УДК 004.45 + 658.51 Вестник УрФО № 3(33) / 2019, с. 43–54

Басыня Е. А., Сафронов А. В.

DOI: 10.14529/secur190305

ДЕЦЕНТРАЛИЗОВАННЫЙ ПОДХОД К СБОРУ И ОБРАБОТКЕ ДАННЫХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

Уровень защищенности информационно-коммуникационного сектора предприятия является следствием эффективности решения задач системного анализа, управления и обработки информации корпоративной вычислительной сети. В статье анализируется проблематика реагирования на инциденты в киберпространстве на основе существующих централизованных и распределенных систем сбора и анализа событий. Рассматриваются угрозы несанкционированных воздействий со стороны доверенных пользователей. На обзор выносится оригинальный метод системного анализа, управления и обработки информации корпоративной вычислительной сети. Научная новизна предлагаемого решения заключается в возможности автоматического управления трафиком вычислительной сети и локальными информационными процессами ее хостов на основе объективного и информативного реестра событий, защищенного от различных внешних возмущений (от атак имперсонации до фальсификации записей) посредством использования модифицированного децентрализованного блокчейн-хранилища с системой управления доверием к регистрируемым событиям.

Ключевые слова: *системный анализ, управление, обработка, логи, блокчейн-хранилище, управление доверием, многослойная инкапсуляция.*

Basinya E. A., Safronov A. V.

DECENTRALIZED APPROACH FOR COLLECTING AND PROCESSING DATA OF THE ENTERPRISE INFORMATION INFRASTRUCTURE

The level of security of the information and communication sector of the enterprise is a consequence of the effectiveness of solving the problems of system analysis, management and in-

formation processing of a corporate computer network. The article analyzes the issue of responding to incidents in cyberspace based on existing centralized and distributed systems for collecting and analyzing events. Threats of unauthorized influences from trusted users are considered. An original method of system analysis, management and information processing of a corporate computer network is reviewed. The scientific novelty of the proposed solution consists in the possibility of automatic management of the traffic of the computer network and the local information processes of its hosts based on an objective and informative register of events protected from various external disturbances (from impersonation attacks to falsification of records) by using a modified decentralized blockchain storage with a logged events trust management system.

Keywords: *system analysis, management, processing, logs, blockchain storage, trust management, multilayer encapsulation.*

Введение

Кибербезопасность выступает одним из ключевых факторов развития стратегии национальной безопасности Российской Федерации, затрагивает все сферы жизни общества: от экономической до социальной и политической. Международным сообществом разрабатываются различные стратегии кибербезопасности, призванные обеспечить защищенное, надежное и отказоустойчивое функционирование инфраструктуры киберпространства с автоматическим контролем над возникающими рисками. К сожалению, транснациональное сотрудничество в этой области подорвано взаимными обвинениями различных государств и производителей информационно-коммуникационных решений в промышленном шпионаже и политической ангажированности. В качестве примера стоит привести конфликт США и Huawei. Соответственно, усиливается тренд развития собственных проприетарных систем защиты критической национальной инфраструктуры.

С целью эффективного реагирования на инциденты в киберпространстве учеными разрабатываются различные алгоритмы и методы функционирования систем обнаружения и предотвращения вторжений. Оригинальные подходы в области идентификации сетевых аномалий и распараллеливания на основе встраиваемых микропроцессорных систем описаны в работах Бондякова А.С., Ефимова А.Ю., Доценко С.М., Владыко А.Г., Летенко И.Д. [1–3]. Другой концепцией выступает применение машинного обучения и развитие автоматического тестирования на проникновение в подобные классы систем, изложенное в работах P.R. Chandre, P.N. Mahalle, G.R. Shinde, T. Zitta, M. Neruda, L. Vojtech, M. Matejkova [4–6]. К сожалению, данные системы не ориентированы на функционирование в реальных инфраструктурах, где используются технологии виртуальных защищенных каналов связи и протоколы шифрования. Соответственно, возрастает актуальность разработки методов комплексного сбора и обработки данных с возможностью проверки их подлинности и достоверности.

1. Цель работы

Целью данной работы являлась разработка оригинального метода системного анализа, управления и обработки информации корпоративной вычислительной сети, функционирующей на основе стека протоколов TCP/IP.

Научная новизна предлагаемого решения заключается в возможности автоматического управления трафиком вычислительной сети и локальными информационными процессами ее хостов на основе объективного и информативного реестра событий, защищенного от различных внешних возмущений (от атак имперсонации до фальсификации записей) посредством использования модифицированного децентрализованного блокчейн-хранилища с системой управления доверием к регистрируемым событиям.

2. Предлагаемое решение

Для нивелирования ранее описанных угроз на обзор выносится оригинальный метод системного анализа, управления и обработки информации корпоративной вычислительной сети с применением модифицированного децентрализованного блокчейн-хранилища и авторской системы управления доверием к регистрируемым событиям. Целью данного подхода является организация автоматического управления трафиком вычислительной сети и локальными информационными процессами ее хостов на основе объективного и информативного реестра событий, защищенного от различных внешних возму-

щений: от атак имперсонации до фальсификации записей.

Объективность события подразумевает прозрачную доказуемость факта его существования в сочетании с обеспечением конфиденциальности, целостности и подлинности данных.

Информативность событий достигается путем использования авторской распределенной системы сбора, обработки и анализа событий сетевой инфраструктуры предприятия. Над штатными агентами первичного сбора информации (журналами событий операционной системы, приложений, сетевого трафика и др.) вводится слой абстракции в виде одноименного модуля системы (рис. 1).

чения подлежит обязательной установке на межсетевые хосты (маршрутизаторы, коммутаторы, шлюзы и другие объекты, интегрированные с системой интеллектуально-адаптивного управления сетевой инфраструктурой предприятия). Установка на клиентские электронно-вычислительные машины желательна, но не является обязательным требованием. Принятие решения об интеграции выполняется на основе оценки свободного дискового пространства для системы и мощности клиентского компьютера.

Рассмотрим предлагаемый подход к построению модифицированного децентрализованного блокчейн-хранилища реестра событий (логов) с системой управления довери-

Рис. 1. Последовательность идентификации и обработки событий на хосте

Модуль под индексом 2 осуществляет не только парсинг, но и идентификацию, структуризацию, ранжирование, объединение событий с выявлением корреляции. Что позволяет существенно снизить объем данных, унифицировать их формат для всех операционных систем, а также повысить информативность. Его функционирование выполняется на основе оригинального сигнатурного и статистического метода составления базы знаний системы посредством тестирования и имитации известных сетевых и локальных возмущений с отслеживанием реакции операционных систем и приложений в среде виртуализации. Производится автоматизированное исследование коррелирующих событий с применением глубокого анализа содержимого пакетов и мониторинга локальной работы пользователей [7, 8].

Данный комплекс программного обеспе-

ем к регистрируемой информации на упрощенной принципиальной схеме корпоративной вычислительной сети, представленной на рис. 2.

На представленной схеме функционируют следующие объекты:

• комплексные межсетевые экраны «А» и «Б», взаимодействующие на основе виртуального защищенного канала связи в глобальной сети Интернет;

• управляемые сетевые коммутаторы «В», «Г», «Д», постфикс L2+ отражает их частичную работу на вышележащих уровнях базовой эталонной модели взаимодействия открытых систем OSI (англ. open systems interconnection basic reference model). Ряд устройств различных производителей позволяет осуществлять их конфигурирование через HTTPS протокол (англ. HyperText Transfer Protocol Secure), но это не означает включение полно-

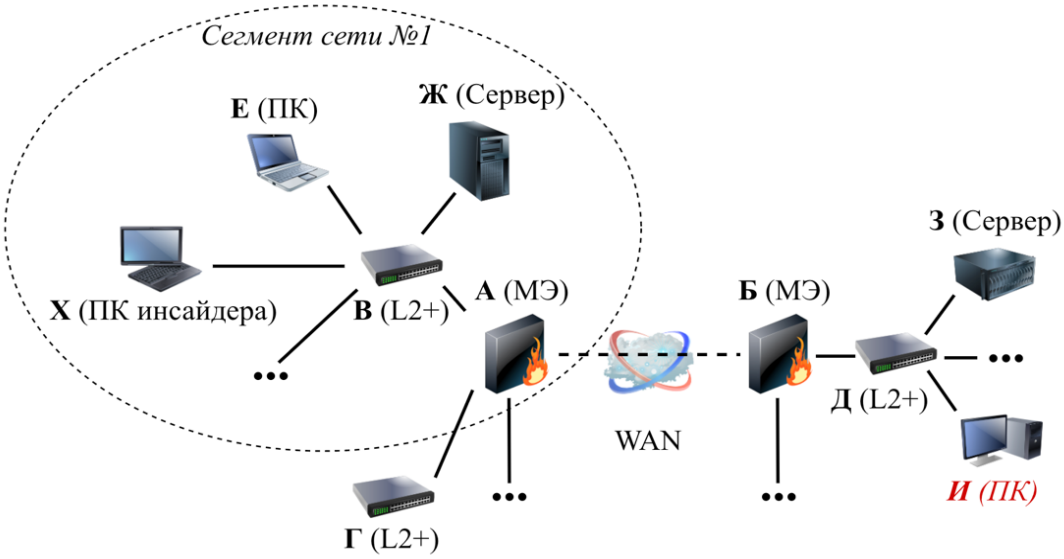

Рис. 2. Принципиальная схема корпоративной вычислительной сети

ценного функционала до прикладного уровня;

• различные серверные решения «Ж», «З»;

• персональные (корпоративные) компьютеры на базе различных операционных систем «Е», «И», «Х».

Хосты (объекты, узлы, ноды) «А», «Б», «В», «Г», «Д», «Ж», «З», «Е» подключены к модифицированному децентрализованному блокчейн-хранилищу с системой управления доверием к реестру событий (далее просто Системе), в режиме подключения находится компьютер «И». Электронно-вычислительное устройство «Х» не подключено к Системе, к нему получил доступ злоумышленник из числа доверенных лиц.

Все клиенты блокчейн-хранилища равноправны вне зависимости от предназначения хост системы, сервисов, запущенных на ней, и ее вычислительных ресурсов. Обмен между клиентами Системы осуществляется по зашифрованному каналу связи. В момент передачи логов любого хоста (далее log), остальными участниками сети проверяется правомерность возникновения этого события. Каждый из участников после своей проверки правомерности/доказательности события выставляет ему собственный коэффициент доверия k, при этом $-1 \leq k \leq 1$. После этого все участники подписывают своей цифровой подписью выработанные коэффициенты. В блокчейн-хранилище осуществляется запись log файла, зашифрованного хостом, генерирующим это событие, а также всех оценок событий (даже с отрицательными коэффициентами доверия), выработанными участниками Системы. Коэффициенты доверия используются для анализа работы сети и выявления несанкционированных внешних возмущений.

В качестве примера стоит привести различные атаки с использованием широковещательных запросов от инсайдера «Х». Данные несанкционированные возмущения производятся и являются прозрачными в сегменте сети №1, поскольку управляемый сетевой коммутатор «В» не блокирует широковещательные рассылки, а на комплексный межсетевой экран «А» дублируется весь сетевой трафик с данного устройства технологией зеркалирования портов. Узел «Е» первым зафиксировал атаку и инициализировал передачу события другим хостам для проверки и оценки достоверности информации. Все хосты данного сетевого сегмента могут проверить факт произведения такого события посредством агентов первичного сбора информации и модулем распределенной системы сбора, обработки и анализа событий сетевой инфраструктуры предприятия. Объекты «А», «В», «Ж», «Е» подтверждают событие посредством выставления ему коэффициентов доверия «1», а далее осуществляется безопасная запись log файла в базу знаний (блокчейн-хранилище).

Таким образом осуществляется верификация, проверка объективности, информативности и подлинности произошедшего события, на базе которого можно осуществить автоматическое управление трафиком вычислительной сети и локальными информа-

ционными процессами ее хостов с использованием специализированных средств защиты. Далее следует подробно рассмотреть отдельные компоненты Системы.

2.1. Система хранения и обработки логов

Информация о событиях сетевой инфраструктуры предприятия может представлять интерес для злоумышленников в качестве набора исходной информации для подготовки атаки, недопустимым является решение хранить все логи в открытом виде. Однако, хранение данных в полностью зашифрованном виде усложняет поиск по ним. В качестве компромисса было решено тело log записи хранить в зашифрованном виде, а для поиска использовать ключевые слова, которые хранятся в открытом виде. В этом случае ключевые слова могут быть использованы для предвыборки данных. А сам поиск осуществляется в три этапа:

1) первичный поиск предвыборных данных по ключевым словам;

2) расшифровка log тела предвыборных данных;

3) точный поиск по расшифрованным данным.

После третьего этапа на выходе будут получены данные, полностью соответствующие поисковому запросу. Отметим, что при таком подходе достигается многократное ускорение поиска за счет сохранения времени на расшифровку большого объема информации.

Необходимо соблюдать баланс между точностью описания и раскрытием информации путем публикации в открытом виде ключевых слов. Например, такие ключевые слова как «19.06.2019 15:47:23 192.168.2.3:9999 FTP server start» могут раскрыть информацию о том, что в указанное время на указанном IP адресе на нестандартном порту 9999 начал работу FTP сервер. Это вполне может быть достаточно для первичного составления стратегии несанкционированного воздействия на объект. В качестве ключевых слов предлагается использовать: дату и время события, название службы, генерирующей log запись (событие). В таком случае ячейка записи будет выглядеть следующим образом (рис. 3).

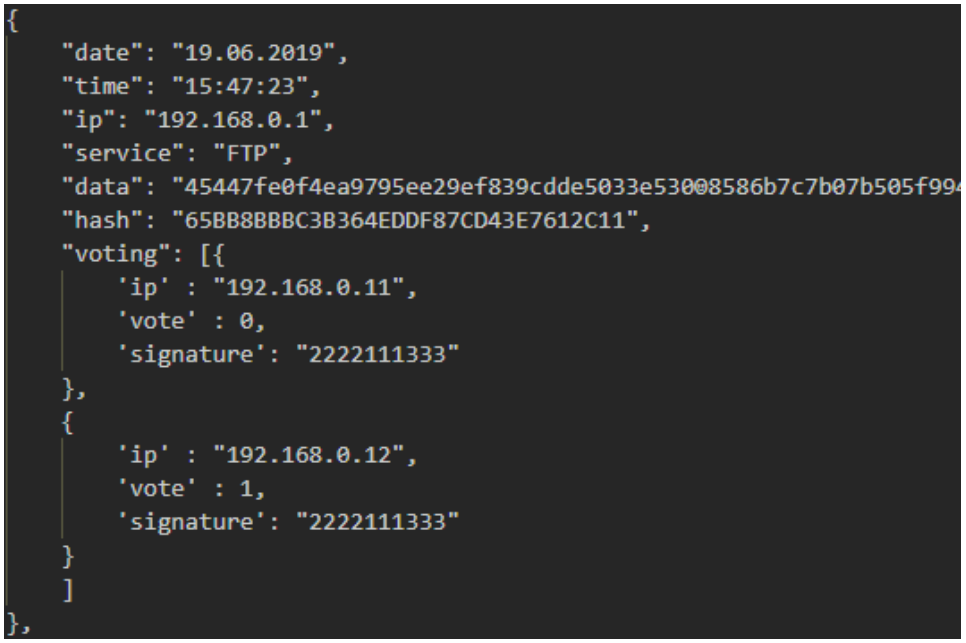

Рис. 3. Пример данных для записи в блокчейн-хранилище

Важно отметить, что приведен упрощенный пример данных для записи в блокчейн-хранилище. Формализация и унификация типов записей организована сигнатурным подходом для различных типов событий.

2.2. Система управления доверием к регистрируемой информации

Одним из ключевых отличий предлагаемого метода является введение системы управления доверием к регистрируемой информации, использующей коэффициенты доверия log сообщения. В этом случае любой log, перед тем как он будет записан в блокчейн-хранилище, предлагается к проверке клиентами Системы. Рассмотрим вновь на примере принципиальной схемы корпоративной вычислительной сети, представленной на рис. 2. Клиент «Ж» предлагает к про-

верке сообщение о произведении широковещательного запроса на получение пула настроек стека TCP/IP v4 узлом «X» посредством протокола DHCP v4 (англ. Dynamic Host Configuration Protocol). Инсайдер за хостом «X» поставил цель отключить статические настройки сетевого интерфейса и инициализировать динамическое конфигурирование. Остальные клиенты сети пытаются найти в своем доступе информацию для подтверждения или опровержения этого события посредством агентов первичного сбора информации и модулем распределенной системы сбора, обработки и анализа событий сетевой инфраструктуры предприятия.

Всего существует три возможных действия проверяющего хоста:

1) хост может подтвердить факт возникновения события: «+1»;

2) хост может отрицать факт возникновения события: «-1»;

3) хост не может ни подтвердить, ни опровергнуть факт возникновения события: «0».

В этом случае каждый из проверяющих выставляет сообщению оценку: «+1», «-1» или «0» соответственно и подписывает её своей цифровой подписью. В представленном примере действия узла «X» являются прозрачными для сетевого сегмента №1. Соответственно, объекты «A», «B», «Ж», «E» вновь подтверждают событие посредством выставления ему коэффициентов доверия «1». Остальные хосты, находящиеся за пределами рассматриваемого сетевого взаимодействия, не могут ни подтвердить, ни опровергнуть факт возникновения события и выставляют оценку «0». Далее осуществляется безопасная запись log файла в базу знаний (блокчейн-хранилище).

В дальнейшем система обнаружения и предотвращения вторжений при управлении информационными потоками и процессами на основе децентрализованного реестра событий будет анализировать рейтинг доверия с учетом сегментирования инцидентов.

2.3. Система безопасного локального и сетевого взаимодействия

Для подключения к системе хост должен сгенерировать приватный и публичный ключи, далее на их базе сгенерировать самоподписанный сертификат (англ. Self-signed Certificate). В системе не применяется единый удостоверяющий центр для подписания запросов сертификации, так как подобная централизация привнесла бы дополнительные риски безопасности корпоративных ресурсов. Сертификат используется для сопоставления подписи коэффициентов доверия при анализе логов, а также для организации безопасного группового взаимодействия хостов в критических ситуациях.

После генерации ключей и сертификатов хост выполняет подключение к системе. При этом Система с учетом присутствия нового участника обмена генерирует сессионный ключ для шифрования канала обмена данными между участниками. Для генерации сессионного ключа используется алгоритм Диффи–Хеллмана для неограниченного количества участников. При этом в случае отключения хоста вырабатывается новый сессионный ключ, аналогично случаю подключения нового хоста.

Старый сессионный ключ каждый из участников шифрует своим публичным ключом и делает запись об этом в блокчейн-хранилище. Это необходимо для восстановления всех сессионных ключей и дешифрования всех log сообщений в хранилище всеми клиентами Системы. Далее все хосты публикуют свои сертификаты публичных ключей в блокчейн-хранилище. Данные децентрализованного реестра событий зашифрованы симметричным криптографическим ключом, сгенерированным на базе текущего сессионного ключа.

После совершения события, повлекшего за собой генерацию log сообщения, узел Системы следует алгоритму:

1) на основе log сообщения генерирует ключевые слова;

2) получает хеш log сообщения;

3) с помощью сессионного ключа шифрует log сообщение;

4) отправляет сообщение в блокчейн-сеть.

Каждый из участников сети, применяя тот же сессионный ключ, расшифровывает сообщение и выставляет ему коэффициент доверия. После того, как все оценки будут выставлены, log запись вместе со всеми оценками будет записана в блокчейн-хранилище.

Промежуточное сохранение сессионного ключа в системе необходимо для того, чтобы в любой момент времени каждый из участников мог расшифровать все свои логи. При этом соблюдается две важных политики:

1) любой из новых участников имеет доступ ко всем логам всех участников Системы начиная с того момента, как он был добавлен в сеть (за исключением приватных записей).

Дешифровка более ранних логов Системы для него невозможна;

2) любой из удаленных участников сети может читать логи только до момента своего удаления. Дешифровка более поздних логов для него невозможна.

Поскольку в действующих системах реконфигурация сети с удалением или добавлением новых нод происходит редко, предлагается искусственно генерировать процедуру создания новой сессии в краткосрочные интервалы времени (каждые 30 минут). Данный параметр настраивается опционально при интеграции. Даже если злоумышленник получит сессионный ключ, он сможет дешифровать логи только за короткий интервал времени, в рамках которого не будет раскрыта конфиденциальная информация объектов критической инфраструктуры предприятия.

2.4 Осуществление приватных записей

При данном подходе, чтобы участники системы могли выставить оценку доверия log сообщению, то есть подтвердить или опровергнуть log событие, все log события, посылаемые в Систему, должны быть прочитаны всеми его участниками. Если при этом могут быть раскрыты конфиденциальные сведения объектов критической инфраструктуры, для шифрования тела log сообщения может быть применен симметричный криптографический ключ, сгенерированный на основе сессионного ключа и приватного ключа пользователя. В этом случае сообщение помечается как приватное: «public = False» и коэффициент доверия не будет выставлен, так как остальные участники системы не смогут его дешифровать.

Такой поход применяется для записи приватных данных, не подлежащих разглашению – они могут быть прочитаны только тем хостом, с которого осуществлялась их запись в блокчейн-хранилище. Поскольку оценка не может быть выставлена в силу отсутствия подтверждения идентичности log сообщения, которое клиент хочет записать в блокчейн в зашифрованном публичным ключом виде, и log сообщения, которое клиент отправил определённым узлам Системы.

При этом публикация всеми участниками Системы своих сертификатов публичного ключа в момент генерации сессии позволяет участникам отправлять друг другу зашифрованные сообщения. Следует рассматривать эту возможность только для передачи информационных сообщений между хостами, но не как систему подтверждений событий для узкого числа проверяющих. Таким образом, возможные способы организации формата хранения данных представлены на рис. 4 в обобщенном виде:

Основным форматом был выбран способ I для ускорения анализа данных за счет выполнения поисковых запросов по открытым записям (ключевым словам) с последующей дешифровкой нужной информации о событиях.

Формат II подразумевает хранение приватных записей, для которых участниками сети не выставляется рейтинг доверия. При этом задействуется многослойное шифрование конфиденциальной информации.

Существует множество подобных форматов, опционально они настраиваются через панель администрирования. При этом возможны различные комбинации распределенного многослойного шифрования в зависимости от целевых потребностей и архитектуры вычислительной сети предприятия заказчика. В качестве примера проиллюстрирован формат N, где M – количество слоев шифрования, а K – количество сочетаний полей для многослойного шифрования M.

Последний является наиболее изощренным подходом к хранению данных, при котором возможны любые комбинации шифруемых полей и любое число слоев шифрования. Баланс между скоростью работы системы и уровнем безопасности информационных ресурсов зависит от потребностей конечного потребителя продукта.

Стоит отметить, что, независимо от выбранного формата хранения данных, дополнительно осуществляется шифрование на уровне операционной системы.

2.5. Вопросы надежности и отказоустойчивости

Защита данных в штатном режиме функционирования Системы осуществляется симметричным криптографическим ключом, сгенерированным на базе сессионного ключа. Если злоумышленник похитит базу, он не сможет его дешифровать, так как последний сессионный ключ нигде не хранится в явном виде. А прошлые сессионные ключи зашифрованы для каждого хоста асимметричным шифрованием.

Защита от распределенных атак на отказ в обслуживании (от англ. Distributed Denial of Service, DDoS) осуществляется системным ад-

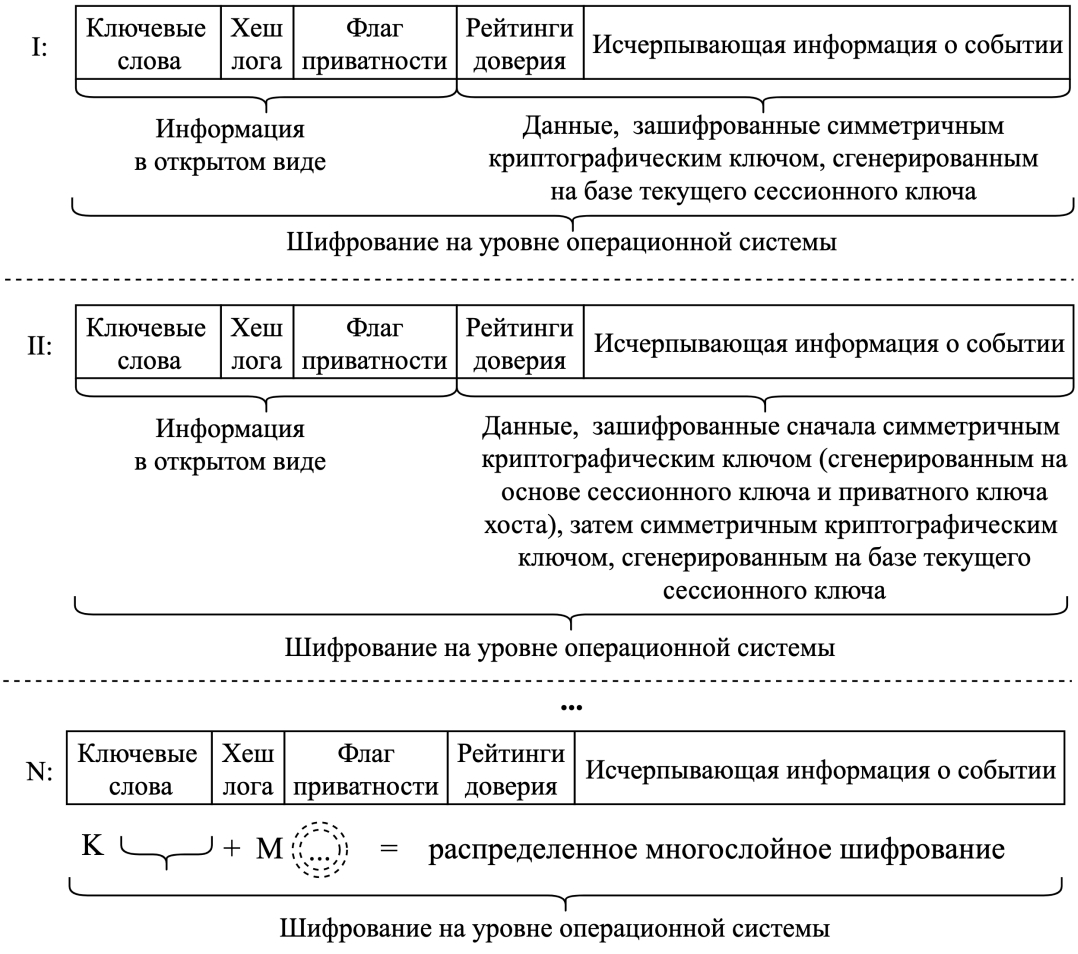

Рис. 4. Пример данных для записи в блокчейн-хранилище

министратором. Корпоративная вычислительная сеть в обязательном порядке задействует интеллектуальные функции управляемого сетевого оборудования, ресурсов для DDoS атаки в ней быть не может. Системой осуществляется контроль и блокировка нод с подозрительной сетевой активностью.

В случае атаки «хвостовой части», при которой атакующий удаляет первые блоки цепочки (усекает хвост), проверяющий хост при условии незнания исходной длины цепочки хешей не способен обнаружить факт осуществления атаки. Решением данного вопроса является сквозная нумерация всех блоков, при этом первому блоку цепи, так называемому генезис блоку, присваивается номер, равный нулю.

Организация сетевого взаимодействия в децентрализованных сетях не исключает возникновения коллизий при одновременной обработке информационных потоков. Два и более хоста могли одновременно идентифицировать сетевое событие и транслировать его в Систему для проверки перед записью в блокчейн-хранилище. Это влечет за собой два нежелательных последствия: разрастание объема хранилища и замедление поиска информации по нему. Второй момент является более критичным: многократная запись одного события расходует вычислительные мощности сетевой инфраструктуры. Такое событие перед записью в хранилище предлагается к проверке всем клиентам системы многократно. Следовательно, участники сетевого взаимодействия при проверке этих данных потратят ресурсы для многократной выработки коэффициентов доверия информации, которая на самом деле представляет собой одно и то же событие. Учитывая возможное достаточно большое количество клиентов и их низкую вычислительную мощность, такие ситуации могут сильно снизить скорость записи в хранилище.

Для предотвращения описанной ситуаций на каждом клиенте в модуле распределенной системы сбора, обработки и анализа

событий (элемент под номером 2 на рис. 1) предлагается производить предварительную обработку (маркировку) локальной истории инцидентов, состоящую из следующих этапов:

1) сопрограмма идентификации при обнаружении инцидента помещает информацию о событии в локальное хранилище инцидентов, помечая его как требуемое к сохранению в блокчейне;

2) сопрограмма синхронизации читает из локального хранилища последние инциденты и инициализирует сохранение их в блокчейне, если они помечены соответствующим флагом, после чего помечает их, как сохраненные. По умолчанию их удаление из локального хранилища не производится, но может быть опционально настроено, в том числе с указанием требуемых временных интервалов очистки.

Полноценная интеграция с распределенной системой сбора, обработки и анализа событий позволяет не только избежать коллизий, но еще и повышает быстродействие Системы в целом. Когда клиенту предлагается очередное событие к проверке, он сначала осуществляет поиск по своему локальному хранилищу. Если ему удается найти подтверждение события, он сразу выставляет ему соответствующий критерий доверия, не прибегая к проверке инцидента средствами подпрограмм. Если обнаруженное в локальном хранилище событие помечено, как требующее сохранения в блокчейне, ему выставляется статус «Сохранено другим клиентом». Таким образом, сопрограмма синхронизации в клиенте системы не отправит информацию об этом инциденте в блокчейн, что предотвращает дублирование записей в основном хранилище. Если клиент при проверке очередного события находит опровержение события другим инцидентом, то он выставляет ему соответствующий коэффициент. Изменения статуса инцидента в локальном хранилище при этом не происходит, и сопрограмма синхронизации при следующем такте сможет отправить информацию об этом в глобальное хранилище. В таком случае в системе будет сделано две записи: первая об инциденте А с отрицательным коэффициентом доверия, и запись об инциденте Б с положительным коэффициентом доверия. При этом запись Б можно считать опровергающей запись А.

Если клиент при проверке события не может найти ни подтверждающих, ни опровергающих проверяемое событие записей, он запускает проверку события на уровне подпрограмм, использующих средства операционных систем, сервисов и различных программ. В этом случае процесс выработки коэффициента доверия будет занимать большее время в связи с необходимостью сбора, обработки и анализа данных. Запись этой информации не производится в локальном хранилище, так как сопрограмма обнаружения инцидентов не посчитала нужным его учесть. Клиент Системы только произвел попытку проверки инцидента. Если подпрограммы проверки инцидентов не могут ни подтвердить, ни опровергнуть событие, то ему выставляется соответствующий коэффициент доверия, равный нулю.

Возможна настройка взаимодействия с дублирующими проверками не только распределенной системой сбора, обработки и анализа событий, но и с агентами первичного сбора информации. Баланс между избыточностью информации, потребляемыми вычислительными мощностями и скоростью работы метода определяет рентабельность конфигурации Системы в зависимости от поставленных задач. В общем случае процедуру обработки события можно графически изобразить следующим образом (рис. 5).

Важно при этом отметить, что интеграция с распределенной системой сбора, обработки и анализа событий может быть настроена несколькими способами в зависимости от требований технического задания. В первом случае она будет дублировать информацию децентрализованного реестра событий, привнося избыточность, но увеличивая скорость доступа к данным. Во втором случае локальное хранилище событий не будет включать информацию основного блокчейна. Записи в нем будут представлять ценность только на коротком или среднесрочном интервале времени, по истечению которого будут удаляться. Локальное хранилище после запуска и перед прекращением работы клиента Системы будет очищаться от устаревших записей, сохраняя тем самым место на жестком диске. Третий режим позволяет профилировать и разносить информацию по двум источникам, оптимизируя скорость работы программ с различным целевым назначением. Выбор способа интеграции зависит от требований технического задания, в том числе вычислительных мощностей и объема информации сетевой инфраструктуры предприятия.

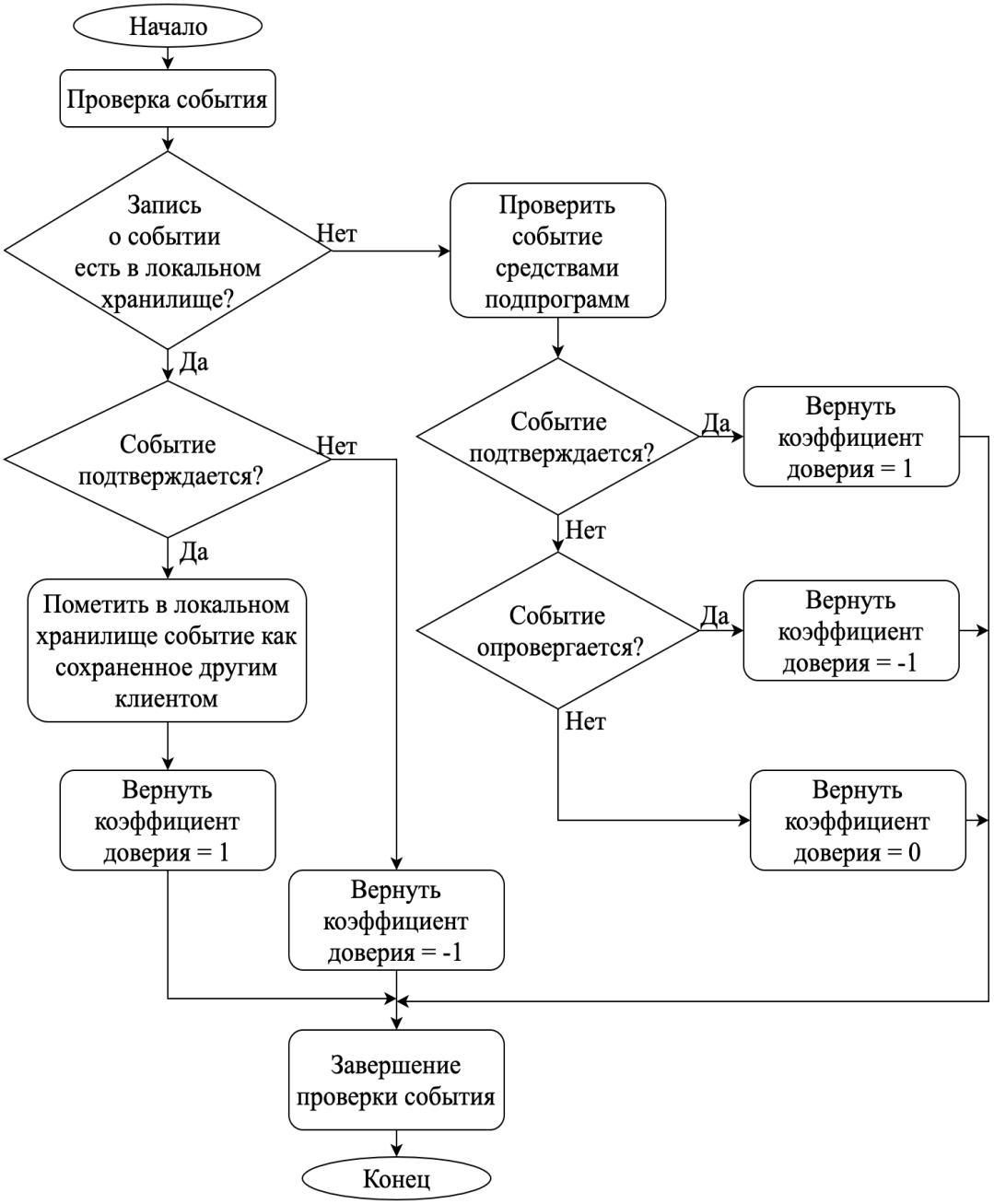

Рис. 5. Блок-схема процедуры обработки события

Заключение

В рамках данной статьи был представлен оригинальный метод системного анализа, управления и обработки информации корпоративной вычислительной сети, функционирующей на основе стека протоколов TCP/IP. Научная новизна предлагаемого решения заключается в возможности автоматического управления трафиком вычислительной сети и локальными информационными процессами ее хостов на основе объективного и информативного реестра событий, защищенного от различных внешних возмущений (от атак имперсонации до фальсификации записей) посредством использования модифицированного децентрализованного блокчейн-хранилища с системой управления доверием к регистрируемым событиям. Другим немаловажным аспектом научной новизны выступает профилирование доступа к информации и защита процесса передачи данных на основе группового, а также итерационного многослойного шифрования.

В следующем выпуске журнала будет

представлен метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия, функционирующий на основе предлагаемого подхода. Планируется осветить этап проектирования и программной реализации решения с последующим экспериментальным исследованием эффективности его функционирования.

Литература

1. Бондяков А.С. Основные режимы работы системы предотвращения вторжений (IDS/IPS SURICATA) для вычислительного кластера // Современные информационные технологии и ИТ-образование. 2017. Т. 13. № 3. С. 31–37.

2. Ефимов А.Ю. Проблемы обработки статистики сетевого трафика для обнаружения вторжений в существующих информационных системах // Программные продукты и системы. 2016. № 1. С. 17–21.

3. Доценко С.М. Системы обнаружения вторжений на основе встраиваемых микропроцессорных систем / С.М. Доценко, А.Г. Владыко, И.Д. Летенко // Телекоммуникации. 2013. № S7. С. 15–18.

4. Chandre P.R. Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification / P.R. Chandre, P.N. Mahalle, G.R. Shinde // Proceedings of the IEEE Global Conference on Wireless Computing and Networking (GCWCN). - Lonavala, India. – 2018. - P. 135 – 140.

5. Zitta T. Penetration Testing of Intrusion Detection and Prevention System in Low-Performance Embedded IoT Device / T. Zitta, M. Neruda, L. Vojtech, M. Matejkova and oth. // Proceedings of the 18th International Conference on Mechatronics - Mechatronika (ME). - Brno, Czech Republic. – 2018. – P. 1 – 5.

6. Сафонов М. Централизованное хранение журналов / Сафонов М. // Системный администратор. 2012. №. 5 (114). С. 28–33.

7. Басыня Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия / Безопасность информационных технологий. 2018. Т. 25. № 4. С. 43–52.

8. Французова, Г. А. Самоорганизующаяся система управления трафиком вычислительной сети: метод противодействия сетевым угрозам / Г.А. Французова, А.В. Гунько, Е.А. Басыня // Программная инженерия. – 2014. – № 3. – С. 16–20.

References

1. Bondjakov A.S. Osnovnye rezhimy raboty sistemy predotvrashhenija vtorzhenij (IDS/IPS SURICATA) dlja vychislitel'nogo klastera [Main modes of operation of the intrusion prevention system (IDS / IPS SURICATA) for the computing cluster] // Modern information technology and IT education. 2017. T. 13. № 3. S. 31–37. (in Russian)

2. Efimov A.Ju. Problemy obrabotki statistiki setevogo trafika dlja obnaruzhenija vtorzhenij v sushhestvujushhih informacionnyh sistemah [Problems of processing network traffic statistics for intrusion detection in existing information systems] // Software Products and Systems. 2016. № 1. S. 17–21. (in Russian)

3. Docenko S.M. Sistemy obnaruzhenija vtorzhenij na osnove vstraivaemyh mikroprocessornyh sistem [Intrusion detection systems based on embedded microprocessor systems] / S.M. Docenko, A.G. Vladyko, I.D. Letenko // Telecommunications. 2013. № S7. S. 15–18. (in Russian)

4. Chandre P.R. Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification / P.R. Chandre, P.N. Mahalle, G.R. Shinde // Proceedings of the IEEE Global Conference on Wireless Computing and Networking (GCWCN). - Lonavala, India. – 2018. - P. 135 – 140.

5. Zitta T. Penetration Testing of Intrusion Detection and Prevention System in Low-Performance Embedded IoT Device / T. Zitta, M. Neruda, L. Vojtech, M. Matejkova and oth. // Proceedings of the 18th International Conference on Mechatronics - Mechatronika (ME). - Brno, Czech Republic. – 2018. – P. 1 – 5.

6. Safonov M. Centralizovannoe hranenie zhurnalov [Centralized log storage] / Safonov M. // System Administrator. 2012. №. 5 (114). S. 28–33. (in Russian)

7. Basinya E. A. Raspredelennaja sistema sbora, obrabotki i analiza sobytij informacionnoj bezopasnosti setevoj infrastruktury predprijatija [Distributed system of collecting, processing and analysis of security information events of the enterprise network infrastructure] / IT Security. 2018. T. 25. № 4. S. 43–52. (in Russian)

8. Francuzova, G. A. Samoorganizujushhajasja sistema upravlenija trafikom vychislitel'noj seti: metod protivodejstvija setevym ugrozam [Self-organizing computer network traffic management system: a method to counteract network threats] / G.A. Francuzova, A.V. Gun'ko, E.A. Basinya // Software engineering. – 2014. – № 3. – S. 16–20. (in Russian)

БАСЫНЯ Евгений Александрович, кандидат технических наук, доцент Новосибирского государственного технического университета, директор Научно-исследовательского института информационно-коммуникационных технологий. 630073, РФ, г. Новосибирск, пр. К. Маркса, 20. E-mail: director@nii-ikt.ru

САФРОНОВ Антон Валерьевич, кандидат технических наук, технический директор Научно-исследовательского института информационно-коммуникационных технологий 630099, РФ, г. Новосибирск, ул. Депутатская, 48. E-mail: it-director@nii-ikt.ru

BASINYA Evgeny Aleksandrovich, Ph.D., prof. in the Novosibirsk State Technical University, director of the Research Institute of Information and Communication Technologies. 20 Prospekt K. Marksa, Novosibirsk,630073, Russia. E-mail: director@nii-ikt.ru

SAFRONOV Anton Valerevich, Ph.D., technical director of the Research Institute of Information and Communication Technologies. 48 Deputatskaya Street, Novosibirsk, 630099, Russia. E-mail: it-director@nii-ikt.ru