СОБЫТИЙНО-ОРИЕНТИРОВАННАЯ ПОЛИТИКА БЕЗОПАСНОСТИ И ФОРМАЛЬНАЯ МОДЕЛЬ МЕХАНИЗМА ЗАЩИТЫ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

С.Д. Ерохин[1], **А.Н. Петухов**[1*], **П.Л. Пилюгин**[1]

[1]Московский технический университет связи и информатики,
Москва, 111024, Российская Федерация
[*]Адрес для переписки: anpetukhov@yandex.ru

Информация о статье
УДК 004.056.5
Статья поступила в редакцию 22.11.2019

Ссылка для цитирования: Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Событийно-ориентированная политика безопасности и формальная модель механизма защиты критических информационных инфраструктур // Труды учебных заведений связи. 2019. Т. 5. № 4. С. 99–105. DOI:10.31854/1813-324X-2019-5-4-99-105

Аннотация: *в статье рассматриваются возможности управления безопасностью критических информационных инфраструктур. Предлагаются подходы к построению политики неориентированных на фиксированный список угроз. Обосновывается возможность построения курса безопасности на основе мониторинга событий безопасности. Предлагается формальное описание событий безопасности и механизмов защиты на основе их мониторинга. Рассматриваются особенности такого подхода для защиты критических информационных инфраструктур в целях повышения качества защиты.*

Ключевые слова: *информационная безопасность, политика безопасности, события безопасности, мониторинг событий безопасности, субъектно-объектная формальная модель механизма защиты, характеристика сетевых событий, критические информационные инфраструктуры.*

Методологические основы моделирования политик и механизмов защиты

Для исследования механизмов, систем защиты и решения задач информационной безопасности использовались различные модели, позволяющие формально определить нарушение защиты. Однако методологической основой практически всех таких моделей является модель системы защиты с полным перекрытием [1]. В основе этой модели лежит задача минимизации или (что практически невозможно) исключения всех негативных воздействий (угроз), направленных на защищаемые объекты (ресурсы, информацию и т. д.).

Развитие этой модели предусматривает введение вероятности появления таких угроз, степени противодействия механизмов защиты и стоимости ущерба для объектов в случае успешной реализации угрозы [1]. Это позволяет оценить вероятности инцидента и уровень, как возможного ущерба, так и остаточного допустимого риска (в случае учета затрат на реализацию механизмов защиты, и предположения, что эти затраты не должны превышать возможный ущерб).

По сути известны классы моделей защиты: дискреционные, мандатные и их разновидности: ролевые, тематические. Они описывают механизмы ограничения / предотвращения негативных воздействий. Основой всех этих моделей (рисунок 1) является возможность различения легитимных действий (valid access) и несанкционированных (illegal access) со стороны пользователей (user domain) или «противника» (threat domain) в отношении защищаемых объектов (protected domain).

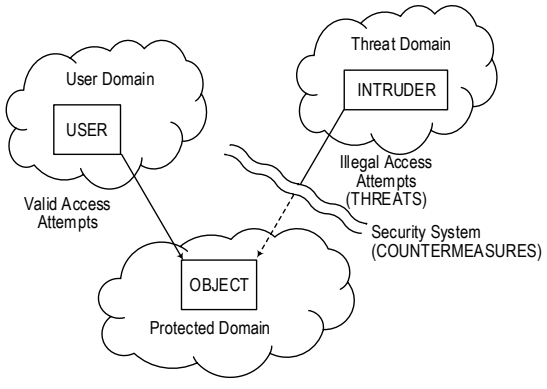

Рис. 1. Модель Клементса – Хоффмана [2]

Все различия этих описаний сводятся к уточнению / обобщению свойств элементов этих моделей, определяемых как субъекты и объекты, их взаимосвязи (управляющие воздействия – доступы или потоки информации) и к используемому для их описания математическому аппарату: матрицам, графам, множествам, формальным языкам, алгебраическим решеткам и т. д. При этом все модели таких систем защиты, имеющие практическую направленность, являются, как правило, гибридными. Например, модель Адепт-50, Белла-Лападуллы или MMS – MilitaryMessageSystem [3].

Общие принципы формального описания политик и механизмов защиты

В целях формального обобщения практически всех известных моделей используется субъектно-объек-тная модель систем защиты, рассматривающая взаимодействие активных (субъектов) и пассивных (объектов) сущностей. Все процессы безопасности в компьютерных системах описываются разрешением и запрещением доступа субъектов к объектам (дискреционные модели) либо управлением информационными потоками, которые эти доступы инициируют (мандатные модели). Например, доступы по записи и чтению инициируют различные по направлению информационные потоки:

$$\text{Stream}\ (S_i, O_j) \rightarrow O_k,$$

$$\text{Stream}\ (S_i, O_j) \leftarrow O_k,$$

где $\{S_i\}$ – множество субъектов доступа, а $\{O_j\}$ – множество объектов доступа.

Решение задачи защиты информационной безопасности в модели составляет контроль при помощи специального монитора безопасности и анализ возникающих потоков. И если мы можем различать легитимные / разрешенные и нелегитимные / запрещенные потоки информации, то задача монитора состоит в том, чтобы управлять (разрешать или запрещать / реагировать) ими. А соответствующие правила, которые определяют управление доступом субъектов к объектам. Такие правила контроля информационных потоков – это формализованная политика безопасности, которая может использовать любую (дискреционную, мандатную, ролевую и т.д.) модель обеспечения безопасности. По сути субъектно-объектная модель – это конкретизации модели Клементса – Хоффмана, позволяющая формализовать все элементы модели и взаимодействия между ними. В основе этой модели также лежит контроль и исключение возможных негативных воздействий (запрещенных доступов \ потоков информации).

Однако для модели Клементса – Хоффмана и, следовательно, для всего формализованного на ее основе класса моделей характерны следующие свойства.

Во-первых, это статичность (адекватность) таких моделей. Действительно, кроме известных недостатков дискреционных и мандатных моделей, допускающих фактическое нарушение безопасности при формальном ее сохранении [4], состав элементов модели может со временем существенно отличаться от реальных защищаемых систем. Это требует постоянного отслеживания адекватности модели и ее развития. Например, изменения состава субъектов, объектов и их возможных взаимодействий или более глубокой модернизации.

Во-вторых, это полнота / ограниченность модели, так как их реальной целью является «полное перекрытие» только всех идентифицированных угроз, а не «всех возможных». Действительно, все формальные модели изначально ограниченны [5] и, следовательно, не обеспечивают полноту описания всех возможных угроз.

В-третьих, подход, предполагающий «минимизацию» негативных воздействий, допускает возможность исчисления качественной или количественной оценки ущерба или допустимого риска таких воздействий на защищаемые объекты, что может быть не всегда приемлемо [6].

Представляется, что именно эти свойства существенны для управления безопасностью критической информационной инфраструктуры (КИИ) [6].

Действительно, когда речь идет «о защите критически важных объектов (КВО), основной задачей системы информационной безопасности является обеспечение» их «нормального функционирования без существенных нарушений, последствия которых и определяют категорию значимости информационной системы, используемой в этих процессах, а категория значимости – состав мер защиты» [7].

Событийно-ориентированная политика безопасности КИИ

Однако если рассматривать динамически адаптируемую в смысле угроз, условий и т. д. модель и не ориентироваться на оценку остаточного риска или не рассматривать, как цель, «полное перекрытие», то следует опираться на подход к моделированию отличный от описанного выше.

Такая альтернативная модель может исходить из понятия события безопасности – «возникновения состояния системы, сервиса или сети, ***указывающего на возможное нарушение*** политики информационной безопасности, или сбой средств контроля, или ранее ***неизвестную ситуацию***, которая может быть ***значимой для безопасности***» [8]. Основываясь на событиях безопасности, можно управлять доступом субъектов к объектам и информационными потоками, не разделяя их на легитимные / разрешенные и нелегитимные / запрещенные. Основой принятия решения должно быть наступление

события безопасности или совокупности событий безопасности в более сложном случае.

Чтобы уточнить понятия события безопасности для различных конкретных реализаций, необходимо предложить информационную базу, которая формирует описание системы [9]. В общем случае событием является изменение состояния системы. Однако справедливо замечание, что для обеспечения безопасности может быть значимым отсутствие изменения состояния, например, отсутствие обязательной смены криптографических ключей, однако в этом случае должен существовать процесс отслеживания регламента и состояние этого процесса (индикатора выполнения регламента) при подобном нарушении должно меняться.

Тогда для определения политики требует уточнение самого понятия события безопасности, которое выше определялось через нарушение политики безопасности. В этом случае корректнее связать событие безопасности с нарушениями основных требований ИБ (конфиденциальность, целостность и доступность) или нарушениями «критических» процессов (информационных, технологических, управленческих и т. п.), которое может привести к нарушениям нормального функционирования КВО [7, 10].

Традиционно обработку событий безопасности (сбор, анализ, реагирование) осуществляли системы обнаружения вторжений – СОВ. В последнее время в целях расширения функциональности СОВ для анализа событий используются SIEM-системы (*от англ.*, Security Information and Event Management). В системах обнаружения вторжений обработка событий предполагает, как правило, два основных подхода: сигнатурный подход и обнаружение аномалий.

Для сигнатурного подхода должны быть сформулированы правила принятия решений, основанные на совпадении / корреляции с шаблонами (сигнатурами различных атак) для параметров системы, описанных в номинальных шкалах или нахождении в допустимых интервалах для количественных параметров.

Для обнаружения аномалий также определяются шаблоны «нормального поведения» системы. Однако совпадение / корреляция с таким шаблоном не дает информации об отсутствии атаки, важнее определить существенное отличие от этого шаблона, что свидетельствует о возможной атаке.

Для метода обнаружения аномалий можно сделать одно важно замечание. В случае, когда критическая информационная инфраструктура является одновременно защищаемым критическим объектом, т.е. можно условно считать, что КВО и КИИ совпадают, тогда механизм обнаружения аномалий становится одновременно средством индикации инцидента.

В общем случае можно выделить три основные группы подходов к определению взаимосвязи /корреляции событий и инцидентов безопасности, исходя из особенностей их реализации и решаемых задач [11]:

– использование сходства с ранее известными значимыми событиями безопасности;

– использование устойчивых причинно-следственных связей, исходя из знания тактик и методов, используемых во время атак;

– выявление статистических закономерностей (корреляционных связей).

Последние два подхода можно рассматривать как способы построения шаблонов, сходство с которыми выявляется.

Центром обработки событий безопасности является монитор безопасности, а в качестве источников информации могут выступать различные системы регистрации или специальные сенсоры контроля состояния системы. Например, для учета событий безопасности в [12] предложена структура, приведенная ниже на рисунке 2.

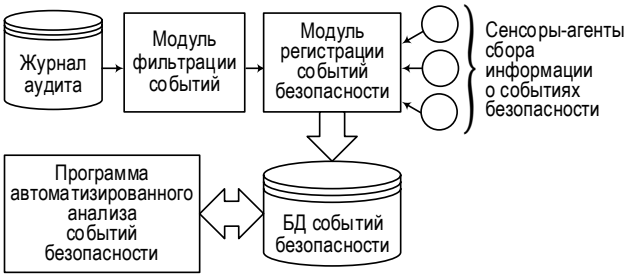

Рис. 2. Структура формирования событий безопасности [12]

Так как основой принятия решения должно быть наступление события безопасности или цепочки событий безопасности, то это соответствует понятиям простой и сложной обработки событий [13].

Простая обработка событий никаких ложных действий не предполагает, в этом случае само событие рассматривается как значимый факт [13]. Когда такое событие происходит, оно, как правило, связано с запуском определенных возможно негативных вычислительных процессов. Такое событие может быть «простым» по форме, но может иметь заметное значение и предоставлять информацию о возникающей или осуществляемой атаке. Такая обработка событий может включать некоторые действия, которые, однако, должны рассматривать каждое событие – факт независимо. Для уточнения и более удобного представления события могут преобразовываться (переформатироваться, разбиваться на части или наоборот – объединяться). Кроме того, они могут дополняться нужными данными, расширяющими их информативность и даже порождать новые события на основе этой информации.

Сложная обработка событий предполагает соответствующий анализ отдельных событий или наборов / последовательностей событий. В этом случае она может приводить к созданию новых сложных событий. Сложная обработка событий

направлена на построение шаблонов (корреляционный анализ или выявление причинно-следственных связей) атак или профилей для определения аномалий (статистические методы) [13]. Сложность такой обработки определяется не только количеством таких событий и их структурой, они могут происходить в течение определенного периода времени, они могут быть взаимосвязаны по многим аспектам и иметь достаточно сложное временное и пространственное соотношение.

Задача любой обработки событий безопасности является определить тенденции функционирования системы и идентифицировать угрозы. Однако для формирования такого эффективного набора событий безопасности необходимо выявление их связи с нарушениями функциональности КВО. Для большинства механизмов защиты (межсетевые экраны, системы обнаружения вторжений) такая связь заранее явно или неявно подразумевается, однако адаптивные механизмы защиты в составе систем обработки событий безопасности (SIEM системы) должны устанавливать зависимость с нарушениями функциональности КВО, которые могут не наблюдаться мониторами безопасности системы защиты КИИ. Возможное исключение составляют случаи (как это отмечалось выше), когда КВО и КИИ могут условно совпадать. Например, когда в качестве КВО рассматриваются: ЦОД, телекоммуникационная или вычислительная сеть и т. п. В этом случае монитор безопасности будет способен индицировать нарушения функциональности системы как существенные отклонения от принятого режима работы – «существенные аномалии» – возникновения «нештатных ситуаций».

Формальное описание событий безопасности

События безопасности с позиций субъектно-объектной модели – это информационная база для принятия решения реагирования монитором безопасности, которая в терминах модели определена как ассоциированные с монитором информационные объекты. При таком подходе упомянутые выше формальные политики безопасности (дискреционная, мандатная и др.) могут рассматриваться как частные случаи форм записи правил / шаблонов для событий безопасности, не ограничивая тем самым общность описываемого подхода. Это позволяет рассматривать все существующие механизмы безопасности для управления доступом к информации как событийно ориентированные.

Для формального описания событий безопасности могут быть использованы различные формальные модели и использовать различный математический аппарат [14, 15].

Наиболее общие описания основаны на теоретико-множественном и языковом подходах, что позволяет при необходимости привлекать аппарат теории графов или теории конечных автоматов. Можно предполагать, что множество таких событий информационной безопасности (ISE, *от англ.*, Information Security Events) является конечным набором таких событий $ISE = \{ise_1, ..., ise_i\}$ в каждый конкретный момент времени. Каждое такое событие однозначно описывается последовательностью признаков [15]: $ise_i = (w_1, ..., w_{i\text{-}ise})$, где *i*-ise длина *i*-ого вектора параметров.

Состав параметров может быть уточнен в зависимости от различных технологических особенностей системы [16].

Данный подход к формальному описанию событий безопасности в целом соответствует формальной модели на основе языкового подхода для описания состояний системы безопасности [17]. Если исходить из того, что любая информация представлена в виде слова в некотором языке, то состояние любого устройства в вычислительной системе, процесс их изменения может быть достаточно полно описан словом в некотором языке. Следовательно, можно представлять события безопасности как подмножество языка описывающего состояния системы.

Следует отметить, что подобное формальное описание событий безопасности исходит из конечности алфавита и слов языка, следовательно, это приводит к выводу о конечности множества событий безопасности *ISE*. Однако это не является недостатком, так как речь идет об описании множества *ISE* в конкретный момент времени и с течением времени, как состав этого множества, так и набор параметров ise_i может изменяться.

К составу сетевых параметров – источников событий безопасности могут быть, например, отнесены различные сетевые протоколы и их характеристики, например, IP, ISNP, UDP, TCP, SMTP, SQL, WMI, HTTP (GET/POST), SDEE, SMB, SNMP, Syslog [18].

Вместе с тем сбор фактической информации об атаках в компьютерных вычислительных сетях позволил создать ряд стандартных наборов данных для обучения и тестирования систем обнаружения вторжений [19]. Хотя каждый из этих наборов предназначен для обучения адаптивных IDS\IPS или для их тестирования, однако в рамках работы протоколов TCP, UDP и ICMP можно выделить следующие наиболее востребованные наборы данных: KDD99, NSL-KDD DataSet [20, 21].

Эти наборы представляют различные типы уязвимостей и технологии их эксплуатации. В частности, для обозначения атак используются 4 класса: DOS, Probe, U2R, R2L [20].

В контексте рассматриваемой проблемы важно, что в наборах NSL-KDD DataSet предложена и практически реализованная структура описания событий безопасности, включающая 41 параметр. Однако, несмотря на практическую значимость и от-

носительную полноту, данное описание ограничено и не является расширяемым, поэтому при рассматриваемом подходе может быть рекомендовано только как начальное значение для набора вектора параметров событий безопасности (или алфавита упомянутой выше языковой модели). Состав параметров, их абсолютные или относительные количественные оценки простых и сложных событий в ряде случаев требует сложной обработки сетевых событий. Например, для определения параметров: 8 (количество неправильных фрагментов), 8 (количество неудачных попыток входа в систему) или 25 (процент соединений TCP с ошибками SYN).

Такой алфавит описания событий безопасности может быть дополнен параметрами элементарных событий, которые, как правило, используются в различных механизмах защиты. Например, таблицы шаблонов в межсетевых экранах или правила в коммутаторах при создании VLAN и т. п.

Заключение

В работе предлагается альтернативный метод построения политики безопасности. Данный подход не отрицает возможности использования на начальном этапе традиционных методов, ориентированных на противодействие наборам возможных внешних воздействий – угроз. Однако стремление к повышению защищенности в процессе функционирования системы приводит к требованию ее адаптивности к вновь возникающим и пока неизвестным угрозам.

Такое требование особенно важно для критических информационных инфраструктур, где инцидент, строго говоря, недопустим и, поэтому, его возникновение не может рассматриваться в качестве фактора расширения набора угроз. В представленном подходе предлагается отслеживать возникающие события безопасности и их связь с параметрами функционирования КИИ, при этом первоначальный состав событий безопасности должен расширяться в зависимости от состояния наблюдаемых критических процессов.

Таким образом, главной особенностью ориентации политики безопасности на события является возможность строить системы защиты КИИ, основываясь не только на известном наборе внешних угроз, но на сохранении функциональности КВО.

В случае, когда таким критическим объектом является сама КИИ, такая адаптивная система защиты, используя IDS и SIEM системы, может автоматически контролировать не только события безопасности, но и функциональность КИИ-КВО.

Для использования предлагаемого событийно-ориентированного подхода к описанию политик безопасности предлагается в качестве формальной модели механизмов защиты рассматривать предлагаемые в субъектно-объектной модели механизмы мониторинга. Это позволяет учитывать все существующие механизмы безопасности как событийно ориентированные. То есть предлагается рассматривать как основу системы защиты набор различных механизмов мониторинга и обеспечивающих их функций.

В этом случае можно построить отображение множества механизмов защиты (защитных активностей) на множество событий безопасности и при управлении информационной безопасностью выбирать стратегию на улучшение качества защиты, как увеличении множества контролируемых событий, обеспечивающих лучшее сохранение функциональности КВО.

Кроме того, данный подход позволяет ввести ряд дополнительных параметров / ограничений для управления информационной безопасностью.

Во-первых, показатель сложности реализации (затраты) процедур выявления событий безопасности, по составу и распределению в сети соответствующих событиям механизмов защиты.

Во-вторых, возможны оценки эффективности защиты в смысле уровня ошибочных реагирований априорно (по составу событий ИБ и их корреляционной связи с инцидентами) и апостериорно с учетом частоты появления этих событий, что также позволит уточнять их корреляцию.

Вместе с тем, использование описанного подхода требует более строгого формального описания событий безопасности: уточнения алфавита, который должен учитывать не только особенности различных политик безопасности, но и быть специфицирован для соответствующего уровня модели ISO\OSI и технологических особенностей защищаемой системы. Кроме того, должны быть формализованы правила обработки событий: морфология образования слов языка для описания событий безопасности и грамматика для построения подмножества слов языка связанных с событиями безопасности (сложных событий).

Список используемых источников

1. Хофман Л.Д. Современные методы защиты информации. Пер. с англ. М.: Советское радио, 1980. 264 с.
2. Clements D., Hoffman L.J. Computer Assisted Security System Design. Berkeley: University of California, 1974.
3. Зегжда Д.П. Информационная безопасность. М.: МГТУ им. Н.Э. Баумана, 2010. 236 с.
4. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2011. 320 с.
5. Успенский В.А. Теорема Гёделя о неполноте. М.: Наука, 1982. 112 с.

6. Erokhin S., Petukhov A., Pilyugin P. Critical Information Infrastructures Security Modeling // Proceeding of the 24th Conference of Open Innovations Association FRUCT (Moscow, Russia, 8–12 апреля 2019). С. 83–88. URL: https://fruct.org/publications/fruct24/files/Ero.pdf (дата обращения 22.12.2019)
7. Кузнецов Д. Моделирование угроз на основе сценариев или Как CyberKillChain и ATT&CK помогают анализировать угрозы ИБ // Безопасность пользователей в интернете. URL: https://safe-urf.ru/specialists/article/5247/626649 (дата обращения 22.12.2019)
8. ГОСТ Р ИСО/МЭК 18028-1-2008 (10/2009). Информационная технология (ИТ). Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности.
9. Гуснин С.Ю., Петухов А.Н. Информационная база управления кибербезопасностью // Проблемы современной науки и образования. 2016. № 40. С. 22–26.
10. Петухов А.Н., Пилюгин П.Л. Нормативное определение событий безопасности // Доклады Всероссийской конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий. РЭУС-2019» (Москва, Россия, 29–31 мая 2019). Сер. «Научные конференции, посвященные дню Радио». М.: Московское НТО радиотехники, электроники и связи им. А.С. Попова, 2019. С. 313–317.
11. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 // Труды СПИИРАН. 2016. № 6(49). С. 208–225. DOI:10.15622/sp.49.11
12. Макаревич О.Б., Шелудько И.А. Регистрация и анализ событий безопасности в информационных системах // Известия ТРТУ. 2003. № 4(33). С. 211–216.
13. Edwards M., Etzion O., Ibrahim M., Iyer S., Lalanne H., et al. A Conceptual Model for Event Processing Systems // developer Works. 43 p. URL: https://www.ibm.com/developerworks/webservices/library/ws-eventprocessing/ws-eventprocessing-pdf.pdf (Access 18th April 2019)
14. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН. 2016. № 4(47). С. 5–27. DOI:10.15622/sp.47.1
15. Гайнов А.Е., Заводцев И.В. Модель процесса обработки событий информационной безопасности // Современная наука: Актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2017. № 3-4. С. 44–49.
16. Проноза А.А., Чечулин А.А., Котенко И.В. Математические модели визуализации в SIEM-системах // Труды СПИИРАН. 2016. № 3(46). С. 90–107. DOI:10.15622/sp.46.8
17. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. М.: Академия. 2009.
18. Графов С.А., Белявцев А.Ю., Воронов Д.А., Трофимов А.А. Грани SIEM // Защита информации. Инсайд. 2017. № 1(73). С. 56–62.
19. Бурлаков М.Е. Применение метода анализа соответствий для оптимизации комбинаций атрибутов у наборов данных // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2018. № 26. С. 7–28.
20. Datasets // University of New Brunswick. URL: http://www.unb.ca/cic/research/datasets/ids.html (Accessed 07th August 2017)
21. Al-Hamami A.H., Al-Saadoon G.M.W. Handbook of Research on Threat Detection and Countermeasures in Network Security. Derry: IGI Global, 2014. 450 p. DOI:10.4018/978-1-4666-6583-5

* * *

EVENT-BASED SECURITY POLICY AND FORMAL MODEL OF CRITICAL INFORMATION INFRASTRUCTURES PROTECTING MECHANISM

S. Erokhin[1], **A. Petukhov**[1], **P. Pilyugin**[1]

[1]Moscow Technical University of Communications and Informatics,
Moscow, 111024, Russia

Article info
The article was received 22th November 2019

For citation: Erokhin S., Petukhov A., Pilyugin P. Event-based Security Policy and Formal Model of Critical Information Infrastructures Protecting Mechanism. *Proceedings of Telecommunication Universities.* 2019;5(4):99–105. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-4-99-105

Abstract: *The article considers the possibilities of security management of critical information infrastructures. Approaches to the construction of policies not focused on a fixed list of threats are proposed. It substantiates the possibility of building a security policy based on security events monitoring. A formal description of security events and formal model of protection mechanisms based on monitoring security events is proposed. The features of this approach for the protection of critical information infrastructures in order to improve the quality of protection are considered.*

Keywords: *information security, security policy, security events, monitoring of security events, subject-object formal model of the protection mechanism, characteristics of network events, critical information infrastructures.*

References

1. Hoffman L.J. *Modern Methods for Computer Security and Privacy*. New York: Prentice Hall; 1977. 268 p.
2. Clements D., Hoffman L.J. *Computer Assisted Security System Design*. Berkeley: University of California; 1974.
3. Zegzhda D.P. I*nformatsionnaia bezopasnost* [Information Security]. Moscow: Bauman Moscow State Technical University Publ.; 2010. 236 p. (in Russ.)
4. *Devianin P.N. Modeli bezopasnosti kompiuternykh sistem. Upravlenie dostupom i informatsionnymi potokami. Uchebnoe posobie dlia vuzov* [Security Models of Computer Systems. Access and Information Management]. Moscow: Goriachaia liniia – Telekom; 2011. 320 p. (in Russ.)
5. Uspenskii V.A. *Teorema Gedelia o nepolnote* [Gödel's Incompleteness Theorem]. Moscow: Nauka; 1982. 112 p. (in Russ.)
6. Erokhin S., Petukhov A., Pilyugin P. Critical Information Infrastructures Security Modeling. *Proceeding of the 24th Conference of Open Innovations Association FRUCT (Moscow, Russia, 8–12 April 2019)*. p.83–88. Available from: https://fruct.org/publications/fruct24/files/Ero.pdf [Access 22nd December 2019]
7. Kuznetsov D. Modelirovanie ugroz na osnove stsenariev ili Kak CyberKillChain i ATT CK pomogaiut analiziro-vat ugrozy [Scenario-based threat modeling or How CyberKillChain and ATT & CK help analyze IS threats]. *Bezopasnost polzovatelei v internete*. (in Russ.) Available from: https://safe-urf.ru/specialists/article/5247/626649 [Access 22nd December 2019]
8. GOST R ISO/MEK 18028-1-2008. Informatsionnaia tekhnologiia (IT). Metody i sredstva obespecheniia bezopasnosti. Setevaia bezopasnost informatsionnykh tekhnologii. Chast 1. Menedzhment setevoi bezopasnosti [National Standard of the Russian Federation. Information Technology (IT). Methods and Means of Ensuring Safety. Network Security Information Technology. Part 1. Network Security Management. October 2009. (in Russ.)
9. Gusnin S., Petukhov A. Management information base of cybersecurity. *Problems of Modern Science and ducation*. 2016;40:22–26. (in Russ.)
10. Petukhov A.N., Pilyugin P.L. Statutory Definition Of Security Events. *Doklady Vserossiiskoi konferentsii "Radioelektronnye ustroistva i sistemy dlia infokommunikatsionnykh tekhnologii", REUS-2019, 29–31 May 2019, Moscow, Russia. Ser. Nauchnye konferentsii posviashchennye dniu Radio* [Reports of the All-Russian Conference "Radioelectronic Devices and Systems for Infocommunication Technologies", REUS-2019, 29–31 May 2019, Moscow, Russia. Series "Scientific conferences Dedicated to Radio Day"]. Moscow: Moscow Scientific and Technical Society Radio Engineering, Electronics and Communications Publ.; 2019. p.313–317. (in Russ.)
11. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. An Analysis of Security Event Correlation Techniques in Siem-Systems. Part 2. *SPIIRAS Proceedings*. 2016;6(49):208-225. (in Russ.) Available from: https://doi.org/10.15622/sp.49.11
12. Makarevich O.B., Sheludko I.A. Registratsiia i analiz sobytii bezopasnosti v informatsionnykh sistemakh [Registration and Analysis of Security Events in Information Systems]. *Izvestiya TRTU*. 2003;4(33):211–216. (in Russ.)
13. Edwards M., Etzion O., Ibrahim M., Iyer S., Lalanne H., et al. A Conceptual Model for Event Processing Systems. *developer Works*. 43 p. Available from: https://www.ibm.com/developerworks/webservices/library/ws-eventprocessing/ws-eventprocessing-pdf.pdf [Access 18th April 2019]
14. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. An Analysis of Security Event Correlation Techniques in Siem-Systems. Part 1. *SPIIRAS Proceedings*. 2016;4(47):5–27. (in Russ.) Available from: https://doi.org/10.15622/sp.47.1
15. Gaynov A.E., Zavodtsev I.V. The Model of Processing Events of Information Security. Modern Science: actual problems of theory and practice". Series "Natural and Technical Sciences". 2017;3-4:44–49 (in Russ.)
16. Pronoza A.A., Chechulin A.A., Kotenko I.V. Mathematical Models of Visualization in SIEM Systems. *SPIIRAS Proceedings*. 2016;3(46):90–107. (in Russ.) Available from: https://doi.org/10.15622/sp.46.8
17. Grusho A.A., Primenko E.A., Timonina E.E. *Teoreticheskie osnovy kompiuternoi bezopasnosti* [Theoretical Foundations of Computer Security]. Moscow: Academy Publ. 2009. (in Russ.)
18. Grafov S.A., Beliavtsev A.Y., Voronov D.A., Trofimov A.A. SIEM-profile. *Zaŝita informacii. Inside*. 2017;1(73):56–62. (in Russ.)
19. Burlakov M.E. Application the Method of Correspondence Analysis to Optimize Combinations of Attributes from Datasets. *PNRPU Bulletin. Electrotechnics, Informational Technologies, Control Systems*. 2018;26:7–28. (in Russ.)
20. Datasets. *University of New Brunswick*. Available from: http://www.unb.ca/cic/research/datasets/ids.html [Accessed 07th August 2017]
21. Al-Hamami A.H., Al-Saadoon G.M.W. *Handbook of Research on Threat Detection and Countermeasures in Network Security*. Derry: IGI Global; 2014. 450 p. Available from: https://doi.org/10.4018/978-1-4666-6583-5