УДК 004.056.5
DOI:10.25729/ESI.2023.30.2.015

Повышение эффективности систем защиты информации с помощью категоризации событий безопасности

Исхаков Андрей Юнусович[1], Исхаков Сергей Юнусович[2]
[1]Институт проблем управления РАН, Россия, Москва, *iay@ipu.ru*
[2]ПАО Промсвязьбанк, Россия, Москва

Аннотация. В статье рассмотрены основные принципы построения системы категоризации событий безопасности, сформулированы требования к ней и предложена методика ее применения, обеспечивающая возможность избегать необходимость корректировки наборов правил детектирования при добавлении новых источников событий или обновления подсистемы регистрации событий. При этом рассмотренные варианты категоризации применяются только для событий безопасности и не затрагивают события общесистемного программного обеспечения. Приведены примеры вариантов категоризации событий для различных средств защиты информации. Определены возможности масштабирования системы категоризации и методы ее адаптации для применения в промышленных системах автоматизации и управления. Также представлены результаты эксперимента по применению методики для повышения эффективности защиты автоматизированных систем на примере виртуального киберполигона, подтверждающие эффективность подобной методики и возможность ее применения для защиты промышленных систем.

Ключевые слова: корреляция, категоризация данных, нормализация, таксономия, система управления событиями безопасности, сценарии атак, инцидент

Цитирование: Исхаков А.Ю. Повышение эффективности систем защиты информации с помощью категоризации событий безопасности / А.Ю. Исхаков, С.Ю. Исхаков // Информационные и математические технологии в науке и управлении. – 2023. – № 2(30). – С. 152-164. – DOI:10.25729/ESI.2023.30.2.015.

Введение. Выстраивание процессов защиты в современных автоматизированных системах сопряжено с необходимостью сложной многоаспектной корреляции данных, генерируемых как в самой системе, так и ее инфраструктуре. При этом одним из источников являются журналы событий безопасности различных объектов, анализ которых позволяет формировать в системах защиты правила корреляции [1], чтобы сосредотачиваться на наиболее важных цепочках событий, свидетельствующих о возможных инцидентах.

Правила корреляции ориентированы на обработку уже нормализованных событий, каждое из которых представляет собой совокупность полей, заполненных данными из необработанного события. Набор полей определяется в рамках принятой в системе защиты таксономии [2], а отнесение данных исходного события к конкретным полям осуществляется в соответствии с заранее определенной формулой нормализации для данного источника.

В [3] подробно рассмотрены проблемы потери данных при обработке событий безопасности от различных источников и предложено методическое обеспечение процесса нормализации. Тем не менее для защиты реальных объектов при написании правил корреляции необходимо иметь возможность оперировать семантикой регистрируемых событий – учитывать контекст события для корректного определения его смысла.

Одним из способов решения этой задачи является применение категоризации – назначения обработанному событию некоторых меток, позволяющих однозначно трактовать регистрируемое событие. Инструментарий категорирования событий безопасности [4] представлен в ряде решений класса систем управления событиями безопасности (Security information and event management, SIEM) [5]. Однако, данная функциональность в основном ориентирована на выполнение поиска событий без привязки к исходному формату, источнику или ключевым словам. В то же время анализ научной литературы [6-13] свидетельствует о слабой проработке методических указаний по применению категоризации на этапе построения

комплексной эшелонированной защиты, реализующей взаимосвязь контента не только с целью структурирования информации и гибкого поиска при расследовании инцидентов, но и при интеграции средств защиты информации (СЗИ) и обновлении источников событий.

В статье рассматривается подход к разработке систем категоризации событий с точки зрения формирования методических основ разработки контента для выявления инцидентов. Под контентом здесь понимается совокупность формул нормализации, правил корреляции, политик и других инструментов, применяемых в СЗИ для выявления инцидентов. При этом подход не ориентирован на определенный тип средств защиты, будь то SIEM, межсетевые экраны для веб-приложений (Web Application Firewall, WAF) [14], системы контроля доступа к неструктурированным данным и т.д.

Предлагаемая методика применения категоризации ориентирована на формирование методических основ разработки и управления контентом различных систем защиты, как однокомпонентных, так и состоящих из нескольких эшелонов.

1. Категоризация как средство повышения эффективности системы защиты. Под эффективностью СЗИ понимается степень решения поставленной совокупности задач защиты информации. В данном исследовании в качестве СЗИ рассматриваются системы, включающие обработку событий безопасности, а в качестве критерия повышения эффективности СЗИ предлагается оценивать снижение значений показателя «Доля пропущенных цепочек атак (инцидентов)».

Одной из основных проблем построения комплексных систем защиты, состоящих из нескольких СЗИ, является необходимость верификации всего контента, который обеспечивает логику выявления инцидентов, при добавлении новых источников или объектов защиты. Ее решение может быть достигнуто за счет использования высокоуровневых критериев, опирающихся не на конкретные значения в определенных полях, а на некоторые метки, определяющие категории и отражающие физический смысл регистрируемых событий. Для этого необходима система категоризации данных, которая позволяла бы применять одинаковые критерии к событиям с одинаковым семантическим значением [3]. Такой подход не только позволяет конструировать более гибкие правила корреляции, но и обеспечивает возможность бесшовного (с точки зрения интеграции со средствами защиты информации) масштабирования инфраструктуры без необходимости переработки политик безопасности и правил корреляции на комплексах защиты. Приведем примеры:

1) в некоторой SIEM системе установлен пакет правил корреляции, обеспечивающий выявление конкретных типов атаки; правила при этом базируются на определенных значениях в полях нормализованных событий (идентификатор типа сообщения, значения поля «статус» и т.д.); при добавлении нового источника или обновлении текущих необходимо проверить наличие и корректность формул нормализации для него, а также удостовериться, что события от него попадут под критерии в вышеупомянутых правилах корреляции; на практике зачастую необходимо корректировать часть правил или даже весь набор, поскольку в противном случае они не сработают и инцидент не будет выявлен;
2) в некотором WAF используется набор правил, генерирующих события безопасности при обнаружении в журналах веб-сервера определенной последовательности значений; срабатывание таких правил формирует набор атомарных событий, на основе которых могут формироваться правила корреляции, генерирующие события о предполагаемом инциденте, при этом такая корреляция может выполняться как средствами самого межсетевого экрана для веб-приложений, так и внешними системами (например, на стороне SIEM через передачу туда атомарных событий); при добавлении нового

защищаемого веб-приложения необходимо проверить, подходят ли текущие правила для выявления аналогичных событий в его работе; на практике необходимость этого действия обусловлена широким спектром имеющихся на рынке фреймворков и технологий веб-разработки, поэтому зачастую необходимо добавлять новые правила под конкретное защищаемое приложение; в случае добавления или корректировки таких правил необходимо проверить, что они учтены во всех вышестоящих корреляциях, в противном случае корреляция не сработает и инцидент не будет выявлен.

Аналогичные проблемы характерны и для других типов СЗИ, принцип функционирования которых основан на использовании в явном виде журналов событий или «разборе» конкретных протоколов и формализации наблюдаемых взаимодействий. Применение категоризации позволяет избежать необходимость корректировки наборов правил детектирования при добавлении новых источников событий или обновления подсистемы регистрации событий существующих. Также нивелируются ситуации, когда правила корреляции не срабатывают из-за привязки к конкретным значениям в полях нормализованных событий.

2. Методика и принципы категорирования событий. Предлагаемый подход подразумевает, что все объекты защищаемой системы и ее инфраструктуры могут быть разделены на источники ИТ-событий и ИБ-событий (ИБ – информационная безопасность). При этом ИТ-источники создают записи в журналах о событиях на объекте без оценки происходящего с точки зрения ИБ, например, факт успешного скачивания файла. В свою очередь, ИБ-источники генерируют записи в журналах, содержащие дополнительные данные о фиксируемом событии с точки зрения ИБ, например, событие потокового антивируса об успешно заблокированной попытке скачать вредоносный файл.

В то же время источники событий безопасности могут генерировать ИТ-события, например, фиксировать факты обновления антивирусных баз, перезагрузки системы и т.д. Также общесистемное и прикладное программное обеспечение (ПО) часто содержит в себе модули защиты и может генерировать как ИТ-события, так и ИБ-события, поэтому категоризацию необходимо применять, основываясь на типе самого события, а не на типе источника. Данное исследование сфокусировано на событиях безопасности.

Категоризация должна применяться к нормализованным событиям и является существенным дополнением к этому процессу, обеспечивая возможность повысить эффективность правил корреляции при выявлении атак. В большинстве случаев это достигается за счет указания категории событий на последнем этапе создания формул нормализации или разработке вспомогательных правил. При разработке системы категоризации предлагается использовать следующие принципы.

Во-первых, каждое нормализованное событие должно иметь не более одной метки в рамках отдельной категории. Это позволяет определить правила наполнения таксономических полей на предшествующем этапе – нормализации событий. Кроме того, такой подход позволяет снизить количество условий в правилах корреляции и не делать дополнительных проверок для определения контекста события.

Во-вторых, масштаб системы категорирования должен обеспечивать необходимый и достаточный уровень для формирования правил корреляции. Другими словами, количество и структура категорий неразрывно связаны с механизмом корреляции событий и должны формировать единую методическую базу при выявлении и расследовании инцидентов.

В общем случае, методика применения категоризации выглядит следующим образом.

Шаг 1. Экспертная оценка события. На данном этапе эксперт определяет, относится ли это событие к типу событий ИБ и попадает ли оно к данной системе категоризации.

Шаг 2. Проведение нормализации события.

Шаг 2.1. Выявление основных сущностей в событии.

Шаг 2.2. Определение схемы взаимодействия основных сущностей.

Шаг 2.3. Извлечение значимых данных и назначение их в таксономические поля, определенные схемой нормализации.

Шаг 3. Проведение категоризации события.

Шаг 3.1. Определение среды, откуда получено событие.

Шаг 3.2. Определение основного типа инцидента.

Шаг 3.3. Определение подтипа инцидента, к которому относится событие. Данный шаг может повторяться несколько раз в зависимости от детализации и количества уровней выделенных подтипов.

При этом для успешного применения методики должны выполняться следующие требования:

- должны быть определены справочники полей нормализации и уровней категоризации;
- для каждой категории событий должен быть определен набор полей нормализации, которые подлежат заполнению.

Таким образом, схемы категоризации и нормализации событий должны быть напрямую связаны между собой. Это позволяет обеспечить соответствие семантики события всей важной информации в нем и набору полей, куда эта информация должна быть помещена. При появлении новых источников, события от которых не укладываются в данную схему, следует:

- скорректировать справочники категорий и соответствующие им наборы полей нормализации;
- провести проверку всех формул нормализации для событий изменившихся категорий;
- провести проверку правил корреляции, использующих в своих условиях затронутые категории событий.

3. Варианты применения категоризации. Рассмотрим вариант применения категоризации в SIEM-системе. Определенные в [3] сущности, используемые для нормализации событий, взаимодействуют между собой. Для описания среды взаимодействия в предлагаемой системе категоризации выделим основные уровни – сетевое взаимодействие, уровень хоста и уровень прикладного ПО. В ряде случаев допустимо выделить в отдельный уровень события, фиксируемые средствами физической охраны, поскольку многие из них снабжены развитыми механизмами регистрации событий, которые используются при выявлении инцидентов.

С учетом текущего уровня развития ИТ-инфраструктуры для предлагаемой системы категоризации введем предположение, что любой инцидент в автоматизированной системе будет отражен на одном или нескольких уровнях среды взаимодействия, определенных выше. На каждом из этих уровней могут иметься СЗИ, которые выявляют следы инцидента или отдельные атомарные события из общей цепочки действий атакующих. При этом на уровне сети речь идет о характерных следах в сетевом трафике, на уровне хоста могут быть использованы журналы аудита операционной системы и встроенных средств удаленного управления сервером, а в случае с прикладным ПО нередко присутствуют модули защиты, которые фиксируют аномалии на уровне системы и генерируют события безопасности.

Наличие событий от средств физической охраны весьма опционально. К тому же, далеко не всегда можно построить цепочки атаки, связав эти события. В связи с этим для подобных событий предлагается вводить отдельные категории. Поскольку к подобным источникам обычно относятся охранно-пожарные системы или системы контроля и управления доступом, то детектируемые ими события предлагается разделить на три типа – обнаружение

физического проникновения (проход через турникет, движение в охраняемой зоне и т.д.), повреждение объекта (например, срабатывание датчика разбития стекла), а также сигнал тревоги (обнаружение пожара, включение оповещения и т.д.).

Определив среду, в которой зафиксировано событие, необходимо определить основной тип, отражающий его физический смысл. Поскольку ранее было определено, что работа с одинаковыми по своей семантике событиями должна строиться по одинаковым критериям, то категорировать их надо одинаково, независимо от среды взаимодействия, поэтому в случае с уровнями сетевого взаимодействия, хоста и прикладного ПО набор таких типов подлежит объединению. Именно этот перечень типов формирует еще один уровень категоризации и, в целом, определяет некоторый рубрикатор инцидентов, который, в свою очередь, должен быть необходим и достаточен в рамках защищаемого объекта.

Для обеспечения масштабируемости системы категорий допускается введение дополнительных уровней, уточняющих различные подтипы инцидентов.

На рис. 1 приведена схема варианта применения категоризации для SIEM.

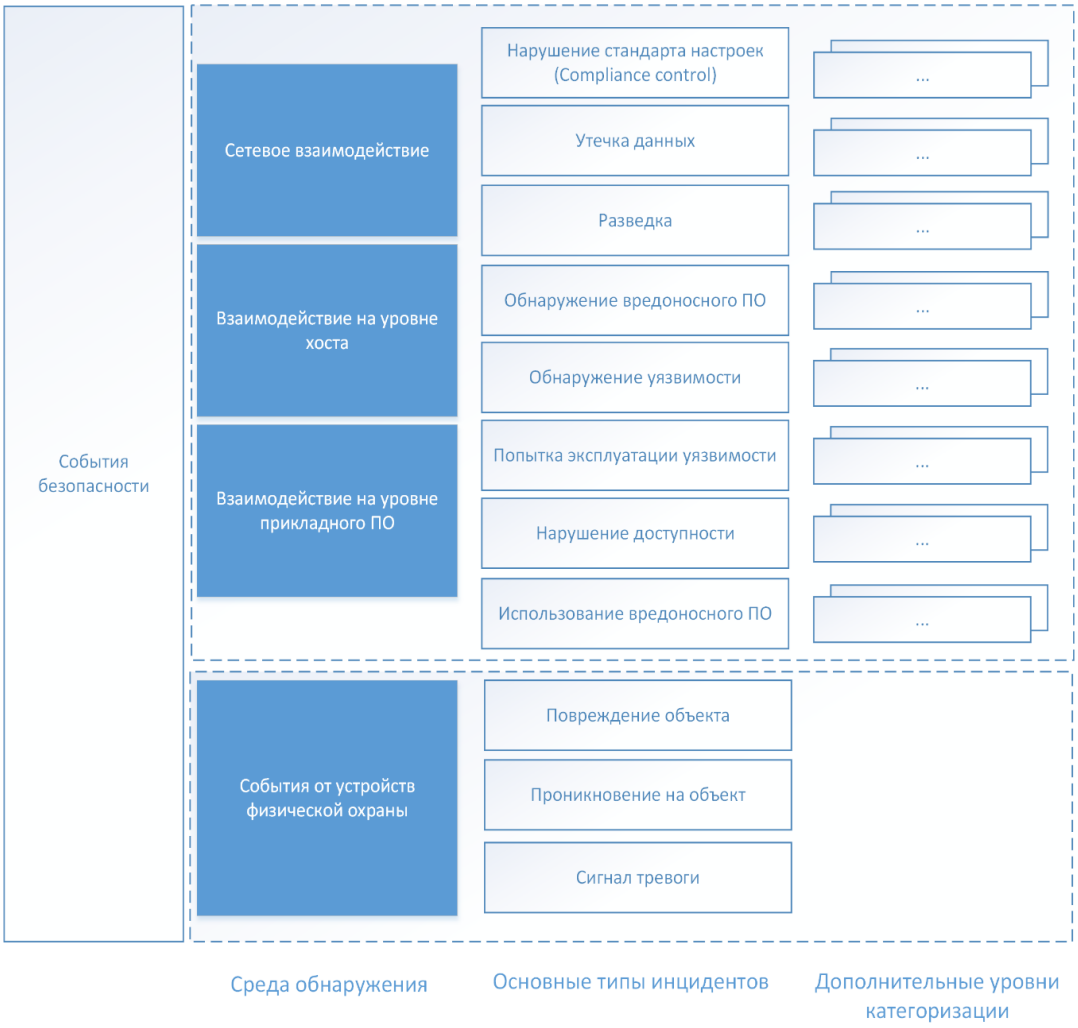

Рис. 1. Пример категоризации событий для SIEM

Рассмотрим преимущества категоризации на другом частном примере – эксплуатации WAF (рисунок 2), установленного в одном из наиболее популярных режимов интеграции Reverse-proxy [14]. В таком режиме WAF терминирует на себе SSL-трафик и выполняет инспекцию трафика для выявления и блокировки атак на веб-приложение. Поскольку функциональность разбора HTTP-запросов [14] является базовым компонентом WAF, будем считать, что этап нормализации (фактически, парсинг заголовков и содержимого HTTP-

запросов и ответов) выполняется без вмешательства оператора. Запросы, содержащие признаки атак (исходя из правил безопасности) будем называть событиями. При этом существует необходимость построения сложных правил, включающих объединение нескольких событий в цепочки (как часто повторяющихся в течение некоторого промежутка времени, так и последовательности нескольких событий разного типа).

Поскольку в данном примере функционирование СЗИ строится на основе событий о сетевом взаимодействии, применять уровни среды, аналогичные примеру на рисунке 1, некорректно. Если же WAF обеспечивает защиту нескольких приложений, можно определить в качестве среды обнаружения классы критичности защищаемых систем. Типы инцидентов также, как и в случае с предыдущим примером, будут общими, поскольку работа с одинаковыми по своей семантике событиями должна строиться по одинаковым критериям. При этом понимание среды обнаружения может быть использовано в дальнейшем для выработки сценариев реагирования.

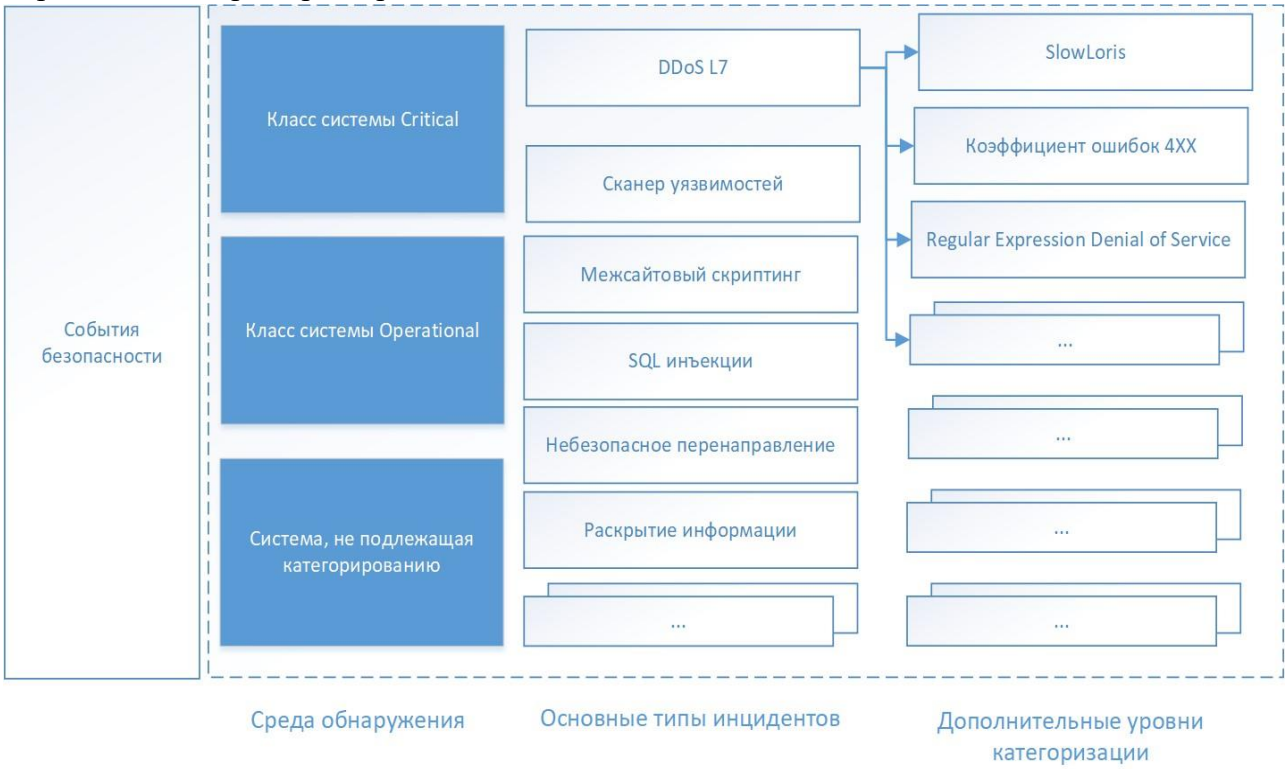

Рис. 2. Пример категоризации событий для WAF

Рассмотрим задачу защиты от DDoS-атаки [15] на уровне L7 модели OSI [14, 15] для систем класса Critical и систем, не подлежащих классификации. Наличие эшелонированной защиты на других СЗИ, кратная избыточность в части предоставляемых ресурсов системы и бизнес-логика обусловливают необходимость для оператора СЗИ устанавливать высокие пороги для блокировки источников запросов по признаку DDoS на основе счетчика ошибок. Для систем, не подлежащих категорированию, исходя из отсутствия других эшелонов защиты и запаса в части вычислительных ресурсов, требуется обеспечить незамедлительную отправку источников запросов в списки блокировок. Таким образом, при добавлении новой системы, исходя из присвоения соответствующей метки, обновление правил корреляции не требуется.

Приведенные на рисунках 1 и 2 схемы не претендуют на полноту обзора возможных типов инцидентов, а предназначены для демонстрации разработки категоризации для разных СЗИ, исходя из приоритизации защищаемых компонент и особенностей эксплуатации объекта. Важно отметить, что у разных вендоров и даже разных классов СЗИ одного вендора имеются существенные отличия в терминологии функциональности разработки контента.

4. Особенности применения методики для промышленных систем автоматизации и управления. Внедрение любой системы защиты требует адаптации к защищаемому объекту, что особенно характерно для промышленных систем автоматизации и управления (ПСАиУ). Это связано с большим количеством разнородных источников событий и широкой вариативностью их версий [16]. Даже на двух схожих ПСАиУ могут оказаться объекты одного класса, но с разными версиями системного ПО, что может привести к различиям в регистрируемых событиях безопасности, поэтому необходимо адаптировать контент для выявления атак, учитывая приведенные выше принципы категоризации событий.

В первую очередь, необходимо оценить и актуализировать перечень имеющихся источников событий, в том числе:

- проверить, что все необходимые для срабатывания правил корреляции источники присутствуют в ПСАиУ и с них возможен сбор событий безопасности;
- убедиться, что на требуемых источниках событий применены требуемые настройки аудита (поскольку несоответствие этих настроек может привести к отсутствию необходимых для детектирования событий);
- организовать подключение всех необходимых источников и проверку корректности доставки событий от них (в зависимости от процессов в ПСАиУ могут значительно отличаться интервалы сбора событий с пассивных источников либо иметь место задержки и потери событий от активных источников);
- провести верификацию системы категоризации и нормализации событий на предмет соответствия данным, получаемым с источников (при необходимости провести корректировку справочников полей в соответствии с указаниями к предлагаемой методике).

После этого следует провести анализ самого набора правил корреляции и, при необходимости, его корректировку. При корректировке имеющихся или создании новых правил корреляции необходимо:

- учитывать временные интервалы и особенности доставки событий и, при необходимости, подобрать необходимые периоды корреляции данных; поскольку в ПСАиУ могут иметь место длительные задержки в поступлении событий от ряда источников [17], то может быть нарушена логика детектирования; в данных случаях следует рассмотреть возможность проведения «отложенной корреляции», осуществляя периодическую выборку событий, уже поступивших в базу; это позволит корректно восстановить последовательность действий и выявить случившийся инцидент, хоть и постфактум, вместо того, что он будет пропущен;
- определить сегменты ПСАиУ, для которых будут действовать тот или иной контент, поскольку большинство правил объективно лишь для определенных участков системы; например, зачастую не стоит реагировать на попытки сканирования ресурсов во внешнем dmz-контуре, тогда как подобные явления внутри закрытых сегментов сети требуют незамедлительного реагирования;
- определить и внести список исключений, заполнив необходимые справочники; в любой реальной системе существуют объекты, активность которых должна быть исключена из логики детектирования, поскольку данные процессы являются легитимной активностью.

Помимо вышеуказанных действий, также необходимо провести анализ системы критичности инцидентов, основываясь на важности активов либо на типе инцидентов, определяемом на втором уровне системы категоризации.

5. Стенд киберполигона и апробация методики. Для апробации разработанной методики был разработан стенд (рисунок 3), входящий в состав киберполигона ИПУ РАН.

Пользователями методики выступали операторы СЗИ – эксперты по направлениям сетевой безопасности и безопасности веб-приложений. В основе стенда лежит система усиленной проверки подлинности субъектов [18], анализирующая, в том числе, данные из системы управления событиями информационной безопасности. Усиленная проверка подлинности заключается в применении дополнительных механизмов адаптивного подбора факторов и способов аутентификации, исходя из категории выявленной аномалии, детектируемой посредством применения моделей машинного обучения [14].

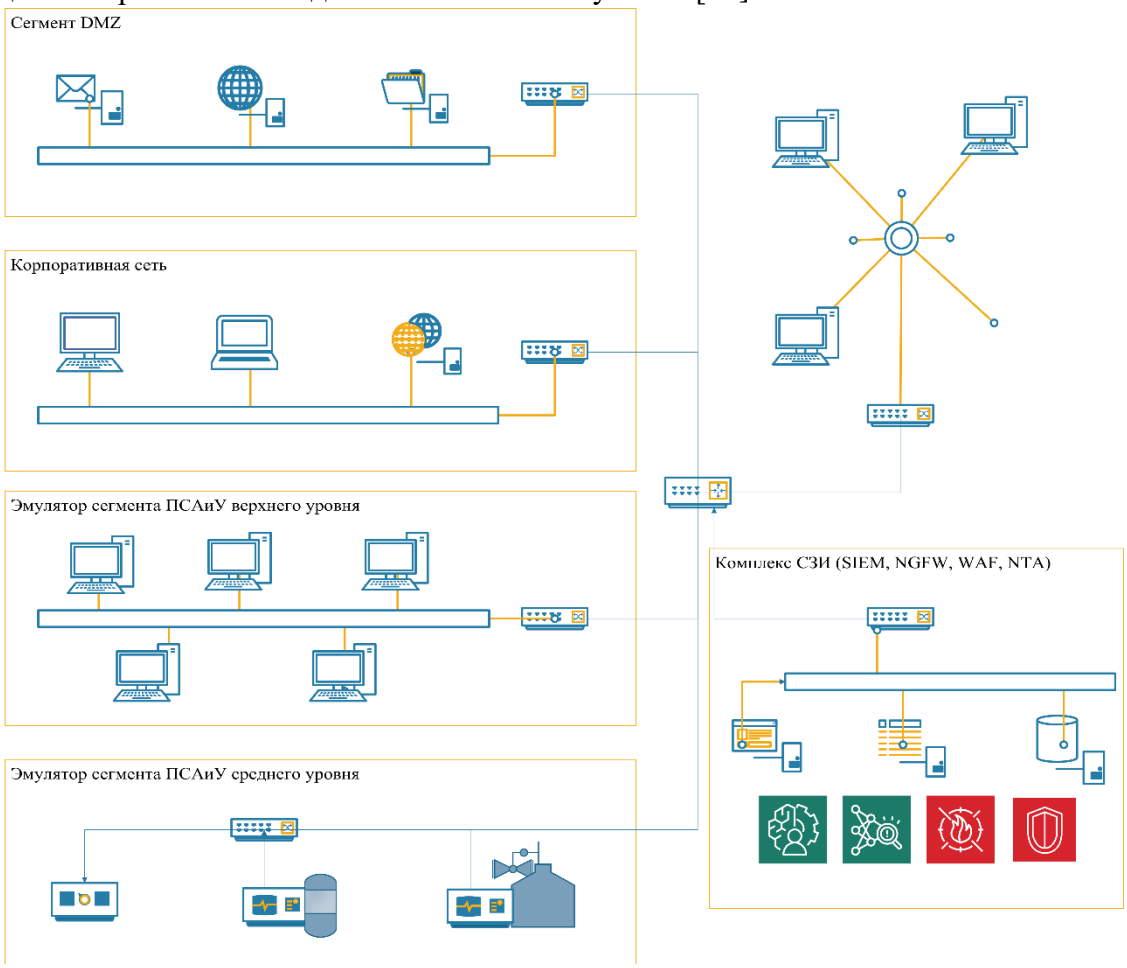

Рис. 3. Структурная схема задействованного стенда

Сегментация различных участков сети киберполигона выполняется на логическом уровне, что в рамках поставленных исследовательских задач является допустимым. В составе полигона реализован сегмент средств обеспечения безопасности, который включает в себя систему управления событиями безопасности, межсетевые экраны различных классов (Next Generation Firewall, Web Application Firewall), потоковую песочницу. Гибкость управления и возможность масштабирования основных эмулируемых хостов реализована за счет технологии контейнеризации. Была поставлена задача оценить эффективность применения предложенной методики категоризации посредством оценки пропущенных инцидентов безопасности в ходе эмуляции жизненного цикла различных сегментов киберполигона.

Реализация предложенной методики непосредственно на СЗИ выполнялась с помощью механизма тэгирования атомарных правил безопасности (листинги 1 и 2).

Листинг 1. Пример псевдокода правила корреляции до применения категоризации

```
alert_to_BL
{
   correlation_brute_acs_vuln12(times=100, time_frame=5, period=3)
   {
```

```
        Policy_rule equals a323dcf19403 // Vendor1
        or
        Policy_rule equals a109f34c3987 // Vendor1_new_firmware
        or
        Policy_rule equals 384124hfb324 // Vendor2
        or
        Policy_rule equals 324145453cc2 // Vendor3
    }
}
```

Листинг 2. Пример псевдокода правила корреляции после применения категоризации

```
alert_to_BL_upgrade
{
   correlation_brute_acs_upgrade(times=100, time_frame=5, period=3)
   {
      Event_tag.name contains “Brute_vuln_acs”
   }
}
```

На период проведения эксперимента были зафиксированы 72 сценария атак, ранее верифицированных вышеуказанными экспертами, применявшими данную методику. Все сценарии запускались автоматически с помощью скриптов, каждый из которых рассчитан на конечное количество выполнений атак для фиксации эталонного количества инцидентов. В течение 14 дней случайным образом в каждый из сегментов вносились корректировки по составу хостов, запущенных служб, сервисов и ПО. За указанный период апробации методики получены результаты, представленные на рис. 4 и в таблице 1.

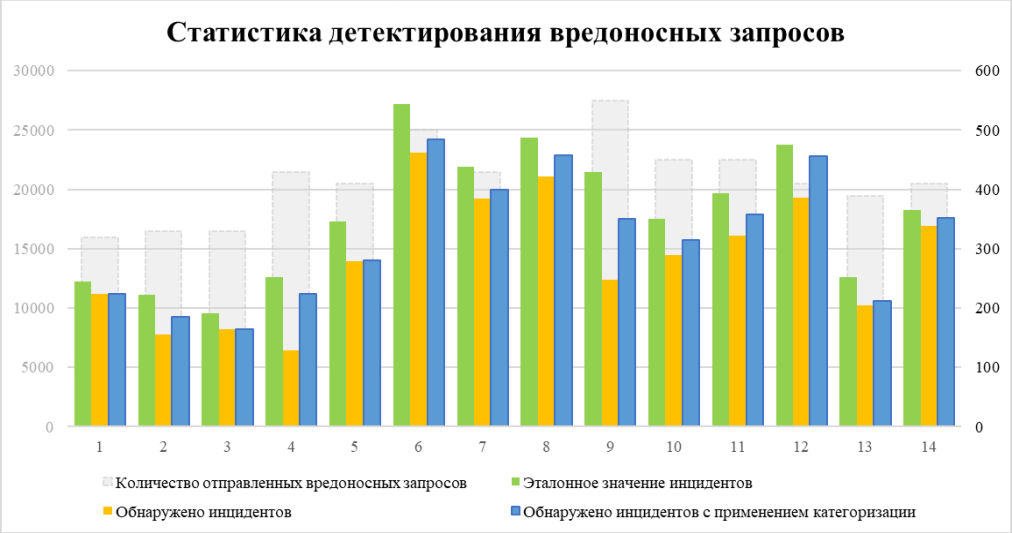

Рис. 4. Статистика обнаруженных инцидентов безопасности

Таблица 1. Результаты апробации методики

Критерий	Число изменений в защищаемую инфраструктуру (исходя из статичной базы сигнатур)	Корреляции без категоризации	Применение категоризации событий безопасности
Доля пропущенных цепочек атак (инцидентов) *	Среднее значение	19%	11%
	<10	12%	8%
	⩾10	23%	15%

* *Комментарий.* Важно отметить, что полученные характеристики не следует сравнивать с общепринятыми оценками False Acceptance Rate и False Rejection Rate, используемыми при оценке эффективности систем обнаружения вторжений, систем

биометрической идентификации и т.д. В качестве эталона рассматривались предопределенные сценарии, которые были заложены в скрипты генерации цепочек атак. При этом большое количество пропусков обусловлено особенностями эмулирования жизненного цикла, а именно хаотичного ввода и вывода из эксплуатации защищаемых узлов, изменения сервисов и служб. В случае подхода, основанного на корреляции без применения категоризации, пропуск обусловлен длительной задержкой по автоматизированному сканированию активов и необходимостью ручного конфигурирования правил корреляции. Пропуски детектирования событий безопасности при условии проведенной категоризации согласно вышеперечисленной методике обусловлены объективной невозможностью формирования всеобъемлющего перечня категорий, учитывающих будущие изменения в составе защищаемых активов. На практике при использовании предложенного подхода минимизация доли пропущенных инцидентов достигается за счет регламентации и контроля изменений по защищаемым объектам при условии валидации со стороны администраторов безопасности.

Заключение. Текущий уровень развития инфраструктуры промышленных систем автоматизации и управления обусловливает необходимость учитывать контекст событий для обеспечения эффективности выявления атак в реальных условиях. Основываясь на созданном на предыдущих этапах исследования методическом обеспечении процесса нормализации, предложен подход к построению систем категоризации событий безопасности, научная новизна которого состоит в применении категорий не только для поиска и обработки событий, но и для формирования методических основ разработки контента для выявления инцидентов.

В статье рассмотрены основные принципы построения системы категоризации событий безопасности, сформулированы требования к ней и предложена оригинальная методика ее применения, обеспечивающая возможность избегать необходимость корректировки наборов правил детектирования при добавлении новых источников событий или обновления подсистемы регистрации существующих событий. При этом рассмотренные варианты категоризации применяются только для событий безопасности и не затрагивают события общесистемного программного обеспечения.

Основным положением методики является требование наличия для каждого события одной четко определенной категории. Предусмотрены возможности масштабирования системы категоризации, определены методы адаптации системы категоризации для применения в промышленных системах автоматизации и управления. Также представлены результаты эксперимента по применению методики для повышения эффективности защиты автоматизированных систем на примере стенда, созданного на базе киберполигона. Полученные результаты показали эффективность подобной методики и подтвердили возможность ее применения для защиты промышленных систем.

Благодарности. Исследование выполнено при частичной финансовой поддержке РНФ в рамках научного проекта № 21-71-00125 «Алгоритмическое обеспечение для усиленной проверки подлинности субъектов доступа в критически важных объектах».

Список источников

1. Федорченко А.В. Анализ методов корреляции событий безопасности в siem-системах. Часть 1 / А.В. Федорченко, Д.С. Левшун, А.А. Чечулин, И.В. Котенко // Труды СПИИРАН, 2016. – № 4 (47). – С. 5-27.
2. Reference incident classification taxonomy task force status and way forward. Available at: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/@@download/fullReport (accessed: 05/01/2023).
3. Исхаков А.Ю. Модели нормализации данных в системах управления событиями безопасности РТК / А.Ю. Исхаков, С.Ю. Исхаков // Управление развитием крупномасштабных систем MLSD'2020. Труды тринадцатой международной конференции. Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. М.: ИПУ РАН, 2020. – С. 1390-1399.

4. Rajivan P., Konstantinidis E., Ben-Asher N., Gonzalez C. Categorization of events in security scenarios: the role of context and heuristics. Proceedings of the human factors and ergonomics society annual meeting, 2016, no. 60(1), pp. 274-278, DOI: 10.1177/1541931213601063.
5. Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors, 2021, no. 21, 4759, DOI:10.3390/s21144759.
6. Kin J.-Y., Kwon H.-Y. Threat classification model for security information event management focusing on model efficiency. Computers & Security, 2022, no. 120, 102789, DOI: 10.1016/j.cose.2022.102789.
7. Шишкин В.М. Исследование применения прогнозной модели в процессе управления безопасностью / В.М. Шишкин, К.Е. Колесников // Информационные и математические технологии в науке и управлении, 2018. – № 4 (12). – С. 96-104.
8. Котенко И.В. Модель системы управления информацией и событиями безопасности / И.В. Котенко, И.Б. Паращук // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика, 2020. – № 2. – С. 84-94.
9. Микрюков А.А. Классификация событий в системах обеспечения информационной безопасности на основе нейросетевых технологий / А.А. Микрюков, А.В. Бабаш, В.А. Сизов // Открытое образование, 2019. – № 1. – С. 57-63.
10. Новикова Е.С. Обзор алгоритмов корреляции событий безопасности для обеспечения безопасности облачных вычислительных сред / Е.С. Новикова, Я.А. Бекенева, А.В. Шоров, Е.С. Федотов // Информационно-управляющие системы, 2017. – № 5 (90). – С. 95-104. – DOI: 10.15217/issn1684-8853.2017.5.95.
11. Hossain S.M, Couturier R., Rusk J., Kent K.B. Automatic event categorizer for SIEM. Proceedings of the 31st annual international conference on computer science and software engineering (CASCON '21). IBM Corp., USA, 2021, pp. 104-112.
12. Miloslavskaya N., Furnell S. Network Security Intelligence centres for information security incident management. Brain-Inspired cognitive architectures for artificial intelligence: BICA*AI 2020. BICA 2020. Advances in Intelligent Systems and Computing, vol. 1310, 2020, pp. 270-282, DOI: 10.1007/978-3-030-65596-9_34.
13. Cinque M., Cotroneo D., Pecchia A. Challenges and Directions in Security Information and Event Management (SIEM). 2018 IEEE International symposium on software reliability engineering workshops (ISSREW), Memphis, TN, USA, 2018, pp. 95-99, DOI: 10.1109/ISSREW.2018.00-24.
14. Iskhakov A.Y., Mamchenko M.V., Khripunov S.P. Enhanced user authentication algorithm based on behavioral analytics in Web-based cyberphysical systems. 2023 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation, 2023, pp. 253-258, DOI: 10.1109/SmartIndustryCon 57312.2023.10110791.
15. Çakmakçı S.D., Hutschenreuter H., Maeder C., Kemmerich T. A framework for intelligent DDoS attack detection and response using SIEM and ontology. 2021 IEEE International conference on communications workshops (ICC Workshops), Montreal, QC, Canada, 2021, pp. 1-6, DOI: 10.1109/ICCWorkshops50388.2021. 9473869.
16. Manjeet M., Sharma M. A Basis on prestige gotten better SIEM for nefarious link tracking in IoT. 2022 11th International conference on system modeling & advancement in research trends (SMART), Moradabad, India, 2022, pp. 352-355, DOI: 10.1109/SMART55829.2022.10046875.
17. Singh V.K., Callupe S.P., Govindarasu M. Testbed-based evaluation of SIEM tool for cyber kill chain model in power grid SCADA system. 2019 North American Power Symposium (NAPS), Wichita, KS, USA, 2019, pp. 1-6, DOI: 10.1109/NAPS46351.2019.9000344.
18. Ходашинский И.А. Технология усиленной аутентификации пользователей информационных процессов / И.А. Ходашинский, М.В. Савчук, И.В. Гобунов, Р.В. Мещеряков // Доклады ТУСУРа, 2011. – № 2(24). – С. 236-248.

Исхаков Андрей Юнусович. *Кандидат технических наук, старший научный сотрудник ИПУ РАН. Область научных интересов: информационная безопасность, идентификация и аутентификация субъектов доступа, анализ данных, интернет вещей, системы поддержки и принятия решений. AuthorID: 925433, SPIN: 3390-0291, ORCID: 0000-0002-6603-265X, iskhakovandrey@gmail.com, 117997, Россия, Москва, Профсоюзная улица, 65.*

Исхаков Сергей Юнусович. *Кандидат технических наук, начальник отдела анализа и автоматизации реагирования на компьютерные инциденты ПАО Промсвязьбанк. Основные научные интересы: информационная безопасность, проактивный поиск угроз, расследование инцидентов информационной безопасности. AuthorID: 852777, SPIN: 8178-1455, ORCID: 0000-0003-3346-9262, iskhakov.sy@gmail.com, 117997, Россия, Москва, Профсоюзная улица, 65.*

UDC 004.056.5
DOI:10.25729/ESI.2023.30.2.015

Improving the efficiency of information protection systems by categorizing security events

Andrey Y. Iskhakov[1], Sergey Y. Iskhakov[2]

[1]V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Russia, Moscow, *iay@ipu.ru*

[2]Public Joint-Stock Company Promsvyazbank, Russia, Moscow

Abstract. The article considers the basic principles of categorization of security events, formulates the requirements to it and offers a methodology for its application. Examples of event categorization options for various information protection tools are given. Possibilities of scaling the categorization system and methods of its adaptation for use in industrial automation and control systems are determined. The results of an experiment on the application of the methodology to improve the protection of automated systems on the example of a virtual cyber polygon are also presented, confirming the effectiveness of this methodology and the possibility of its application to the protection of industrial systems.

Keywords: correlation, data categorization, normalization, taxonomy, security information and event management, attack scenarios, incident

Acknowledgements: This research was funded by Russian Science Foundation, project 21-71-00125.

References

1. Fedorchenko A., Levshun D., Chechulin A., Kotenko I. Analiz metodov korrelyatsii sobytiy bezopasnosti v siem-sistemakh. Chast' 1 [An analysis of security event correlation techniques in siem-systems. Part 1]. Trudy SPIIRAN [SPIIRAS Proceedings], 2016, col. 4 (47), pp. 5-27.
2. Reference incident classification taxonomy task force status and way forward. Available at: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/@@download/fullReport (accessed: 05/01/2023).
3. Iskhakov A.Y., Iskhakov S.Y. Modeli normalizatsii dannykh v sistemakh upravleniya sobytiyami bezopasnosti RTK [Data normalization models in security event management systems of Robotics Complexes] Upravlenie razvitiem krupnomasshtabnyh sistem MLSD'2020. Trudy trinadcatoj mezhdunarodnoj konferencii. Pod obshchej redakciej S.N. Vasil'eva, A.D. Cvirkuna [Management of large-scale systems development MLSD'2020. Proceedings of the Thirteenth International Conference. Edited by S.N. Vasiliev, A.D. Tsvirkun], 2020, pp. 1390-1399.
4. Rajivan P., Konstantinidis E., Ben-Asher N., Gonzalez C. Categorization of events in security scenarios: the role of context and heuristics. Proceedings of the human factors and ergonomics society annual meeting, 2016, no. 60(1), pp. 274-278, DOI: 10.1177/1541931213601063.
5. Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors, 2021, no. 21, 4759, DOI:10.3390/s21144759.
6. Kin J.-Y., Kwon H.-Y. Threat classification model for security information event management focusing on model efficiency. Computers & Security, 2022, no. 120, 102789, DOI: 10.1016/j.cose.2022.102789.
7. Shishkin V.M., Kolesnikov K.E. Issledovaniye primeneniya prognoznoy modeli v protsesse upravleniya bezopasnost'yu [Investigation of the forecasting model of application in the process of security management] Informatsionnyye i matematicheskiye tekhnologii v nauke i upravlenii [Information and mathematical technologies in science and management], 2018, vol. 4 (12), pp. 96-104.
8. Kotenko I.V., Parashchuk I.B. Model' sistemy upravleniya informatsiyey i sobytiyami bezopasnosti [Model of security information and event management system]. Vestnik AGTU. Seriya: Upravleniye, vychislitel'naya tekhnika i informatika [Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics], 2020, vol. 2, pp. 84-94.
9. Mikryukov A.A., Babash A.V., Sizov V.A. Klassifikatsiya sobytiy v sistemakh obespecheniya informatsionnoy bezopasnosti na osnove neyrosetevykh tekhnologiy [Classifcation of events in information security systems based on neural networks]. Otkrytoye obrazovaniye [Open education], 2019, vol. 1, pp. 57-63.
10. Novikova E. S., Bekeneva Y. A., Shorov A. V., Fedotov E. S. Obzor algoritmov korrelyatsii sobytiy bezopasnosti dlya obespecheniya bezopasnosti oblachnykh vychislitel'nykh sred [A survey of security event correlation techniques for cloud computing environment security]. Informatsionno-upravlyayushchiye sistemy [Information and control systems]. 2017, vol. 5 (90), pp. 95-104, DOI: 10.15217/issn1684-8853.2017.5.95.

11. Hossain S.M., Couturier R., Rusk J., Kent K.B. Automatic event categorizer for SIEM. Proceedings of the 31st annual international conference on computer science and software engineering (CASCON '21). IBM Corp., USA, 2021, pp. 104-112.
12. Miloslavskaya N., Furnell S. Network Security Intelligence centres for information security incident management. Brain-Inspired cognitive architectures for artificial intelligence: BICA*AI 2020. BICA 2020. Advances in Intelligent Systems and Computing, vol 1310, 2020, pp. 270-282, DOI: 10.1007/978-3-030-65596-9_34.
13. Cinque M., Cotroneo D., Pecchia A. Challenges and Directions in Security Information and Event Management (SIEM). 2018 IEEE International symposium on software reliability engineering workshops (ISSREW), Memphis, TN, USA, 2018, pp. 95-99, DOI: 10.1109/ISSREW.2018.00-24.
14. Iskhakov A.Y., Mamchenko M.V., Khripunov S.P. Enhanced user authentication algorithm based on behavioral analytics in Web-based cyberphysical systems. 2023 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation, 2023, pp. 253-258, DOI: 10.1109/SmartIndustryCon 57312.2023.10110791.
15. Çakmakçı S.D., Hutschenreuter H., Maeder C., Kemmerich T. A framework for intelligent DDoS attack detection and response using SIEM and ontology. 2021 IEEE International conference on communications workshops (ICC Workshops), Montreal, QC, Canada, 2021, pp. 1-6, DOI: 10.1109/ICCWorkshops50388.2021. 9473869.
16. Manjeet M., Sharma M. A Basis on prestige gotten better SIEM for nefarious link tracking in IoT. 2022 11th International conference on system modeling & advancement in research trends (SMART), Moradabad, India, 2022, pp. 352-355, DOI: 10.1109/SMART55829.2022.10046875.
17. Singh V.K., Callupe S.P., Govindarasu M. Testbed-based evaluation of SIEM tool for cyber kill chain model in power grid SCADA system. 2019 North American Power Symposium (NAPS), Wichita, KS, USA, 2019, pp. 1-6, DOI: 10.1109/NAPS46351.2019.9000344.
18. Hodashinskiy I. A., Savchuk M. V., Gorbunov I. V., Mescheryakov R.V. Meshcheryakov R.V. Tekhnologiya usilennoy autentifikatsii pol'zovateley informatsionnykh protsessov [Strong authentication technology of the users of information processes]. Doklady TUSURa [Proceedings of TUSUR University], 2011, vol. 2(24), pp. 236-248.

Andrey Y. Iskhakov. *Candidate of Sciences (Engineering), Senior Researcher at the ICS RAS. Research interests: information security, identification and authentication of access subjects, data analysis, Internet of things, decision support and decision-making systems. AuthorID: 925433, SPIN: 3390-0291, ORCID: 0000-0002-6603-265X, iskhakovandrey@gmail.com, 65 Profsoyuznaya str., Moscow, Russia.*

Sergey Y. Iskhakov. *Candidate of Sciences (Engineering), Head of the Department for Analysis and Automation of Computer Incident Response at Promsvyazbank. Main scientific interests: information security, proactive threat detection, investigation of information security incidents. AuthorID: 852777, SPIN: 8178-1455, ORCID: 0000-0003-3346-9262, iskhakov.sy@gmail.com, 65 Profsoyuznaya str., Moscow, Russia.*

Статья поступила в редакцию 01.05.2023; одобрена после рецензирования 10.05.2023; принята к публикации 10.05.2023.
The article was submitted 05/01/2023; approved after reviewing 05/10/2023; accepted for publication 05/10/2023.