Фам Ван Куонг, студент,
Краснодарское высшее военное училище

Кубенко Егор Георгиевич,
Старший преподаватель,
Краснодарское высшее военное училище

Шеин Сергей Леонидович,
Преподаватель,
Краснодарское высшее военное училище

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ЭЛЕКТРОННЫХ ЖУРНАЛОВ С ИСПОЛЬЗОВАНИЕМ HYPERLEDGER FABRIC ДЛЯ ВЫЯВЛЕНИЯ И РАССЛЕДОВАНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Аннотация. В статье рассматривается обеспечение целостности электронных журналов, используемых при выявлении и расследовании несанкционированного доступа. Показано, что после компрометации системы журналы могут быть изменены или удалены, что снижает их доказательную ценность. В качестве дополнительного механизма доверия предлагается использовать разрешённый блокчейн Hyperledger Fabric, в котором фиксируются хэш-значения журналов, временные метки и служебные метаданные, необходимые для последующей проверки. Сделан вывод, что применение Hyperledger Fabric позволяет повысить проверяемость и достоверность журналов, не заменяя при этом традиционные средства журналирования и мониторинга.

Ключевые слова: Электронные журналы, несанкционированный доступ, целостность журналов, цифровые следы, блокчейн, Hyperledger Fabric, , расследование инцидентов.

В современных условиях выявление и расследование несанкционированного доступа невозможно без опоры на журналы событий. Согласно подходу NIST, управление журналами событий представляет собой необходимую практику, обеспечивающую формирование, хранение, доступ и анализ журналов в целях выявления и расследования инцидентов [1].

Однако само наличие журналирования еще не гарантирует, что журнал сохранит доказательную ценность после инцидента. Если нарушитель получил административные полномочия или контроль над сервером логирования, он способен изменить либо удалить записи, имеющие критическое значение для реконструкции атаки. Вследствие этого проблема сводится не только к регистрации событий безопасности, но и к сохранению доверия к уже зарегистрированным цифровым следам. Именно в этой точке возникает потребность во внешнем механизме подтверждения целостности, который не заменяет журналирование, а усиливает его проверяемость.

Роль электронных журналов в выявлении и расследовании несанкционированного доступа и ограничения традиционных подходов к обеспечению их целостности

Электронные журналы являются основным источником цифровых следов инцидента. По их данным восстанавливается временная последовательность действий нарушителя, устанавливаются использованные учетные записи, фиксируются изменения прав доступа, обращения к защищаемым объектам, попытки повышения привилегий, изменения конфигурации и действия по сокрытию следов. В практической логике расследования именно журналы позволяют связать субъекта, время, объект воздействия и результат действия в единую причинно-временную картину.

При этом журналы важны не только для текущего мониторинга, но и для последующего доказывания. В момент расследования они превращаются из технического средства эксплуатации в источник цифровых доказательств. Поэтому критическим свойством журнала становится не просто наличие записей, а подтверждаемая неизменность их содержания после формирования. Если это свойство утрачено, то нарушается хронология событий, снижается достоверность выводов и становится затруднительным различение между исходными действиями нарушителя и позднейшей фальсификацией.

Традиционный централизованный подход к журналированию не решает эту задачу полностью. Системы журналирования, SIEM-платформы и централизованные хранилища хорошо подходят для сбора, нормализации, корреляции и анализа событий, однако после компрометации сервера хранения или привилегированной учетной записи появляется возможность выборочного удаления, подмены или дописывания записей. В результате журналы могут сохранять внешнюю формальную корректность, но уже не гарантировать достоверность зафиксированной истории [1].

Резервное копирование также не устраняет проблему в полном объеме. Оно повышает доступность и помогает восстановить данные после отказа, но не дает независимого подтверждения того, что конкретная версия журнала не была изменена до архивации или между копиями. Аналогично цифровая подпись усиливает защиту только при сохранении доверенного контура; если субъект, контролирующий контур, способен повторно сформировать файл и повторно инициировать процедуру подписания, то исходная точка доверия остается незащищенной. Следовательно, требуем не новый способ хранения журналов вместо SIEM, а внешний механизм, выносящий подтверждение целостности за пределы одного сервера, одной базы и одного администратора.

Технологические основы блокчейн и обоснование выбора Hyperledger Fabric

Применительно к рассматриваемой задаче блокчейн целесообразно понимать не как абстрактно «неизменяемую технологию», а как механизм фиксации и проверки ранее подтвержденного состояния данных. Записи или их агрегированные представления сначала хэшируются, затем включаются в транзакции и блоки, а блоки связываются между собой криптографически. Поэтому последующее изменение исходного подтвержденного состояния становится обнаруживаемым: повторно вычисленный хэш уже не совпадает с ранее зафиксированным значением [2].

Для данной задачи не требуется помещать в блокчейн полные тексты журналов. Напротив, практический смысл состоит в фиксации компактного подтверждения их состояния: хэш-значения, временной метки и набора служебных метаданных. Такой подход уменьшает нагрузку на реестр, не раскрывает избыточные сведения и одновременно позволяет доказуемо установить, совпадает ли исследуемый журнал с тем состоянием, которое было ранее подтверждено.

Выбор именно Hyperledger Fabric обусловлен архитектурными особенностями данной платформы. В официальной документации Hyperledger Fabric 2.5 она характеризуется как разрешенная распределенная реестровая платформа корпоративного уровня, обладающая модульной и гибкой архитектурой [2]. Данный вывод подтверждается и в работе E. Androulaki и соавторов, где Hyperledger Fabric рассматривается как модульная блокчейн-платформа, пригодная для использования в организационной среде благодаря поддержке различных механизмов консенсуса, смарт-контрактов и интеграции с системами управления идентификацией. Архитектура Hyperledger Fabric основана на модульном принципе, что позволяет адаптировать ключевые компоненты системы в соответствии с прикладными требованиями [3]. Основные элементы платформы включают [2]:

1. Смарт-контракты (chaincode) – исполняемые модули логики, реализуемые на языках Go, Java или JavaScript, выполняемые в контейнерной среде;

2. Реестр (ledger) – неизменяемая история транзакций, которая хранится локально на каждом узле-пире;

3. Узлы-пиры (peer nodes), на которых размещаются и исполняются контракты;

4. Узлы-упорядочиватели (orderer nodes), отвечающие за упорядочивание транзакций и формирование блоков;

5. Поставщик членства (Membership Service Provider, MSP), реализующий идентификацию участников сети на основе криптографических сертификатов;

6. Политики одобрения (endorsement policies), определяющие условия валидности транзакций.

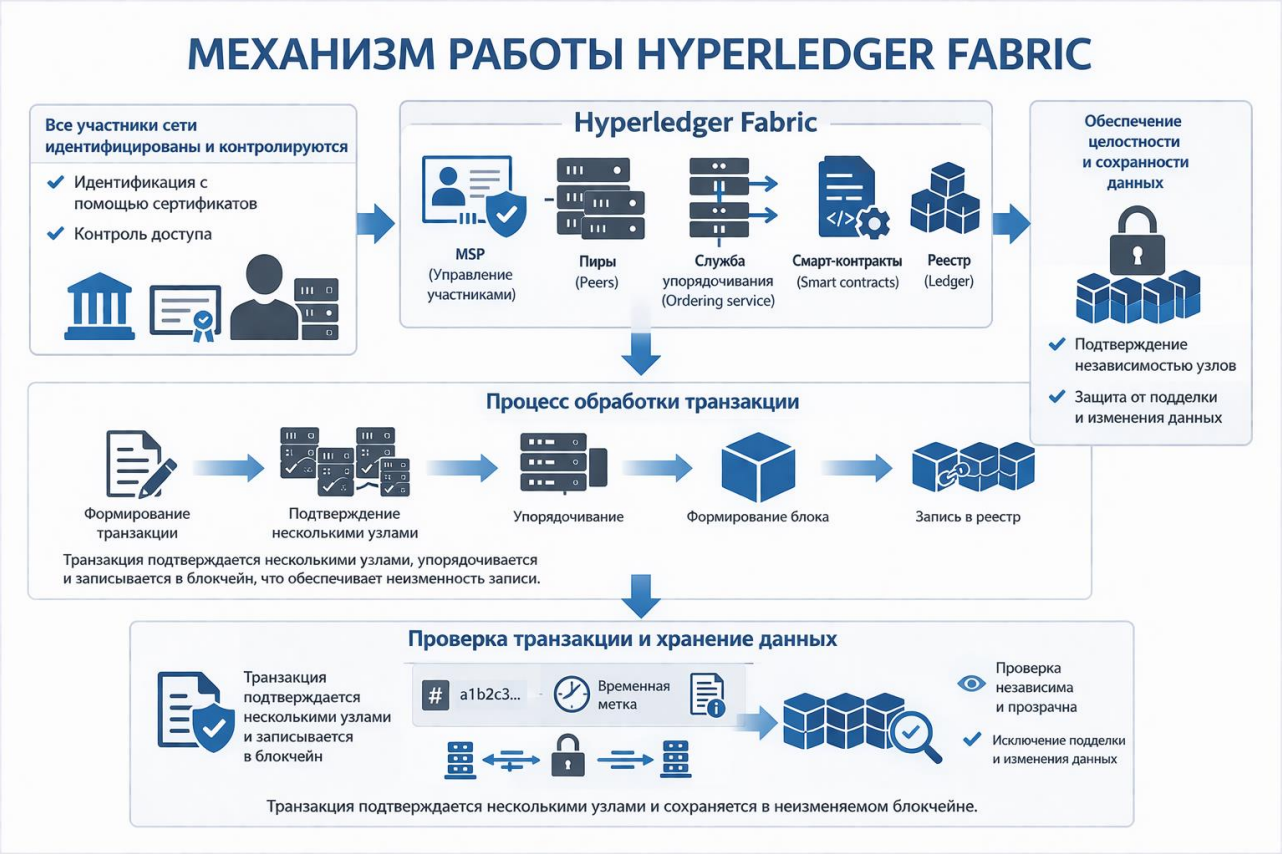

Рисунок 1

Для рассматриваемого исследования особое значение имеют те свойства Hyperledger Fabric, которые непосредственно связаны с подтверждением целостности журналов. Прежде всего, разрешенный характер сети и механизм Membership Service Provider исключают анонимность участников и позволяют точно установить, какой субъект инициировал ту или иную операцию. Не менее важна политика подтверждения транзакций, при которой запись признается действительной только после согласования со стороны заранее определенного набора участников. Это означает, что фиксация сведений о целостности журналов не зависит от одного сервера или одного администратора, а осуществляется в распределенной и контролируемой среде.

С практической точки зрения важна и архитектура каналов, позволяющая изолировать взаимодействие между группами участников и ограничивать доступ к данным. Кроме того, Hyperledger Fabric использует модель обработки транзакций execute-order-validate, при которой выполнение, упорядочивание и проверка транзакций разделены между различными

компонентами сети. Это повышает управляемость системы и делает ее пригодной для применения в задачах, где требуется не только регистрация действий, но и воспроизводимая проверка их корректности и целостности.

Таким образом, Hyperledger Fabric является подходящей платформой для обеспечения целостности электронных журналов, поскольку сочетает контролируемый состав участников сети, криптографическую идентификацию, многостороннее подтверждение транзакций, гибкость настройки и возможность изолированного взаимодействия между участниками. В рамках предлагаемой модели это позволяет использовать Hyperledger Fabric не как замену традиционной системы журналирования, а как независимый слой доверия, предназначенный для подтверждения целостности журналов и сохранения их доказательной значимости при выявлении и расследовании несанкционированного доступа.

Модель обеспечения целостности электронных журналов на основе Hyperledger Fabric, порядок их хранения и использование при расследовании

Предлагаемая модель строится как дополнительный слой доверия поверх существующей системы журналирования. Ее смысл состоит не в замене традиционных средств регистрации и анализа событий, а в вынесении подтверждения целостности журналов в независимую распределенную среду. Основная система журналирования и платформа класса SIEM продолжают выполнять сбор, хранение, нормализацию, корреляцию и анализ событий безопасности, тогда как Hyperledger Fabric используется только для фиксации подтверждающих данных о состоянии журналов. Такой подход позволяет сохранить совместимость с существующей инфраструктурой и одновременно повысить доверие к журналам, применяемым при выявлении и расследовании несанкционированного доступа.

Рисунок 2

Состав модели включает источники событий безопасности, подсистему сбора и нормализации журналов, модуль хэширования, модуль формирования транзакций, сеть Hyperledger Fabric и подсистему проверки целостности при расследовании. Источниками

событий выступают операционные системы, серверы приложений, сетевые устройства, службы аутентификации, механизмы контроля доступа и иные компоненты защищаемой информационной среды. После регистрации событие передается в подсистему сбора, где приводится к унифицированному формату и при необходимости агрегируется в логические пакеты. Затем вычисляется хэш отдельной записи либо пакета записей, после чего формируется транзакция для передачи в сеть Hyperledger Fabric. В реестре сохраняется не полный журнал, а подтверждение того, что определенный набор записей существовал в конкретном состоянии в конкретный момент времени.

Порядок хранения в рамках данной модели должен быть строго разделен на off-chain и on-chain части. Полные тексты журналов, расширенные атрибуты событий, корреляционные признаки SIEM и иные объемные данные должны храниться вне блокчейна - в штатной системе журналирования, SIEM или специализированном архиве. В блокчейн целесообразно записывать только хэш-значения, временные метки, идентификаторы источников и служебные метаданные, необходимые для воспроизводимой проверки. Основным режимом фиксации следует считать пакетную запись через заранее заданные интервалы времени или по достижении определенного объема данных. Вместе с тем для критически значимых событий, таких как изменение прав доступа, действия привилегированных учетных записей, отключение защитных механизмов или попытки удаления журналов, должна предусматриваться возможность немедленной отдельной фиксации. Именно такой порядок позволяет не перегружать распределенный реестр и одновременно сохранять доказуемую проверяемость наиболее значимых записей.

Использование журналов при расследовании строится на обратной процедуре проверки. Из off-chain-хранилища извлекается интересующий журнал или пакет журналов, после чего по тем же правилам нормализации повторно вычисляется хэш-значение. Далее это значение сопоставляется с ранее зафиксированным значением в реестре Hyperledger Fabric. Если значения совпадают, можно сделать вывод, что соответствующий фрагмент журнала после момента фиксации не подвергался изменению, и использовать его для восстановления временной шкалы инцидента, установления задействованных учетных записей, фактов изменения прав доступа, объектов воздействия и попыток сокрытия следов. Если же значения не совпадают, это должно рассматриваться как признак вмешательства в доказательную базу. В таком случае расследование необходимо расширять за счет резервных копий, сетевых журналов, журналов аутентификации, данных SIEM, EDR и иных цифровых следов. При этом принципиально важно подчеркнуть, что блокчейн не восстанавливает автоматически утраченные записи, а только позволяет установить факт нарушения их целостности.

Практическая ценность предлагаемой модели состоит в том, что она делает обнаружимым вмешательство не только в информационную систему, но и в сами журналы, на которые опирается расследование. Это особенно важно в случаях, когда нарушитель стремится скрыть факт проникновения или исказить хронологию инцидента. Вместе с тем модель имеет и ограничения. Она не предотвращает сам несанкционированный доступ, не заменяет SIEM, IAM, мониторинг, цифровую криминалистику и иные базовые механизмы защиты. Ее задача уже и конкретнее: обеспечить дополнительную проверяемость электронных журналов и сохранить их доказательную значимость после инцидента. Следовательно, эффективность такого подхода определяется не только выбором Hyperledger Fabric, но и качеством архитектурной увязки между журналированием, хранением, расследованием и управлением доверенным контуром подтверждения.

Заключение

Проведенный анализ показывает, что электронные журналы являются критически важным источником данных для выявления и расследования несанкционированного доступа,

однако их аналитическая и доказательная ценность сохраняется только при наличии подтверждаемой целостности. Традиционные централизованные модели журналирования обеспечивают удобство хранения и анализа, но не устраняют проблему доверия к журналам после компрометации сервера, администратора или доверенного контура хранения [1].

Основная ценность Hyperledger Fabric в данной задаче состоит не в замене журналирования, SIEM, IAM или иных средств защиты, а в создании независимого слоя доверия, который позволяет подтверждать целостность электронных журналов и сохранять их доказательную ценность при выявлении и расследовании несанкционированного доступа. При такой архитектуре полные журналы остаются в привычной системе хранения и анализа, а блокчейн фиксирует подтверждающие данные об их состоянии. Именно это сочетание делает подход практически обоснованным для организационной и корпоративной среды [2, 4].

Список литературы:

1. Kent K., Souppaya M. Guide to Computer Security Log Management. NIST Special Publication 800-92. Gaithersburg: National Institute of Standards and Technology, 2006. DOI: 10.6028/NIST.SP.800-92.

2. Hyperledger Fabric Documentation. Release 2.5 [Электронный ресурс]. Hyperledger Foundation, 2026. Доступно по документации release-2.5; дата обращения: 08.04.2026.

3. Androulaki E., Barger A., Bortnikov V., et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains // Proceedings of the Thirteenth EuroSys Conference. Porto, 2018. Article No. 30. DOI: 10.1145/3190508.3190538.

4. Shekhtman L., Waisbard E. EngraveChain: A Blockchain-Based Tamper-Proof Distributed Log System // Future Internet. 2021. Vol. 13, No. 6. Article 143. DOI: 10.3390/fi13060143.