УДК 159.9.016.4

# КОНТРОЛЬ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЙ ОБРАЗОВАНИЯ НА УРОВНЕ ФАЙЕРВОЛОВ

Марцинкевич В.А., Бегляк Е.В., Мигалевич С.А.

*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Беларусь, vlad@bsuir.by*

**Аннотация.** Рассмотрены основные принципы работы файерволов, функции и методы обнаружения и предотвращения, используемые для контроля инцидентов информационной безопасности. Проведен сравнительный анализ различных типовых схем подключения межсетевых экранов. Выполнено сравнение использования файерволов с маршрутизаторами и прокси – серверами.

**Ключевые слова.** Информационная безопасность, инцидент информационной безопасности, файервол.

Информационная безопасность является крайне актуальной темой в современном мире, особенно в связи с увеличением числа кибератак и утечек конфиденциальной информации. Важно обеспечивать защиту данных как на личном уровне, так и на уровне организаций и государств. Стремительное развитие технологий также требует постоянного обновления методов защиты информации.

Согласно данным отчета Check Point Research количество кибератак в июле 2022 года на сектор образования во всём мире в два раза превысило средний показатель по всем остальным отраслям. Также можно отметить, что за 2021 и 2022 годы объём образовательных услуг и научных исследований вырос на 114 %.

«Переход к дистанционному обучению значительно увеличил зону потенциальной атаки хакеров. Другими словами, перед ними открываются гораздо более широкие возможности для проникновения в компьютерные сети. Всё, что нужно, – это чтобы один преподаватель, учащийся или родитель нажал на фишинговое электронное письмо, созданное киберпреступником, и атака вымогателей может начаться» [1].

Также, можно отметить, что в 2022 году с началом приемной кампании перестали работать сайты ряда вузов России, например, Российского университета дружбы народов и Московского политехнического университета.

По данным компании StormWall, что за год к сентябрю 2021-го число DDoS-атак на российские учебные заведения, включая школы, увеличилось на 118 %.

Инциденты информационной безопасности – это события, которые нарушают конфиденциальность, целостность или доступность информации. Они могут быть вызваны различными причинами, включая кибератаки, утечки данных, вирусы и мошенничество.

Инциденты информационной безопасности могут иметь серьезные последствия для учреждений образования. Они могут привести к утечке конфиденциальной информации, повреждению систем и сетей, потере данных и нарушению доверия клиентов.

Некоторые из наиболее распространенных типов инцидентов информационной безопасности включают:

1. Кибератаки: включают в себя взломы, фишинг, вредоносные программы и денежные мошенничества.

2. Утечка данных: несанкционированный доступ к конфиденциальной информации, такой как персональные данные клиентов или корпоративные секреты.

3. Сетевые нарушения: нарушение безопасности сети, такое как перехват трафика или отказ в обслуживании (DDoS) атаки.

4. Физические инциденты: кража или потеря компьютеров, носителей информации или другого оборудования, содержащего конфиденциальные данные.

5. Нарушение политик безопасности: невыполнение правил и процедур, установленных организацией для обеспечения безопасности информации.

Для предотвращения и реагирования на инциденты информационной безопасности организации могут использовать различные меры, включая установку защитного программного обеспечения, обучение сотрудников, регулярное обновление систем и мониторинг сетей на предмет аномалий.

Контроль инцидентов информационной безопасности – это процесс управления и реагирования на нарушения безопасности информационных систем.

Одним из основных инструментов обеспечения безопасности локальной сети являются файерволы. Файерволы представляют собой программное или аппаратное оборудование, которое контролирует и фильтрует сетевой трафик, позволяя только разрешенным пользователям получать доступ к ресурсам сети. Они играют ключевую роль в предотвращении несанкционированного доступа и защите от различных видов кибератак [2].

При выборе схемы подключения файервола (межсетевого экрана) необходимо учитывать структуру Компьютерной сети, требования безопасности и потребности организации.

Среди многообразия схем подключения файерволов типовыми являются следующие:

– схема единой защиты локальной сети;

– схема с защищаемой закрытой и не защищаемой открытой подсетями;

– схема с раздельной защитой закрытой и открытой подсетей.

На рисунке 1 представлена схема единой защиты локальной сети. Это является наиболее простым решением, при котором файервол экранирует внутреннюю сеть от внешней. Между маршрутизатором и межсетевым экраном существует единственный путь, по которому проходит весь трафик. Такую схему подключения рекомендуется использовать при отсутствии открытых серверов во внутренней сети.


Рисунок 1 – Схема единой защиты локальной сети

На рисунке 2 представлена схема с защищаемой закрытой и не защищаемой открытой подсетями, такое подключение целесообразно использовать при невысоких требованиях по безопасности к открытой подсети.

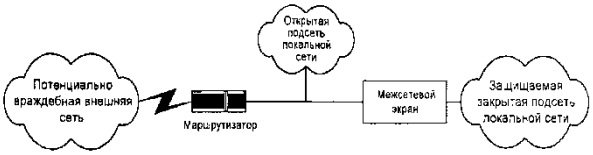


Рисунок 2 – Схема с защищаемой закрытой и не защищаемой открытой подсетями

Реализация схем подключения с раздельной защитой закрытой и открытой подсетей возможна с использованием одного файервола с тремя сетевыми интерфейсами или двух файерволов с двумя сетевыми интерфейсами. В обоих вариантах реализации доступ к открытой и закрытой подсетям осуществляется через файервол. При этом доступ к открытой сети не дает права осуществлять доступ к закрытой внутренней подсети.

На рисунке 3 приведена типовая схема подключения с раздельной защитой закрытой и открытой подсетей с использованием одного межсетевого экрана с тремя интерфейсами.

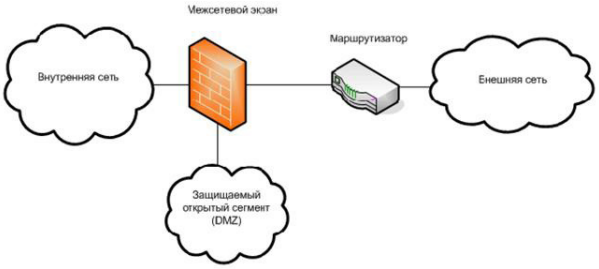


Рисунок 3 – Схема с раздельной защитой закрытой и открытой подсетей на основе одного файервола с тремя сетевыми интерфейсами

На рисунке 4 представлен вариант реализации схемы подключения с раздельной защитой закрытой и открытой подсетей с использованием двух файерволов с двумя сетевыми интерфейсами.


Рисунок 4 – Схема с раздельной защитой закрытой и открытой подсетей на основе двух файерволов с двумя сетевыми интерфейсами

Из представленных двух вариантов подключения с раздельной защитой закрытой и открытой подсетей наибольшую безопасность обеспечивает схема на основе двух межсетевых экранов с двумя сетевыми интерфейсами.

***1. Основные принципы работы файерволов.*** Файерволы работают на основе набора правил, которые определяют, какой сетевой трафик разрешен, а какой – блокируется. Они могут быть настроены на разных уровнях: уровне сети, уровне приложений или уровне пользователей. Ключевыми принципами работы файерволов являются:

– Фильтрация трафика: файерволы анализируют пакеты данных, проходящие через них, и блокируют нежелательный трафик, основываясь на заранее определенных правилах.

– Аутентификация: файерволы могут требовать от пользователей предоставления учетных данных для получения доступа к сети.

– Шифрование: файерволы могут использовать шифрование для защиты передаваемых данных от несанкционированного доступа.

***2. Основные функции файерволов.*** Файерволы выполняют ряд функций, направленных на обеспечение безопасности локальной сети:

– Блокировка нежелательного трафика: файерволы могут блокировать доступ к определенным веб-сайтам или приложениям, а также предотвращать передачу конфиденциальной информации.

– Ограничение доступа: файерволы могут ограничивать доступ к определенным ресурсам сети, основываясь на учетных данных пользователя, IP-адреса или протокола.

– Обнаружение и предотвращение атак: файерволы могут обнаруживать и блокировать попытки несанкционированного доступа или другие виды кибератак.

– Мониторинг сетевого трафика: файерволы могут анализировать сетевой трафик и регистрировать любые подозрительные активности.

***3. Основные методы контроля инцидентов информационной безопасности. Некоторые из них включают:***

– Сигнатурное обнаружение: файерволы могут использовать базу данных сигнатур для обнаружения известных видов атак или вирусов.

– Анализ поведения: файерволы могут анализировать сетевой трафик и обнаруживать аномальное поведение, которое может указывать на наличие инцидента безопасности.

– Инспекция содержимого: файерволы могут анализировать содержимое пакетов данных и блокировать нежелательные или вредоносные файлы.

– Расширенные уровни безопасности: некоторые файерволы могут предоставлять дополнительные функции безопасности, такие как защита от DDoS-атак или веб-фильтрация.

– Отслеживание и регистрация инцидентов: Файервол должен быть настроен на регистрацию всех событий и инцидентов, связанных с сетевым трафиком. Это позволяет Вам отслеживать и анализировать активность, выявлять аномалии и реагировать на возможные инциденты.

– Обновление и патчи: Важно регулярно обновлять программное обеспечение файервола и устанавливать патчи для устранения известных уязвимостей. Это помогает предотвратить атаки, связанные с уязвимыми версиями программного обеспечения.

– Анализ журналов и инцидентов: При просмотре журналов файервола требуется обращать внимание как на источник, так и на место назначения трафика, а также на тип трафика, который блокируется или разрешается. При просмотре журналов брандмауэра надо искать закономерности, которые могут указывать на подозрительную активность, например несколько неудачных попыток входа в систему с одного и того же IP-адреса или большое количество попыток подключения к одному порту. На рисунке 5 представлен журнал логирования программного файервола Check Point.

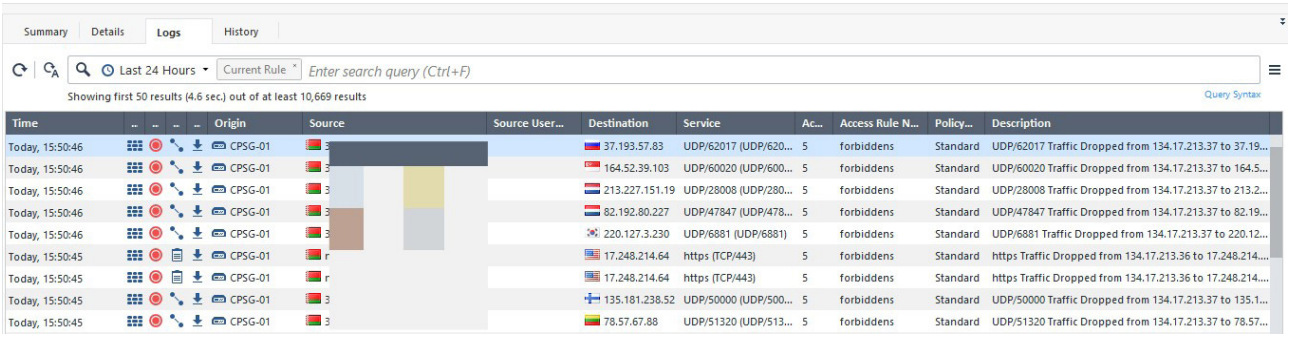


Рисунок 5 – Журнал логирования программного файервола Check Point

Понимая, как читать журналы брандмауэра, можно эффективно выявлять потенциальные угрозы безопасности и принимать меры по их устранению [3].

***Сравнение файерволов с маршрутизаторами и прокси – серверами.*** Маршрутизатор может использоваться для фильтрации трафика, но его функциональность в области безопасности ограничена, так как имеют доступ лишь к ограниченной части заголовка пакетов, не поддерживают хранение информации о истории соединения, имеют очень ограниченные возможности по действиям над информацией.

Прокси – сервер может использоваться для контроля доступа к веб-ресурсам, фильтрации содержимого и защиты от угроз. Прокси-серверы могут обеспечивать дополнительный уровень безопасности, например, блокируя доступ к вредоносным сайтам или контролируя использование приложений. Прокси-серверы не всегда эффективны в обнаружении и блокировании всевозможных угроз на уровне сети.

Важно отметить, что контроль инцидентов информационной безопасности учреждений образования на уровне файервола является только одной из составляющих общей стратегии безопасности. Для достижения наивысшего уровня безопасности рекомендуется использовать комплексный подход, включающий в себя также другие меры безопасности, такие как антивирусное программное обеспечение, системы обнаружения вторжений и политики безопасности.

**Литература**

1. Skillbox Образование 4.0 [Электронный ресурс]. – Режим доступа: https://skillbox.ru/media/education/sektor-obrazovaniya-okazalsya-naiboleepodverzhen-risku-kiberatak/. – Дата доступа: 24.02.2024.

2. Информационные технологии [Электронный ресурс]. – Режим доступа: https://kunegin.com/ref3/ipsec/firewall.htm. – Дата доступа: 17.02.2024.

3. Cybriant [Электронный ресурс]. – Режим доступа: https://cybriant.com/what-is-firewall-logging-and-why-is-it-important/. – Дата доступа: 17.02.2024.

## CONTROL OF INFORMATION SECURITY INCIDENTS OF EDUCATIONAL INSTITUTIONS AT THE FIREWALL LEVEL

U.A. Martsinkevich, C.V. Begliak, S.A. Migalevich

*Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus, vlad@bsuir.by*

**Annotation.** The basic principles of firewall operation, functions and methods of detection and prevention used to control information security incidents are considered. A comparative analysis of various typical firewall connection schemes was carried out. A comparison has been made of the use of firewalls with routers and proxy servers.

**Keywords:** information security, information security incident, firewall.