-запросов и правильно настроенного Web application firewall (WAF). При более серьезных организованных многоэтапных атаках этими средствами уже не защититься, так как сам канал связи перестанет корректно функционировать. В этих случаях могут помочь только специальные средства защиты. Проведем сравнение и анализ современных средств защиты.

Средства защиты от DDoS-атак. В связи с высокой актуальностью данной проблемы на рынке представлено множество решений, позволяющих защищаться от распределенных атак типа «Отказ в обслуживании».

Существующие решения можно классифицировать по типу решения (рис. 5).

Рисунок 5 – Виды средств защиты от DDoS-атак по типу развёртывания

Достоинства локально развертываемых средств защиты заключаются в минимальной задержке, гибкой встраиваемости и самостоятельной настройке. При этом недостатки в виде высокой стоимости, необходимости нанимать и обучать персонал сопровождения, ограниченности функционала фильтрации и низкой пропускной способности явились причиной появления облачных и гибридных решений.

Облачные решения лишены недостатков высокой стоимости и необходимости содержать персонал сопровождения. Кроме того, они обладают высокой емкостью фильтрации и скоростью

подключения, имеют возможности получения экспертизы по эффективной нейтрализации атак и фильтрации атак на уровне веб-приложений. Из минусов можно выделить только увеличение задержки и необходимость пропуска конфиденциальных данных через облако.

Гибридные, в свою очередь, объединяют в себе как все хорошее от локальных и облачных типов, так и все плохое, нивелируя некоторые минусы друг друга.

Как правило, DDoS-атаки используют уязвимости и особенности сетевого и транспортного уровней модели взаимосвязи открытых систем (Open Systems Interconnection, OSI) [14], либо работают на уровне приложений и программных сервисов. В связи с этим появляется необходимость строить комплексную защиту, обеспечивающую высокий уровень детектирования и предотвращения подобных инцидентов. Определив требования, можно выделить следующие типы по уровню реализуемой защищенности, которую они осуществляют (рис. 6).

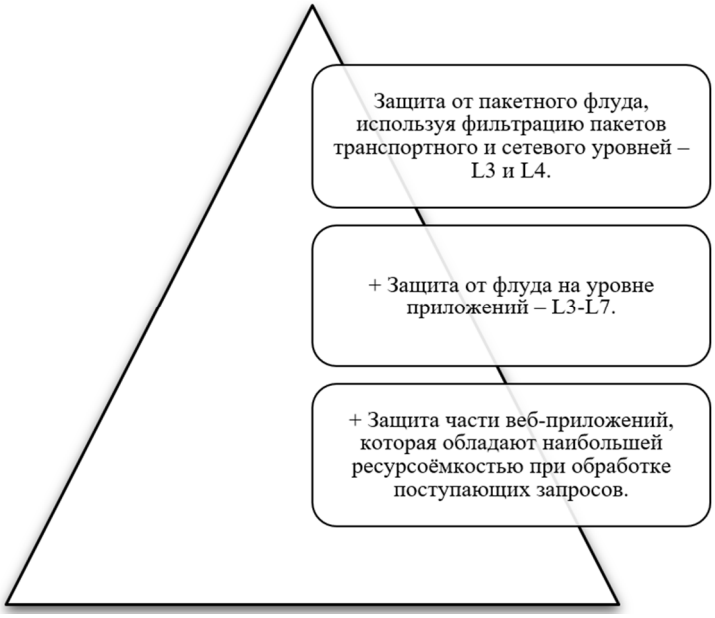


Рисунок 6 – Типы средств защиты от DDoS-атак по уровню защищенности

Включим в наше сравнение только те решения, которые обеспечивают минимум 2-й уровень защищенности и не являются индивидуальными решениями отдельных компаний. После анализа существующих решений сформировался список: Kaspersky DDoS Prevention, StormWall, Qrator, Ростелеком Anti-DDOS, DDoS-Guard Protection, CloudFlare DDoS Protection, Incapsula by Imperva.

Для сравнения будем использовать критерии комплексной оценки, которые были сформированы исходя из анализа мнений экспертов и подходящие для этого класса систем [15, 16, 17]:

1. Техническая поддержка – 7 %.
1.1. Дежурная смена реагирования на атаки 24 х 7.
1.2. Наличие русскоязычной технической поддержки.
2. Тестовый период – 3 %.
2.1. Наличие тестового периода.
2.2. Ограничения по функционалу во время тестового периода.
3. Инфраструктура – 10 %.
3.1. Наличие собственного/арендованного оборудования в ЦОД.
3.2. Используемое оборудование и ПО для очистки трафика.
4. Доступные типы подключаемой защиты – 25 %.
4.1. Защита сайта (смена А-записи DNS).
4.2. Защита сети (пула IP-адресов).
4.3. Защита автономной системы (ASN).
4.4. Услуги защищённого от DDoS ЦОД.
5. Возможности сервисов – 25 %.
5.1. Максимальная заявляемая мощность отражения атак в режиме statefull.
5.2. Фильтрация HTTPS без раскрытия ключей.
5.3. Возможность выделения нескольких IP для back-end.
5.4. Возможность балансировки между несколькими IP для back-end.

5.5. Заявленное время реакции на DDoS-атаку.

5.6. Заявленный процент ложных срабатываний под атакой (от легитимного трафика).

5.7. Возможность самостоятельно управлять фильтрацией трафика (включение/отключение/изменение параметров митигации).

5.8. Коридор гарантируемой доступности, в зависимости от тарифа (SLA), %.

5.9. Защита от ботов.

6. Дополнительные опции – 10 %.

6.1. Межсетевой экран уровня веб-приложений (WAF) (собственный, партнёрский).

6.2. Выделенные каналы MPLS VPN L2.

7. Система оповещения и отчетность – 5 %.

7.1. Экспорт отчётов.

7.2. Аналитика по трафику в личном кабинете.

8. Лицензирование – 15 %.

8.1. Ценовая политика (стоимость среднего тарифа).

Проведем сравнительный анализ выбранных систем (табл. 3).

Таблица 3 – Сравнение сервисов по полученным критериям

№ п/п	Наименование критерия	Kaspersky DDoS Prevention	Storm Wall	Qrator	Ростелеком Anti-DDOS	DDoS-Guard Protection	Incapsula by Imperva
1.1	Дежурная смена реагирования на атаки 24x7	0,07	0,07	0,07	0,07	0,07	0,07
1.2	Наличие русскоязычной технической поддержки	0	0,07	0	0	0,07	0
2.1	Наличие тестового периода	0,03	0,03	0,03	0,03	0,03	0,03
2.2	Ограничения по функционалу	0,03	0,03	0,03	0,03	0,03	0,03
3.1	Наличие собственного (арендованного) оборудования в ЦОД	0,1	0,1	0,1	0,1	0,1	0,1
3.2	Используемое оборудование и ПО для очистки трафика	0,1	0,1	0,1	0,05	0,1	0,1
4.1	Защита сайта (смена A-записи DNS)	0,25	0,25	0,25	0,25	0,25	0,25
4.2	Защита сети (пула IP-адресов)	0,25	0,25	0,25	0,25	0,25	0,25
4.3	Защита автономной системы (ASN)	0,25	0,25	0,25	0,25	0,25	0
4.4	Услуги защищённого от DDoS ЦОД	0	0,125	0,25	0,25	0,25	0
5.1	Максимальная заявляемая мощность отражения атак в режиме stateful	0,005	0,015	0,05	0,05	0,0125	0,05
5.2	Фильтрация HTTPS без раскрытия ключей	0,25	0,2	0,25	0,25	0,25	0,2
5.3	Возможность выделения нескольких IP для back-end	0,25	0,25	0,25	0,25	0,25	0,25
5.4	Возможность балансировки между несколькими IP для back-end	0,25	0,25	0,25	0,25	0,25	0,25
5.5	Заявленное время реакции на DDoS-атаку	0,15	0,15	0,2125	0,15	0,25	0,2375
5.6	Заявленный процент ложных срабатываний под атакой (от легитимного трафика)	0,2	0,2375	0,2375	0,25	0,245	0,25
5.7	Возможность самостоятельно управлять фильтрацией трафика (включение/отключение/изменение параметров митигации)	0	0,25	0	0,25	0,25	0,25
5.8	Коридор гарантируемой доступности, в зависимости от тарифа (SLA)	0,23	0,21	0,21	0,24	0,23	0,24
5.9	Защита от ботов	0,25	0,25	0,25	0,25	0	0,25
6.1	Межсетевой экран уровня веб-приложений (WAF) (собственный, партнёрский)	0,05	0,1	0,1	0,1	0,1	0,1
6.2	Выделенные каналы MPLS VPN L2	0,1	0,1	0,1	0,1	0,1	0
7.1	Экспорт отчётов	0,05	0,05	0,05	0,05	0,05	0,05
7.2	Аналитика по трафику в личном кабинете	0,05	0,05	0,05	0,05	0,05	0,05
8.1	Ценовая политика (стоимость среднего тарифа)	0,0135	0,054	0,0225	0,0405	0,15	0,0015
Итого:		2,93	3,44	3,36	3,56	3,59	3,01

Анализ результатов показывает, что сервисы DDoS-Guard Protection и StromWall являются самыми оптимальными. Решения от других компаний хоть и выигрывают по некоторым показателям, но в остальных либо проигрывают, либо предоставляют услуги, аналогичные с конкурентами за значительно большую стоимость. Так как система DDoS-Guard Protection предоставляет качество услуг на уровне с решением StromWall, но за меньшую стоимость, остановимся на ней и представим практическую реализацию дополнительных средств защиты на примере этой системы.

Практическая реализация. Функционал системы DDoS-Guard Protection покрывает практически все критерии эффективности, кроме пункта 5.9 – Защита от ботов. В рамках данной статьи мы рассмотрим способ интеграции данного решения с возможностью удовлетворять этому критерию, благодаря дополнительному модулю testcookie для NGINX, написанному на языке C.

Данный модуль позволит отсеять запросы ботов, которые используют HTTP-флуд и не имеют механизмов HTTP cookie и редиректа (рис. 7). В случае, если бот содержит данные механизмы, происходит проверка наличия в нем полноценного JavaScript Core (рис. 8). Если какое-либо условие является истиной, происходит отсеивание запросов от бота во время распределенной DDoS-атаки на уровень L7, некоторые из которых может пропустить DDoS-Guard Protection.

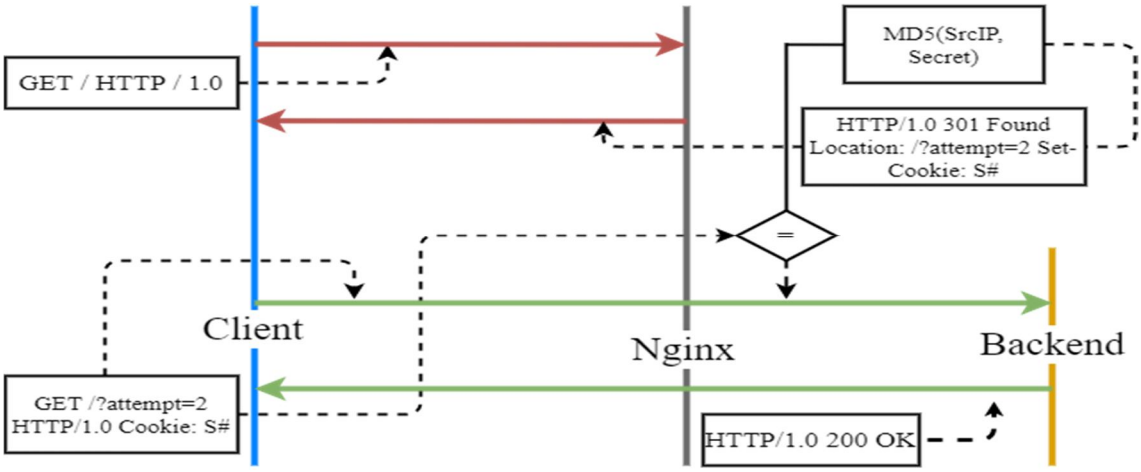


Рисунок 7 – Алгоритм работы модуля при отсутствии в боте механизмов редиректа и cookies

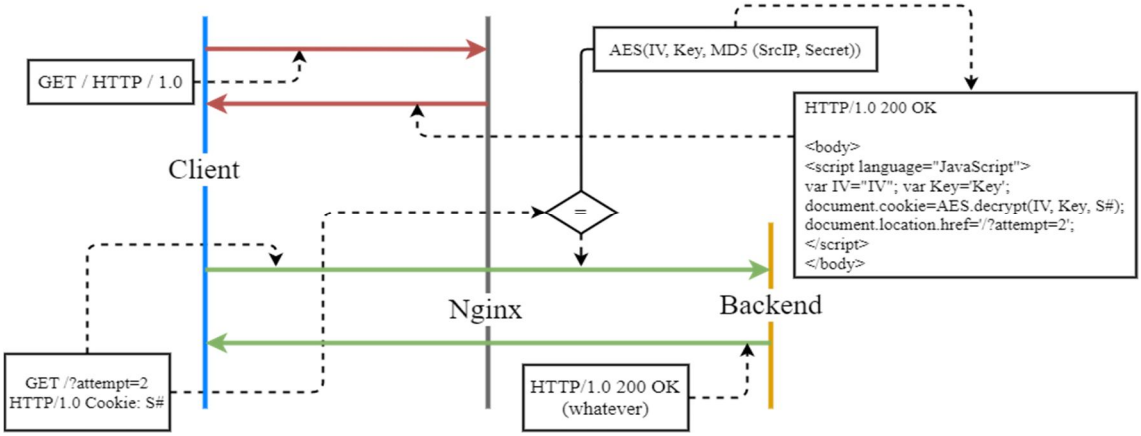


Рисунок 8 – Алгоритм работы модуля с механизмами редиректа и cookies в боте, но без JavaScript Core.

Модуль обладает широким функционалом (рис. 9).

Для установки данного модуля в NGINX-сервере последовательно выполняем команды на linux-сервере:

yum install gcc gcc-c++ kernel-devel
yum groupinstall 'Development Tools'
wget 'http://nginx.org/download/nginx-1.8.0.tar.gz'
tar -xzvf nginx-1.8.0.tar.gz
rpm -Uhv http://rpms.southbridge.ru/southbridge-rhel7-stable.rpm
yum install nginx nginx-module-testcookie

--add-module=/root/testcookie-nginx-module
make
make install
service nginx restart

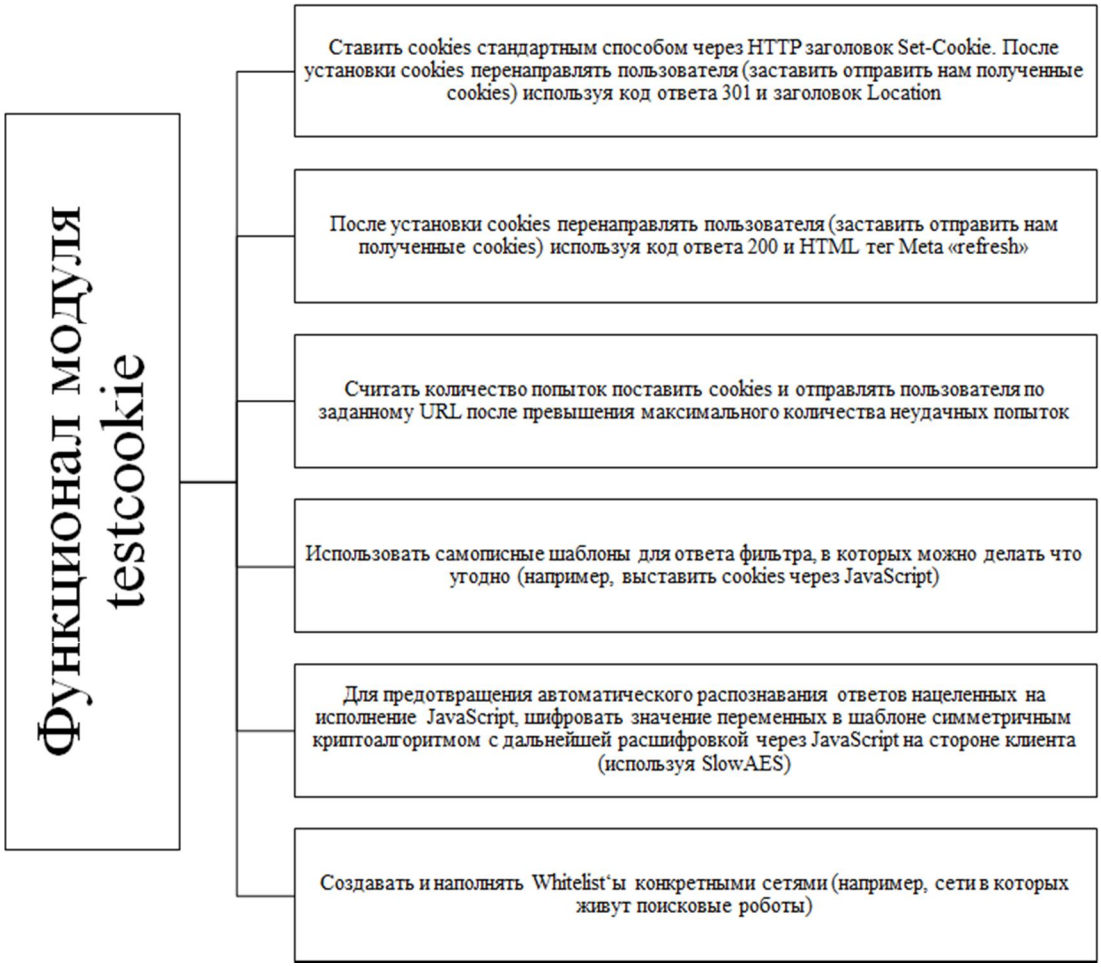


Рисунок 9 – Функционал модуля testcookie-nginx

После установки данного модуля и получения его в результате команды *nginx –V* должна появиться строка *--add-module=/root/testcookie-nginx-module*, можно приступать к формированию и настройке файлов конфигурации модуля.

Далее все зависит от сценария, который мы хотим применять:

1. Боты принимают редиректы и cookies, тот вариант, который будет использоваться в нашей конфигурации системы:

```
server {
    listen 80;
    server_name domain.com;

    testcookie off;
    testcookie_name BPC;
    testcookie_secret keepmescret;
    testcookie_session $remote_addr;
    testcookie_arg attempt;
    testcookie_max_attempts 3;
    testcookie_fallback /cookies.html?backurl=http://$host$request_uri;
    testcookie_get_only on;
    testcookie_redirect_via_refresh on;
```

```
        testcookie_refresh_template
'<html><body><script>document.cookie="BPC=$testcookie_set";document.location.href="$testcookie_
nexturl";</script></body></html>';

        location = /cookies.html {
          root /var/www/public_html;
        }
        location / {
          testcookie on;
          proxy_set_header Host $host;
          proxy_set_header X-Real-IP $remote_addr;
          proxy_pass http://127.0.0.1:8080;
        }
    }
```

2. Конфигурация сценария, где боты не понимают редиректы и cookies будет отличаться тем, что параметр *testcookie_refresh_template* указываться не будет.

Дополнение сервиса DDoS-Guard Protection, обеспечивающего эффективную защиту от DDoS-атак, тонко настроенным модулем testcookie-nginx-module позволило с большей вероятностью отсеивать трафик от ботов, благодаря этому эффективность защиты от большинства распределенных атак типа «Отказ в обслуживании» значительно возросла.

Заключение. В результате проведенного обзора, были обозначены темпы развития ботнетов и оценены риски атак, которые совершаются с помощью них. Обозначена важность и распространённость атаки типа «Отказ в обслуживании» (DDoS) с использованием распределенных сетей.

Были выделены основные классификации средств защиты по типу развертывания и по уровню защищенности. Анализ существующих реализаций позволил сформировать критерии сравнения систем, обеспечивающих безопасность сетевых ресурсов от распределенных DDoS-атак. Исходя из анализа этих критериев, были выбраны наиболее эффективные системы, такие как: Kaspersky DDoS Prevention, StormWall, Qrator, Ростелеком Anti-DDOS, DDoS-Guard Protection, CloudFlare DDoS Protection, Incapsula by Imperva. Анализ результатов показывает, что сервисы DDoS-Guard Protection и StromWall являются самыми оптимальными.

Модификация функциональных возможностей DDoS-Guard Protection, обеспечивающих эффективную защиту от DDoS-атак, тонко настроенным модулем testcookie-nginx-module позволила с большей вероятностью отсеивать трафик от ботов, благодаря этому эффективность защиты от большинства распределенных атаки типа «Отказ в обслуживании» значительно возросла.

Проведенные исследования формируют среду для дальнейшего изучения и совершенствования подходов, связанных с алгоритмическим, математическим и методическим обеспечением процесса защиты от DDoS-атак.

Библиографический список

1. Осторожно: DDoS // comnews.ru. – 2020. – Режим доступа: https://www.comnews.ru/content/211360/2020-11-02/2020-w45/ostorozhno-ddos, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

2. Что такое ботнет Mirai, и как я могу защитить свои устройства? // habr.com. – 2019. – Режим доступа: https://habr.com/ru/post/444436/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 30.12.2020).

3. Число DDoS-атак за год выросло на 241% // ixbt.com. – 2019. – Режим доступа: https://www.ixbt.com/news/2019/11/19/chislo-ddosatak-za-god-vyroslo-na-241.html, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

4. Ростелеком: объем DDoS-атак в Рунете вырос в 5 раз // xakep. – 2020. – Режим доступа: https://xakep.ru/2020/07/03/runet-ddos/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

5. Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»). ГОСТ Р 56938-2016 Защита информации. Защита информации при использовании технологий виртуализации. Общие положения. – 2017.

6. DDoS-атаки в III квартале 2020 года // securelist. – 2020. – Режим доступа: https:// securelist.ru/ddos-attacks-in-q3-2020/99091/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

7. Бабаш А. В. Актуальные вопросы защиты информации / А. В. Бабаш, Е. К. Баранова. – Москва, 2017. – С. 53–60.

8. Купереев О. DDoS-атаки в первом квартале 2020 года / О. Купереев, Е. Бадовская, А. Гутников // securelist by kaspersky. – 2020. – Режим доступа: https://securelist.ru/ddos-attacks-in-q1-2020/95949/, свободный. – Заглавие с экрана. – Яз. рус.

9. Отчеты о DDoS-атаках // securelist. – 2020. – Режим доступа: https://securelist.ru/category/ddos-reports/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

10. Ущерб от хакерских атак в мире превысил триллион долларов // dw. – 2020. – Режим доступа: https://www.dw.com/ru/ushherb-ot-hakerskih-atak-v-mire-prevysil-trillion-dollarov/a-55858266, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

11. Путято М. М. Кибербезопасность как неотъемлемый атрибут многоуровневого защищенного киберпространства / М. М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 3. – С. 94–102.

12. Путято М. М. Адаптивная система комплексного обеспечения безопасности как элемент инфраструктуры ситуационного центра / М. М. Путято, А. С. Макарян, А. Н. Черкасов, И. Г. Горин // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 4. – С. 75–84.

13. DDoS-атаки (Distributed Denial of Service) // anti-malware. – 2020. – Режим доступа: https://www.anti-malware.ru/threats/ddos-attack, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

14. Московский научно-исследовательский центр (МНИЦ) Государственный Комитет Российской Федерации по связи и информатизации. ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель // gostrf. – 2006. – Режим доступа: http://www.gostrf.com/normadata/1/4294818/4294818276.pdf, свободный. – Заглавие с экрана. – Яз. рус (дата обращения: 14.01.2021).

15. Жуков Р. Сравнение сервисов по защите от DDoS-атак / Р. Жуков // anti-malware. – 2019. – Режим доступа: https://www.anti-malware.ru/compare/DDoS-attack-protection-services, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.01.2021).

16. Подборка: 12 сервисов для защиты от DDoS-атак // Habr. – 2018. – Режим доступа: https://habr.com/ru/post/350384/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.01.2021).

17. Путято М.М. Исследование применения технологии deception для предотвращения угроз кибербезопасности / М. М. Путято, А. С. Макарян, Ш. М. Чич, В. К. Маркова // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 3. – С. 85–98.

References

1. Ostorozhno: DDoS [Caution: DDoS]. *comnews.ru*, 2020. Available at: https://www.comnews.ru/content /211360/2020-11-02/2020-w45/ostorozhno-ddos (accessed 12.01.2021).

2. Chto takoe botnet Mirai, i kak ya mogu zashchiti' svoi ustroystva? [What is the Mirai botnet, and how can I protect my devices?]. *habr.com*, 2019. Available at: https://habr.com/ru/post/444436/ (accessed 30.12.2020).

3. Chislo DDoS-atak za god vyroslo na 241% [The number of DDoS attacks for the year increased by 241%]. *ixbt.com*, 2019. Available at: https://www.ixbt.com/news/2019/11/19/chislo-ddosatak-za-god-vyroslo-na-241.html (accessed 12.01.2021).

4. Rostelekom: obem DDoS-atak v Runete vyros v 5 raz [The number of DDoS attacks for the year increased by 241%]. *xakep*, 2020. Available at: https://xakep.ru/2020/07/03/runet-ddos/ (accessed 12.01.2021).

5. *Gosudarstvennyy nauchno-issledovatelskiy ispytatelnyy institut problem tekhnicheskoy zashchity informatsii Federalnoy sluzhby po tekhnicheskomu i eksportnomu kontrolyu (FAU "GNIII PTZI FSTEK Rossii"). GOST R 56938-2016 Zashchita informatsii. Zashchita informatsii pri ispolzovanii tekhnologiy virtualizatsii. Obshchie polozheniya* [State Research and Testing Institute for Problems of Technical Protection of Information of the Federal Service for Technical and Export Control (FAA "GNII PTZI FSTEC of Russia"). GOST R 56938-2016 Information security. Information protection when using virtualization technologies. General provisions], 2017.

6. *DDoS-ataki v III kvartale 2020 goda* [DDoS attacks in the third quarter of 2020]. *securelist*, 2020. Available at: https://securelist.ru/ddos-attacks-in-q3-2020/99091/ (accessed 12.01.2021).

7. Babash A. V., Baranova E. K. *Aktualnye voprosy zashchity informatsii* [Current issues of information security]. Moscow, 2017, pp. 53–60.

8. Kupereev O., Badovskaya E., Gutnikov A. *DDoS-ataki v pervom kvartale 2020 goda* [DDoS attacks in the first quarter of 2020]. *securelist by Kaspersky*, 2020. Available at: https://securelist.ru/ddos-attacks-in-q1-2020/95949/

9. Otchety o DDoS-atakakh [DDoS Attack Reports]. *securelist*, 2020. Available at: https://securelist.ru/category/ddos-reports/ (accessed 12.01.2021).

10. Ushcherb ot khakerskikh atak v mire prevysil trillion dollarov [The damage from hacker attacks in the world exceeded a trillion dollars]. *dw*, 2020. Available at: https://www.dw.com/ru/ushherb-ot-hakerskih-atak-v-mire-prevysil-trillion-dollarov/a-55858266 (accessed 12.01.2021).

11. Putyato M. M., Makaryan A. S. Kiberbezopasnost kak neotemlemyy atribut mnogourovnevogo zashchishchennogo kiberprostranstva [Cyber Security as an Essential Attribute of Multilevel Protected Cyber Space]. *Prikaspiskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, pp. 94–102.

12. Putyato M. M., Makaryan A. S., Cherkasov A. N., Gorin I. G. Adaptivnaya sistema kompleksnogo obespecheniya bezopasnosti kak element infrastruktury situatsionnogo tsentra [Adaptive Integrated Security Assurance System as an Element of the Infrastructure of the Situation Center]. *Prikaspiskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, pp. 75–84.

13. DDoS-ataki (Distributed Denial of Service) [DDoS Attacks (Distributed Denial of Service)]. *anti-malware*, 2020. Available at: https://www.anti-malware.ru/threats/ddos-attack (accessed 12.01.2021).

14. Moskovskiy nauchno-issledovatelskiy tsentr (MNIC) Gosudarstvennyy Komitet Rossiyskoy Federatsii po svyazi i informatizatsii. GOST R ISO/MEK 7498-1-99 Informatsionnaya tekhnologiya (IT). Vzaimosvyaz otkrytykh

sistem. Bazovaya etalonnaya model. Chast 1. Bazovaya model [Moscow Research Center (MSIC) State Committee of the Russian Federation for Communications and Informatization. GOST R ISO/IEC 7498-1-99 Information technology. Open Systems Interconnection. Basic Reference Model. Part 1. The Basic Model]. *gostrf*, 2006. Available at: http://www.gostrf.com/normadata/1/4294818/4294818276.pdf (accessed 14.01.2021).

15. Zhukov R. Sravnenie servisov po zashchite ot DDoS-atak [Comparison of DDoS protection services]. *anti-malware*, 2019. Available at: https://www.anti-malware.ru/compare/DDoS-attack-protection-services (accessed 15.01.2021).

16. Podborka: 12 servisov dlya zashchity ot DDoS-atak [Selection: 12 services to protect against DDoS attacks]. *Habr*, 2018. Available at: https://habr.com/ru/post/350384/ (accessed 15.01.2021).

17. Putyato M. M., Makaryan A. S., Chich Sh. M., Markova V. K. Issledovanie primeneniya tekhnologii deception dlya predotvrashcheniya ugroz kiberbezopasnosti [Research On the Use of Deception Technology to Prevent Cybersecurity Threats]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, pp. 85–98.

DOI 10.21672/2074-1707.2021.53.1.074-082
УДК 004.051

ИССЛЕДОВАНИЕ IRP-СИСТЕМ НА ОСНОВЕ АНАЛИЗА МЕХАНИЗМОВ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья поступила в редакцию 15.01.2021, в окончательном варианте – 17.02.2021.

Очередько Андрей Романович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID: 0000-0002-1451-995X, e-mail: andrewlisten@mail.ru

Бачманов Дмитрий Андреевич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID:0000-0003-3474-6831, e-mail: bachmanov.dm@gmail.com

Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com

Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru

В статье рассматриваются особенности и функции систем реагирования на инциденты информационной безопасности. Представлен анализ современных решений IRP и описан процесс реагирования на типовые инциденты в системах этого класса. На основании экспертных мнений сформирован перечень критериев, которые были распределены в группы по зонам функциональной ответственности для дальнейшего сравнения работы IRP-систем. Произведена оценка основных и дополнительных характеристик IRP-систем с использованием сформированных критериальных групп. Анализ результатов сравнения показал, что наиболее перспективными решениями являются R-Vision IRP, IBM Resilient IRP и open-source решение – The Hive. Разработан и представлен алгоритм модуля предотвращения фишинговых атак, программная реализация которого произведена с использованием языка Python. В рамках интеграционных возможностей системы The Hive реализована пользовательская функция реагирования, которая не только потенциально улучшила работу системы при предотвращении фишинговых атак, но и увеличила осведомленность сотрудников об этой угрозе. Результатом является IRP-система с персональной гибкой настройкой отдельных элементов и является основой при формировании Центра обеспечения безопасности (SOC), который позволит вывести информационную безопасность организаций на новый уровень.

Ключевые слова: кибербезопасность, IRP-системы, инцидент информационной безопасности, кибератака, механизмы реагирования на инциденты, фишинговые атаки

RESEARCH OF IRP SYSTEMS BASED ON THE ANALYSIS OF MECHANISMS OF RESPONSE TO INFORMATION SECURITY INCIDENTS

The article was received by the editorial board on 15.01.2021, in the final version – 17.02.2021.

Ocheredko Andrey R., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
graduate student, ORCID: 0000-0002-1451-995X, e-mail: andrewlisten@mail.ru