МРНТИ 27.47.15

Е.А. Басыня[1], А.В. Сафронов[2]

[1]Национальный исследовательский ядерный университет «МИФИ», Москва, РФ
[2]Научно-исследовательский институт информационно-коммуникационных технологий, Новосибирск, РФ
E-mail: director@nii-ikt.ru, it-director@nii-ikt.ru

Метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия

Аннотация. В статье описывается проблематика существующих подходов к сбору, обработке и анализу данных информационно-коммуникационного сектора предприятия. Рассматриваются угрозы нештатных внутренних и внешних воздействий на ее объекты и системы. На обзор выносится оригинальный метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия. Научная новизна предлагаемого решения заключается в автоматическом управлении локальными и сетевыми информационными процессами технических объектов на основе данных децентрализованного блокчейн-хранилища с системой управления доверием к регистрируемым событиям. Принятие решений осуществляется на основе объективной и подтвержденной информации. Другим аспектом научной новизны выступает профилирование доступа к информации и защита процесса передачи данных на основе группового, а также итерационного многослойного шифрования. Статья является логическим продолжением работы авторов над децентрализованным подходом к сбору и обработке данных информационной инфраструктуры предприятия. Освещаются разработка, исследование системы обнаружения, предотвращения вторжений и фальсификации реестра событий на основе предложенного подхода для интеграции в качестве модуля системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия.
Ключевые слова: реестр событий, логи, блокчейн-хранилище, системы управления доверием, системный анализ, обработка, управление информационными процессами.

DOI: doi.org/10.32523/2616-7263-2022-139-2-40-50

Введение

Повышение качества функционирования технических систем неотъемлемо связано с вопросами системного анализа, управления и обработки информации в рамках локальных и сетевых взаимодействий. Уровень кибербезопасности является следствием эффективности решения данных задач. Данная работа является логическим продолжением научно-технических изысканий авторов в области децентрализованного подхода к сбору и обработке данных информационной инфраструктуры предприятия [1].

Одним из концептуальных недостатков существующих методов рассматриваемой предметной области выступает уязвимость агрегируемой с агентов/датчиков базы знаний, которая может быть подвержена атакам имперсонации, фальсификации и модификации. Данный аспект затрагивает всю существующую систему хранения логов (событий). Подавляющее большинство управляемого сетевого оборудования функционирует на базе операционных систем семейства Linux и использует систему регистрации событий Syslog (англ. system log — системный журнал). В случае успешного взлома хоста злоумышленник может осуществить различные вредоносные действия с их последующим сокрытием или маскировкой. В качестве простого примера стоит

привести многократное удаление данных на жестком диске по стандарту безопасного стирания магнитных носителей 5220-22 М Министерства обороны США, инициализирующего семикратную перезапись информации. Чтобы событие выхода из системы было также успешно удалено, злоумышленник создает вредоносные скрипты, которые активируются при последующей успешной авторизации легитимного системного администратора, от имени которого происходит повторное удаление данных и ряд других компрометирующих действий. Наиболее распространённым методом защиты от подобных внешних возмущений является зеркалирование логов с использованием расширения системы регистрации событий Rsyslog или систем мониторинга сети и серверов (Zabbix, Observium, Cacti, Icinga и др.). Централизованному сбору и анализу локальных и сетевых логов посвящено множество работ [2–6]. Достоинства подобного подхода заключаются в функциональном удобстве их последующей обработки и анализа. В случаях профессиональных атак на сетевую инфраструктуру предприятия сервер логов становится первоочередной целью. Учитывая типовую настройку локальных и удаленных систем сбора и обработки событий, злоумышленнику не составляет труда взломать локальный объект, получить сведения об удаленном централизованном сервере хранения логов, получить над ним контроль и произвести удаление/модификацию событий. В широком спектре распространенных решений хранение и передача логов по сети осуществляются в открытом виде, создавая опасность инсайдерских атак. Но даже при использовании защищенных каналов связи не осуществляется проверка подлинности и объективности оповещений о событиях, отсутствует их верификация. Является актуальной проблема доверия к журналам событий. В случае, если один из хостов системы будет скомпрометирован злоумышленником, он может отправлять на централизованный сервер большое количество ложной информации, нарушающей функционирование всей инфраструктуры информационно-коммуникационного сектора предприятия.

Цель работы и постановка задач

Целью данной работы являлась разработка, программная реализация и исследование оригинального метода формирования децентрализованного реестра событий информационной инфраструктуры предприятия. Научная новизна предлагаемого решения заключается в автоматическом управлении локальными и сетевыми информационными процессами технических объектов на основе данных децентрализованного блокчейн-хранилища с системой управления доверием к регистрируемым событиям. Принятие решений осуществляется на основе объективной и подтвержденной информации. Другим немаловажным аспектом научной новизны выступают профилирование доступа к информации и защита процесса передачи данных на основе группового, а также итерационного многослойного шифрования.

При проектировании архитектуры программного продукта была учтена необходимость взаимодействия с авторской распределенной системой сбора, обработки и анализа событий сетевой инфраструктуры предприятия [7]. Ставились задачи разработки, исследования системы обнаружения, предотвращения вторжений и фальсификации реестра событий на основе предложенного подхода для интеграции в качестве модуля системы интеллектуально-адаптивного управления инфраструктурой предприятия, разрабатываемой первым автором [8].

Предлагаемое решение

Для нивелирования ранее описанных угроз на обзор выносится оригинальный метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия, ключевые аспекты функционирования которого отражены на рис. 1 и 2. Стоит отметить, что рис. 1 включает описание подключения к Системе нового хоста и инициализацию

сетевого взаимодействия, а рис. 2 описывает штатный режим работы Системы.

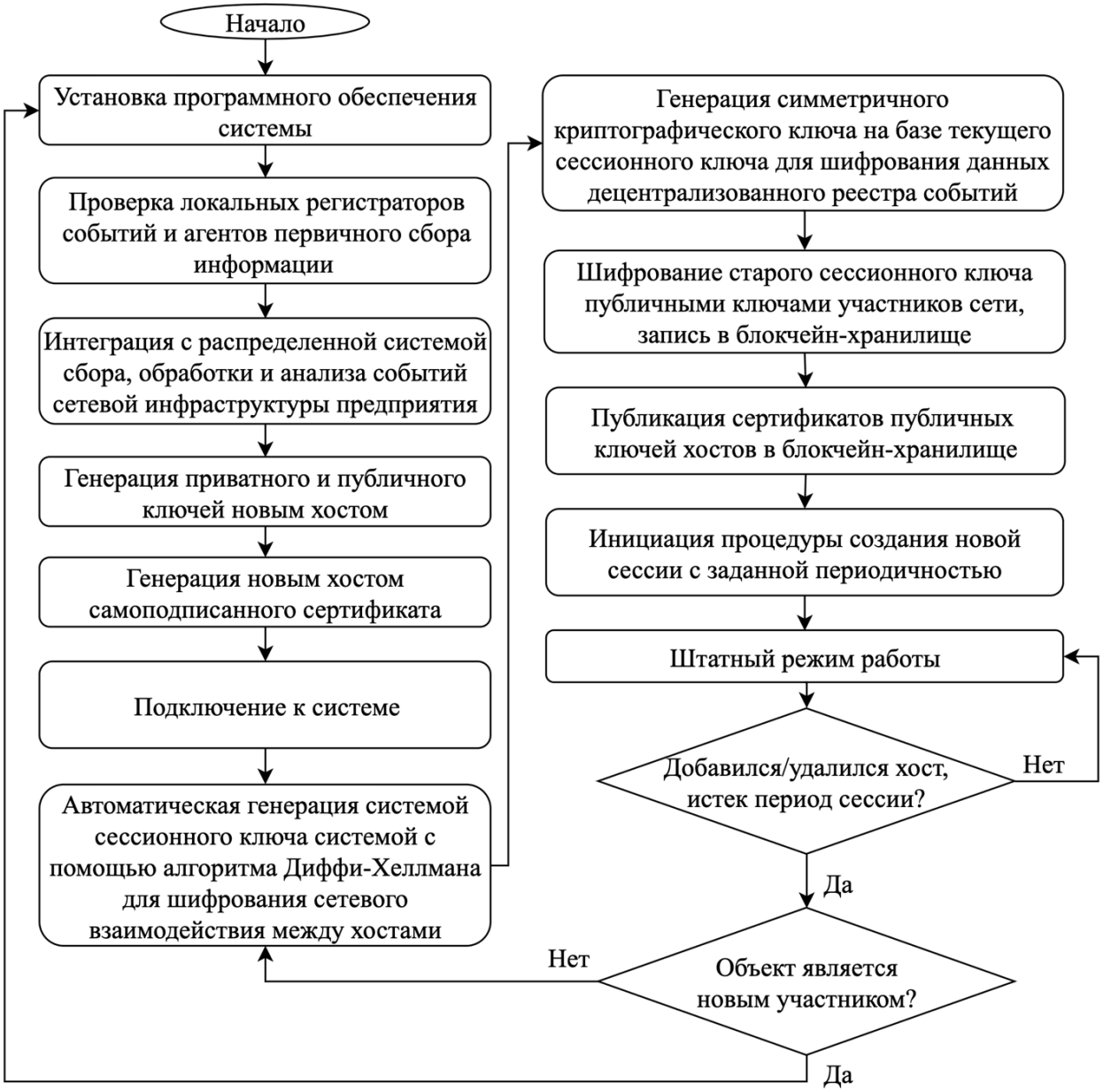

Рис. 1. Блок-схема предлагаемого метода: подключение к системе, инициализация сетевого взаимодействия

Необходимо заметить, что в случаях истечения периода сессии, а также при отключении от Системы хоста либо добавлении ранее подключавшегося объекта производится генерация сессионного ключа в автоматическом режиме с дальнейшей генерацией симметричного ключа на базе сессионного. Тогда как при добавлении узла, ранее не являющегося участником взаимодействия, повторно выполняется инициация полной процедуры подключения к Системе.

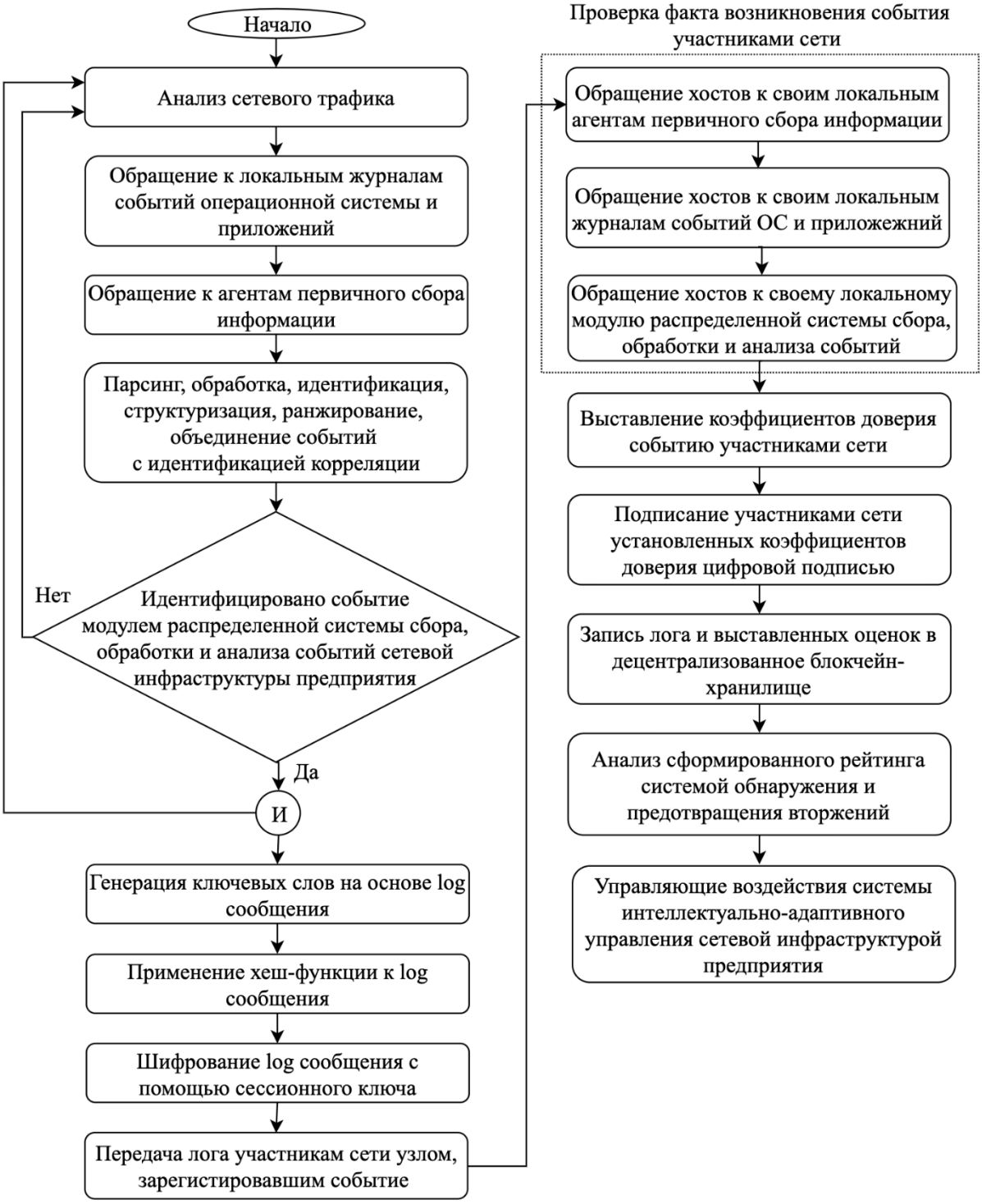

Рис. 2. Блок-схема предлагаемого метода: штатный режим работы

После успешного завершения процесса подключения узла к Системе выполняется переход к штатному функционированию, детально описанному на рис. 2.

Действия, предшествующие генерации и записи лога, а именно: анализ сетевого трафика, обращение к локальным журналам событий ОС и приложений, агентам первичного сбора данных, дальнейшая обработка и идентификация событий модулем авторской распределенной системы сбора, обработки и анализа событий сетевой инфраструктуры предприятия – выполняются непрерывно в фоновом режиме всеми хостами системы. После передачи лога участникам сети

описаны действия, входящие в одну итерацию проверки факта возникновения события каждым хостом. Запись информации в блокчейн-хранилище осуществляется по заранее выбранному формату хранения данных через панель администрирования Системы.

Разработанная система обнаружения и предотвращения вторжений функционирует на базе знаний и событий децентрализованного блокчейн-хранилища. Информативность анализа достигается благодаря использованию авторской распределенной системы сбора, обработки и анализа событий сетевой инфраструктуры предприятия. Объективность исследования обеспечивается путем задействования механизма выставления участниками сети коэффициентов доверия зарегистрированным событиям. Фильтрация трафика и управление информационными процессами осуществляются на основе проверенных фактов. Сигнатуры и паттерны функционирования системы защиты разрабатывались самостоятельно с использованием авторских методов противодействия сетевым угрозам и программы «Researcher» [7-8]. Далее будет рассмотрена программная реализация предлагаемого решения.

Программная реализация предлагаемого решения

Программное решение метода формирования децентрализованного реестра событий информационной инфраструктуры предприятия (являющегося логическим и прикладным развитием метода системного анализа, управления и обработки информации корпоративной вычислительной сети) представляет собой систему обнаружения, предотвращения вторжений и фальсификации реестра событий на основе децентрализованного подхода.

В рамках программной инженерии была произведена интеграция с авторской системой интеллектуально-адаптивного управления сетевой инфраструктурой предприятия (рис. 3), в том числе с ее компонентом - распределенной системой сбора, обработки и анализа событий. При этом ставилась задача организации взаимодействия Системы с другими процессами на локальном или удаленном хосте. Поскольку сведения, хранящиеся в децентрализованном реестре событий, представляют интерес в качестве входных данных для различных утилит и компонентов управления информационными потоками и процессами (в том числе системы обнаружения и предотвращения вторжений, реализованной на базе модифицированной платформы Bro), необходимо обеспечить возможность использования базы знаний сторонними программами. Для решения этой задачи предлагается использовать клиенты мониторинга и доступа.

Первая категория подключается к системе по аналогии со стандартными хостами через выработку сессионного ключа, однако не участвует в выработке коэффициентов доверия и, следовательно, в основной работе Системы. Клиенты мониторинга через механизм подписки уведомляют своих подписчиков о новых записях в блокчейне. Поскольку интерес представляют новые события, любая программа может подписаться на клиента мониторинга, указав, на какие типы событий она хочет получать уведомления.

Например, может быть осуществлена подписка только на атаки с использованием широковещательных запросов или на события, связанные с обнаружением недоступности определенных сервисов на хостах сети.

Важно отметить, что клиенты мониторинга не предоставляют механизмов чтения из блокчейна, это сделано целенаправленно, так как обеспечение уровня информационной безопасности к клиентам мониторинга осуществляется системным администратором и не может быть гарантированно проконтролировано Системой.

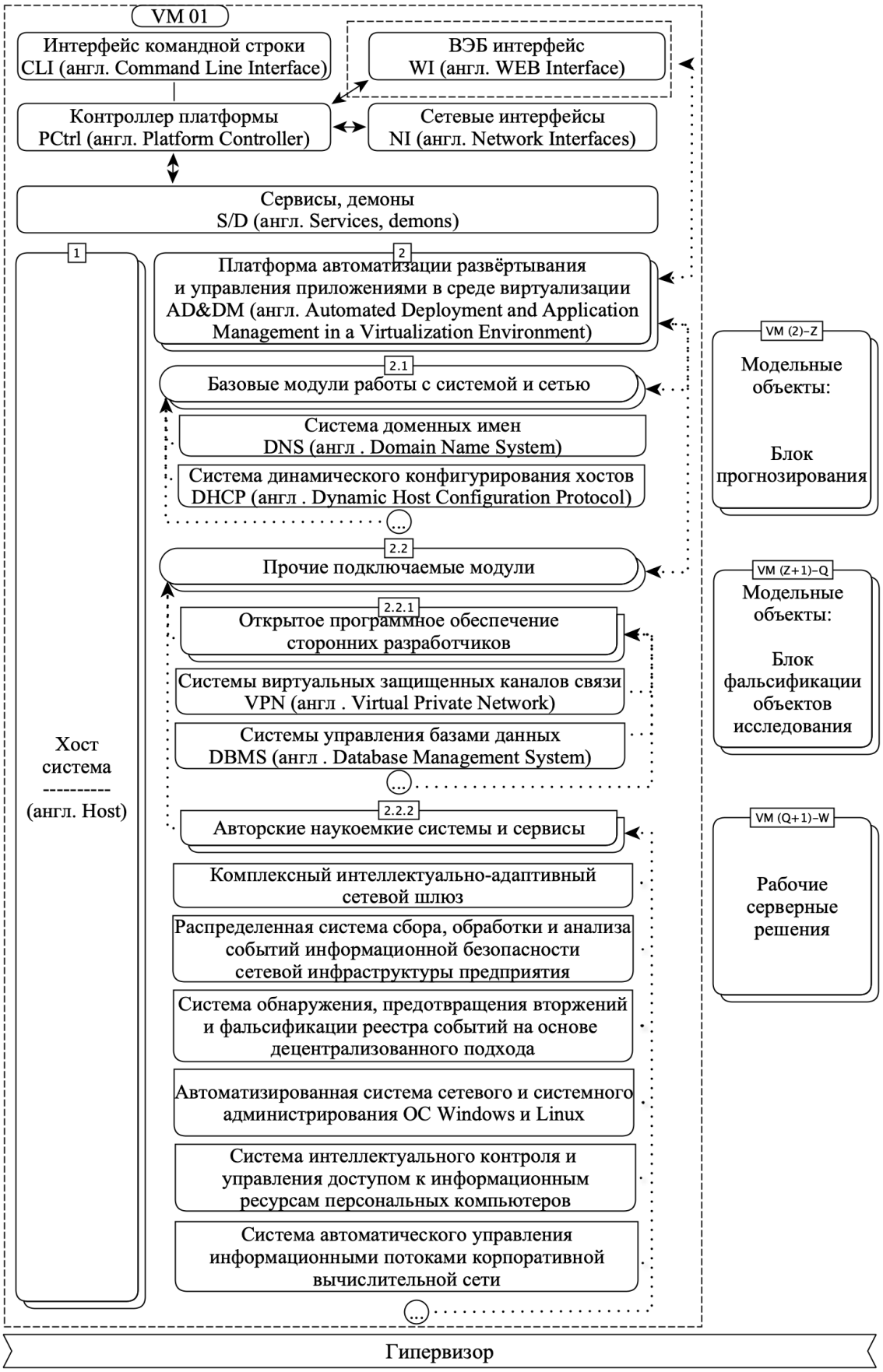

Рис. 3. Архитектура системы интеллектуально-адаптивного управления сетевой инфраструктурой предприятия

В случае ненадлежащей настройки доступ к клиентам мониторинга может быть получен недоверенным пользователем с последующим осуществлением лишь подписки. Не зная архитектуры сети предприятия и адреса размещения сервисов, злоумышленнику будет сложно осуществить первичный сбор данных для осуществления целенаправленной атаки. Штатные системные администраторы, которые владеют информацией об архитектуре сети и расположении сервисов, смогут просто настроить подписки для уведомления об обнаруженных и проверенных инцидентах.

Стоит отметить, что это единственная составляющая архитектуры проекта, через которую может быть осуществлен вывод информации с однослойным шифрованием точка-точка. При использовании клиентов мониторинга и клиентов доступа существует риск утечки информации, поэтому их использование в сети должно быть обосновано.

Несмотря на то, что клиенты мониторинга участвуют в генерации сессионного ключа, и, следовательно, получают доступ к информации для записи в блокчейн, они не могут получить доступ к обмену информацией между хостами, используя личные сообщения на основе опубликованных сертификатов публичного ключа. После выработки сессионного ключа по алгоритму Диффи–Хеллмана для неограниченного количества участников, клиенты мониторинга не генерируют приватный и публичный ключи и не публикуют свой сертификат открытого ключа. Таким образом, с ними не может быть произведен обмен информацией. Поскольку клиенты мониторинга не имеют публичного ключа, они не могут сохранить сессионный в блокчейне, в этом случае каждый из клиентов мониторинга имеет доступ только к текущей сессии.

Таким образом, клиенты мониторинга становятся участниками, осуществляющими только чтение из децентрализованного реестра событий без возможности сетевого взаимодействия с другими участниками Системы. В совокупности с использованием системы подписки на события вместо осуществления доступа на чтение из блокчейна можно сделать предположение, что использование клиентов не вводит критических уязвимостей в Систему.

В дополнении к клиентам мониторинга, осуществляющим доставку сообщения о событиях на основе модели подписчика, существуют клиенты доступа (провайдеры). Принципиально они отличаются от первой категории двумя аспектами:

1) генерируется приватный и публичный ключ, публикуется сгенерированный сертификат публичного ключа;

2) осуществляется чтение из блокчейн-хранилища и передача информации из базы сторонним программам с однослойным шифрованием точка-точка.

Присутствие у клиентов доступа ключей дает им возможность расшифровать информацию, хранящуюся в блокчейне на всем интервале времени их присутствия. Это свойство позволяет использовать их как драйвер для чтения из зашифрованного блокчейн хранилища и создания базы знаний систем предотвращения вторжений.

Для проверки работоспособности программного продукта выполнялось органическое и автоматизированное тестирование на всех этапах разработки, производился технический контроль проекта. На текущий момент продолжается экспериментальное исследование работы предложенного решения в сетевых инфраструктурах пяти предприятий с количеством хостов более 700. За шесть месяцев непрерывной работы Система зарекомендовала себя надежным, отказоустойчивым и безопасным решением. Размер базы данных распределенной системы сбора, обработки и анализа событий сетевой инфраструктуры предприятия составил от 1,25 до 14,3 % суммарного объема штатных баз знаний агентов первичного сбора информации различных систем и сервисов. Размер записей одного хоста в децентрализованное хранилище с учетом многослойного шифрования составлял 4 – 41,7 % от суммарного объема баз знаний локальных агрегаторов. Даже при дублировании всех перечисленных баз знаний введение избыточности является низкой стоимостью повышения надежности, безопасности и эффективности функционирования сетевой инфраструктуры предприятия.

Необходимо упомянуть, что типовые хосты фактически имеют незначительный объем локальных хранилищ (исчисляются десятками Мбайт за год работы среднестатистического офисного работника или домашнего пользователя). Однако в качестве недостатков проекта следует отметить требования к вычислительным мощностям (необходима материнская плата с многоядерным процессором и аппаратной поддержкой алгоритма шифрования AES, оперативной памятью от 2 Гб и поддержкой технологии коррекции ошибок), а также объему носителей информации.

Обсуждение результатов и заключение

В рамках данного проекта был разработан, программно реализован и исследован метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия. Научная новизна предлагаемого решения заключается в автоматическом управлении локальными и сетевыми информационными процессами технических объектов на основе данных децентрализованного блокчейн-хранилища с системой управления доверием к регистрируемым событиям. Принятие решений осуществляется на основе объективной и подтвержденной информации. Другим немаловажным аспектом научной новизны выступают профилирование доступа к информации и защита процесса передачи данных на основе группового, а также итерационного многослойного шифрования.

Программная реализация метода выполнена в виде системы обнаружения, предотвращения вторжений и фальсификации реестра событий на основе децентрализованного подхода. Была реализована интеграция с авторской системой интеллектуально-адаптивного управления сетевой инфраструктурой предприятия, в том числе с ее компонентом - распределенной системой сбора, обработки и анализа событий.

При этом важно отметить, что проект может выступать независимым продуктом. В частности, и модифицированное децентрализованное блокчейн-хранилище с системой управления доверием к регистрируемым событиям может составлять информативную и объективную базу знаний любой локальной или сетевой технической системы. При этом лишается актуальности проблематика доверия к журналам событий и нивелируются нештатные внешние и внутренние возмущения с имперсонацией, модификацией и фальсификацией данных.

Представленный подход имеет несколько особенностей:

1) избыточность на локальном хосте: несмотря на оптимизацию реестра событий и его емкость, Система не удаляет информацию с локальных агентов, оставляя ее в качестве дополнительного слоя проверки;

2) избыточность на всех объектах сетевого взаимодействия: реестры событий дублируются на всех хостах, что преднамеренно вводит избыточность и требует от узлов дополнительного свободного пространства на носителях информации. В рамках проекта данный прием выступает инструментом независимого информационного контроля;

3) существуют ограничения на скорость записей в реестр. В зависимости от сложности проверки вероятности события в системе, скорость записи в цепочку может меняться. Также стоит учитывать требования к вычислительным мощностям объекта для осуществления шифрования и дешифрования данных. Балансировка может быть произведена правильным выбором соответствующего формата хранения данных. Настройка параметров осуществляется через веб-панель администрирования при первичной установке.

Описанные моменты не являются существенными недостатками, а лишь выступают критериями настройки системы при интеграции в сетевую инфраструктуру предприятия и могут потребовать замену устаревшего управляемого сетевого оборудования на современную платформу x86 с процессором, поддерживающим аппаратное шифрование алгоритмом AES,

оперативной памятью от 2 Гб с поддержкой технологии коррекции ошибок, носителем информации от 500 Гб в зависимости от функционирующих сервисов и нагрузки конечной сетевой инфраструктуры предприятия.

Список литературы

1. Статья из 3 номера. Басыня Е.А. Децентрализованный подход к сбору и обработке данных информационной инфраструктуры предприятия / Е.А. Басыня, А.В. Сафронов // Вестник УРФО. Безопасность в информационной сфере. – 2019 -№3. – С. 52 -60.

2. 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.

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

4. Пальчевский Е.В. Разработка системы логирования IP-адресов для анализа активности внешнего сетевого трафика / Е.В. Пальчевский, А.Р. Халиков // Материалы Международной научно-практической конференции «Достижения и перспективы современной науки». - Астана, Казахстан. 2017. С. 96–99.

5. Сосновская М.Ю. Разработка системы идентификации событий ИТ-инфраструктуры на основе разбора и анализа системных журналов // Вестник современных исследований. 2018. № 5.1 (20). С. 520–522.

6. Shaikh J.R. Blockchain based Confidentiality and Integrity Preserving Scheme for Enhancing E-commerce Security / J.R. Shaikh, G. Iliev // Proceedings of the IEEE Global Conference on Wireless Computing and Networking (GCWCN). - Lonavala, India. – 2018. - P. 155 –158.

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.

Е.А. Басыня[1], А.В. Сафронов[2]

[1]«МИФИ» ұлттық зерттеу ядролық университеті, Мәскеу, Ресей

[2]Ақпараттық-коммуникациялық технологиялар ғылыми-зерттеу институты, Новосибирск, Ресей

Кәсіпорынның ақпараттық инфрақұрылымы оқиғаларының орталықтандырылмаған тізілімін қалыптастыру әдісі

Аңдатпа. Мақалада кәсіпорынның ақпараттық-коммуникациялық секторының деректерін жинауға, өңдеуге және талдауға қазіргі тәсілдердің мәселелері сипатталған. Оның объектілері мен жүйелеріне штаттан тыс ішкі және сыртқы әсерлердің қауіптері қарастырылады. Кәсіпорынның ақпараттық инфрақұрылымы оқиғаларының орталықтандырылмаған тізілімін қалыптастырудың өзіндік әдісі шолуға ұсынылады. Ұсынылған шешімнің ғылыми жаңалығы тіркелген оқиғаларға сенімді басқару жүйесі бар орталықтандырылмаған блокчейн қоймасы деректері негізінде техникалық объектілердің жергілікті және желілік ақпараттық процестерін автоматты түрде басқару болып табылады. Шешімдер қабылдау объективті және расталған ақпарат негізінде жүзеге асырылады. Ғылыми жаңалықтың аспектісі-ақпаратқа қол жеткізуді профильдеу және топтық,

сондай-ақ итерациялық көп қабатты шифрлау негізінде деректерді беру процесін қорғау. Мақала авторлардың кәсіпорынның ақпараттық инфрақұрылымының деректерін жинауға және өңдеуге орталықтандырылмаған көзқарас бойынша жұмыстың логикалық жалғасы болып табылады. Кәсіпорынның желілік инфрақұрылымын интеллектуалды-адаптивті басқару жүйесінің модулі ретінде интеграциялауға ұсынылған тәсіл негізінде оқиғаларды анықтау, басып кіруді болдырмау және оқиғалар тізілімін бұрмалау жүйесін әзірлеу, зерттеу қамтылған.

Кілт сөздер: оқиғалар тізілімі, журналдар, блокчейн-қойма, сенімді басқару жүйелері, жүйелік талдау, өңдеу, ақпараттық процестерді басқару.

E.A. Basinya[1], A.V. Safronov[2]

[1]National Research Nuclear University "MEPhI", Moscow, Russia

[2]Scientific Research Institute of Information and Communication Technologies, Novosibirsk, Russia

The method of forming a decentralized register of events of the information infrastructure of the enterprise

Abstract. The article describes the problems of existing approaches to the collection, processing, and analysis of data from the information and communication sector of the enterprise. The article considers threats of abnormal internal and external influences on its objects and systems. The authors review an original method for forming a decentralized registry of the enterprise information infrastructure events. The scientific novelty of the proposed solution lies in the automatic management of local and network information processes of technical objects based on data from decentralized blockchain storage with a trust management system for recorded events. Decision-making is based on objective and verified information. Another aspect of innovation is the profiling of access to information and the protection of the data transfer process based on group as well as iterative multilayer encryption. The article is a logical continuation of the authors' work on a decentralized approach to the collection and processing of data from the enterprise information infrastructure. The article considers the development and research of the system for detecting, preventing intrusions, and falsifying the event register based on the proposed approach for integration as a module of the system of intelligent adaptive management of the enterprise network infrastructure.

Keywords: event registry, logs, blockchain storage, trust management systems, system analysis, processing, information processes management.

References

1. Статья из 3 номера. Басыня Е.А. Децентрализованный подход к сбору и обработке данных информационной инфраструктуры предприятия / Е.А. Басыня, А.В. Сафронов // Вестник УРФО. Безопасность в информационной сфере. – 2019 -№3. – С. 52 -60.

2. 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.

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

4. Pal'chevskij E.V. Razrabotka sistemy logirovanija IP-adresov dlja analiza aktivnosti vneshnego setevogo trafika [Development of an IP address logging system for analyzing the activity of external network traffic] / E.V. Pal'chevskij, A.R. Halikov // International scientific-practical conference "Achievements and prospects of modern science." - Astana, Kazakhstan. 2017. C. 96–99. (in Russian)

5. Sosnovskaja M.J. Razrabotka sistemy identifikacii sobytij IT-infrastruktury na osnove razbora i analiza sistemnyh zhurnalov [Development of an IT infrastructure event identification system based on analysis and analysis of system logs] // Bulletin of modern research. 2018. № 5.1 (20). S. 520–522.

6. Shaikh J.R. Blockchain based Confidentiality and Integrity Preserving Scheme for Enhancing E-commerce Security / J.R. Shaikh, G. Iliev // Proceedings of the IEEE Global Conference on Wireless Computing and Networking (GCWCN). - Lonavala, India. – 2018. - P. 155–158.

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)

Сведения об авторах:

Басыня Е.А. - кандидат технических наук, доцент Национального исследовательского ядерного университета «МИФИ», Москва, Россия.

Сафронов А.В. - кандидат технических наук, технический директор Научно-исследовательского института информационно-коммуникационных технологий, Новосибирск, Россия.

Basinya E.A. - Ph.D., prof. in the National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia.

Safronov A.V. - Ph.D., technical director of the Research Institute of Information and Communication Technologies. 48 Deputatskaya Street, Novosibirsk, 630099, Russia.