МЕТОДИКА ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ НА ОСНОВЕ СЕМАНТИЧЕСКОЙ МОДЕЛИ МЕТРИК И ДАННЫХ

Дойникова Е.В.[1], Федорченко А.В.[2], Котенко И.В.[3], Новикова Е.С.[4]

Цель статьи: *разработка семантической модели метрик и данных, а также, на ее основе, методики оценивания защищенности для получения объективных оценок защищенности информационной системы от кибератак.*

Метод исследования: *теоретический и системный анализ открытых источников данных и метрик защищенности, семантический анализ и классификация данных безопасности для построения семантической модели метрик и данных, разработка методики оценивания защищенности с использованием семантической модели и методов логического вывода, функциональное тестирование разработанной методики.*

Полученный результат: *предложен подход, основанный на семантической модели метрик и данных. Модель представляет собой онтологию, построенную с учетом отношений между источниками данных, объектами информационной системы и данными о них, первичными метриками объектов информационной системы и интегральными метриками и целями оценивания. Разработана методика вывода метрик и оценивания уровня защищенности неопределенных информационных систем в реальном времени с использованием предложенной модели. Представлен пример использования разработанной методики и онтологии, показывающий их применимость для ответа на вопросы оценивания защищенности.*

Область применения предложенного подхода – компоненты оценивания защищенности информационных систем от кибератак, предназначенные для повышения эффективности систем мониторинга и управления информационной безопасностью.

Ключевые слова: *оценивание защищенности, семантика, метрики, онтология, кибератака, информационная система, интеллектуальный анализ данных.*

DOI: 10.21681/2311-3456-2021-1-29-40

1. Введение

Оценивание защищенности информационных систем в реальном времени актуально для современного мира быстро развивающихся угроз. Существующей защиты с учетом класса защищенности информационной системы недостаточно из-за новых типов угроз, таких как целевые кибератаки и внутренние нарушители, что подтверждается зафиксированными случаями успешных кибератак. Кроме того, при таком подходе к защите систем не учитываются особенности относительно новых типов информационных систем, таких как Интернет вещей и индустриальный Интернет вещей, и обрабатываемых ими данных. Как следствие, появляются новые подходы к обеспечению защищенности информационных систем, в том числе, подходы, основанные на постоянном мониторинге поведения информационной системы. Развитию таких подходов к оцениванию защищенности способствует тот факт, что организации научились собирать большие объемы данных, связанные с поведением и безопасностью системы, а также появились открытые источники данных безопасности, собранные различными организациями.

1 Дойникова Елена Владимировна, кандидат технических наук, старший научный сотрудник, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: doynikova@comsec.spb.ru

2 Федоренко Андрей Владимирович, младший научный сотрудник, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: fedorchenko@comsec.spb.ru

3 Котенко Игорь Витальевич, доктор технических, профессор, главный научный сотрудник и заведующий лабораторией проблем компьютерной безопасности, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: ivkote@comsec.spb.ru

4 Новикова Евгения Сергеевна, кандидат технических наук, старший научный сотрудник, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: novikova@comsec.spb.ru

Примерами систем сбора и обработки данных безопасности являются системы управления информацией и событиями безопасности (Security Information and Event Management, SIEM) и системы аналитики поведения пользователей и сущностей (User and Entity Behavior Analytics, UEBA) [1–3]. Примерами открытых источников данных безопасности являются база уязвимостей “National Vulnerability Database” (NVD), база слабых мест программного и аппаратного обеспечения “Common Weakness Enumeration” (CWE), база шаблонов атак “Common Attack Pattern Enumeration and Classification” (CAPEC), и база атак MITRE Att&ck [1].

Кроме того, появились новые методы интеллектуальной обработки данных. Открытыми остаются вопросы применения методов интеллектуального анализа данных в задачах оценивания защищенности [4–8] и вопросы выбора и вычисления метрик (показателей) защищенности с использованием собранных данных, а также вопрос определения полного и адекватного набора метрик, отражающих ситуацию по защищенности. Основной проблемой является формирование связей между «сырыми» данными безопасности и верхнеуровневыми метриками, понятными конечному пользователю или владельцу бизнеса, что, в свою очередь, невозможно без выявления связей между измеряемыми объектами и «сырыми» данными о них, а также связей между первичными и интегральными метриками. Из существующих методов интеллектуальной обработки данных многообещающим с точки зрения описанной проблемы является семантический подход, так как он позволяет структурировать существующие знания о предметной области, прослеживать зависимости между различными объектами, процессами и событиями предметной области, и делать выводы о причинах и последствиях различных событий на основе выявленных зависимостей.

В статье предлагается подход, основанный на семантической модели метрик и данных. Разработанная модель представляет собой онтологию, построенную с учетом отношений между источниками данных, объектами информационной системы и «сырыми» данными о них, первичными метриками объектов информационной системы, вычисляемыми на основе «сырых» данных, и интегральными метриками, определенными в зависимости от целей оценивания, и целями оценивания. Модель применяется в рамках методики вывода метрик и оценивания уровня защищенности неопределенных информационных систем в реальном времени. Методика, использующая метод логического вывода на основе зависимостей модели, позволит ответить на вопросы оценивания защищенности, используя все доступные данные и их взаимосвязи, и получить новые знания о защищенности системы.

Описываемое в статье исследование опирается на предыдущие результаты авторов, в том числе онтологию источников и данных безопасности, набор иерархически взаимосвязанных метрик и исходную онтологию метрик защищенности. Модель, описываемая в данной статье, отличается от онтологии источников и данных безопасности [9] добавлением динамической информации и нового класса метрик защищенности. Выделение метрик в отдельные сущности онтологии позволяет использовать отношения между ними, данными и источниками данных для вывода и вычисления интегральных метрик. Ранее предложенный набор иерархически взаимосвязанных метрик [10] был расширен и лег в основу модели, предлагаемой в данном исследовании. Исходная онтология метрик защищенности [11] была предназначена для ответа только на один вопрос оценивания защищенности, а именно, какова цель атаки. Онтология была расширена, чтобы отвечать на разные вопросы оценивания защищенности [12], и в текущем исследовании детализирована за счет новых метрик защищенности.

Таким образом, в данной статье описываются следующие основные результаты исследования: семантическая модель метрик и данных; методика оценивания защищенности на основе семантической модели; пример, демонстрирующий применение методики. На текущий момент не предложено эффективного автоматического адаптивного механизма для разработки и вычисления метрик в целях оценивания защищенности и выбора контрмер, применимого для систем разного типа и учитывающего условно неограниченное количество исходной информации о защищенности системы. В данном исследовании в качестве такого механизма предлагается использовать разработанные семантическую модель метрик и данных и методику оценивания защищенности, построенную на ее основе.

Статья организована следующим образом. В разделе 2 проанализированы релевантные исследования. В разделе 3 описываются разработанные семантическая модель и методика оценивания защищенности. В разделе 4 приводится пример, демонстрирующий работу методики, и анализируются полученные результаты.

2. Релевантные работы

Рассмотрим следующие группы работ, относящихся к теме исследования: инструменты мониторинга защищенности, источники данных безопасности, а

также онтологии и методики, предназначенные для анализа защищенности.

Исследования в области мониторинга защищенности легли в основу систем классов SIEM и UEBA. В настоящее время в области SIEM и UEBA существует большое количество коммерческих решений, включая QRadar SIEM, ArcSight ESM, Splunk Enterprise Security, Securonix UEBA, Micro Focus Security ArcSight UBA, Splunk User Behaviour Analysis и др. Практический опыт применения таких решений показывает, что их текущие реализации не всегда эффективны при мониторинге защищенности, анализе инцидентов безопасности, определении и анализе причин и последствий атакующих действий и реагировании на инциденты безопасности. Для расширения возможностей таких систем могут использоваться семантические модели и методики, разработанные на их основе.

SIEM и UEBA могут являться одним из источников динамических данных безопасности при оценивании защищенности, наряду с системами обнаружения и предотвращения вторжений, сканерами защищенности, и др. Кроме того, к настоящему времени было создано большое количество открытых баз условно статических данных безопасности. К ним относятся база шаблонов атак CAPEC, база слабых мест программного и аппаратного обеспечения CWE, базы уязвимостей программного и аппаратного обеспечения NVD, CVE, OSVDB, VND, базы эксплойтов EDB и Metasploit и др. [1]. Эти базы содержат как сущности соответствующих объектов предметной области, так и различные метрики. Данные метрики частично использовались при разработке предлагаемой семантической модели метрик и данных.

Семантические модели и подходы используются при решении различных задач, включая задачи управления безопасностью. В частности, онтологии являются эффективным способом интеграции информации [13, 14]. Были предложены онтологии, спроектированные для решения отдельных задач безопасности [15–27], включая онтологии для анализа защищенности [15–19], онтологии для анализа политик безопасности [20], онтологии для поддержки принятия решений по обеспечению защищённости [21, 22], онтология для автоматизации управления безопасностью [23] на основе протокола автоматизации информации безопасности (Security Content Automation Protocol, SCAP), корреляции событий [24] и онтологии, сфокусированные именно на метриках защищенности [25–27]. Идея применения онтологии для разработки метрик, предложенная в [27], близка к идее, исследуемой в данной работе, однако авторы сосредоточены именно на разработке метрик с учетом требований стандартов и привлечением экспертов, а не на автоматическом оценивании защищенности с использованием онтологии. Как следствие, они не рассматривают вопросы автоматического формирования онтологии для информационных систем разных типов в реальном времени.

Анализ существующих исследований показал, что онтологический подход применяется во многих задачах управления защищенностью. В то же время, хотя существует большое количество онтологий, разработанных для разных целей, онтологии, подходящей для заявленной цели разработки методики автоматического оценивания защищенности информационных систем в реальном времени, на текущей момент не существует. Однако, существует необходимая теоретическая и практическая база для создания такой модели и методики.

3. Семантическая модель метрик и данных и методика оценивания защищенности

Предлагаемая методика оценивания защищенности основана на идее вывода новых знаний, связанных с текущим состоянием защищенности информационной системы, на основе уже доступных статических и динамических знаний о системе, представленных в виде семантической модели метрик и данных. При этом под статическими, или условно статическими знаниями, понимается информация, которая практически не изменяется со временем (например, оборудование внутри информационной системы, уязвимости его программного и аппаратного обеспечения, известные угрозы), а под динамическими – постоянно изменяющаяся информация (например, фиксируемые события). Основными особенностями заявленной методики, являются: автоматическое оценивание защищенности в реальном времени; учет динамической информации о событиях в системе для постоянного мониторинга ситуации по защищенности; вывод метрик, отвечающих на вопросы оценивания защищенности, на основе метрик, вычисляемых с использованием «сырых» данных, за счет использования связей между концептами онтологии.

В подразделах данного раздела описываются разработанная семантическая модель и методика оценивания защищенности с использованием разработанной модели.

3.1. Семантическая модель метрик и данных

Разработанная онтология объединяет данные безопасности, представленные объектами процесса оценки защищенности, их источники и метрики защищенности. Источники данных включают открытые базы данных безопасности, такие как CWE, CAPEC, NVD и др. К данным безопасности относятся слабые

DOI: 10.21681/2311-3456-2021-1-29-40

места, атаки, уязвимости, конфигурации, продукты, и др. Наконец, метрики защищенности классифицированы по объектам защищенности, источникам данных для их вычисления и вопросам оценивания защищенности на которые они отвечают.

Источники данных безопасности. Большая часть концептов, соответствующих источникам данных безопасности, определяется на основе открытых баз данных безопасности. Для выделения концептов данных безопасности, определения связей между концептами источников данных и данных безопасности, а также первичных метрик были проанализированы схемы открытых баз данных безопасности.

Каждая из перечисленных баз предоставляет данные для определения концептов данных безопасности, так NVD является источником данных для определения продуктов (или программного и аппаратного обеспечения) в формате CPE, их конфигураций в формате CCE и уязвимостей в формате CVE [1].

Кроме того, данные базы являются источником данных для определения концептов метрик. Выделим идентифицирующие метрики (например, свойства формата CVE, такие как идентификатор уязвимости, дата публикации, дата изменения) и оценивающие метрики (оценки уязвимости, критичность атаки, вероятность атаки, требуемый уровень навыков для реализации атаки).

Наконец, базы данных являются источником данных для определения связей между концептами. Такие связи можно определить через поле «Ссылки» (References) объектов, представленных в базе. Оно включает ссылки на объекты в других источниках данных. Например, для уязвимостей в базе NVD определены ссылки на слабые места в базе CWE (такие ссылки могут использоваться для связи продуктов с их слабыми местами через уязвимости). Сформированные связи между концептами используются для вывода ответов на вопросы оценивания защищенности за счет формирования связей между первичными и интегральными метриками защищенности, источниками данных для их вычисления и объектами, которые они оценивают.

Онтология метрик и данных безопасности. Разработанная онтология является основой предлагаемой методики оценивания защищенности. Она включает концепты и отношения между ними. Фрагмент упрощенной иерархии наследования предложенной онтологии представлен на рис. 1. Онтология включает четыре класса концептов: источники данных безопасности (Source); данные безопасности (SecurityInformation); объекты инфраструктуры (Infrastructure); метрики защищенности (Metric). Выделяются следующие типы отношений: отношения наследования, включая родительские отношения между концептами и отношения «часть-целое» между концептами источников данных безопасности и остальными группами концептов; отношения между концептами метрик, между концептами данных безопасности и объектов инфраструктуры, и концептами метрик и концептами данных безопасности и объектов инфраструктуры (объектные свойства); отношения между концептами и возможными вариантами описания их индивидов (свойства данных) [9].

Первая группа концептов (Source) объединяет источники данных безопасности. Они могут быть связаны отношениями «часть-целое», как, например, NVD и CVE: «NVD is-a CVE».

Вторая группа концептов (SecurityInformation) объединяет данные безопасности, а именно: «Продукт» (Product), «Атака» (Attack), «Атакующий» (Attacker), «Уязвимость» (Vulnerability) и др. [9, 11]. Эти концепты имеют подклассы. Например, концепт «Атака» имеет подкласс «Шаг атаки». Подклассы перечисленных концептов не представлены на рис. 1, чтобы не перегружать рисунок. Можно выделить отношения между концептами внутри второй группы. Так, концепты «Атака» и «Шаг атаки» связаны родительским отношением. Концепты «Уязвимость» и «Атака» связаны отношением между концептами и/или сущностями (объектные свойства), а именно, через свойство «используется в» (isUsedBy): «Уязвимость используется в Атаке» (рис. 2). Также можно выделить отношения между концептами первой и второй групп. Концепты CAPEC и «Атака» (Attack) связаны отношением «часть-целое» (is-a): «CAPEC is-a Attack».

Третья группа концептов (Infrastructure) объединяет объекты инфраструктуры, такие как «Сеть» (Network), «Рабочая станция» (Host) и др. Можно выделить отношения между концептами внутри третьей группы. Так, концепты «Сеть» и «Хост» связаны отношением «часть-целое». Также можно выделить отношения между концептами второй и третьей групп. Концепты «Текущая конфигурация» (CurrentConfiguration) и «Конфигурация хоста» (HostConfiguration) связаны отношением эквивалентности.

Четвертая группа концептов объединяет метрики защищенности. Выделим различные классы метрик в зависимости от объектов, которые они оценивают [10, 12]: метрики инфраструктуры, метрики атаки, метрики атакующего, метрики события, метрики реагирования и интегральные метрики. В свою очередь, каждый класс метрик имеет подклассы. Например, метрики уязвимости (VulnerabilityMetric) содержат подкласс, объединяющий метрики CVSS из базы NVD, представленный с помощью концепта CVSSv2 [10, 28, 29].

Рис. 1. Фрагмент упрощенной иерархии наследования разработанной онтологии

Также выделим различные типы метрик, а именно: идентифицирующие метрики, т.е. метрики, которые уникально идентифицируют объект среди других объектов (например, концепт «Продукт» имеет идентифицирующие метрики «Производитель», «Версия», «Обновление» и др.); оценивающие метрики, которые оценивают объекты с точки зрения различных аспектов защищенности (например, метрики CVSS [10, 28, 29]).

Можно выделить отношения между концептами внутри четвертой группы. Это могут быть отношения «часть-целое»: класс метрик уязвимостей, представленный концептом VulnerabilityMetric, содержит, в свою очередь, подкласс метрик CVSS для уязвимостей, представленный концептом CVSSv2, с которым он связан через отношение is-a, т.е. «CVSSv2 is-a VulnerabilityMetric».

Одна из особенностей разработанной онтологии заключается в том, что метрики защищенности выделены в отдельные классы в рамках класса концептом Metric, т.е. каждая метрика представляет собой отдельный концепт, а метрика с присвоенным значением – отдельную сущность. В результате, метрики связаны с данными безопасности, объектами инфраструктуры и источниками данных через объектные свойства, описывающие тип отношения между концептами и сущностями, а не через свойства данных, которые описывают информацию, специфичную для концепта или сущности.

Например, концепт второй группы «Уязвимость» и концепт четвертой группы CVSSv2 связаны через объектное свойство «оценивает» (evaluates) следующим образом: «CVSSv2 оценивает Уязвимость». Это позволяет выводить связи между интегральными ме-

DOI: 10.21681/2311-3456-2021-1-29-40

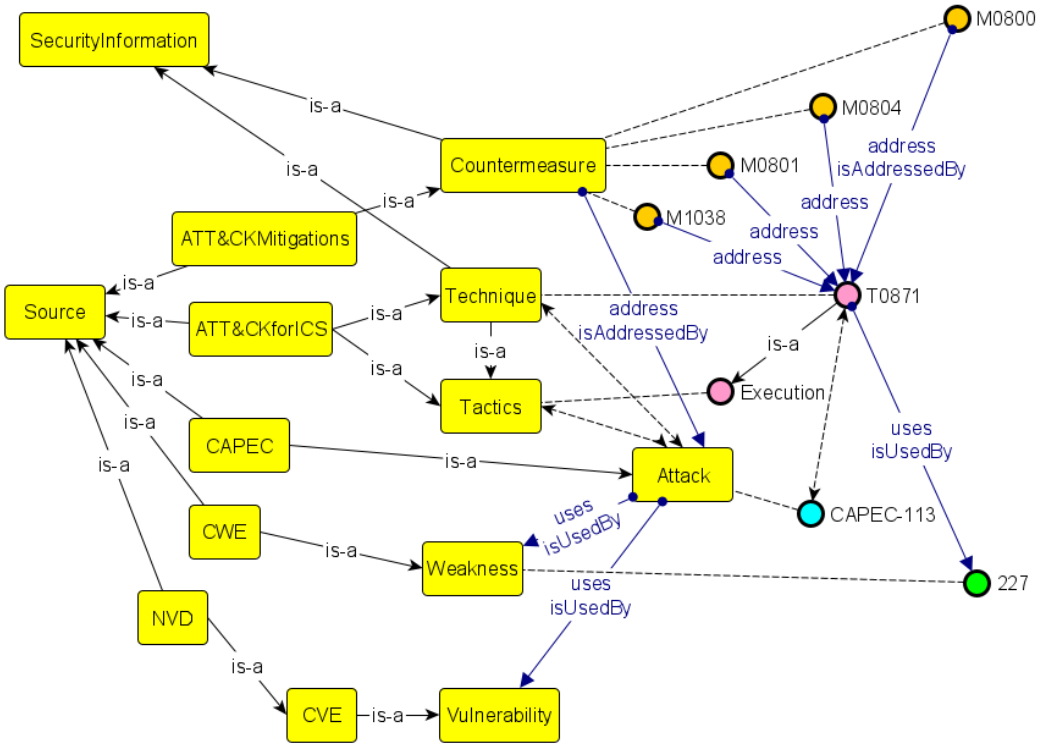

Рис. 2. Фрагмент онтологии, демонстрирующий связи между концептами первой и второй групп

триками, отображающими состояние защищённости системы, и первичными метриками защищенности, связи между первичными метриками защищенности и данными безопасности и объектами инфраструктуры, связи между данными безопасности и объектами инфраструктуры и источниками данных безопасности, и связи между метриками защищенности и источниками данных безопасности. Наличие таких связей позволяет связывать метрики разных объектов и использовать эти связи для вывода и расчета метрик защищенности, т.е. получать новые знания о защищенности системы.

Наконец, выделим различные типы метрик в зависимости от способа вычисления: первичные, получаемые непосредственно из источников данных; интегральные, получаемые на основе других метрик. Для определения и вычисления интегральных метрик на основе разработанной онтологии необходимо собрать доступные данные безопасности и присвоить значения первичным метрикам (на основе информации из открытых баз данных безопасности); начиная с означенных концептов обойти связанные концепты данных безопасности, объектов инфраструктуры и метрик и определить механизм вычисления неизвестных интегральных метрик защищенности с учетом логического типа связей.

3.2. Методика оценивания защищенности

Разработанная методика включает два основных этапа: формирование онтологии; оценивание защищенности с использованием разработанной онтологии.

Формирование онтологии. Первый этап включает два подэтапа: (1) формирование и заполнение семантической модели на основе статической информации, доступной из открытых источников; (2) формирование части семантической модели на основе динамической информации.

Структура семантической модели подробно описана выше. Второй подэтап динамического формирования онтологии, а именно, ее части, связанной с событиями, происходящими в системе, и конфигурацией анализируемой системы, основан на анализе происходящих в системе событий с использованием методов корреляции [30] и включает шаги: определение типов объектов как набора свойств путем анализа и выявления свойств событий, которые появляются только совместно; определение объектов как набора свойств, для которых определены значения; определение связей между объектами на основе наличия взаимодействия между объектами; добавление концептов, соответствующих типам объектов, в онтологию (на уровень инфраструктуры и уровень событий); добавление отношений между концептами

уровня инфраструктуры и событий на основе выделенных связей между объектами; добавление экземпляров в онтологию на основе конкретных объектов; добавление отношений с объектами других уровней. Сформированная таким образом онтология используется для динамического анализа защищенности.

Оценивание защищенности с использованием разработанной онтологии. Данный этап подразумевает ответ на ряд вопросов оценивания защищенности которые должны быть сформированы с учетом стандартов защищенности и целей организации. Составление списка вопросов с учетом целей организации выходит за рамки текущего исследования. Метрики, входящие в модель, выбраны на основе существующих стандартов защищенности. Для получения новых знаний о состоянии защищенности системы используется следующая методика.

Шаг 1. Определение набора доступных данных для ответа на вопрос оценивания защищенности. Это могут быть статические данные, такие как конфигурация и уязвимости системы, и динамические данные, такие как инциденты безопасности. Рассматриваемые концепты зависят от конкретного вопроса оценивания защищенности.

Шаг 2. Расширение знаний с использованием отношений между концептами онтологии и вычисление интегральной метрики защищенности. Данный шаг представляет собой обход концептов онтологии с использованием отношений между ними. Учитываемые отношения и алгоритм обхода зависят от конкретного вопроса оценивания защищенности. По результатам обхода, ввиду того, что метрики представлены концептами онтологии и связаны отношениями друг с другом и объектами инфраструктуры и данных безопасности, генерируется формула вычисления интегральных метрик, отвечающих на вопросы оценивания защищенности.

4. Реализация и тестирование

На данный момент сформирована онтология со статическим содержимым и проведены эксперименты по применению методики анализа защищенности на ее основе. Онтология реализована в Protege 5.5.0 с использованием языка OWL версии 2.0. Семантическая модель на данный момент содержит 639 аксиом, включая 418 логических аксиом, 221 деклараций, 86 классов, и 54 объектных свойства. Методика реализована на языке Python 3. Методика, с использованием онтологии, позволит отвечать на такие вопросы как: «Каковы риски нарушения защищенности системы?». И более конкретные вопросы, такие как: «Какова максимальная критичность уязвимостей серверов Интернет-сегмента инфраструктуры, которые могут быть проэксплуатированы атакующим с высоким уровнем квалификации?». Рассмотрим применение методики оценивания защищенности (второй этап) на примере ответа на данный вопрос. Схема рассматриваемого примера приведена на рис. 3.

Из описания можно выделить значения следующих идентифицирующих метрик:

- «Цель» (Target), значение которой «Серверы Интернет-сегмента». Это метрика объекта «Система» третьей группы концептов, который связан отношением эквивалентности с концептом «Цель».

Также можно определить значения следующих оценивающих метрик:

- «Вектор доступа» (AccessVector), значение которой «Сетевой» (Network). Это метрика объекта «Уязвимость» (Vulnerability), относящегося ко второй группе концептов.
- «Уровень навыков атакующего» (AttackerQualification), значение которой «Высокая» (High). Это метрика объекта «Атакующий» (Attacker), относящегося ко второй группе концептов.

Схему на рис. 3 можно условно поделить на четыре части:

1) неформальное отображение инфраструктуры (верхний левый угол), содержащей уязвимости с оценкой CVSS «Средняя» (максимальная критичность уязвимостей на серверах тестовой инфраструктуры);
2) формальное отображение объектов инфраструктуры как сущностей соответствующих концептов онтологии первой группы (нижняя левая часть);
3) объекты второй группы концептов SecurityInformation (верхняя правая часть);
4) объекты четвертой группы концептов Metric.

В рассматриваемом примере целевая инфраструктура представлена внутренним и внешним сетевыми сегментами, и двумя типами хостов (серверы и рабочие станции). Объекты, входящие в инфраструктуру, представлены отдельными сущностями концепта InfrastructureObject (1-4) в левом нижнем углу рис. 3. Наличие связи между инфраструктурой и отдельными сущностями, входящими в нее, показано пунктирными стрелками. Объект 5 характеризует внутренний сегмент сети. Объект 6 характеризует внешний сегмент сети. Сплошные стрелки обозначают наличие связи через объектные свойства (свойствам назначены номера, которыми помечены стрелки):

- Свойство 1 (hasInfrastructureObjectType) характеризует объекты инфраструктуры с учетом метрики InfrastructureObjectType, идентифицирующей их тип.

DOI: 10.21681/2311-3456-2021-1-29-40

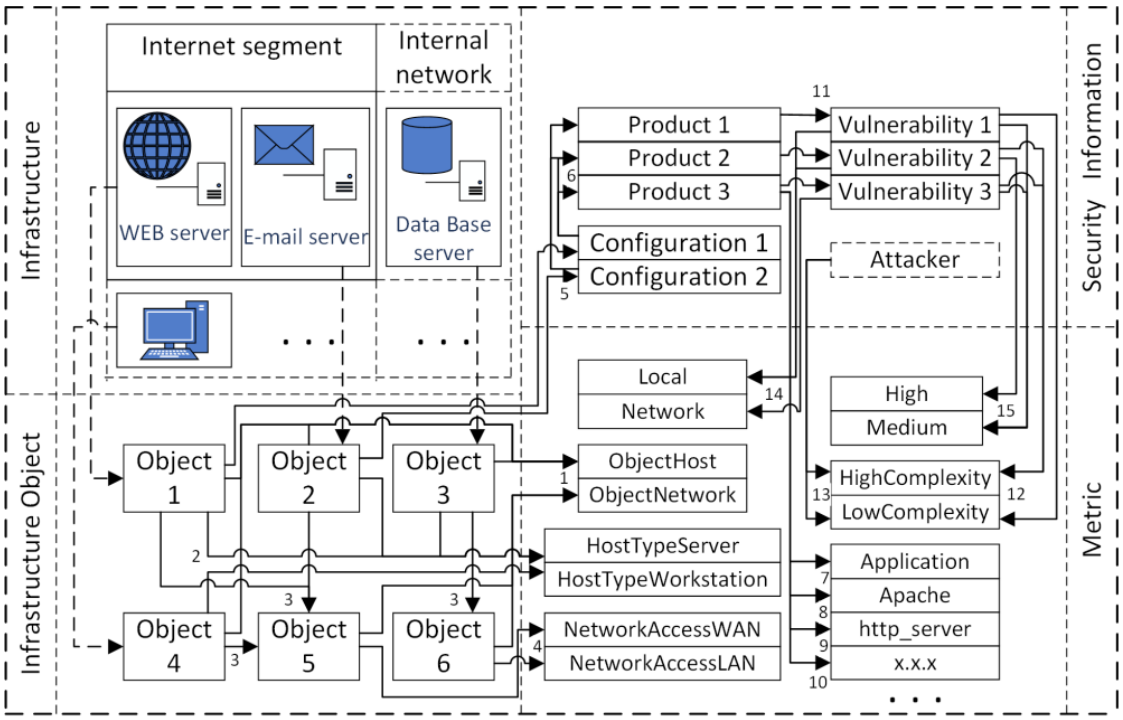

Рис. 3. Описание примера

- Свойство 2 (hasHostType) определяет тип хоста с учетом метрики HostType.
- Транзитивное свойство 3 (connectedWith) позволяет определить взаимосвязь между объектами инфраструктуры. С его помощью выделены две подсети – внутренняя и внешняя (Интернет).
- Свойство 4 (hasNetworkAccess) совместно со свойствами 1-3 позволяет определить объекты-серверы, имеющие Интернет доступ, что в свою очередь позволяет ответить на поставленный вопрос.
- Свойство 5 (hasConfiguration) определяет конфигурацию хостов.
- Свойство 6 (containsProduct) связывает объекты конфигурации хостов с программными и аппаратными продуктами.
- Свойства 7 (hasProductType), 8 (hasProductVendor), 9 (hasProductName) и 10 (hasProductVerstion) позволяют определить связи между продуктами и метриками ProductType, ProductVendor, ProductName, и ProductVersion, соответственно.
- Свойство 11 (containsImplementationOf) реализует связь между сущностями концептов второй группы (данные безопасности): продукты и уязвимости.
- Свойства 12 (hasAccessComplexity), 14 (hasAccessVector) и 15 (hasBaseScoreMetric) отображают отношения уязвимостей с концептами метрик AccessComplexity, AccessVector и BaseScoreMetric, соответственно.
- Свойство 13 (hasAttackerQualification) за счет эквивалентности между концептами AttackerQualification и AccessComplexity, связывает уровень навыков атакующего и сложность доступа эксплуатируемых уязвимостей.

Учитывая описанные свойства и пример на рис. 3, ответ на поставленный выше вопрос: сущность концепта группы метрик BaseScoreMetric – «Средняя» (Medium), что является корректным ответом на вопрос, учитывая тестовую инфраструктуру.

Рассмотренный пример является упрощенным, т.к. в реальных случаях количество концептов, сущностей и связей между ними затруднит интерпретацию.

Заключение

В статье проанализированы источники данных безопасности, характеристики данных и связи между ними. Анализ проводился с целью разработки нового подхода к обработке доступных данных безопасности для получения новых знаний о защищенности системы. В результате был предложен подход, основанный на семантической модели метрик и данных, и методика оценивания защищенности на основе разработанной модели. Модель представляет собой онтологию, построенную с учетом отношений между источниками данных, объектами информационной системы и данными о них, первичными метриками объектов информационной системы и интегральными метриками и целями оценивания. Суть разрабо-

танной модели состоит в отображении характеристик данных безопасности и целей управления защищенностью с помощью набора сопоставленных им метрик. В статье описана разработанная онтология, ее концепты и связи между ними. К преимуществам разработанной модели можно отнести уровень детализации, возможность применения логического вывода для определения и вычисления метрик, отображающих состояние защищенности, и интеграцию знаний по защищенности для ответа на вопросы оценивания защищенности.

Суть разработанной методики оценивания защищенности состоит в использовании отношений между данными безопасности и целями управления защищенностью для определения и вычисления метрик защищенности, позволяющих отвечать на вопросы управления защищенностью. В статье описана предложенная методика вывода интегральных метрик защищенности на основе связей между метриками и объектами оценивания, и оценивания уровня защищенности информационных систем в реальном времени.

В статье описан пример использования разработанной методики и онтологии, показывающий их практическую применимость для ответа на вопросы оценивания защищенности.

В рамках дальнейших исследований планируется реализовать динамическое добавление концептов в онтологию; расширить онтологию за счет не учтенных источников данных безопасности; провести дополнительные эксперименты по применению методики оценивания защищенности.

Работа выполнена при частичной финансовой поддержке РФФИ (проект № 19-07-01246) и бюджетной темы 0073-2019-0002.

Литература

1. Интеллектуальные сервисы защиты информации в критических инфраструктурах / И.В. Котенко, И.Б. Саенко, А.А. Чечулин [и др.]; под общей ред. И.В. Котенко, И.Б. Саенко. СПб.: БХВ-Петербург, 2019. 400 с. ISBN 978-5-9775-3968-5.
2. Рыболовлев Д.А., Карасёв С.В., Поляков С.А. Классификация современных систем управления инцидентами безопасности // Вопросы кибербезопасности. 2018. № 3 (27). С.47-53. DOI: 10.21681/2311-3456-2018-3-47-53.
3. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. № 5 (23). С.2-16. DOI: 10.21681/2311-3456-2017-5-2-16.
4. Grusho, A.A., Grusho, N.A., Zabezhailo, M.I., Timonina E.E. Intelligent data analysis in information security // Aut. Control Comp. Sci. 50, P. 722–725. 2016. https://doi.org/10.3103/S0146411616080307.
5. Miloslavskaya, N. Stream data analytics for network attacks' prediction // Procedia Computer Science. 169, P. 57-62. 2020. DOI: 10.1016/j.procs.2020.02.114.
6. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Автоматизация анализа уязвимостей программного обеспечения на основе технологии text mining // Вопросы кибербезопасности. 2020. № 4 (38). С.22-31. DOI: 10.21681/2311-3456-2020-04-22-31.
7. Фаткиева Р.Р., Левоневский Д.К. Применение бинарных деревьев для агрегации событий систем обнаружения вторжений // Труды СПИИРАН. 2015. Вып. 40. С. 110-121.
8. Granadillo G., el Barbori M., Debar, H. New types of alert correlation for security information and event management systems // Proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security, Larnaca, Cyprus. 2016. P.1–7. DOI: 10.1109/NTMS.2016.7792462.
9. Kotenko I., Doynikova E., Fedorchenko A., Chechulin A. An ontology-based hybrid storage of security information // Information Technology and Control, 18, 3, 2018. P. 655–667.
10. Doynikova E., Kotenko I. CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection // Proc. of the 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP 2017), IEEE, St. Petersburg, Russia, 2017. P. 346–353. DOI: 10.1109/PDP.2017.44.
11. Doynikova E., Kotenko I. Approach for determination of cyber attack goals based on the ontology of security metrics // Proc. of the IOP Conference Series: Materials Science and Engineering, vol. 450, Data protection in automation systems, 2018. P. 1–6.
12. Doynikova E., Fedorchenko A., Kotenko I. A Semantic Model for Security Evaluation of Information Systems // Journal of Cyber Security and Mobility. 9, 2. 2020. P. 301–330. DOI: 10.13052/jcsm2245-1439.925.
13. Elahi G., Yu E., Zannone N. A modeling ontology for integrating vulnerabilities into security requirements conceptual foundations // Lecture Notes in Computer Science 5829, P. 99–114, 2009.
14. Kotenko I., Fedorchenko A., Chechulin A. Integrated repository of security information for network security evaluation // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 6, P. 41–57, 2015.

DOI: 10.21681/2311-3456-2021-1-29-40

15. Guo M., Wang J. A. An ontology-based approach to model Common Vulnerabilities and Exposures in information security // Proc. of the 2009 ASEE Southeast Section Conference, 2009. P. 1–10.
16. Wang J. A., Guo M. Security data mining in an ontology for vulnerability management // Proc. of the International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing, Shanghai, 2009, P. 597–603.
17. Syed Z., Padia A., Finin T., Mathews L., Joshi A. UCO: a Unified Cybersecurity Ontology // Proc. of the AAAI Workshop on Artificial Intelligence for Cyber Security, Phoenix, Arizona, USA, P. 195–202, 2016.
18. Мирзагитов А.А., Пальчунов Д.Е. Методы разработки онтологии по информационной безопасности, основанные на прецедентном подходе // Вестник НГУ. Серия: Информационные технологии. 2013. №3. С. 37–46.
19. Петренко А.С., Петренко С.А. Онтология кибербезопасности самовосстанавливающихся smart grid // Труды Третьей Всероссийской научно-технической конференции молодых конструкторов и инженеров, посвященной 70-летию Радиотехнического института имени академика А.Л. Минца и 70-летию ФИЗТЕХА. 2016. С. 200–210.
20. Javanmardi S., Amini M., Jalili R., Ganjisaffar Y. SBAC : a Semantic-Based Access Control model, 2006. P. 1–12.
21. Granadillo G. G., Mustapha Y. B., Hachem N., Debar H. An ontology-based model for SIEM environments // Global Security, Safety and Sustainability & eDemocracy, Springer Berlin Heidelberg, 2012. P. 148–155. DOI: 10.1007/978-3-642-334481_21.
22. Mozzaquatro B., Melo R., Agostinho C., Jardim-Goncalves R. An ontology-based security framework for decision-making in industrial systems // Proc. of the 4th International Conference on Model-Driven Engineering and Software Development, P. 779–788, 2016.
23. Parmelee M. C. Toward an ontology architecture for cyber-security standards // Proc. of the 2010 Semantic Technology for Intelligence, Defence, and Security. Fairfax, P. 116–123, 2010.
24. Kenaza T., Aiash M. Toward an Efficient Ontology-Based Event Correlation in SIEM // Procedia Computer Science. 83. P. 139-146. 2016. DOI:10.1016/j.procs.2016.04.109.
25. Kotenko I., Polubelova O., Saenko I., Doynikova E. The ontology of metrics for security evaluation and decision support in SIEM systems // Proc. of the ARES 2013, 2013. P. 638–645.
26. Aviad A., Węcel K., Abramowicz W. The semantic approach to cyber security. Towards ontology based body of knowledge // Proc. of the 14th European Conference on Cyber Warfare and Security, P. 328–336, 2015.
27. Cho J.-H., Xu S., Hurley P. M., Mackay M., Benjamin T., Beaumont M. STRAM: Measuring the Trustworthiness of Computer-based Systems // ACM Computing Surveys, Vol. 51, No. 6, Article 128, P. 1–47. 2019. Режим доступа: http://www.cs.utsa.edu/~shxu/socs/STRAM_paper.pdf (дата обращения: 3.01.2021).
28. Scarfone, K., Mell P. An analysis of CVSS version 2 vulnerability scoring // 3rd International Symposium on Empirical Software Engineering and Measurement, Lake Buena Vista, FL, 2009, P. 516-525. DOI: 10.1109/ESEM.2009.5314220.
29. Younis, A. A., Malaiya, Y. K. Comparing and evaluating CVSS base metrics and Microsoft rating system // Proceedings of the The 2015 IEEE International Conference on Software Quality, Reliability and Security. 2015. P. 252-261. 10.1109/QRS.2015.44.
30. Федорченко А.В., Дойникова Е.В., Котенко И.В. Автоматизированное определение активов и оценка их критичности для анализа защищенности информационных систем // Труды СПИИРАН. 2019. Т. 18. № 5. С. 1182–1211. DOI: 10.15622/sp.2019.18.5.1182-1211.

SECURITY ASSESSMENT METHODOLOGY BASED ON THE SEMANTIC MODEL OF METRICS AND DATA

Doynikova E.V.[5], Fedorchenko A.V.[6], Kotenko I.V.[7], Novikova E.C[8].

The purpose of the article: *development of semantic model of metrics and data and technique for security assessment based on of this model to get objective scores of information system security.*

5 Elena Doynikova, Ph.D, Senior researcher at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: doynikova@comsec.spb.ru

6 Andrey Fedorchenko, Junior researcher at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: fedorchenko@comsec.spb.ru

7 Igor Kotenko, Dr.Sc., Professor, Head of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: ivkote@comsec.spb.ru

8 Evgenia Novikova, Ph.D, Senior researcher at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: novikova@comsec.spb.ru

Research method: *theoretical and system analysis of open security data sources and security metrics, semantic analysis and classification of security data, development of the security assessment technique based on the semantic model and methods of logical inference, functional testing of the developed technique.*

The result obtained: *an approach based on the semantic model of metrics and data is proposed. The model is an ontology generated considering relations among the data sources, information system objects and data about them, primary metrics of information system objects and integral metrics and goals of assessment. The technique for metrics calculation and assessment of unspecified information systems security level in real-time using the proposed model is developed. The case study demonstrating applicability of the developed technique and ontology to answer security assessment questions is provided.*

The area of use of the proposed approach are security assessment components of information security monitoring and management systems aimed at increasing their efficiency.

Keywords: *security assessment, semantics, metrics, ontology, cyber attack, information system, data mining.*

References

1. Kotenko I., Saenko I., Chechulin A., Polubelova O., Novikova E., Doinikova E., Shorov A., Desnitsky V. Intelligent information security services in critical infrastructures. Monography / Ed. Igor Kotenko and Igor Sayenko. St. Petersburg: BHV Publishing House, 2019. ISBN 978-5-9775-3968-5 (in Russian).
2. Rybolovlev D., Karasev S., Poljakov S. Classification of modern security information and event management systems // Cybersecurity issues. 2018. No. 3 (27). P. 47-53. DOI: 10.21681/2311-3456-2018-3-47-53 (in Russian).
3. Kotenko I., Fedorchenko A., Saenko I., and Kushnerevich A. Big-data technologies for security event correlation based on types relations // Cybersecurity issues. 2017. No. 5(23). P. 2-16. DOI: 10.21681/2311-3456-2017-5-2-16 (in Russian).
4. Grusho, A.A., Grusho, N.A., Zabezhailo, M.I., Timonina E.E. Intelligent data analysis in information security // Aut. Control Comp. Sci. 50, P. 722–725. 2016. https://doi.org/10.3103/S0146411616080307.
5. Miloslavskaya, N. Stream data analytics for network attacks' prediction // Procedia Computer Science. 169, P. 57-62. 2020. 10.1016/j.procs.2020.02.114.
6. Vasilyev V, Vulfin A., Kuchkarova N. Automation of software vulnerabilities analysis on the basis of text mining technology // Cybersecurity issues. 2020. No. 4 (38). P.22-31. DOI: 10.21681/2311-3456-2020-04-22-31 (in Russian).
7. Fatkieva R.R., Levonevskiy D.K. Application of Binary Trees for the IDS Events Aggregation Task. SPIIRAS Proceedings. 2015. Issue 40. P. 110-121 (in Russian).
8. Granadillo G., el Barbori M., Debar, H. New types of alert correlation for security information and event management systems // Proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security, Larnaca, Cyprus. 2016. P.1–7. 10.1109/NTMS.2016.7792462.
9. Kotenko I., Doynikova E., Fedorchenko A., Chechulin A. An ontology-based hybrid storage of security information // Information Technology and Control, 18, 3, 2018. P. 655–667.
10. Doynikova E., Kotenko I. CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection // Proc. of the 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP 2017), IEEE, St. Petersburg, Russia, 2017. P. 346–353. DOI: 10.1109/PDP.2017.44.
11. Doynikova E., Kotenko I. Approach for determination of cyber attack goals based on the ontology of security metrics // Proc. of the IOP Conference Series: Materials Science and Engineering, vol. 450, 'Data protection in automation systems', 2018. P. 1–6.
12. Doynikova E., Fedorchenko A., Kotenko I. A Semantic Model for Security Evaluation of Information Systems // Journal of Cyber Security and Mobility. 9, 2. 2020. P. 301–330. DOI: 10.13052/jcsm2245-1439.925. Режим доступа: http://dx.doi.org/10.13052/jcsm2245-1439.925.
13. Elahi G., Yu E., Zannone N. A modeling ontology for integrating vulnerabilities into security requirements conceptual foundations // Lecture Notes in Computer Science 5829, 99-114, 2009.
14. Kotenko I., Fedorchenko A., Chechulin A. Integrated repository of security information for network security evaluation // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 6, P. 41–57, 2015.
15. Guo M., Wang J. A. An ontology-based approach to model Common Vulnerabilities and Exposures in information security // Proc. of the 2009 ASEE Southeast Section Conference, 2009. P. 41–57.
16. Wang J. A., Guo M. Security data mining in an ontology for vulnerability management // Proc. of the International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing, Shanghai, 2009, 597-603.
17. Syed Z., Padia A., Finin T., Mathews L., Joshi A. UCO: a Unified Cybersecurity Ontology // Proc. of the AAAI Workshop on Artificial Intelligence for Cyber Security, Phoenix, Arizona, USA, 195-202, 2016.

DOI: 10.21681/2311-3456-2021-1-29-40

18. Mirzagitov A., Palchunov D. Methods for development of the ontology on information security based on precedent approach // NSU Vestnik. Series: Information technologies. 2013. No. 3. P. 37–46 (in Russian).
19. Petrenko A., Petrenko S. Cybersecurity ontology for self-healing smart grid // Proceedings of the third All-Russian Scientific and Technical Conference of Young Designers and Engineers dedicated to the 70th anniversary of the Academician A.L. Mints and the 70th anniversary of FIZTECH. 2016. P. 200–210 (in Russian).
20. Javanmardi S., Amini M., Jalili R., Ganjisaffar Y. SBAC : a Semantic-Based Access Control model, 2006. P. 1–12.
21. Granadillo G. G., Mustapha Y. B., Hachem N., Debar H. An ontology-based model for SIEM environments // Global Security, Safety and Sustainability & eDemocracy, Springer Berlin Heidelberg, 2012. P. 148–155. DOI: 10.1007/978-3-642-334481_21.
22. Mozzaquatro B., Melo R., Agostinho C., Jardim-Goncalves R. An ontology-based security framework for decision-making in industrial systems // Proc. of the 4th International Conference on Model-Driven Engineering and Software Development, 779-788, 2016.
23. Parmelee M. C. Toward an ontology architecture for cyber-security standards // Proc. of the 2010 Semantic Technology for Intelligence, Defence, and Security. Fairfax, 116-123, 2010.
24. Kenaza T., Aiash M. Toward an Efficient Ontology-Based Event Correlation in SIEM // Procedia Computer Science. 83. P. 139-146. 2016. 10.1016/j.procs.2016.04.109.
25. Kotenko I., Polubelova O., Saenko I., Doynikova E. The ontology of metrics for security evaluation and decision support in SIEM systems // Proc. of the ARES 2013, 2013. P. 638–645.
26. Aviad A., Węcel K., Abramowicz W. The semantic approach to cyber security. Towards ontology based body of knowledge // Proc. of the 14th European Conference on Cyber Warfare and Security, 328-336, 2015.
27. Cho J.-H., Xu S., Hurley P. M., Mackay M., Benjamin T., Beaumont M. STRAM: Measuring the Trustworthiness of Computer-based Systems // ACM Computing Surveys, Vol. 51, No. 6, Article 128, P. 1–47. 2019. Режим доступа: http://www.cs.utsa.edu/~shxu/socs/STRAM_paper.pdf (дата обращения: 3.01.2021).
28. Scarfone, K., Mell P. An analysis of CVSS version 2 vulnerability scoring // 3rd International Symposium on Empirical Software Engineering and Measurement, Lake Buena Vista, FL, 2009, P. 516-525. DOI: 10.1109/ESEM.2009.5314220.
29. Younis, A. A., Malaiya, Y. K. Comparing and evaluating CVSS base metrics and Microsoft rating system // Proceedings of the The 2015 IEEE International Conference on Software Quality, Reliability and Security. 2015. P. 252-261. 10.1109/QRS.2015.44.
30. Fedorchenko A., Doynikova E., Kotenko I. Automated Detection of Assets and Calculation of their Criticality for the Analysis of Information System Security // SPIIRAS Proceedings, vol. 18 (5), 2019. P. 1182–1211. DOI: 10.15622/sp.2019.18.5.1182-1211.