УДК 004.738.5

# *КИБЕРБЕЗОПАСНОСТЬ В ГОСУДАРСТВЕННЫХ СТРУКТУРАХ: СТРАТЕГИИ ЗАЩИТЫ ОТ КИБЕРАТАК*

***Исрафилов А.***

*магистр, индивидуальный исследователь*

*Москва, Россия*

**Аннотация**

В данной статье анализируются такие киберугрозы, как фишинг, типы DDoS-атак, программы-вымогатели (ransomware), целью которых являются государственные органы. Также исследуется принцип действия кибератак. Изучается эффективность современных стратегий защиты таких, как файрвол (firewall), ПО Kaspersky DDoS Protection, системы обнаружения вторжения (Intrusion Detection System, IDS) и предотвращения вторжений (Intrusion Prevention System, IPS). В статье рассматриваются реальные кейсы атак на государственные структуры, которые повлекли за собой серьёзные последствия для различных инфраструктур, национальной безопасности и экономики.

**Ключевые слова:** кибербезопасность, государственные структуры, стратегии защиты, кибератаки, технологические решения, организационные меры.

# *CYBERSECURITY IN GOVERNMENT STRUCTURES: DEFENSE STRATEGIES AGAINST CYBERATTACKS*

***Israfilov A.***

*master's degree, individual researcher,*

*Moscow, Russia*

**Abstract**

This article analyzes cyber threats such as phishing, types of DDoS attacks, and ransomware programs, which target government agencies. It also explores the principles of cyber-attacks. The effectiveness of modern defense strategies such as firewalls, Kaspersky DDoS Protection software, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) is examined. The article discusses real cases of attacks on government structures that have had serious consequences for various infrastructures, national security, and the economy.

**Keywords:** cybersecurity, government structures, defense strategies, cyberattacks, technological solutions, organizational measures.

## Введение

В современном мире, где информационные технологии охватывают многочисленные сферы жизни общества, вопросы кибербезопасности государственных структур приобретают актуальность, так как правительственные объекты являются центрами принятия решений, хранения конфиденциальной информации и поддержания критически важных инфраструктур. Так, например, компания Atlas VPN (США), опираясь на данные Центра стратегических и международных исследований (CSIS), в первой половине 2023 года зарегистрировала 49 кибератак на государственные органы, что на 11% больше по сравнению с прошлым годом. Правительственные объекты были затронуты как минимум в 27 странах, в частности в США, на которые пришлось 16% от общего числа атак [1].

Целью данной работы является анализ киберугроз, с которыми сталкиваются государственные структуры, а также оценка эффективности существующих стратегий защиты, направленных на укрепление информационной защиты правительственных объектов в условиях постоянно меняющегося цифрового ландшафта.

**Основная часть**

История кибербезопасности включает в себя многочисленные примеры атак, оказавших существенное давление на государственные органы. Одно из первых упоминаний кибератак описывается в 1988 году. «Червь Морриса», разработанный Робертом Моррисом в Корнельском университете (США), изначально предназначался для академических задач: обнаружения слабостей в системах сетевой защиты и изучения масштабов Интернета. Однако в результате программирования кода была допущена ошибка: вместо однократного заражения каждой машины червь мог заразить одну и ту же систему неоднократно, что привело к значительному потреблению системных ресурсов и сбою в работе многих компьютеров. Более 6000 устройств вышли из строя. Это привело к значительным финансовым потерям, которые The US Government Accountability Office (GAO) оценил в диапазоне от 100 тысяч до 10 миллионов долларов США.

На текущий момент фишинг (вид интернет-мошенничества, цель которого – получение любой конфиденциальной информации пользователя или компании) является одной из главных киберугроз, с которой сталкиваются организации [2]. В основном злоумышленники отправляют сотрудникам электронные письма или сообщения, имитирующие официальные запросы или уведомления. Эти сообщения содержат опасные вложения, которые при переходе собирают конфиденциальную информацию, такую как логины и пароли, а также получают доступ к секретным данным. Так в январе 2024 года на Австралийское правительство была совершена крупнейшая в истории страны кибератака, в результате которой хакеры похитили свыше 2,5 миллиона документов, содержащих информацию государственной значимости.

DDoS-атаки (Distributed Denial of Service, DDoS) на государственные органы предназначены для перегрузки информационных систем и сервисов избыточным объемом запросов. Такая атака приводит к нарушению нормальной работы сервисов, делая их недоступными для пользователей. Злоумышленники

часто применяют DDoS-атаки в качестве метода киберпротеста, целью которого является дестабилизация ключевых функций в стране или распространение пропаганды. Например, правительство Новой Зеландии столкнулось в 2020 году с масштабной атакой на веб-сайт Новозеландской фондовой биржи (NZX). Торговля ценными бумагами приостановилась на 4 дня и это привело к многомиллиардным убыткам. Схема DDoS-атаки включает в себя три основных компонента (рис. 1): хакер (атакующий), центр управления и сеть ботнетов или компьютеров-зомби (компьютеры, зараженные вредоносным ПО и находящиеся под контролем злоумышленника без ведома владельца). Эти устройства генерируют огромное количество запросов к целевому ресурсу, например веб-сайту, что приводит к его перегрузке и отсутствию доступа для пользователей [3].

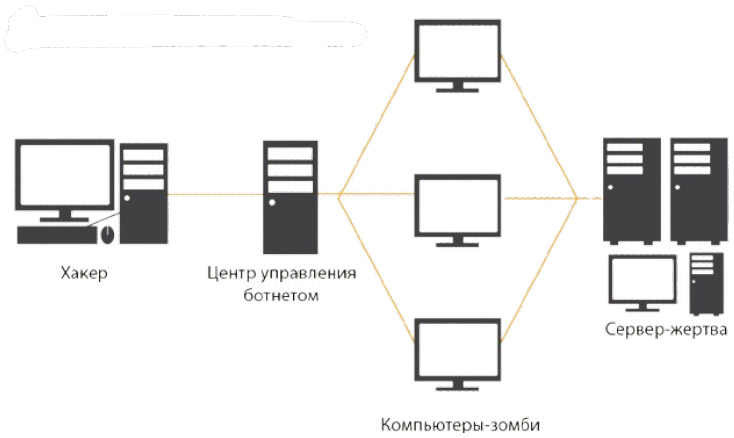


Рис. 1. Схема DDoS-атаки [3]

В таблице 1 рассмотрены основные типы DDoS- атак, активно используемые хакерами.

Таблица 1. Типы DDoS-атак [4, 5]

| Классификация | Название | Характерные черты |
|---|---|---|
| Объемные атаки | UDP floods, ICMP floods. | Производят огромное количество запросов, целью которых является перегрузка пропускной способности сетевой инфраструктуры. Измеряются в битах в секунду (Bps). |
| Атаки на протокол | Ping of Death, Smurf DDoS. | Направлены на истощение серверных ресурсов. Измеряются в пакетах в секунду (Pps). |

| Классификация | Название | Характерные черты |
|---|---|---|
| Атаки на прикладной протокол | Low-and-slow attacks, GET/POST floods | Замаскированы под обычные пользовательские запросы, нацелены на выведение из строя веб-сервер.<br>Измеряется в количестве запросов в секунду (Rps). |

Другие киберугрозы такие, как программы-вымогатели (ransomware) заражают компьютер сотрудника через вредоносные ссылки в фишинговых электронных письмах, шифруют файлы, делая их недоступными для пользователя или организации. Затем злоумышленники требуют выкуп за восстановление доступа к данным. Например, в мае 2021 года Управление здравоохранения Ирландии подверглось обширной атаке с использованием программы-вымогателя Conti, что привело к временному прекращению работы большинства IT-систем, вызвав перебои и задержки в предоставлении медицинской помощи и отмену запланированных процедур, а также произошла утечка медицинских данных пациентов и сотрудников.

**Основные стратегии защиты.** Государственные структуры активно внедряют передовые технологии для усиления защиты своих информационных систем [6]. Одним из основных инструментов, обеспечивающих кибербезопасность, является файрвол (firewall) или межсетевой экран, который используется для мониторинга и контроля входящего и исходящего сетевого трафика. Он может представлять из себя программу или сервер, защищающего, например, от фишинга и DDoS-атак (рис. 2).

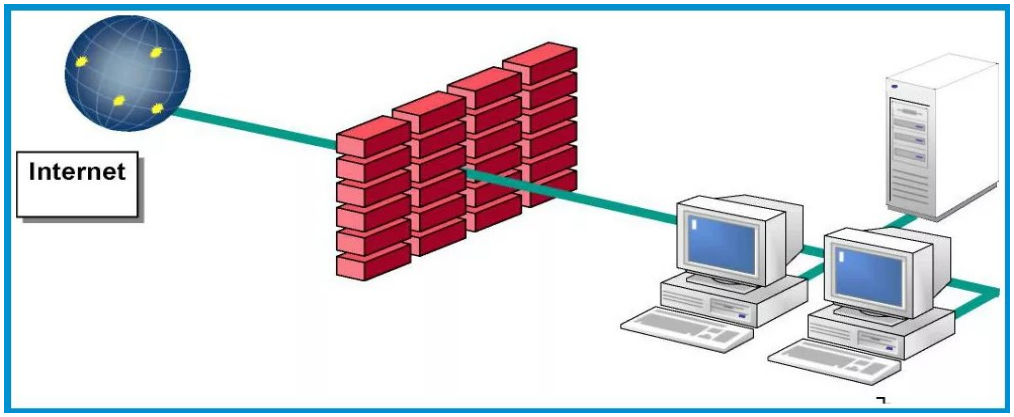


Рис. 2. Схема работы firewall

Примечание – составлено автором

Межсетевой экран действует как барьер между защищаемой внутренней сетью и внешним миром, определяя, какие пакеты данных допущены к прохождению через сеть на основе анализа встроенного списка разрешенных или запрещенных адресов [7]. Однако данный способ защиты неэффективен против угроз, которые уже проникли в сеть.

В качестве дополнительной защиты от DDoS-атак, а также от троянов (вредоносное ПО, проникающее в устройство под видом легитимного) и программ-вымогателей, обычно используют специальные антивирусные программы, например, Kaspersky DDoS Protection, разработанный в 2014 году компанией Kaspersky Lab (Россия). Программа устанавливает в локальной среде сенсор, собирающий данные о трафике, и в случае угрозы в реальном времени оперативно принимает ответные меры (рис. 3). Из-за фоновой работы сенсора, возможно снижение производительности устройства.

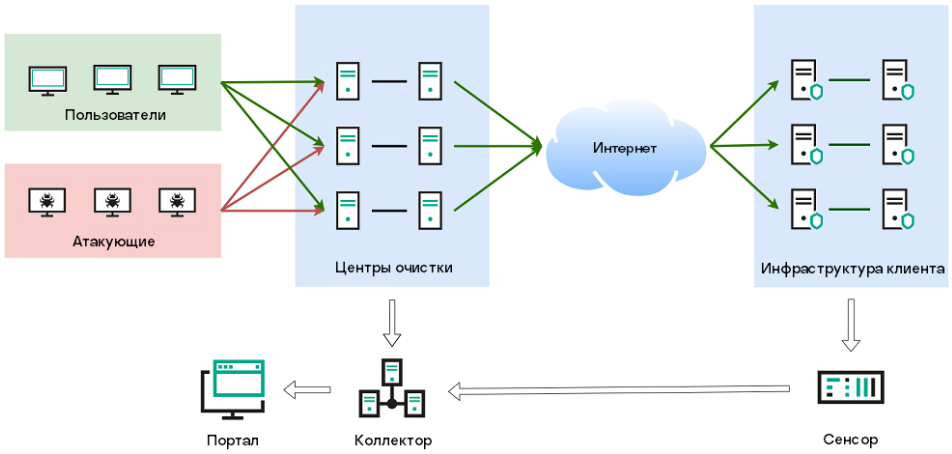


Рис. 3. Схема работы Kaspersky DDoS Protection [8]

Данные от пользователя сначала поступают в центры очистки, которые анализируют и фильтруют проходящие через них сетевые трафики, а коллектор, представляющий собой программно-аппаратный комплекс, обрабатывает информацию, полученную от центров очистки и сенсора, а затем определяет атаку и устраняет сбой сети [8]. Основным преимуществом антивирусных программ можно отметить простоту установки ПО, а также обеспечение защиты

не только на уровни сети, но и на уровне файлов, приложений, в то время как, например, межсетевой экран поддерживает безопасность только проходящего трафика, а также требует тщательной ручной настройки правил доступа и постоянного обновления внутреннего списка угроз.

Системы предотвращения вторжений (Intrusion Prevention System, IPS) и системы обнаружения вторжений (Intrusion Detection System, IDS) также анализируют сетевой трафик в реальном времени. В таблице 2 представлены преимущества и недостатки IDS и IPS [9].

Таблица 2. Преимущества и недостатки систем IDS и IPS [9]

| Система | Преимущества | Недостатки |
|---|---|---|
| IDS | Мониторинг сети в реальном времени. Оперативное оповещение администратора. | Возможно ложное срабатывание системы. Ограниченная эффективность против неизвестных атак. |
| IPS | Активная защита сети от угроз (блокировка IP- адреса, сброс соединение с ненадежным сервером). Возможность интеграции с существующими технологиями защиты. | Ложная блокировка обычной пользовательской сети. Сложность настройки политики безопасности. |

Работа данных систем в связке обеспечивает более высокий уровень защиты. IPS и IDS действуют путем сравнения трафика с базой данных известных угроз, а также способны адаптироваться к меняющимся атакам, постоянно обновляя хранилища информации [10]. Выбор между данными системами зависит от специфических потребностей организации, уровня желаемой защиты и финансовых возможностей. Стоимость внедрения систем IDS и IPS варьируется в зависимости от масштаба сети и требуемой функциональности. К общим затратам, например, можно отнести лицензионные платежи за ПО, расходы на настройку систем и обучение персонала. Малые организации могут внедрять базовые системы за несколько тысяч долларов, тогда как крупные могут тратить сотни тысяч или даже миллионы долларов.

Еще одним способом защиты от кибератак можно отметить шифрование. Оно позволяет преобразовать и скрыть конфиденциальные данные, например,

хранящиеся на жестких дисках или находящиеся в процессе передачи по сети Интернета, в зашифрованный код, доступ к которому возможен только у тех, у кого есть ключ шифрования. В качестве повышения уровня защиты можно использовать многофакторную аутентификацию (Multi-Factor Authentication, MFA), которая способна обеспечить безопасность доступа, но не к данным, а к учетным записям или сетевым ресурсам. MFA может запрашивать, помимо пароля, к пользовательскому профилю еще два или более доказательства своей личности (SMS с кодом, биометрические данные).

Каждый из перечисленных методов защиты сетевого трафика обеспечивает определённый уровень безопасности: некоторые только выявляют угрозы, в то время как другие активно участвуют в их нейтрализации. Использование комбинации различных стратегий обеспечивает создание эффективной многоступенчатой системы защиты.

**Вывод**

Исследование кибербезопасности в правительственных структурах подчеркивает её важность в поддержании государственной безопасности и защиты конфиденциальной информации. В свете роста кибератак необходимо применять комплексный подход защиты, что позволит правительственным объектам избежать определенных рисков, финансовых затрат на восстановление работоспособности поврежденных систем и деятельности специалистов. Дальнейшая разработка новых стратегий защиты сможет поспособствовать созданию более безопасного цифрового пространства для государственных органов.

**Библиографический спсиок**

1. Яковишин А.Д. РАЗВИТИЕ АЛГОРИТМОВ ИИ ДЛЯ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК // Дневник науки. – 2024. – №1.

2. Зиборев А.В. Использование цепочек blockchain и искусственного интеллекта в сфере логистики и автоперевозок // Инновационная наука. – 2023. – №8-2.

3. Zakharau A. The impact of fintech application implementation on improving consumer credit ratings // Sciences of Europe. – 2024. – №138. – pp. 14-16.

4. Богомолова Л.В. КЛАССИФИКАЦИЯ DDOS-АТАК И ИХ РЕАЛИЗАЦИЯ // Современные инновации. – 2022. – №1(41).

5. Голубятников А. О. DDOS-АТАКИ И МЕТОДЫ БОРЬБЫ С НИМИ // E-Scio. – 2022. – №10(73).

6. Tiumentsev D. Application of cryptographic technologies for information protection in cloud services // Stolypin Annals. – 2024. – Vol. 6. – № 3.

7. Артемов А.А. DATA CONTRACT В АНАЛИТИЧЕСКИХ СИСТЕМАХ: ОСНОВНЫЕ ПРИНЦИПЫ, ПРАКТИЧЕСКАЯ ПОЛЬЗА И МЕТОДЫ РЕАЛИЗАЦИИ // Вестник науки. – 2023. – №12(69).

8. Схема работы Kaspersky DDoS Protection // Kaspersky [Электронный ресурс]. — Режим доступа — URL: https://support.kaspersky.com/KDP/1.0/ru-RU/203022.htm (дата обращения 21.03.2024).

9. Давлетов А.Р. СОВРЕМЕННЫЕ МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ И ТЕХНОЛОГИЯ OCR ДЛЯ АВТОМАТИЗАЦИИ ОБРАБОТКИ ДОКУМЕНТОВ // Вестник науки. – 2023. – №10(67).

10. Галимов Р., Безруков П., Карпов М., Тюменцев Д., Киселев И. Будущее IT: как ИИ изменяет правила игры в индустрии // Информационные ресурсы России. – №1(196). – 2024. – с. 44-53.

*Оригинальность 80%*