ТРУДЫ МОЛОДЫХ УЧЕНЫХ

Научная статья
УДК 004.456; DOI: 10.61260/2218-13X-2023-4-159-168

К ВОПРОСУ О ФОРМАЛИЗАЦИИ ЗАДАЧИ РАНЖИРОВАНИЯ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

✉**Ярошенко Александр Юрьевич.**
Департамент информационных технологий и связи МЧС России, Москва, Россия
✉***alexagz@mail.ru***

Аннотация. Работа посвящена вопросу выполнения требований, направленных на обеспечение информационной безопасности в организации. Указано основное противоречие затронутой предметной области, заключающееся в наличии огромного числа различных вариаций выполнения требований при отсутствии способа выбора их корректного и оптимального порядка. Ставится задача ранжирования требований, и описывается идея предлагаемого решения в виде семи положений, направленных на согласованную запись разнородных требований в единой нотации, а также синтезируется интуитивно понятная схема идеи (с указанием на ней всех семи положений).

Для представления идеи вводятся следующие сущности: объект-организация и его элементы, к которым предъявляются требования; обобщенные условия выполнения требований, не зависящие от специфики организации; вариации наборов условий, учитывающие конкретную организацию; базовые условия, проверяющие наличие/отсутствие элементов объекта и значения их параметров; алгоритмы мероприятий в организации для ее удовлетворения условиям; приоритеты требований и ресурсы, необходимые алгоритмам. Делается вывод, что такая формализация органически приведет к алгоритмизации решения задачи ранжирования и, в конечном счете, к автоматизации.

Указаны наиболее подходящие автоматизированные способы решения задачи ранжирования требований информационной безопасности – алгоритмическое применение комбинаторной оптимизации и методов машинного обучения. Прогнозируется их высокая эффективность по сравнению с «ручными» способами, применяемыми в современной практике защиты информации.

Отмечена новизна, теоретическая и практическая значимость полученных результатов, а также перспектива дальнейших исследований – построение аналитической модели выполнения требований, которая могла бы лечь в основу соответствующего метода, за которым последует его программная реализация и проведение необходимых экспериментов.

Ключевые слова: информационная безопасность, требования, ранжирование, формализация, автоматизация

Для цитирования: Ярошенко А.Ю. К вопросу о формализации задачи ранжирования требований информационной безопасности // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2023. № 4. С. 159–168. DOI: 10.61260/2218-13X-2023-4-159-168.

Scientific article

TOWARD FORMALIZING THE TASK OF RANKING INFORMATION SECURITY REQUIREMENTS

✉**Yaroshenko A.Yu.**
Department of information technologies and communications of EMERCOM of Russia, Moscow, Russia
✉***alexagz@mail.ru***

Abstract. The article is devoted to the issue of requirements fulfillment aimed at ensuring information security in an organization. The main contradiction of the subject area concerned is pointed out, which consists in the presence of a huge number of different variants of requirements fulfillment in the absence of a possibility to choose their correct and optimal order. The task of requirements ranking is set and the idea of the proposed solution is described in the form of seven provisions aimed at coordinated recording of heterogeneous requirements in a single notation, and an intuitive scheme of the idea is synthesized (with all seven provisions indicated on it).

To represent the idea, the following entities are introduced: an object-organization and its elements to which requirements are imposed; generalized conditions for satisfying requirements that do not depend on the specifics of the organization; variations of sets of conditions that take into account a particular organization; basic conditions that check the presence/absence of elements of the object and the values of their parameters; algorithms of activities in the organization to satisfy the conditions; priorities of requirements and resources needed by the algorithms. It is concluded that such formalization will lead organically to the algorithmic solution of the ranking problem and, eventually, to automation.

The most suitable automated ways of solving the problem of ranking information security requirements – algorithmic application of combinatorial optimization and machine learning methods – are specified. Their high efficiency in comparison with «manual» methods used in modern information protection practice is predicted.

The novelty, theoretical and practical significance of the obtained results are noted, as well as the prospect of further research – the construction of an analytical model of requirements fulfillment, which could be the basis of an appropriate method, followed by its program implementation and conducting of necessary experiments.

Keywords: information security, requirements, ranking, formalization, automation

For citation: Yaroshenko A.Yu. Toward formalizing the task of ranking information security requirements // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2023. № 4. P. 159–168. DOI: 10.61260/2218-13X-2023-4-159-168.

Введение

Безопасности информации в современном мире отводится первостепенное место [1, 2]. Без должного внимания реализация информационных угроз может привести не только к краже конфиденциальных данных, но и к финансовым потерям, а также человеческим жертвам. Так, например, если взлом персонального компьютера в компании позволит злоумышленнику только похитить личные файлы пользователей или коммерческие секреты организации, то несанкционированный доступ к внутренней инфраструктуре промышленных объектов может стать уже причиной техногенной катастрофы.

Для противодействия такого рода угрозам в организациях (здесь и далее под организацией понимается владелец информационных ресурсов, систем и инфраструктуры, подлежащих защите. В качестве организации выступают компании, учреждения, предприятия и т.п.) создаются специальные подразделения или назначаются должностные лица, ответственные за информационную безопасность и защиту информации, к которым предъявляются соответствующие требования, исходя из Best Practices (*пер. на русс.* – Лучшие практики) [3] и научно-практических изысканий «экспертов-безопасников»

от Регуляторов (в сфере информационной безопасности в России являются следующие федеральные службы: Федеральная служба по техническому и экспертному контролю, Федеральная служба безопасности и Роскомнадзор).

Однако ситуация усложняется тем, что реализация угроз (атаки) на информационные ресурсы, системы и инфраструктуру могут происходить по качественно разным каналам [4, 5], источником которых является не только люди (например, хакеры или инсайдеры), но и природа (например, пожар или наводнение) или физические поля (например, утечки информации по техническим каналам или индустриальные помехи). То есть следует констатировать, что «защитники информации» вынуждены противодействовать угрозам абсолютно различного генеза [6–8]. Как результат – измеряемое сотнями количество требований безопасности, основанных на мерах и правилах из различных областей (например, пожарной, сетевой или социальной), которые к тому же используют различную терминологическую базу, принципы формулирования, цели, задач и т.п. [9].

Помимо того, между требованиями могут возникать различные коллизии, обусловленные их взаимопротиворечивостью, вложенностью или взаимозаменяемостью; а одно и то же требование в каждой конкретной организации может быть выполнено различными способами. Также при формировании итоговых действий по выполнению требований необходимо учитывать приоритеты последних, время их выполнения и затрачиваемые средства (например, материальные).

Вышесказанное приводит к логичному противоречию предметной области, заключающемуся в существовании огромного числа различных вариаций выполнения всех требований информационной безопасности при отсутствии способа формирования и выбора их корректной и оптимальной (как минимум – рациональной) последовательности. Для его частичного разрешения может быть поставлена задача по созданию метода ранжирования требований, заключающаяся в выборе необходимых и достаточных мероприятий в организации, с учетом определения их оптимального порядка выполнения [10–13].

Исходя из значительного числа всех предъявляемых требований информационной безопасности, их возможных коллизий и различных целевых функций (например, по критериям уменьшения общего времени их выполнения или снижения стоимости), решение задачи «вручную» даже высококлассными специалистами практически не представляется возможным, что приводит к необходимости автоматизации процесса. Для этого, в частности, требуется подход к согласованной записи всех разнородных требований в единой форме (нотации), для которой возможно применение подходящего математического аппарата. Такая формализация органически приведет к алгоритмизации решения задачи ранжирования через ее формализацию и, в конечном счете, к автоматизации.

Идея формализации

Основная идея предлагаемого инновационного подхода к согласованной записи требований информационной безопасности различного рода может быть представлена с помощью следующих положений (на сквозном примере).

Положение 1. Организация, к которой предъявляются требования, представляет собой абстракцию в виде объекта, состоящего из совокупности элементов [14]. Например, простейшая компания состоит из проходной, кабинета директора и его персонального компьютера, комнаты сотрудников и их автоматизированных рабочих мест, внутренней сети, а также серверной.

Положение 2. Каждое требование представляет собой некое условие, выполнение которого тождественно выполнению организацией требования [15]. Например, требование по контролю и управлению доступом в организацию тождественно наличию соответствующей системы (СКУД) на проходной (в общем случае – по всему периметру).

Положение 3. В каждой конкретной организации требование информационной безопасности может соответствовать нескольким наборам условий, выполнение любого из которых (то есть одного из набора) приводит и к выполнению требования [16]. Например, СКУД может быть выполнена как с помощью полностью автоматического комплекса из камеры с модулем распознаванием лиц и подключенного к нему турникета, так и с применением считывателя типа touch-memory («таблетка»), такого же турникета и визуального контроля лица или фотографии сотрудника (или посетителя) вахтером.

Положение 4. Каждое отдельное условие из набора проверяет наличие/отсутствие элемента в объекте-организации (то есть имеет структурный тип), или же значение параметра этого элемента (то есть имеет параметрический тип) [17]. То есть условие считается заданным на множестве элементов. Так, условие наличия турникета будет проверять существование элемента «турникет (на проходной)», а условие «антипаники» – силу «проламывания» турникета при выходе из организации (например, при экстренном покидании помещения или территории в случае пожара).

Положение 5. Для выполнения каждого условия предназначен соответствующий алгоритм, который адаптирован к конкретной организации и изменяет ее элементы соответствующим образом [18]. Действие алгоритма осуществляется на множестве элементов. Например, для выполнения условия «наличие турникета» предназначен алгоритм – установка турникета на проходной. Важно отметить, что поскольку все алгоритмы реализуются на едином множестве элементов, то действия одного алгоритма могут способствовать или препятствовать действиям другого; например, добавление вахтера приведет к появлению нового элемента – «потенциального инсайдера на проходной», что потребует осуществления мероприятий по противодействию этой новой угрозе (то есть выполнению условий соответствующих требований).

Положение 6. У каждого требования есть определенный приоритет выполнения, а каждый алгоритм выполнения условий расходует ресурсы – время и средства. Так, очевидно, что требования пожарной безопасности должны выполняться в более приоритетном порядке, чем экологические требования, что повлияет на порядок их выполнения [19]. Каждый же алгоритм будет иметь собственное время применения, а также (как правило) финансовые затраты, что соответствующим образом повлияет на его выбор в случае вариации наборов условий (см. положение 3). Например, СКУД в виде полностью автоматического комплекса будет дороже, чем внедрение считывателя меток и оплата работы вахтера (естественно, на коротком сроке), хотя время установки комплекса будет меньше (с учетом того, что для вахтера на проходной может потребоваться отдельная минимально необходимая инфраструктура).

Положение 7. Итоговая задача ранжирования требований может быть сведена к «подбору» такой последовательности алгоритмов, чтобы в результате все требования были выполнены, и при этом учитывались бы изначальные целевые функции ранжирования – приоритетность требований (а затем и остальных подцелей), оперативность выполнения требований или же минимизация общих расходов [20].

Схема формализации

Обобщенная схема идеи представлена на рисунке, где синим фоном обозначены исходные условия, зеленым – требуемое решение, желтым – дополнительные критерии, красным (с числами) – условные номера соответствующих положений.

Как видно из рисунка, приведенная схема полностью соответствует всем введенным положениям и по сути является некоторой формализующей базой для нивелирования разнородности всех предъявляемых требований. Так, если множество требований представляют собой достаточно обобщенные человеко-ориентированные описания, то условия не просто позволяют проверять некую организацию на наличие и диапазон параметров ее вполне конкретных элементов, но и имеют вполне строгую форму:

а) структурное условие:

$$\text{Условие}^{\text{Структурное}} \equiv \begin{bmatrix} \text{Элемент} \subset \text{Объект} \\ \text{Элемент} \not\subset \text{Объект} \end{bmatrix},$$

которое проверяет принадлежность Элемента к множеству элементов Объекта;

б) параметрическое условие:

$$\text{Условие}^{\text{Параметрическое}} \equiv \text{Элемент}^{\text{Параметр}} \in \text{Диапазон},$$

которое проверяет принадлежность значения Параметра для Элемента заданному Диапазону значений.

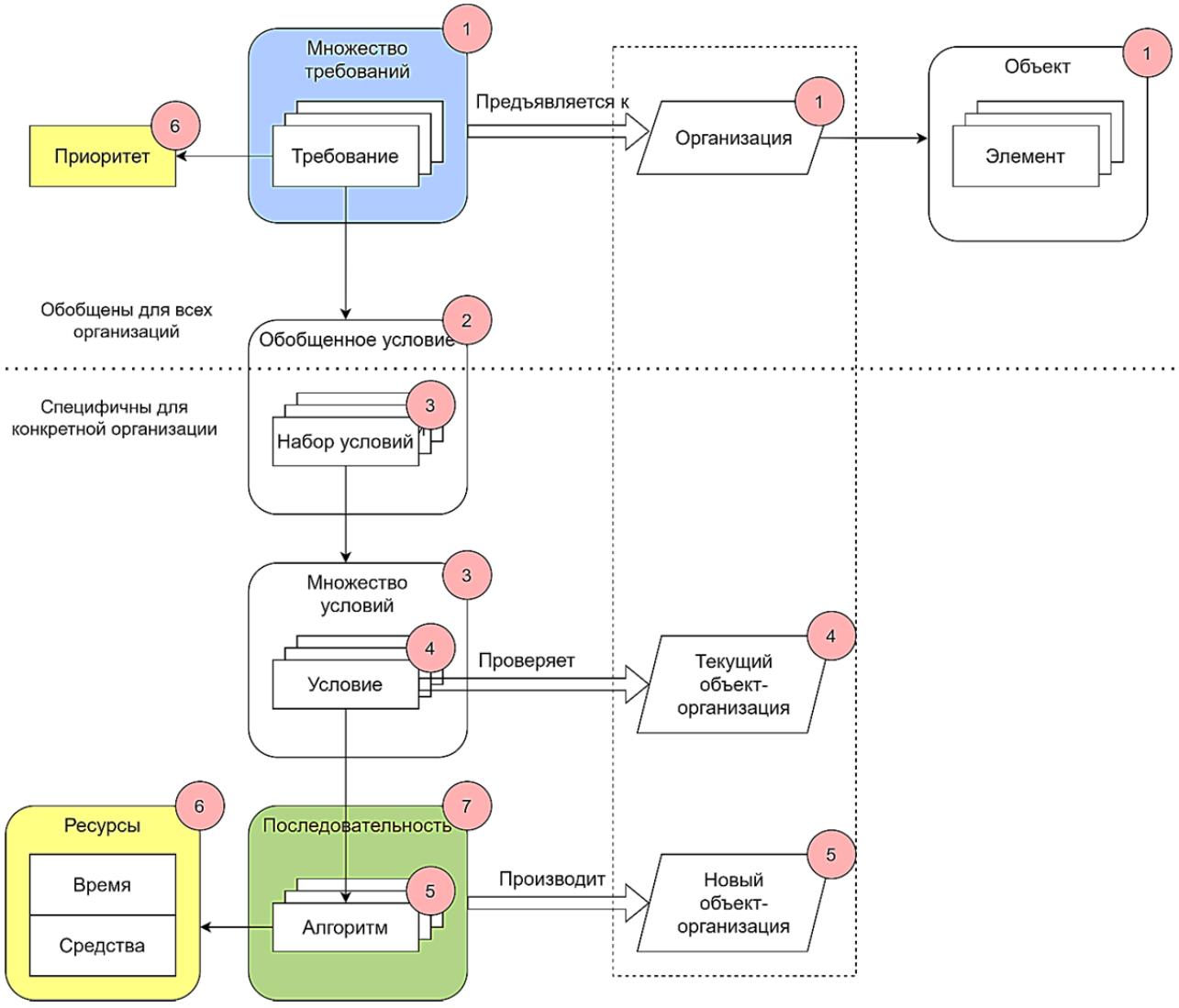

Рис. **Обобщенная схема предлагаемой идеи ранжирования требований**

Тогда способ выполнения всех требований заключается в применении к объекту-организации алгоритмов (соответствующих условиям), которые изменяют его элементы:

$$\begin{cases} \text{Алгоритм}^{\text{Условие}} \equiv \text{Объект} \to \text{Объект}' \\ \text{Условие}(\text{Объект}) = \text{Не выполняется}, \\ \text{Условие}(\text{Объект}') = \text{Выполняется} \end{cases}$$

где Объект – множество элементов исходного объекта-организации; Объект′ – множество элементов объекта-организации после применения алгоритма; Условие (Объект) – проверка выполнения условия для элементов объекта-организации.

Естественно, возможны ситуации, когда применение алгоритма для выполнения одного условия меняет множество элементов так, что другое условие перестает выполняться, что и подчёркивает сложность «ручного» ранжирования алгоритмов. Выбор же конкретной последовательности алгоритмов (естественно, в случае альтернативных вариантов) позволит учесть различные оптимизационные критерии целевых функций.

Одним из наиболее подходящих автоматизированных (например, за счет программной реализации) способов решения задачи ранжирования требований информационной безопасности является алгоритмическое применение комбинаторной оптимизации [21, 22], которая как раз и направлена на поиск «условно-идеальной» последовательности в конечном их множестве. Другим перспективным автоматизированным решением является применение методов машинного обучения [23–26]), которые, безусловно, имеют множество преимуществ по сравнению с «ручными» способами, применяемыми в современной практике.

Заключение

Признаком инновационности исследования, результаты которого изложены выше, безусловно, является синтезированная обобщенная схема ранжирования требований, сводящая их к единому представлению. Это представление, использующее такие сущности, как объект-организация и его элементы, вариации наборов и базовые условия, алгоритмы удовлетворения условиям, приоритеты требований и ресурсы, вводится в научный оборот впервые.

Его теоретическая значимость обусловлена аксиоматическим характером семи положений о согласованной записи требований информационной безопасности и состоит в создании формализующей базы для нивелирования разнородности всех предъявляемых требований.

Практическая значимость полученной схемы состоит в том, что запись способа, а также структурных и параметрических условий выполнения требований доведена до строгой математической формы. Такая запись позволяет проводить их (условий) исследование с использованием математических методов.

Естественно, возможны ситуации, когда применение алгоритма для выполнения одного условия меняет множество элементов так, что другое условие перестает выполняться, что и подчёркивает сложность «ручного» ранжирования алгоритмов. Выбор же конкретной последовательности алгоритмов (естественно, в случае альтернативных вариантов) позволит учесть различные оптимизационные критерии целевых функций.

Продолжением исследования должно стать построение аналитической модели ранжирования требований, которая может лечь в основу соответствующего метода на основе комбинаторной оптимизации и/или машинного обучения, за которым последует его программная реализация и проведение необходимых экспериментов.

Список источников

1. Цифровые технологии и проблемы информационной безопасности / Т.И. Абдуллин [и др.]: монография. СПб.: СПГЭУ, 2021. 163 с.

2. Защита информации в компьютерных системах / М.В. Буйневич [и др.]: монография. СПб.: СПГЭУ, 2017. 163 с.

3. Ghadeer D., Jaafar H., Vorobeva A.A. Security in kubernetes: best practices and security analysis // Journal of the Ural Federal District. Information Security. 2022. № 2 (44). С. 63–69.

4. Буйневич М.В., Покусов В.В., Израилов К.Е. Эффекты взаимодействия обеспечивающих служб предприятия информационного сервиса (на примере службы пожарной безопасности) // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2018. № 4. С. 48–55.

5. Основные принципы проектирования архитектуры современных систем защиты / М.В. Буйневич [и др.] // Национальная безопасность и стратегическое планирование. 2020. № 3 (31). С. 51–58. DOI: 10.37468/2307-1400-2020-3-51-58. EDN VPRMIB.

6. Максимова Е.А. Методы выявления и идентификации источников деструктивных воздействий инфраструктурного генеза // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2022. № 2. С. 86–99.

7. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема // Вопросы кибербезопасности. 2023. № 3 (55). С. 90–100. DOI: 10.21681/2311-3456-2023-3-90-100.

8. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 2. Алгоритм, модель и эксперимент // Вопросы кибербезопасности. 2023. № 4 (56). С. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93.

9. Ярошенко А.Ю. Формирование требований к организациям для противодействия атакам на информационные ресурсы методами социальной инженерии // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сб. науч. статей X Междунар. науч.-техн. и науч.-метод. конф. СПб., 2021. Т. 2. С. 452–456.

10. Ярошенко А.Ю. Ранжирование требований информационной безопасности для высокоприоритетных объектов организационной системы защиты // Информатизация и связь. 2022. № 5. С. 30–41.

11. Ярошенко А.Ю. Предпосылки к необходимости непрерывного ранжирования требований пожарной безопасности // Национальная безопасность и стратегическое планирование. 2021. № 3 (35). С. 100–105. DOI: 10.37468/2307-1400-2021-3-100-105. EDN LQIIKJ.

12. Буйневич М.В., Ахунова Д.Г., Ярошенко А.Ю. Комплексный метод решения типовой задачи риск-менеджмента в инфологической среде (на примере ранжирования требований пожарной безопасности). Часть 1 // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2020. № 3. С. 88–99.

13. Буйневич М.В., Ахунова Д.Г., Ярошенко А.Ю. Комплексный метод решения типовой задачи риск-менеджмента в инфологической среде (на примере ранжирования требований пожарной безопасности). Часть 2 // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2020. № 4. С. 78–89.

14. Лесюк Е.А., Уркинеев А.В. Модель организации технического обслуживания распределенных элементов сложного технического объекта // Качество. Инновации. Образование. 2016. № 7 (134). С. 39–43.

15. Требования к электрооборудованию, предназначенного для работы в условиях Арктики / А.В. Крымов [и др.] // Арктика: инновационные технологии, кадры, туризм. 2020. № 1 (2). С. 414–419.

16. Сошников А.В. Выбор рациональной очередности выполнения работ на технологической установке с учетом требования по сокращению времени переналадок // Наука и бизнес: пути развития. 2020. № 1 (103). С. 55–59.

17. Куликов Е.В., Бенамгхар А., Скоморохов Г.И. Системная формализация структурно-параметрического описания функционального центра технических систем // Компьютерные технологии автоматизированного проектирования систем машиностроения и аэрокосмической техники: труды Рос. конф., посвящ. 105-летию со дня рождения основателя КБХА С.А. Косберга. Воронеж, 2008. С. 203–207.

18. Разработка алгоритма выполнения требований по квотированию выбросов загрязняющих веществ в атмосферный воздух / О.А. Киселева [и др.] // Энергетик. 2023. № 3. С. 39–41.

19. Анализ требований к современным системам безопасности и системам пожарной безопасности защищаемых объектов / А.С. Кривобородов [и др.] // Пожарная безопасность: проблемы и перспективы. 2018. Т. 1. № 9. С. 477–479.

20. Брыкова Е.И. Основные принципы построения безопасных операционных систем // Вестник Астраханского государственного технического университета. Сер.: Управление, вычислительная техника и информатика. 2013. № 2. С. 52–57.

21. Левин М.Ш. О реконфигурации решений в комбинаторной оптимизации // Информационные процессы. 2016. Т. 16. № 4. С. 414–429.

22. Болотин С.А., Нефедова В.К. Комбинаторная оптимизация в программах управления проектами // Известия высших учебных заведений. Строительство. 2003. № 6 (534). С. 47–51.

23. Израилов К.Е., Ярошенко А.Ю. Исследование возможностей машинного обучения для автоматического ранжирования уязвимостей по их текстовому описанию // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): сб. науч. статей XII Междунар. науч.-техн. и науч.-метод. конф. СПб., 2023. Т. 1. С. 586–590.

24. Израилов К.Е. Концепция генетической декомпиляции машинного кода телекоммуникационных устройств // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 10–17. DOI: 10.31854/1813-324X-2021-7-4-95-109.

25. Identifying characteristics of software vulnerabilities by their textual description using machine learning / K.E. Izrailov [et al.]: World Automation Congress. Taiwan, Taipei 2021. P. 186–192. DOI: 10.23919/WAC50355.2021.9559470.

26. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. P. 1335. DOI: 10.3390/s22041335.

References

1. Cifrovye tekhnologii i problemy informacionnoj bezopasnosti / T.I. Abdullin [i dr.]: monografiya. SPb.: SPGEU, 2021. 163 s.

2. Zashchita informacii v komp'yuternyh sistemah / M.V. Bujnevich [i dr.]: monografiya. SPb.: SPGEU, 2017. 163 s.

3. Ghadeer D., Jaafar H., Vorobeva A.A. Security in kubernetes: best practices and security analysis // Journal of the Ural Federal District. Information Security. 2022. № 2 (44). S. 63–69.

4. Bujnevich M.V., Pokusov V.V., Izrailov K.E. Effekty vzaimodejstviya obespechivayushchih sluzhb predpriyatiya informacionnogo servisa (na primere sluzhby pozharnoj bezopasnosti) // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MCHS Rossii». 2018. № 4. S. 48–55.

5. Osnovnye principy proektirovaniya arhitektury sovremennyh sistem zashchity / M.V. Bujnevich [i dr.] // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2020. № 3 (31). S. 51–58. DOI: 10.37468/2307-1400-2020-3-51-58. EDN VPRMIB.

6. Maksimova E.A. Metody vyyavleniya i identifikacii istochnikov destruktivnyh vozdejstvij infrastrukturnogo geneza // Elektronnyj setevoj politematicheskij zhurnal «Nauchnye trudy KubGTU». 2022. № 2. S. 86–99.

7. Izrailov K.E., Bujnevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnye ob"ekty na osnove informacii sostoyaniya. CHast' 1. Predposylki i skhema // Voprosy kiberbezopasnosti. 2023. № 3 (55). S. 90–100. DOI: 10.21681/2311-3456-2023-3-90-100.

8. Izrailov K.E., Bujnevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnye ob"ekty na osnove informacii sostoyaniya. Chast' 2. Algoritm, model' i eksperiment // Voprosy kiberbezopasnosti. 2023. № 4 (56). S. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93.

9. Yaroshenko A.Yu. Formirovanie trebovanij k organizaciyam dlya protivodejstviya atakam na informacionnye resursy metodami social'noj inzhenerii // Aktual'nye problemy

infotelekommunikacij v nauke i obrazovanii: sb. nauch. statej X Mezhdunar. nauch.-tekhn. i nauch.-metod. konf. SPb., 2021. T. 2. S. 452–456.

10. Yaroshenko A.Yu. Ranzhirovanie trebovanij informacionnoj bezopasnosti dlya vysokoprioritetnyh ob"ektov organizacionnoj sistemy zashchity // Informatizaciya i svyaz'. 2022. № 5. S. 30–41.

11. Yaroshenko A.Yu. Predposylki k neobhodimosti nepreryvnogo ranzhirovaniya trebovanij pozharnoj bezopasnosti // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2021. № 3 (35). S. 100–105. DOI: 10.37468/2307-1400-2021-3-100-105. EDN LQIIKJ.

12. Bujnevich M.V., Ahunova D.G., Yaroshenko A.Yu. Kompleksnyj metod resheniya tipovoj zadachi risk-menedzhmenta v infologicheskoj srede (na primere ranzhirovaniya trebovanij pozharnoj bezopasnosti). Chast' 1 // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MCHS Rossii». 2020. № 3. S. 88–99.

13. Bujnevich M.V., Ahunova D.G., Yaroshenko A.Yu. Kompleksnyj metod resheniya tipovoj zadachi risk-menedzhmenta v infologicheskoj srede (na primere ranzhirovaniya trebovanij pozharnoj bezopasnosti). CHast' 2 // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MCHS Rossii». 2020. № 4. S. 78–89.

14. Lesyuk E.A., Urkineev A.V. Model' organizacii tekhnicheskogo obsluzhivaniya raspredelennyh elementov slozhnogo tekhnicheskogo ob"ekta // Kachestvo. Innovacii. Obrazovanie. 2016. № 7 (134). S. 39–43.

15. Trebovaniya k elektrooborudovaniyu, prednaznachennogo dlya raboty v usloviyah Arktiki / A.V. Krymov [i dr.] // Arktika: innovacionnye tekhnologii, kadry, turizm. 2020. № 1 (2). S. 414–419.

16. Soshnikov A.V. Vybor racional'noj ocherednosti vypolneniya rabot na tekhnologicheskoj ustanovke s uchetom trebovaniya po sokrashcheniyu vremeni perenaladok // Nauka i biznes: puti razvitiya. 2020. № 1 (103). S. 55–59.

17. Kulikov E.V., Benamghar A., Skomorohov G.I. Sistemnaya formalizaciya strukturno-parametricheskogo opisaniya funkcional'nogo centra tekhnicheskih sistem // Komp'yuternye tekhnologii avtomatizirovannogo proektirovaniya sistem mashinostroeniya i aerokosmicheskoj tekhniki: trudy Ros. konf., posvyashch. 105-letiyu so dnya rozhdeniya osnovatelya KBHA S.A. Kosberga. Voronezh, 2008. S. 203–207.

18. Razrabotka algoritma vypolneniya trebovanij po kvotirovaniyu vybrosov zagryaznyayushchih veshchestv v atmosfernyj vozduh / O.A. Kiseleva [i dr.] // Energetik. 2023. № 3. S. 39–41.

19. Analiz trebovanij k sovremennym sistemam bezopasnosti i sistemam pozharnoj bezopasnosti zashchishchaemyh ob"ektov / A.S. Krivoborodov [i dr.] // Pozharnaya bezopasnost': problemy i perspektivy. 2018. T. 1. № 9. S. 477–479.

20. Brykova E.I. Osnovnye principy postroeniya bezopasnyh operacionnyh sistem // Vestnik Astrahanskogo gosudarstvennogo tekhnicheskogo universiteta. Ser.: Upravlenie, vychislitel'naya tekhnika i informatika. 2013. № 2. S. 52–57.

21. Levin M.Sh. O rekonfiguracii reshenij v kombinatornoj optimizacii // Informacionnye processy. 2016. T. 16. № 4. S. 414–429.

22. Bolotin S.A., Nefedova V.K. Kombinatornaya optimizaciya v programmah upravleniya proektami // Izvestiya vysshih uchebnyh zavedenij. Stroitel'stvo. 2003. № 6 (534). S. 47–51.

23. Izrailov K.E., Yaroshenko A.Yu. Issledovanie vozmozhnostej mashinnogo obucheniya dlya avtomaticheskogo ranzhirovaniya uyazvimostej po ih tekstovomu opisaniyu // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2023): sb. nauch. statej XII Mezhdunar. nauch.-tekhn. i nauch.-metod. konf. SPb., 2023. T. 1. S. 586–590.

24. Izrailov K.E. Koncepciya geneticheskoj dekompilyacii mashinnogo koda telekommunikacionnyh ustrojstv // Trudy uchebnyh zavedenij svyazi. 2021. T. 7. № 4. S. 10–17. DOI: 10.31854/1813-324X-2021-7-4-95-109.

25. Identifying characteristics of software vulnerabilities by their textual description using machine learning / K.E. Izrailov [et al.]: World Automation Congress. Taiwan, Taipei 2021. P. 186–192. DOI: 10.23919/WAC50355.2021.9559470.

26. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. P. 1335. DOI: 10.3390/s22041335.

Информация о статье:
Статья поступила в редакцию: 27.10.2023; одобрена после рецензирования: 10.11.2023; принята к публикации: 25.11.2023
The information about article:
The article was submitted to the editorial office: 27.10.2023; approved after review: 10.11.2023; accepted for publication: 25.11.2023

Информация об авторах:
Ярошенко Александр Юрьевич, начальник отдела организации защиты информации Департамента информационных технологий и связи МЧС России (121357, Москва, ул. Ватутина, д. 1), e-mail: alexagz@mail.ru, SPIN-код: 8826-5683,

Information about the authors:
Yaroshenko Alexander Yu., head of the information security organization department of the information technology and communications Department of EMERCOM of Russia (121357, Moscow, Vatutina str., 1), e-mail: alexagz@mail.ru, SPIN: 8826-5683