Методика нормализации событий, получаемых от различных источников и отражающих любую ситуацию в системе или сети автоматизированной системы управления

Козлов Денис Викторович
адъюнкт Военной академии Воздушно-космической обороны, г. Тверь, Россия, kozlov.den.vikt@mail.ru

АННОТАЦИЯ

Введение: в работе осуществлено обоснование подхода к разработке методики нормализации событий, получаемых от различных источников и отражающих любую существенную ситуацию в системе или сети автоматизированной системы управления. **Цель исследования:** увеличить количество идентифицированных признаков инцидентов информационной безопасности в автоматизированной системе управления за счет исключения потери данных в процессе нормализации исходного события. **Результаты:** методика нормализации событий, получаемых от различных источников и отражающих любую ситуацию в системе или сети автоматизированной системы управления позволит исключить проблему потери данных, возникающую в процессе нормализации исходного события, создать единообразную схему полей для событий любого типа и источника, четко описывать, кто с кем и как взаимодействовал, а также сохранить суть и контекст взаимодействия, для того, чтобы специалисты по расследованию инцидентов ИБ и ответственные за разработку правил корреляции однозначно трактовали нормализованные события. **Практическая значимость:** методика нормализации событий, получаемых от различных источников и отражающих функциональность общесистемного прикладного программного и аппаратного обеспечения и специализированного программного и аппаратного обеспечения в автоматизированных системах управления, позволяет при ее реализации привести все события к единой форме, то есть провести процедуру анализа содержащейся в исходном событии информации в соответствии с заранее заданной для источника и типа события формулой нормализации без потери данных. **Обсуждение:** новизна предложенной постановки задачи состоит в том, что система регистрации и анализа событий, поступающих от различных источников в автоматизированной системе управления, включает единообразную схему полей для событий любого типа и источника.

КЛЮЧЕВЫЕ СЛОВА: информационная безопасность; инцидент; событие; нормализация; прогнозирование; автоматизированная система управления; категорирование.

Введение

С ростом числа информационных систем и совершенствованием методов и форм автоматизации процессов обработки и передачи информации повышается уязвимость системных процессов и ресурсов, напрямую влияющая на возможность нарушения конфиденциальности, целостности и доступности информации, и как следствие, прерывания процессов государственного и военного управления. Эти уязвимости влияют на информационную безопасность (ИБ) автоматизированных систем управления (АСУ) и могут привести к негативным последствиям. Такие последствия и определяют понятие инцидента, под которым понимается одно или несколько событий, которые влекут за собой нарушение целостности, конфиденциальности и доступности информации [1]. Событие – это любая ситуация в системе или сети, отражающая функциональность общесистемного прикладного программного и аппаратного обеспечения и специализированного программного и аппаратного обеспечения[2].

В большинстве случаев проблемы в работе АСУ вызваны нерегулярностью или низким качеством обслуживания оборудования, отсутствием надлежащего контроля над состоянием и работой установленных приложений. Причины аппаратно-программных сбоев и ошибок могут быть разными: это и скрытый производственный брак, и недостаточная совместимость некоторых устройств, и неаккуратность действий персонала, и устаревание техники, и резкое неконтролируемое возрастание нагрузки. Сбои в работе программного обеспечения также могут быть следствиями отказов в работе оборудования, нехватки системных ресурсов, недостаточно грамотной настройки, ошибок самого программного обеспечения, допущенных в процессе его разработки, намеренных действий злоумышленников или некорректной работы пользователей. Чтобы не допустить резкого снижения производительности информационной системы и возникновения сбоев, которые могут привести к простоям в работе, потерям критически важных данных, необходимо постоянно следить за состоянием оборудования и работой программного обеспечения. Правильность и своевременность принятия решений напрямую зависит от оперативности поступления и достоверности информации. Утрата критически важной информации может парализовать деятельность АСУ, а то и вовсе привести к ее исчезновению. Наличие системы мониторинга и предупреждения сбоев дает возможность сотрудникам, отвечающим за информационную безопасность, выявлять и устранять мелкие неполадки еще до того, как они перерастут в большие. За счет прямого мониторинга происходящих событий, состояния и производительности сетевых ресурсов выявляется и фиксируется для дальнейшего анализа актуальная информация, которая в дальнейшем используется для предотвращения аппаратно-программных сбоев и ошибок.

Для прогнозирования инцидентов ИБ в АСУ необходимо иметь инструменты, позволяющие анализировать в реальном времени происходящие события, число которых только растет.

Потеря информации в результате нормализации данных мониторинга

В базе данных совокупных условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации, сформированной Федеральной службой по техническому и экспертному контролю России (ФСТЭК России), имеется более 38 тыс. записей. Порядка 80% от общего числа записей относится к уязвимостям, возникающим в результате различных ошибок, сбоев и неполадок, вызванных несовместимостью отдельных устройств, версий драйверов, дефектами, проблемами интерфейсов, архивов, инфраструктуры и т.д.

---

[1] ГОСТ Р ИСО/МЭК 18044 – 2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – Москва : Стандартинформ, 2007. – XII, 20 с.

[2] NIST SP 800-61 Rev.2 Computer Security Incident Handling Guide – 2020. – 63 с.

Рано или поздно АСУ поступает в эксплуатацию. Пользователю важно, чтобы система работала без сбоев. Если внештатная ситуация все же произойдет, она должна устраняться с минимальными задержками. Для упрощения технической поддержки программной-аппаратной среды, особенно если автоматизированных рабочих мест и серверов много, обычно используются системы регистрации, анализа и управления в реальном времени событиями, исходящими от сетевых устройств и приложений, которые дают возможность сотрудникам, отвечающим за информационную безопасность, выявлять и устранять мелкие неполадки еще до того, как они перерастут в большие. За счет прямого мониторинга происходящих событий, состояния и производительности сетевых ресурсов, выявляется и фиксируется для дальнейшего анализа актуальная информация, которая в дальнейшем используется для предотвращения вероятной поломки оборудования.

В последнее время ведущие разработчики в области защиты информации выпустили на рынок целый спектр программных и программно-аппаратных решений, позволяющих осуществлять управление событиями, отражающими функциональность общесистемного прикладного и специализированного программного и аппаратного обеспечения в АСУ, получаемыми из подсистем журналирования различных источников. Подобные разработки относятся к классу систем регистрации, анализа и управления в реальном времени событиями, исходящими от сетевых устройств и приложений (SIEM) [1]. Среди отечественных разработак таких систем можно выделить программные средства, как Комрад (разработчик акционерное общество «Научно-производственное объединение «Эшелон»), СёрчИнформ SIEM (разработчик общество с ограниченной ответственностью «СерчИнформ»), Security Capsule (разработчик общество с ограниченной ответственностью «Инновационные технологии в бизнесе»). Целевой сегмент этих систем – банковский и государственный секторы, а также крупный и средний бизнес. Система Комрад успешно прошла сертификацию на соответствие стандартам Министерства обороны Российской Федерации.

Средний поток событий, обрабатываемых SIEM-системами в 2021 году составил 110,7 млрд событий в сутки, превысив прошлогодний показатель на 28 % [3]. Всего за 2021 год было зафиксировано свыше 1,9 млн событий с подозрением на инцидент ИБ, что превышает показатель прошлого года на 73 %. Доля выявленных инцидентов ИБ составила 19 %, причем 50,8 % из них были зафиксированы с помощью основных сервисов ИТ-инфраструктуры и средств обеспечения базовой безопасности: межсетевых экранов и сетевого оборудования, VPN-шлюзов, контроллеров доменов, почтовых серверов, базовых средств защиты, а оставшиеся 49,2 % были выявлены с помощью SIEM-систем. Причем от общего числа инцидентов ИБ, выявленных в 2021 году, 80% составили – ошибки, сбои, аварии, нарушения политик, дефекты технического и морального старение, проблемы интерфейсов, архивов, инфраструктуры и всего 20% – это целенаправленные вредоносные онлайн-действия. В 2020 году это соотношение составляло 54,6 % и 45,4 % соответственно. Увеличение инцидентов ИБ, выявляемых с помощью специализированных средств, говорит о том, что базовые средства защиты все чаще не справляются с их выявлением, а тем более прогнозированием.

Самая сложная часть процесса прогнозирования инцидентов ИБ – это точная идентификация признаков еще не произошедшего инцидента.

Сложность этого определяется комбинацией четырех факторов:

1. Инциденты могут быть обнаружены через многие различные средства, с различными уровнями детализации и точности. Автоматизированные средства обнаружения включают сетевой и хостовый IDPSs, антивирусное программное обеспечение и анализаторы логов.

[3] Rt-Solar.ru: [сайт]. – URL: tttps://www.rt-solar.ru/analytics/reports/ 2135/ (дата обращения: 28.01.2022). – Текст: электронный.

2. Инциденты могут быть также обнаружены ручными средствами, такими как сообщения пользователей о проблемах. У некоторых инцидентов есть явные признаки, которые могут быть легко обнаружены, тогда как другие почти невозможно обнаружить.

3. Объем потенциальных признаков инцидентов, как правило, высок.

4. Глубокие, специализированные технические знания и обширный опыт необходимы для надлежащего и эффективного анализа связанных с инцидентом данных.

Признаки инцидента попадают в одну из двух категорий: предшественники и индикаторы.

Предшественник – признак того, что инцидент может произойти в будущем. Индикатор – признак того, что инцидент, возможно, произошел или возможно происходит сейчас.

Предшественники и индикаторы идентифицируются с использованием различных других источников, наиболее общими для безопасности компьютерного программного обеспечения являются предупреждения, журналы регистрации, общедоступная информация и люди.

При обработке инцидентов детальный анализ событий с устройств является одним из ключевых этапов. Для решения задачи обработки инцидентов ИБ логично рассуждать, что чем больше данных мониторинга мы собираем, храним и анализируем, тем проще нам будет в дальнейшем не только оперативно идентифицировать признаки инцидентов ИБ, но и расследовать обстоятельства произошедших инцидентов ИБ для поиска причин их возникновения [4]. Большое количество данных мониторинга, генерируемых различными источниками в автоматизированных системах управления, необходимо привести в единообразный, пригодный для дальнейшего использования формат, то есть провести процедуру анализа содержащейся в исходном событии информации в соответствии с заранее заданной для источника и типа события формулой нормализации. Нормализованное событие представляет собой совокупность некоторых полей, состав которых определен в рамках некоторой таксономии, заполненных данными из необработанного события согласно правилам, указанным в формуле нормализации. Проблема потери данных при обработке в системах регистрации, анализа и управления событиями связана с несколькими этапами «упрощения» концептуальной модели исходного объекта или процесса. Примером такого упрощения может служить запуск и выполнение отдельно взятого процесса в операционной системе (ОС), представленного на рис.1 [2].

Первое упрощение. Процесс занимает определенную часть оперативной памяти, после чего ОС начинает выполнять описанные в нем инструкции. ОС передает в сервис журналирования (rsyslog, messages и т.п.) часть информацию об этой операции, при этом набор регистрируемых данных зависит от настроек логирования. Если не включить расширенный аудит действий, то часть информации в данный сервис журналирования не попадает. Но даже при расширенном аудите часть информации все же будет отброшена, потому что перечень данных регламентирован при разработке ОС.

Второе упрощение. После поступления данных в модуль логирования их необходимо сохранить в журнале событий. Если сервис журналирования ведет структурированный лог, где в качестве ограничителей могут выступать формат хранения записей или протокол, используемый для передачи информации на внешний сервер, то в нем заложена некоторая схема события с определенными полями и размером данных этих полей. Вероятно, что на этом этапе произойдет очередное «упрощение» модели и часть информации будет потеряна, поскольку данные, не уместившиеся в эту схему, будут отброшены, так как разработчики ОС решили, что именного такого объема информации достаточно для понимания происходящего явления.

[4] ГОСТ Р 59547 – 2021. Защита информации. Мониторинг информационной безопасности. Общие положения. – Москва : Стандартинформ, 2021. – VII, 13 с.

В результате потери деталей какого-то явления мы имеем событие, представленное записью в лог-файле. SIEM, получая такое событие, нормализует его путем распределения данных по полям своей схемы. Количество полей в схеме не может содержать их столько, сколько необходимо чтобы покрыть все возможные семантики всех событий от всех источников, то есть на этом шаге также происходит упрощение модели и потеря данных. И, если потерянные данные крайне важны в идентификации признаков инцидента и написании правил корреляции, их придется откуда-то извлечь. Получается, что «концептуальная модель» исходного объекта или процесса путем упрощения трансформируется в другую модель при этом теряя в детальности [3].

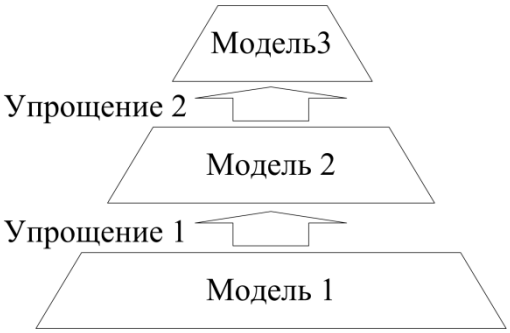

Рис.1. Потеря данных в результате упрощения одной модели в другую

Методика нормализации событий

Сложно найти способ, который бы позволил проводить упрощение одной модели в другую без потери данных. Зная это, необходимо сформулировать такой подход к нормализации и формированию перечню полей схемы событий, при котором не терялись бы информация, важная при корреляции и дальнейшем прогнозировании инцидентов ИБ.

В рамках SIEM модель представлена схемой – набором полей P_S, в которые в процессе нормализации, полученная информация из исходного события распределяется. В дальнейшем именно эта схема будет использоваться ответственными специалистами при создании правил корреляции [1]. Данная схема должна удовлетворять основным свойствам [4, 5, 6], а именно быть унифицированной для событий любого типа и источника, описывать суть взаимодействия и сохранять контекст взаимодействия.

В процессе разработки формулы нормализации информацию о взаимодействии необходимо найти в исходном событии и разложить ее в специально отведенные поля схемы. То же самое необходимо сделать с контекстом и сутью взаимодействия.

При выделении и построении типовых схем взаимодействия, основными уровнями на которых происходит основная часть итераций по сбору и обработке событий, является уровень сети L_N и уровень приложений L_{AP} [1, 7, 8, 9].

Атрибуты, которые всегда присутствуют в событиях на уровне сети L_N $\{A_S, A_O, A_I, A_P, A_{IP}\}$ (рис. 2). К ним относятся [9, 10, 11, 12, 13, 14]:

– субъект A_S (атрибут, оказывающий воздействие на объект);

– объект A_O (атрибут, на который оказывает воздействие субъект);

– источник A_I (как правило, хост, который регистрирует взаимодействие субъекта с объектом и порождает само событие);

– передатчик A_P (есть случаи, когда SIEM получает события не напрямую с источника, а с промежуточного сервера, через который данные события проходят).

Основной идентификатор атрибутов сетевого уровня – IP-адреса (A_{IP}). Могут быть и иные связанные идентификаторы – MAC-адреса на канальном уровне, FQDN – на прикладном [1].

Типовые схемы взаимодействия этого уровня можно условно разделить на два класса – основные и особые.

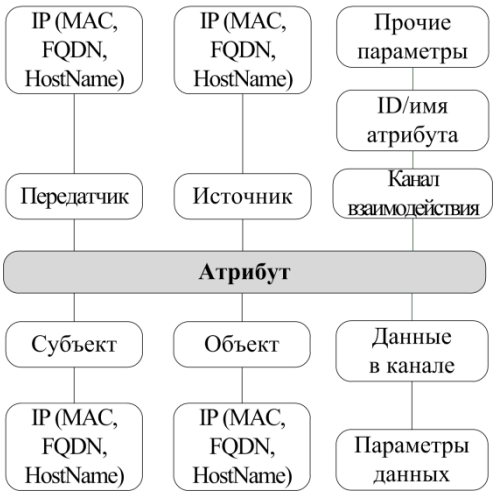

Рис. 2. Уровень сети

В рамках основной схемы взаимодействия, в событии, поступившем на вход SIEM, будет можно выделить все основные атрибуты: субъект, объект, источник, передатчик. Субъект воздействует на объект. Это воздействие регистрирует (наблюдает) источник и порождает событие. Событие от источника поступает в передатчик и с него попадает в SIEM (рис. 3).

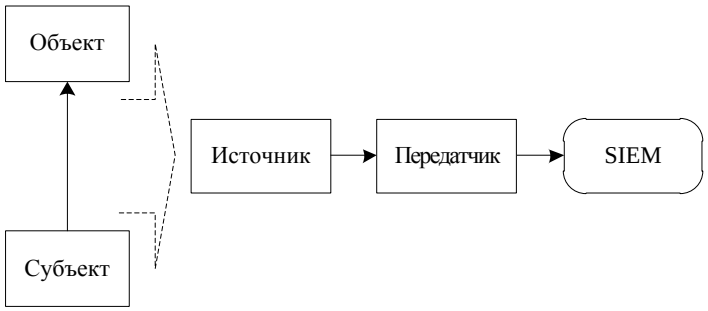

Рис. 3. Полная схема взаимодействия

Если передатчик отсутствует, то события попадают в SIEM напрямую из источника. Большая часть всех событий описывается именно этой схемой.

Нередки случаи, когда в событии один из атрибутов может отсутствовать. Такая схема взаимодействия называется особой. Зачастую такая схема характерна в ситуациях, при которой субъект сообщает об изменении своего внутреннего состояния, то есть он выступает одновременно в роли субъекта и объекта [15, 16, 17, 18].

Последняя особая схема взаимодействия характерна для ситуации, когда SIEM получает события от источника, сообщающего об изменении своего внутреннего состояния. В такой схеме роль источника совпадает с ролью субъекта и объекта. В отличие от предыдущей схемы, здесь события в SIEM приходят напрямую (рис. 4).

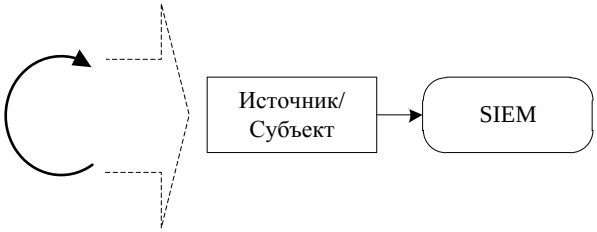

Рис. 4. Совмещение роли субъекта и объекта в источнике

На уровень приложений также присутствуют взаимодействия атрибутов: субъекта A_S, объекта A_O (рис. 5). Однако вся информация об источнике и передатчике остается непосредственно на уровне сети и не имеет своего отражения на уровне приложений. Большая часть всех типов событий имеет в своем составе взаимодействия одновременно на уровне сети и уровне приложений [1]. Однако отметим, что события, генерируемые непосредственно прикладным программным обеспечением, могут содержать в себе исключительно взаимодействия уровня приложений. Кроме того, на уровне приложений появляется дополнительный атрибут – Ресурс A_R [9]. Ресурс – промежуточный атрибут, через который субъект оказывает влияние на объект без прямого взаимодействия. Субъект опосредованно воздействует на объект через промежуточный ресурс.

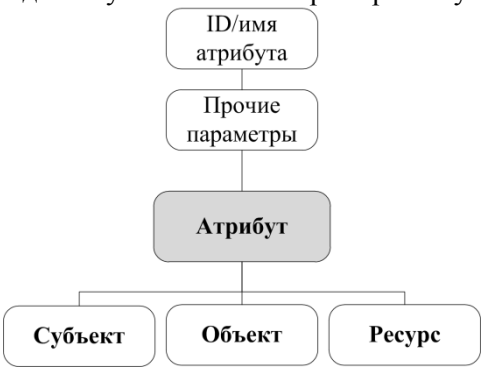

Рис. 5. Уровень приложений

Каждое событие, которое получает SIEM, может содержать информацию, описывающую: параметры канала передачи данных, передаваемые по этому каналу данные. Как правило, канал описывается такими параметрами, как идентификатор сессии A_{ID}, протокол передачи данных, время установления канала, время завершения, длительность. Данные в событиях характеризуются форматом, используемыми алгоритмами шифрования, количеством переданных пакетов, количеством переданных байт.

Таким образом, модель, которая строится в SIEM и представляется набором полей (схемой), должна содержать разделы для описания P_S $\{L_N, L_{AP}\}$ (рис. 6) [19, 20]:

1. На уровне сети L_N $\{A_S, A_O, A_I, A_P, A_{IP}, A_{ID}\}$ (субъект, объект, источник, передатчик, канал взаимодействия, данные передаваемые по каналу).

2. На уровне приложений L_{AP} $\{A_S, A_O, A_R, A_{ID}\}$ (субъект, объект или множества объектов, ресурс или множества ресурсов, канал взаимодействия).

Для каждого атрибута необходимо определить набор свойств, который ее однозначно идентифицирует. На уровне сети атрибуты идентифицируются IP-, MAC-адресами или FQDN. На уровне приложений – именами или ID. Схема должна иметь выделенные поля для хранения этих идентификаторов.

При написании правил корреляции важно четко понимать, с событиями какой схемы и какого уровня взаимодействия мы работаем. Это поможет правильно интерпретировать роли атрибутов, участвующих в событиях.

Заключение

Таким образом, методика нормализации событий, получаемых от различных источников и отражающих любую существенную ситуацию в системе или сети АСУ, позволит исключить проблему потери данных, возникающую на разных этапах нормализации исходных событий, создать единообразную схему полей для событий любого типа и источника, для того, чтобы ответственные за разработку правил корреляции однозначно трактовали нормализованные события, что позволит увеличить количество идентифицированных признаков инцидентов ИБ в АСУ.

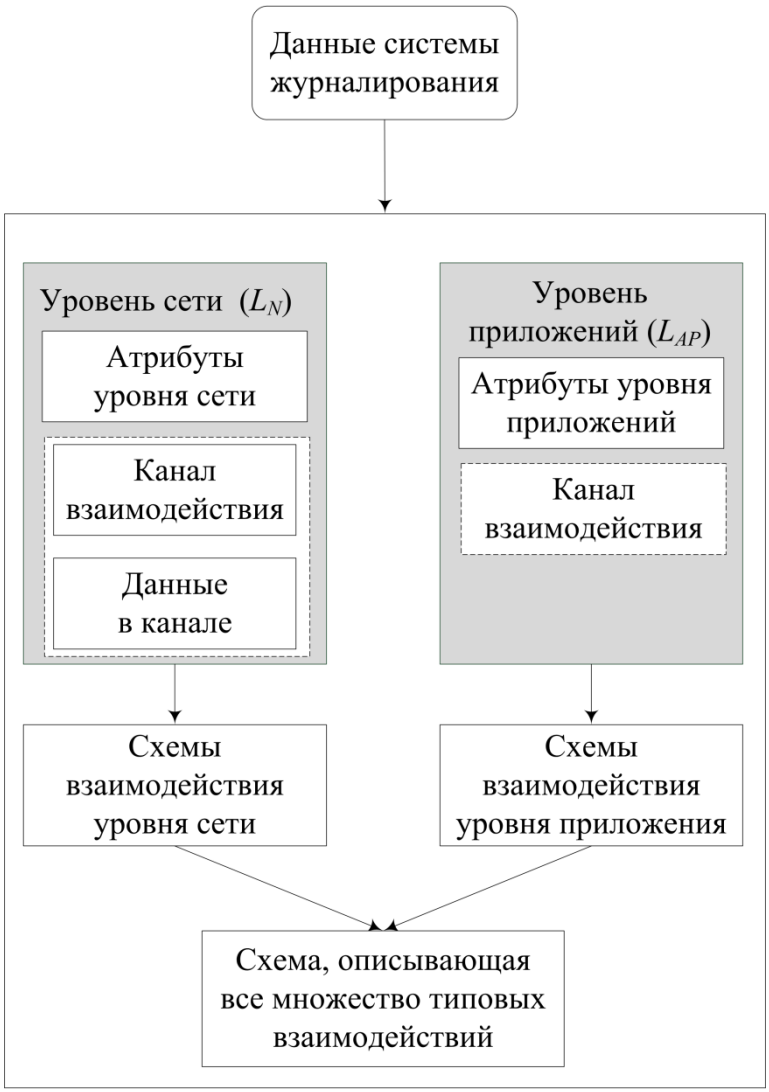

Рис. 6. Общая схема

Литература

1. *Miller D. R., Harris S., Harper A. A., VanDyke S., Blask C.* Security Information and Event Management (SIEM) Implementation / New York : McGraw-Hill Education-Europa, 2010. С. 53-56.

2. *Исхаков А. Ю., Исхаков С.Ю.* Модели нормализации данных в системах управления событиями безопасности РТК. М.: Институт проблем управления им. В.А. Трапезникова РАН, 2020. С. 1390 – 1399.

3. *Козлов Д.В.* Постановка научной задачи по разработке комплексной методики автоматического прогнозирования признаков инцидентов информационной безопасности в автоматизированных системах управления. Тверь: ФКУ НИИИТ ФСИН России, 2022. С. 84 – 91.

4. *Мельников Е. А.* Типовые схемы взаимодействия в системах сбора и анализа событий информационной безопасности SIEM // Электронный научный журнал. 2020. № 3(32). С. 21 – 24.

5. *Лексиков Е.В.* Разработка методики реагирования на инциденты информационной безопасности в организации. // Моя профессиональная карьера. 2019. Т. 3. № 5. С. 238-245.

6. *Королев И.Д.* Способ прямого синтаксического преобразования данных как средство минимизации объема данных о событиях и инцидентах информационной безопасности // Моделирование, оптимизация и информационные технологии. 2021. Т. 9. № 3(34).

7. *Котенко И.В.* Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Труды СПИИРАН. 2017. № 54. С. 5-34.

8. *Исхаков А.Ю.* Модели нормализации данных в системах управления событиями безопасности РТК. М.: Институт проблем управления им. В.А. Трапезникова РАН, 2020. С. 1390-1399.

9. *Попов В.И.* Корреляция и категорирование событий для расследования инцидентов информационной безопасности в информационной инфраструктуре // Информационная безопасность - актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. 2020. № 1(12). С. 202-208.

10. *Крыжановский А.В.* Управление инцидентами информационной безопасности. Волгоград: Волгоградский государственный университет, 2019. С. 30-33.

11. *Карташевский В.Г.* Анализ методов и средств выявления инцидентов информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. 2018. № 3(29). С. 50-54.

12. *Власенко А.В.* Событийное реагирование на инциденты информационной безопасности // Цифровая трансформация науки и образования. НАЛЬЧИК, 2021. С. 230-236.

13. *Николаенко Е.П.* Управление инцидентами информационной безопасности // ЭМПИ: экономика, менеджмент, прикладная информатика. Брянск: Брянский государственный технический университет, 2019. С. 207-210.

14. *Васильев В.И.* Интеллектуальная система анализа инцидентов информационной безопасности (на основе методологии SIEM-систем с применением механизмов иммунокомпьютинга) // Моделирование, оптимизация и информационные технологии. 2019. Т. 7. № 1(24). С. 536-547.

15. *Величко Д.В.* Регистрация, категоризация и приоритезация инцидентов информационной безопасности // Интернаука. 2020. № 17-1(146). С. 14-16.

16. *Аманбаева Ж.Ш.* Инциденты информационной безопасности. SIEM-системы // Уральский научный вестник. 2022. Т. 8. № 4. С. 94-99.

17. *Сауренко Т.Н.* Прогнозирование инцидентов информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2019. № 3. С. 24-28.

18. *Отакулов А.С.* Способы реагирования на инциденты информационной безопасности // E-Scio. 2020. № 1(40). С. 448-452.

19. Патент РФ 2664018. Система и способ автоматического расследования инцидентов безопасности в автоматизированной системе / Козлов Д.В. Заявл. 21.06.2017. Опубл. 14.08.2018. Бюл. № 23.

20. Патент РФ 2742179. Способ построения системы обнаружения инцидентов информационной безопасности в автоматизированных системах управления / Дроботун Е.Б., Козлов Д.В., Погорелов В.В., Аксенов М.А. Заявл. 03.03.2020. Опубл. 03.02.2021. Бюл. № 4.

THE METHOD OF NORMALIZATION OF EVENTS RECEIVED FROM VARIOUS SOURCES AND REFLECTING ANY SITUATION IN THE SYSTEM OR NETWORK OF AN AUTOMATED CONTROL SYSTEM

DENIS V. KOZLOV
Postgraduate student ,
Tver, Russia, kozlov.den.vikt@mail.ru

ABSTRACT

Introduction: the paper substantiates the approach to the development of a methodology for normalizing events received from various sources and reflecting any significant situation in the system or network of an automated control system. Purpose: to increase the number of identified signs of information security incidents in an automated control system by eliminating data loss in the process of normalization of the initial event. Results: the method of normalization of events received from various sources and reflecting any situation in the system or network of an automated control system will eliminate the problem of data loss arising in the process of normalization of the original event, create a uniform scheme of fields for events of any type and source, clearly describe who interacted with whom and how, and also preserve the essence and the context of interaction, so that the specialists in the investigation of information security incidents and those responsible for the development of correlation rules unambiguously interpret normalized events. Practical relevance: the method of normalization of events received from various sources and reflecting the functionality of system-wide application software and hardware and specialized software and hardware in automated control systems, allows for its implementation to bring all events to a single form, that is, to conduct a procedure for analyzing the information contained in the initial event in accordance with a predefined source and event type by normalization formula without data loss. Discussion: the novelty of the proposed formulation of the problem is that the system of registration and analysis of events coming from various sources in an automated control system includes a uniform scheme of fields for events of any type and source.

Keywords: information security; incident; event; normalization; forecasting; automated control system; categorization.

REFERENCES

1. Miller D. R., Harris S., Harper A. A., VanDyke S., Blask C. Security Information and Event Management (SIEM) Implementation / New York : McGraw-Hill Education-Europa, 2010. Pp. 53-56.
2. Iskhakov A. YU., Iskhakov S.YU. Modeli normalizacii dannyh v sistemah upravleniya sobytiyami bezopasnosti RTK. M.: Institut problem upravleniya im. V.A. Trapeznikova RAN, 2020. Pp. 1390 – 1399.
3. Kozlov D.V. Postanovka nauchnoj zadachi po razrabotke kompleksnoj metodiki avtomaticheskogo prognozirovaniya priznakov incidentov informacionnoj bezopasnosti v avtomatizirovannyh sistemah upravleniya. Tver': FKU NIIIT FSIN Rossii, 2022. Pp. 84 – 91.
4. Mel'nikov E. A. Tipovye skhemy vzaimodejstviya v sistemah sbora i analiza sobytij informacionnoj bezopasnosti SIEM // Elektronnyj nauchnyj zhurnal. 2020. No. 3(32). Pp. 21 – 24.
5. Leksikov E.V. Razrabotka metodiki reagirovaniya na incidenty informacionnoj bezopasnosti v organizacii. Moya professional'naya kar'era. 2019. Vol. 3. No.5. Pp. 238-245.
6. Korolev I.D. Sposob pryamogo sintaksicheskogo preobrazovaniya dannyh kak sredstvo minimizacii ob"ema dannyh o sobytiyah i incidentah informacionnoj bezopasnosti. Modelirovanie, optimizaciya i informacionnye tekhnologii. 2021. Vol. 9. No. 3(34).
7. Kotenko I.V. Sistema sbora, hraneniya i obrabotki informacii i sobytij bezopasnosti na osnove sredstv Elastic Stack // Trudy SPIIRAN. 2017. No. 54. Pp. 5-34.
8. Iskhakov A.YU. Modeli normalizacii dannyh v sistemah upravleniya sobytiyami bezopasnosti RTK. M.: Institut problem upravleniya im. V.A. Trapeznikova RAN, 2020. Pp. 1390-1399.
9. Popov V.I. Korrelyaciya i kategorirovanie sobytij dlya rassledovaniya incidentov informacionnoj bezopasnosti v informacionnoj infrastructure. Informacionnaya bezopasnost' - aktual'naya problema sovremennosti. Sovershenstvovanie obrazovatel'nyh tekhnologij podgotovki specialistov v oblasti informacionnoj bezopasnosti. 2020. No. 1(12). Pp. 202-208.
10. Kryzhanovskij A.V. Upravlenie incidentami informacionnoj bezopasnosti. Volgograd: Volgogradskij gosudarstvennyj universitet, 2019. Pp. 30-33.
11. Kartashevskij V.G. Analiz metodov i sredstv vyyavleniya incidentov informacionnoj bezopasnosti. Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2018. No. 3(29). Pp. 50-54.
12. Vlasenko A.V. Sobytijnoe reagirovanie na incidenty informacionnoj bezopasnosti. Cifrovaya transformaciya nauki i obrazovaniya. NAL'CHIK, 2021. Pp. 230-236.
13. Nikolaenko E.P. Upravlenie incidentami informacionnoj bezopasnosti. EMPI: ekonomika, menedzhment, prikladnaya informatika. Bryansk: Bryanskij gosudarstvennyj tekhnicheskij universitet, 2019. Pp. 207-210.
14. Vasil'ev V.I. Intellektual'naya sistema analiza incidentov informacionnoj bezopasnosti (na osnove metodologii SIEM-sistem s primeneniem mekhanizmov immunokomp'yutinga). Modelirovanie, optimizaciya i informacionnye tekhnologii. 2019. Vol. 7. No. 1(24). Pp. 536-547.
15. Velichko D.V. Registraciya, kategorizaciya i prioritezaciya incidentov informacionnoj bezopasnosti. Internauka. 2020. No.17-1(146). Pp. 14-16.
16. Amanbaeva ZH.SH. Incidenty informacionnoj bezopasnosti. SIEM-sistemy. Ural'skij nauchnyj vestnik. 2022. Vol. 8. No.4. Pp. 94-99.
17. Saurenko T.N. Prognozirovanie incidentov informacionnoj bezopasnosti. Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy. 2019. No. 3. Pp. 24-28.
18. Otakulov A.S. Sposoby reagirovaniya na incidenty informacionnoj bezopasnosti. E-Scio. 2020. No 1(40). Pp. 448-452.
19. Patent RF 2664018. Sistema i sposob avtomaticheskogo rassledovaniya incidentov bezopasnosti v avtomatizirovannoj sisteme. Kozlov D.V. Zayavl. 21.06.2017. Opubl. 14.08.2018. Byul. № 23.

20. Patent RF 2742179. Sposob postroeniya sistemy obnaruzheniya incidentov informacionnoj bezopasnosti v avtomatizirovannyh sistemah upravleniya. Drobotun E.B., Kozlov D.V., Pogorelov V.V., Aksenov M.A. Zayavl. 03.03.2020. Opubl. 03.02.2021. Byul. № 4.