УДК 004.056.53

МЕТОДЫ И СПЕЦИФИКА ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ ПРИ РАБОТЕ С BIG DATA

Е.А. Лещенко
Инженер-программист отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР, ассистент кафедры информатики, магистрант кафедры ПИКС
e.leshchenko@bsuir.by

Е.В. Бегляк
Инженер-программист 1 категории отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР, ассистент кафедры ВМиП, магистрант кафедры ПИКС
katarina@bsuir.by

В.А. Марцинкевич
Ведущий инженер-электроник отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР, ассистент кафедры ЭВМ, магистрант кафедры ИКТ
vlad@bsuir.by

Е.А. Лещенко

Окончил Белорусский государственный университет информатики и радиоэлектроники. Инженер-программист отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР, ассистент кафедры информатики БГУИР, магистрант кафедры проектирования информационно-компьютерных систем БГУИР.

Е.В. Бегляк

Окончила Белорусский государственный университет информатики и радиоэлектроники. Инженер-программист отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР, ассистент кафедры вычислительных методов и программирования БГУИР, магистрант кафедры проектирования информационно-компьютерных систем БГУИР.

В.А. Марцинкевич

Окончил Минский радиотехнический институт. Ведущий инженер-электроник отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР, ассистент кафедры электронных вычислительных машин БГУИР, магистрант кафедры инфокоммуникационных технологий БГУИР.

Аннотация. В данной работе рассмотрены методы и принципы защиты компьютерных сетей, в которых выполняется передача *Big Data*.

Показано, что необходим комплексный подход из различных методов безопасной передачи информации для защиты компьютерных сетей при работе с большими данными.

Ключевые слова: защита компьютерной сети, шифрование, передача больших данных

Введение. В современном информационном обществе компьютерные сети являются неотъемлемой частью бизнес-процессов и повседневной жизни многих людей. Однако, с ростом зависимости от компьютерных сетей, возрастает объем данных, генерируемых, собираемых анализируемых вычислительными системами и вопросы безопасности становятся все более актуальными. Особенно важно обеспечить защиту при работе с большими данными, так как такие сети обычно содержат большое количество

конфиденциальной информации. Злоумышленники могут использовать различные методы для вторжения в компьютерные сети и получения несанкционированного доступа к конфиденциальной информации.

Безопасность больших данных. Сегодня почти каждая организация рассматривает возможность внедрения больших данных, потому что они видят их потенциал и пытаются его использовать. Независимо от размера организации, каждый пытается защитить свои данные.

Согласно отчету IBM и Института Понемона за 2023 год, средняя стоимость утечки данных в 2023 году достигнет 4,45 миллиона долларов США, увеличившись на 2% по сравнению с 2022 годом (4,35 миллиона долларов США).

Обеспечение безопасности больших данных затруднено по нескольким причинам.

Некоторые из них упомянуты ниже:

– В режиме реального времени поступает множество данных из разных источников с разными потребностями в защите.

– Существует несколько типов данных, объединенных вместе.

– Доступ к данным получают множество разных пользователей с различными аналитическими требованиями.

– Быстро развивающиеся инструменты, финансируемые сообществом открытого исходного кода.

– Автоматическая репликация данных между несколькими узлами [1].

Методы защиты компьютерных сетей. Методы защиты компьютерной сети при работе с большими данными включают в себя несколько аспектов. Во-первых, необходимо обеспечить защиту самой сети от внешних угроз. Во-вторых, необходимо обеспечить защиту данных, хранящихся и передаваемых по сети. Большие данные часто содержат конфиденциальную информацию, и их утечка может привести к серьезным последствиям. Для защиты данных применяются различные методы шифрования, аутентификации и авторизации.

Защита сети сети от внешних угроз включает в себя:

1 Использование брандмауэра – это программное или аппаратное устройство, которое контролирует и фильтрует трафик, проходящий через сеть. Он позволяет установить правила доступа к сети и блокировать подозрительный или вредоносный трафик. Брандмауэр также может обнаруживать и предотвращать атаки на сеть, такие как *DDoS*-атаки или попытки взлома. Брандмауэр также может предоставлять функции аутентификации и шифрования данных, а также возможность мониторинга и журналирования сетевой активности.

2 Использование виртуальных частных сетей (*VPN*) – создание защищенного канала связи между удаленными участниками сети.

3Контроль доступа – установление политик и правил, определяющих, кто имеет доступ к данным и какие операции он может выполнять.

4 Шифрование данных – преобразование информации в неразборчивый вид для посторонних лиц.

5 Резервное копирование – создание резервных копий данных для их восстановления в случае катастрофы или взлома.

Использование антивирусного программного обеспечения – для обнаружения и удаления вредоносных программ, таких как вирусы, трояны, шпионское ПО и другие угрозы безопасности. Она может быть установлена на отдельные компьютеры в сети или на центральный сервер для защиты всех устройств в сети. Антивирусная программа сканирует файлы и систему на наличие вредоносных программ, блокирует их действия и предупреждает пользователя о потенциальных угрозах. Она также может обновляться

регулярно для получения новых определений вирусов и обновлений программы, чтобы эффективно бороться с новыми угрозами.

Принципы защиты компьютерной сети при работе с большими данными. Одним из принципов защиты компьютерной сети является принцип делегирования полномочий. Делегирование полномочий в компьютерной сети – это процесс передачи определенных прав и обязанностей от одного пользователя или группы пользователей другому пользователю или группе пользователей. Это позволяет распределить ответственность и управление в сети, обеспечить эффективное выполнение задач, а также это ограничивает возможности злоумышленников в случае взлома аккаунта или устройства. Делегирование полномочий может включать следующие аспекты:

1 Права доступа. Администратор сети может делегировать определенные права доступа к файлам, папкам, приложениям или другим ресурсам сети. Например, администратор может предоставить право на чтение, запись или выполнение определенных файлов или папок пользователю или группе пользователей.

2 Управление учетными записями. Администратор сети может делегировать управление учетными записями, включая создание, удаление и изменение учетных записей пользователей или групп.

3 Управление политиками безопасности. Администратор сети может делегировать управление политиками безопасности, включая настройку правил брандмауэра, шифрование данных, установку антивирусного программного обеспечения и т. д.

4 Мониторинг и аудит. Администратор сети может делегировать задачи мониторинга и аудита определенным пользователям или группам.

Регулярная установка обновлений и исправлений программного обеспечения для закрытия уязвимостей также необходима при работе с большими данными. Уязвимости могут быть использованы злоумышленниками для взлома системы, поэтому регулярное обновление является важным аспектом безопасности. Приложения, работающие в компьютерной сети, должны быть защищены от уязвимостей и возможных атак. Для этого можно использовать патчи безопасности, аудит кода и использование безопасных разработочных практик.

Согласно принципу непрерывности работы компьютерной сети, система должна быть способна продолжать свою работу даже в случае возникновения сбоев или атак. В случае возникновения непредвиденных событий или катастрофических ситуаций этот метод позволяет минимизировать потери и простои в работе. В компьютерной сети он включает в себя меры по защите и восстановлению данных, приложений и инфраструктуры, чтобы минимизировать потери и простои в работе.

Принцип обучения пользователя основам безопасности состоит в том, чтобы обучить пользователей правильным практикам и процедурам, которые помогут им избежать угроз безопасности и защитить компьютерную сеть от потенциальных атак. Они должны понимать, какие действия могут представлять угрозу и какие меры предосторожности следует принять. Основные аспекты этого подхода включают в себя осведомленность о рисках; обучение пользователя основам безопасности, включая правила использования паролей, распознавание подозрительных электронных писем и ссылок и т. д.; постоянное обновление знаний; обратная связь и наказание за нарушение правил безопасности, чтобы создать ответственность и мотивацию для соблюдения правил; регулярные проверки и аудиты.

Шифрование больших данных. Как было сказано выше, необходимо обеспечить защиту данных, хранящихся и передаваемых по сети. Большие данные часто содержат конфиденциальную информацию, и их утечка может привести к серьезным последствиям. Для защиты данных применяются различные методы шифрования, аутентификации и авторизации.

С помощью ключей шифрования компьютерный алгоритм преобразует текстовые символы в непонятную форму, гарантируя, что только авторизованные лица, обладающие необходимыми ключами, смогут разблокировать и получить доступ к контенту. В определенной степени важно обеспечить безопасность различных форм данных, включая файлы, базы данных и сообщения электронной почты.

Одним из основных подходов к шифрованию больших данных является использование асимметричного шифрования. Этот метод основан на использовании пары ключей: открытого и закрытого. Открытый ключ используется для шифрования данных, а закрытый ключ – для их расшифровки. Такой подход позволяет безопасно передавать данные, так как открытый ключ может быть распространен публично, в то время как закрытый ключ хранится в секрете у владельца данных.

Для шифрования больших данных также широко применяются алгоритмы блочного шифрования, такие как *AES* (*Advanced Encryption Standard*) и *Blowfish*. Эти алгоритмы разбивают данные на блоки фиксированного размера и применяют к каждому блоку операции шифрования. Блочные алгоритмы обеспечивают высокую степень безопасности и эффективности при шифровании больших объемов данных [2].

Кроме того, при шифровании больших данных важным аспектом является управление ключами. Ключи шифрования должны быть хранены в безопасном месте и доступны только авторизованным пользователям. Для обеспечения безопасности ключей можно использовать различные методы, включая аппаратное шифрование и многофакторную аутентификацию. Также необходимо регулярное обновление шифровальных ключей для предотвращения возможности их взлома.

Важно отметить, что шифрование больших данных может быть ресурсоемким процессом, особенно при использовании сильных алгоритмов шифрования. Поэтому для эффективного шифрования больших объемов данных могут применяться различные оптимизации, такие как параллельное шифрование и использование специализированных аппаратных решений.

Эффективность шифрования проистекает из его способности делать данные нерасшифрованными, даже когда злоумышленники перехватывают пакеты данных или получают доступ к конфиденциальным файлам.

Шифрование каналов связи является одним из наиболее важных аспектов современной информационной безопасности.

Основной целью шифрования каналов связи является обеспечение конфиденциальности передаваемой информации. Путем применения криптографических алгоритмов и протоколов (как пример, использование *SSL*/*TLS* протокола для защиты коммуникаций между клиентом и сервером) можно предотвратить несанкционированный доступ к данным и гарантировать, что только сами участники общения могут расшифровать сообщения [3].

Кроме конфиденциальности, шифрование каналов связи также обеспечивает целостность передаваемой информации. Целостность означает, что данные не могут быть изменены в процессе передачи без обнаружения этого факта.

Заключение. Таким образом, защита компьютерной сети при работе с большими данными является сложным и многогранным процессом. Она требует применения различных методов и технологий, а также постоянного мониторинга и анализа угроз. Только комплексный подход к защите может обеспечить надежность и безопасность работы с большими данными.

Список литературы

[1] IBM Security опубликовала отчет о стоимости утечки данных за 2023 год: [Электронный ресурс]. URL: https://www.codetd.com/ru/article/16598851. (Дата обращения: 10.02.2024).

[2] Современные зарубежные шифры: [Электронный ресурс]. URL: https://xakep.ru/2016/06/30/crypto-part4/. (Дата обращения: 12.02.2024).

[3] Big Data – Data Encryption in Big Data: [Электронный ресурс]. URL: https://www.encryptionconsulting.com/data-protection-in-big-data-using-encryption/. (Дата обращения: 13.02.2024).

Авторский вклад

Авторы внесли равноценный вклад

METHODS AND SPECIFICS OF COMPUTER NETWORK PROTECTION WHEN WORKING WITH BIG DATA

E.A. Leshchenko
Software Engineer of the Network Technology Department of the Center of Informatization and Innovation Elaborations, Assistant of the Department of Computer Science of BSUIR, Master's student of the Department of ICSD of BSUIR

E.V. Beglyak
Software Engineer of the 1st category of the Network Technology Department of the Center of Informatization and Innovation Elaborations, Assistant of the Department of Computational Methods and Programming of BSUIR, Master's student of the Department of ICSD of BSUIR

V.A. Martsinkevich
Leading Electronics Engineer of the Network Technology Department of the Center of Informatization and Innovation Elaborations, Assistant of the Department of Electronic Computing Machines of BSUIR, Master's student of the Department of Information and Communication Technologies of BSUIR

Abstract. This article describes the methods and principles of protecting computer networks in which Big Data is transmitted.

It is shown that an integrated approach is needed from various methods of secure information transmission to protect computer networks when working with big data.

Keywords: computer network protection, encryption, big data transmission