УДК 004.89
doi:10.31799/1684-8853-2022-4-29-43

Научные статьи
Articles

Исследование путей и способов повышения результативности выявления компьютерных атак на объекты критической информационной инфраструктуры

В. Н. Кузьмин[a], *доктор воен. наук, профессор, orcid.org/0000-0002-6411-4336, vka@mil.ru*
А. Б. Менисов[a], *канд. техн. наук, докторант, orcid.org/0000-0002-9955-2694*
[a]*Военно-космическая академия им. А. Ф. Можайского, Ждановская наб., 13, Санкт-Петербург, 197198, РФ*

Введение: *в эпоху информационных технологий практически все организации сталкиваются с широким спектром автоматизированных и быстро распространяющихся угроз безопасности информации. Это обусловлено не только растущей сложностью, разнообразием и масштабом цифровизации, но и увеличением угроз и областей их возможной реализации.* ***Цель:*** *сравнить возможные пути повышения результативности подходов к выявлению компьютерных атак на объекты критической информационной инфраструктуры: обнаружение редкого события, аномалии и новизны функционирования объектов критической информационной инфраструктуры.* ***Результаты:*** *принцип работы предлагаемого (результативного) подхода к обнаружению компьютерных атак заключается в выявлении и отделении аномалий от нормального функционирования объектов с использованием концепции динамического изменения меток для переменного класса с течением времени. Динамическое обнаружение новизны сравнивается с другими подходами по показателю F1-меры. Для данных SWaT, который представляет собой макет объекта критической информационной инфраструктуры — автоматизированной системы управления, было определено, что количество выявленных атак с использованием предложенного подхода увеличилось на 7 %.* ***Практическая значимость:*** *результаты исследований показали снижение риска проведения (развития) компьютерной атаки на объектах критической информационной инфраструктуры. Возможное целевое применение подхода динамического обнаружения новизны заключается в оптимизации средств защиты информации на объектах критической информационной инфраструктуры, а также интеграции предложенного подхода в систему информационной безопасности как интеллектуального детектора.*

Ключевые слова *— информационная безопасность, технологии искусственного интеллекта, критическая информационная инфраструктура, нейронные сети.*

Для цитирования: Кузьмин В. Н., Менисов А. Б. Исследование путей и способов повышения результативности выявления компьютерных атак на объекты критической информационной инфраструктуры. *Информационно-управляющие системы*, 2022, № 4, с. 29–43. doi:10.31799/1684-8853-2022-4-29-43
For citation: Kuzmin V. N., Menisov A. B. A study of ways and solutions to increase the efficiency of detecting computer attacks on the objects of critical information infrastructure. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 4, pp. 29–43 (In Russian). doi:10.31799/1684-8853-2022-4-29-43

Введение

Современный мир переживает период бурного развития и трансформации. В этих условиях достижение цели обеспечения информационной безопасности объектов критической информационной инфраструктуры (КИИ; Critical Information Infrastructure, CII) может осуществляться путем реализации государственной политики, прежде всего в части обоснования и совершенствования комплекса мер, направленных на решение проблемы защиты объектов жизнеобеспечения населения, организаций оборонно-промышленного, атомного энергопромышленного, ядерного оружейного, химического, топливно-энергетического комплексов страны и объектов транспортной инфраструктуры от компьютерных атак.

Среди мер по обеспечению безопасного функционирования объектов КИИ выделяют регламентацию правил и процедур реагирования на компьютерные атаки, их выявление и анализ, а также защиту информации и информирование регуляторов, устранение последствий и принятие мер по недопущению повторного возникновения.

Критическая информационная инфраструктура — это сложная система, элементы которой используют различные программно-аппаратные компоненты при функционировании. Включение Интернета вещей (IoT) в КИИ открывает новые возможности злоумышленникам использовать уязвимости системы для проведения компьютерных атак [1].

За десятилетие, прошедшее с момента компьютерной атаки Stuxnet (2010 г.), увеличилось не только количество целевых компьютерных атак (далее — атак) на объекты КИИ, но и их разнообразие, а также усложнились технологии проведения [2]. На основе выполненного анализа в табл. 1 и 2 отображены действия злоумышленников известных целевых атак [3–12] с выделением соответствующих последствий.

■ ***Таблица 1.*** Сравнение атак на объекты КИИ
■ ***Table 1.*** Comparison of attacks on CII objects

Действие злоумышленников	Атака на объекты КИИ						
	Stuxnet	Havex	Black Energy	Немецкий завод	Duqu2.0	Crash Override	TRISIS
Доступ в Интернет	×	√	√	√	√	√	?
Аудит сети	√	√	√	?	√	√	?
Несанкционированный доступ	√	√	√	?	√	√	√
Отображение производственного процесса	√	√	×	?	×	√	√
Взломанный хост	√	√	√	√	√	√	√
Фальсифицированные данные	√	×	×	?	×	√	×
Несанкционированное выполнение программ	√	√	√	?	√	√	√
Сбор учетных данных	×	×	√	√	×	√	×
Вредоносная прошивка	√	×	×	?	×	√	√

× — не свойственно для атаки;
√ — действия, характерные для атаки;
? — данные отсутствуют.

■ ***Таблица 2.*** Последствия проведения атак на объекты КИИ
■ ***Table 2.*** Consequences of attacks on CII objects

Действие злоумышленников	Последствие
Доступ в Интернет	1. Возможность получать данные из сети через хосты с подключением к Интернету 2. Возможность загружать программное обеспечение
Аудит сети	1. Анализ хостов в сети для будущих атак 2. Предоставление информации о сети
Несанкционированный доступ	1. Утечка данных 2. Загрузка дополнительных исполняемых файлов
Отображение производственного процесса	1. Предоставление информации о цели 2. Возможность разработать целевое вредоносное программное обеспечение для этого процесса
Взломанный хост-компьютер	1. Предоставление информации о системе. Злоумышленники могут создавать профили пользователей системы и определять шаблоны, которые можно использовать для дальнейшего проникновения в сеть 2. Идентификация активов посредством анализа журналов и мониторинга сети
Фальсифицированные данные	1. Потеря доверия к сети, устройству или программному обеспечению 2. Изменение данных 3. Физический ущерб
Несанкционированное выполнение программ	Предоставление дополнительных возможностей по действию в системе и позволение в ней закрепиться
Сбор учетных данных	Предоставление подлинного, замаскированного доступа к службам
Вредоносная прошивка	1. Возвращение оператору фальсифицированных и недостоверных сведений 2. Физический урон

Перечисленные действия злоумышленников вызывают негативные последствия для объектов КИИ. Так, устройства, подключенные к Интернету, позволяют проводить удаленное взаимодействие, хищение данных и загрузку дополнительного программного обеспечения. Каждая из проанализированных атак манипулировала устройством, подключенным к Интернету, за исключением Stuxnet, которая была способна выполнять сложные автоматизированные действия для достижения своих целей.

Несанкционированный доступ к сети — единственный общий элемент для всех атак — заключается в возможности взаимодействовать с другими сетевыми устройствами для получения дополнительных привилегий доступа или дополнительной информации о цели. Обычно несанкционированный доступ выполняется, когда противник уже проник в систему. Важным шагом является снятие образа устройств после их обнаружения. Например, Stuxnet и TRISIS идентифицировали целевые устройства по результатам несанкционированного сканирования сети.

В большинстве атак злоумышленники демонстрируют реализацию угроз, которую можно разделить на следующие этапы: сбор информации, получение первоначального доступа, внедрение и использование вредоносного кода, закрепление в системе и сети, управление вредоносным кодом и компонентом, повышение привилегий, сокрытие действий, получение доступа к другим компонентам, сбор и вывод информации и неправомерный доступ или воздействие.

Существует достаточное количество исследований по определению возникновения угроз безопасности информации с помощью традиционных средств [13–16]. Стоит указать, что ведущие организации в области информационной безопасности [17] отмечают растущее использование возможностей технологий искусственного интеллекта в текущем ландшафте угроз:

— расширение существующих угроз, которое связано со сложными компьютерными атаками на большое количество потенциальных целей и низкой стоимостью атак;

— введение новых угроз, связанных с задачами, которые были бы невыполнимы для человека;

— изменение типичного характера угроз, которое включает в себя новые атрибуты автоматизированных, высокоэффективных, трудно определяемых и крупномасштабных атак в ландшафте угроз.

Для описания способов реализации угроз наиболее хорошо зарекомендовали себя следующие подходы к представлению угроз безопасности информации:

— деревья атак [18], предложенные в 1999 г. Брюсом Шнайером;

— цепочки Kill Chain [19], разработанные в 2011 г. компанией Lockheed Martin для обнаружения нарушителей на протяжении всего жизненного цикла компьютерной атаки;

— набор тактик и техник поведения нарушителей MITRE ATT & CK [20];

— модель жизненного цикла компьютерной атаки [21], в которой особое внимание уделяется моделированию APT-атак и демонстрируется повторяющийся характер нарушителей для дальнейшего повышения привилегий.

Таким образом, система защиты имеет исходные данные о предыдущих состояниях объекта КИИ, а для изменения состояния можно использовать следующую модель, в которой выделены основные параметры, влияющие на функционирование объектов КИИ:

$$\overline{f_k} = \overline{f_k}\left\{s^a_{i_1};\ s^{\tilde{a}}_{i_2};\ s^p_{i_3};\ s^{\tilde{p}}_{i_4};\ g_{\omega_k};\ t_k;\ d_j;\ l_s;\ z_g;\ r_k\right\},$$

где k — номер конкретного объекта КИИ, $k = 1, \ldots, K$; i — номер признака, $i = 1, \ldots, N$, т. е. результата действия злоумышленника; $s^a_{i_1}$, $s^a_{i_2}$ — данные наблюдения предыдущих состояний объекта КИИ, $i_1 = 1, \ldots, m_1$, $i_2 = m_1 + 1, m_2$; $s^p_{i_3}$, $s^{\tilde{p}}_{i_4}$ — данные текущего контроля объекта КИИ, $i_3 = m_2 + 1, m_3$, $i_4 = m_3 + 1, m_4 = m$; $\sim$ — знак, указывающий на признаки, которые подвержены влиянию данной совокупности внешних условий; g_{ω_k} — совокупность внешних условий, $\omega_k = 1, \ldots, \Omega_k$; t_k — условная координата времени, показывающая полноту информации о k-м объекте КИИ; d_j — класс атаки на объект КИИ, $j = 1, \ldots, N$; l_s — методы защиты объекта КИИ, $s = 1, \ldots, S$; z_g — последующие состояния k-го объекта КИИ, $g = 1, \ldots, G$; r_k — помеха, искажающая действительное состояние k-го объекта КИИ.

Формализованная постановка задачи исследования

Процесс обеспечения безопасности объектов КИИ является сложным циклическим процессом, включающим в себя сбор и обработку данных различных систем, определение состояния объекта КИИ, выбор стратегии защиты и проведение защитных мер. Управление процессом обеспечения безопасности функционирования объектов КИИ может происходить с участием и без участия персонала.

Процесс обеспечения безопасности может состоять из различного числа циклов — от двух до многих десятков. Поэтому в каждом цикле проводится оценка и коррекция управляющего воздействия. Сущность обеспечения защиты

объектов КИИ состоит в следующем. После того как установлены специфические особенности функционирования, можно переходить к построению прогноза и исхода защиты объекта КИИ.

Пусть известна модель защищаемого объекта КИИ $\bar{f}_k$. Пусть l_s – защитные воздействия (методы), которые могут объект КИИ $\bar{f}_k$ из состояния z_{g_i} перевести в новое состояние $z_{g'}(g, g', g'' = 0, ..., G; g \neq g' \neq g'')$, и пусть $p(z_{g_j} \to z_{g'})_{l_s}$ – вероятность такого перехода. Обозначим через e_{s_j} меру результативности l_s-го мероприятия защиты объекта КИИ. Тогда задачу нахождения оптимальной совокупности защитных мер можно сформулировать следующим образом.

Необходимо найти такую совокупность защитных воздействий l_s^*, чтобы мера их результативности была максимальна. В этом случае мера результативности

$$e_{s_j}(z_{g_j} \to z_{g'})_{l_s} = p(d_j)_{z_g} p(z_{g_j} \to z_{g'})_{l_s},$$

где $p(d_j)_{z_g}$ – вероятность проведения атаки, а максимальное значение меры результативности, или оптимальная защита объекта КИИ для $(z_{g_j} \to z_{g'})_{l_s}$, достигается при

$$e^*_{s_j} = \min_{l_s} e_{s_j}(z_{g_j} \to z_{g'})_{l_s}.$$

Это определение действует для тех пар $(z_{g_j} \to z_{g'})_{l_s}$, для которых справедливо утверждение о том, что $z_{g'}$ лучше, чем z_{g_j}.

Предположим, что общая результативность защитных мер e_j является аддитивной функцией, состоящей из e_{s_j}. Тогда для определения оптимальной совокупности защитных воздействий можно сформулировать ограничение исследования: оптимальная совокупность защитных воздействий обладает тем свойством, что, каково бы ни было первоначальное защитное воздействие l_s при состоянии защищенности объекта КИИ z_{g_j}, последующие защитные воздействия должны быть оптимальны относительно первоначального защитного воздействия. Исходя из этого принципа максимальную результативность защитных воздействий можно получить в следующем виде:

$$e_j = \min_{l_s} \sum | e_{s_j}(z_{g_j} \to z_{g'})_{l_s} + e_{s_j}(z_{g'} \to z_{g''})_{l_s} |.$$

Таким образом, выбор оптимальной совокупности защитных воздействий начинается с выявления нарушения функционирования объектов (атак на объекты) КИИ.

Пути повышения результативности выявления компьютерных атак на объекты КИИ

В то время как проблемы безопасности объектов КИИ активно рассматриваются в научных кругах и ИТ-сообществе, все решения являются ограниченными для различных условий. Атаки на объекты КИИ в основном остаются слабо идентифицируемыми для традиционных средств информационной безопасности, таких как системы обнаружения вторжений (Intrusion Detection System, IDS) и антивирусные программы. Кроме того, протоколы, используемые системами контроля объектов КИИ (например, Modbus [22] или DNP3 [23] и стандарты IEC [24]), не защищены должным образом традиционными IDS. Следовательно, для защиты объектов КИИ необходимо разрабатывать надежные механизмы безопасности.

В литературе использовались различные подходы для разработки IDS, в том числе на основе методов машинного обучения [25–27]. Большинство этих методов используют доступные данные для разработки модели, которая демонстрирует нормальное поведение объекта КИИ, а затем идентифицирует все различные варианты поведения как ненормальные. Поскольку эти модели обучены только конкретным типам атак, они не могут обнаруживать скрытые или новые типы атак [28]. В последние годы результаты исследований в различных областях внесли свой вклад в решение ряда связанных проблем, основными сущностями которых являются редкие события, аномалии и новизна.

Таким образом, в качестве путей повышения результативности выявления компьютерных атак на объекты КИИ будем рассматривать обнаружение редкого события, аномалии функционирования и новизны функционирования.

Обнаружение редкого события

Почти все работы, в которых используется термин *редкое событие*, представляют время наблюдения за характеристиками функционирования объектов КИИ как общую характеристику. То есть данные могут быть разделены по часовым интервалам или другим фиксированным значениям.

В ранее описанных задачах цель состоит в предсказании наступления редкого события за ограниченный промежуток времени. Основной характеристикой обучения модели выявления атак на объекты КИИ как редкого события с точки зрения классификации является то, что функционирование объекта КИИ представляет собой временной ряд. Цель состоит в том, чтобы классифицировать новые данные о состоянии как

редкие (R, когда произошло редкое событие) или нормальные (N, когда не произошло никакого события), используя ранее обученную модель. Этот подход известен в машинном обучении как классификация временных рядов [29].

Вместе с тем из-за временной природы проблемы в литературе можно найти два различных подхода к обнаружению редких событий.

В первом подходе рассматривается полноразмерная классификация временных рядов. Например, в работе [30] представлен подход к определению неисправности жесткого диска в течение фиксированного периода времени. Авторы формируют модель машинного обучения, используя записанные на жестком диске сенсорные измерения в разное время. Затем, учитывая новые данные датчиков жесткого диска, обнаруживают сбой — редкое событие.

Другой подход к определению редких событий заключается в том, чтобы классифицировать новые наблюдения (временные ряды) как можно раньше, предпочтительно до того, как будет доступен полный временной ряд. Этот подход известен как ранняя классификация временных рядов.

Общий процесс классификации представлен на рис. 1.

В большинстве задач, направленных на определение состояния функционирования объектов КИИ как редкое событие, стоит отметить несбалансированное распределение классов. Таким образом, классификация редких событий может быть формализована как задача классификации несбалансированных временных рядов. В частном случае редкое событие определено как $P(R) << P(N)$.

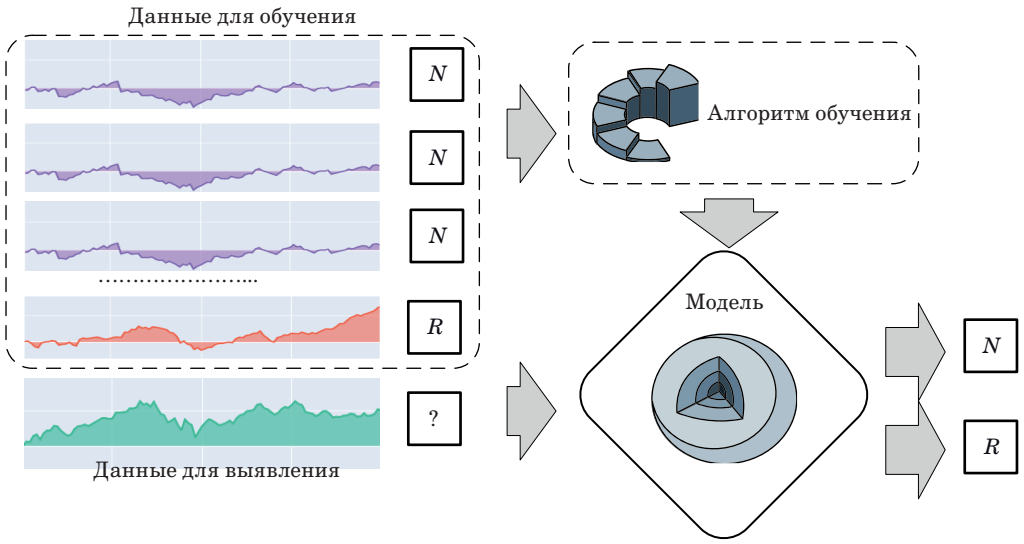
Временной ряд — это упорядоченная совокупность результатов наблюдений пар (временная метка, значение) фиксированной длины m:

$$z_g = \left\{\left(t_1, \tilde{s_1^p}\right), \ldots, \left(t_i, \tilde{s_i^p}\right), \ldots, \left(t_m, \tilde{s_m^p}\right)\right\},$$

где t — условная координата времени, показывающая полноту информации об объекте КИИ, а $\tilde{s_1^p}$ — характеристика функционирования объекта КИИ.

Для выявления редкого события необходим набор для обучения $\{(z_{g1}, y_1), \ldots, (z_{gn}, y_n)\}$. Цель — построить модель-классификатор, которая способна предсказать метку класса новых временных рядов.

Однако несмотря на то, что выявление редкого события в качестве ключевого компонента рассматривает оценку состояния в определенный момент времени, в некоторых решениях данные преобразуются без учета этой характеристики. Например, в работе [31] данные состоят из нескольких измерений датчиков жесткого диска с различными временными интервалами. Поэтому для одного и того же устройства доступно множество показаний одних и тех же датчиков. Однако авторы не учитывали порядок, в котором были записаны измерения, и, учитывая новые неупорядоченные измерения на жестком диске, модель классифицировала диск как неисправный или нормальный. Следовательно, временная природа данных использовалась не совсем корректно. Таким образом, изложенный подход рассматривает проблему как задачу нестационарной несбалансированной классификации, аналогичную тем, которые встречаются в решениях обнаружения аномалий.



■ ***Рис. 1.*** Представление задачи классификации временных рядов
■ ***Fig. 1.*** Representation of the task of classifying time series

Обнаружение аномалий

Большинство проблем, описывающих поиск аномалий (A), не имеют временной природы (рис. 2).

В алгоритме обучения обнаружению аномалий аномальные экземпляры данных редки из-за несбалансированного распределения между нормальными и аномальными классами [32]. Поэтому проблема может быть формально описана как несбалансированная классификация. Что касается распределения вероятностей аномального класса, то $P(A) << P(N)$.

Формально функционирование объекта КИИ определяется как $s^{\tilde{p}} = \left(s^{\tilde{p}}_{i_1}, ..., s^{\tilde{p}}_{i_m}\right)$. Учитывая, что существует набор данных $z_g = \left\{\left(s^{\tilde{p}}_{i_1}, y_1\right), ..., \left(s^{\tilde{p}}_{i_m}, y_m\right)\right\}$, в котором y представляет метку класса (нормальное функционирование или аномалия) соответствующего экземпляра данных, необходимо обучить модель-классификатор, способный предсказать метку класса любого нового экземпляра как можно точнее.

Обнаружение новизны

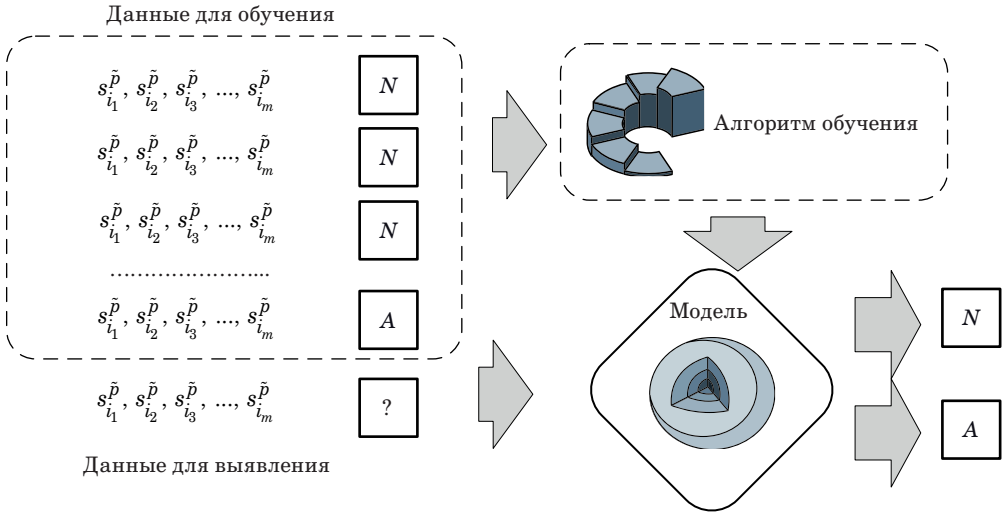
В большинстве работ, направленных на поиск новизны, модель обучают с использованием набора данных, содержащего только один класс. Например, в работах [33, 34] действия системы классифицируются IDS как новые или нормальные. Новый экземпляр соответствует неподдерживаемому или неожиданному действию системы. Для обучения модели используются только обычные действия в системе, собранные в защищенной среде. Когда наступает новое (неизвестное) действие в системе, модель-классификатор предсказывает его как обычное или новое.

Существует два различных способа обучения модели — статическое и динамическое.

Статическое обнаружение новизны может быть представлено как задача бинарной классификации. При наличии набора данных, состоящего только из одного класса, обучается модель. Эта модель изучает границу принятия решения, которая изолирует нормальное поведение. При появлении неизвестного экземпляра его классифицируют как новый или как нормальный. В этих рамках усилия сосредоточены на классификации нормального класса. Поэтому для оценки результативности таких моделей-классификаторов обычно максимизируется полнота определения нормального класса. Формально обучающий набор генерируется только из $P\left(s^{\tilde{p}} \mid z_g = N\right)$. На этапе обучения, даже если классификатор обучается с использованием информации только об одном классе (нормальном функционировании объекта КИИ), он строится с учетом того, что существует другое поведение, отличное от нормального.

Формально любое функционирование объекта КИИ определяется как $s^{\tilde{p}} = \left(s^{\tilde{p}}_{i_1}, ..., s^{\tilde{p}}_{i_m}\right)$. С учетом размеченного набора данных для обучения $z_g = \left\{\left(s^{\tilde{p}}_{i_1}, y_1 = N\right), ..., \left(s^{\tilde{p}}_{i_m}, y_m = N\right)\right\}$. Цель заключается в том, чтобы обучить модель-классификатор, которая будет в состоянии предсказать разницу между нормальным функционированием объекта КИИ и новым.

Динамическое обнаружение новизны (*обнаружение эволюционирующих классов, будущих*



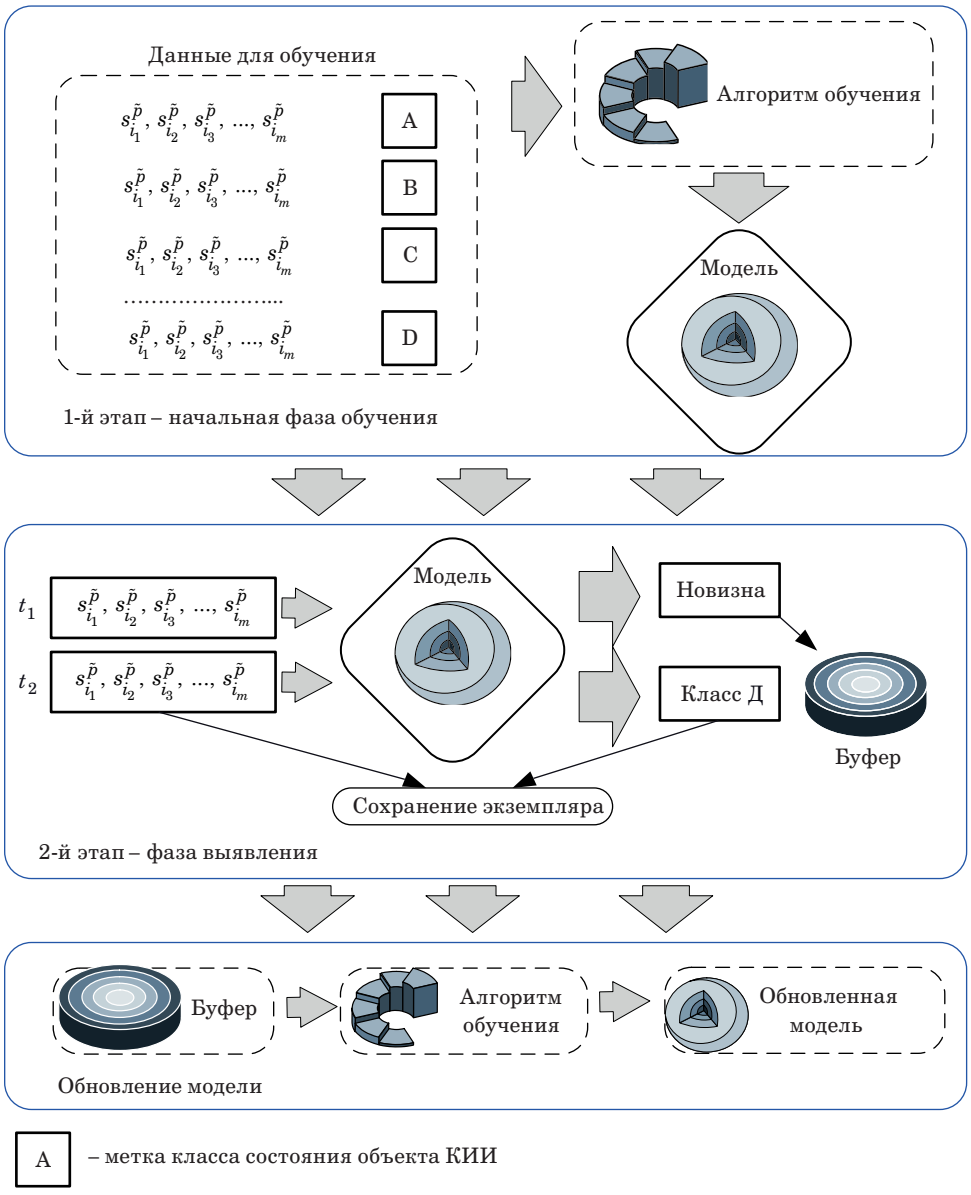
■ ***Рис. 2.*** Представление задачи выявления аномалий
■ ***Fig. 2.*** Representation of the anomaly detection task

классов, *новых классов*). Этот способ обучения может быть формализован как задача классификации, в которой количество меток для переменной класса неизвестно. Другими словами, распределение вероятностей z_g динамически изменяется в процессе классификации, поэтому классификатор должен адаптироваться к этим изменениям. Когда появляется новый экземпляр, модель должна классифицировать его среди текущих классов или хранить в буфере. Учитывая жизненный цикл функционирования объектов КИИ и меняющийся ландшафт угроз, классы состояний объекта КИИ z_g могут появляться, удаляться и появляться вновь. Следовательно, классификатор должен быть обновлен для этих изменений с учетом того, что время адаптации имеет особое значение.

Способ обучения динамическому обнаружению новизны можно разделить на два этапа (рис. 3).

1-й этап — *начальная фаза обучения*. С учетом помеченного обучающего набора данных с набором меток $\left(d_j\right)_{z_g}$ строится модель-классификатор при состоянии объекта КИИ z_{gj}.

2-й этап — *фаза выявления*. Новые классы атак и других воздействий на объекты КИИ могут появляться и исчезать, а старые классы могут изменяться. Данный этап может быть описан как стадия подготовки к адаптации модели-классификатора для обработки потока данных (бес-



■ ***Рис. 3.*** Динамическое обнаружение новизны
■ ***Fig. 3.*** Dynamic novelty detection

■ ***Таблица 3.*** Обобщенные основные характеристики путей повышения результативности выявления атак на объекты КИИ

■ ***Table 3.*** Generalized main characteristics of ways to improve the effectiveness of detecting attacks on CII objects

№ п/п	Путь повышения результативности	Методы	Основные характеристики
1	Обнаружение редкого события	Логистическая регрессия [35, 36], расстояние Кульбака — Лейблера [37], нейронные сети [29], байесовские сети [38], метод опорных векторов [39]	Временные ряды Несбалансированная классификация Все классы в обучающих данных
2	Обнаружение аномалии	Автоэнкодеры [40], k-средних [41], нейронные сети [42–45]	Статистические данные Несбалансированная классификация Все классы в обучающих данных
3	Обнаружение новизны (статическое)	Нейронные сети [46, 47], изолирующий лес [48]	Один класс в обучающих данных
4	Обнаружение новизны (динамическое)	Нейронные сети [46], автоэнкодеры [48]	В обучающих данных не все возможные классы

конечная последовательность результатов наблюдений). В момент времени t_k текущий классификатор предсказывает новый вариант функционирования объекта КИИ. Если новое состояние объекта КИИ не может быть классифицировано в текущем наборе, оно хранится отдельно в буфере и модель не изменяется. Как только буфер заполняется, классификатор обновляется и набор меток t_{k+n} изменяется.

Таким образом, динамическое обнаружение новизны обладает возможностью адаптации к изменениям состояния функционирования объектов КИИ. Характеристики рассмотренных путей повышения результативности выявления атак на объекты КИИ представлены в табл. 3.

Для методов, представленных в табл. 3 (пп. 1 и 2), характерен основной недостаток — зависимость от опыта экспертов по маркировке (разметке) данных. Еще одним недостатком этих подходов является то, что новые аномалии, которые не были частью обучающих данных, могут не обнаруживаться.

Подходы п. 3 могут обнаруживать только кратковременные отказы, вызванные компьютерными атаками [49, 50]. Кроме того, обнаружение новизны должно быть в потоковом режиме. Это позволяет системным администраторам вмешиваться в текущую атаку или устранять проблемы с производительностью системы. В связи с этим подходы статического обнаружения новизны, учитывающие данные устаревших событий, не подходят для современных систем обнаружения компьютерных атак.

Стоит отметить, что для методов п. 4 (динамического обнаружения новизны) не характерно предположение, что данные функционирования объектов КИИ стационарны. При этом всегда существует риск неадекватных защитных мер в будущем из-за «неучтенной динамики». Альтернативные подходы основаны на онлайн-обучении моделей [51]. Однако такие решения обладают угрозами безопасности информации [52], при реализации которых злоумышленники могут снизить эффективность этих решений.

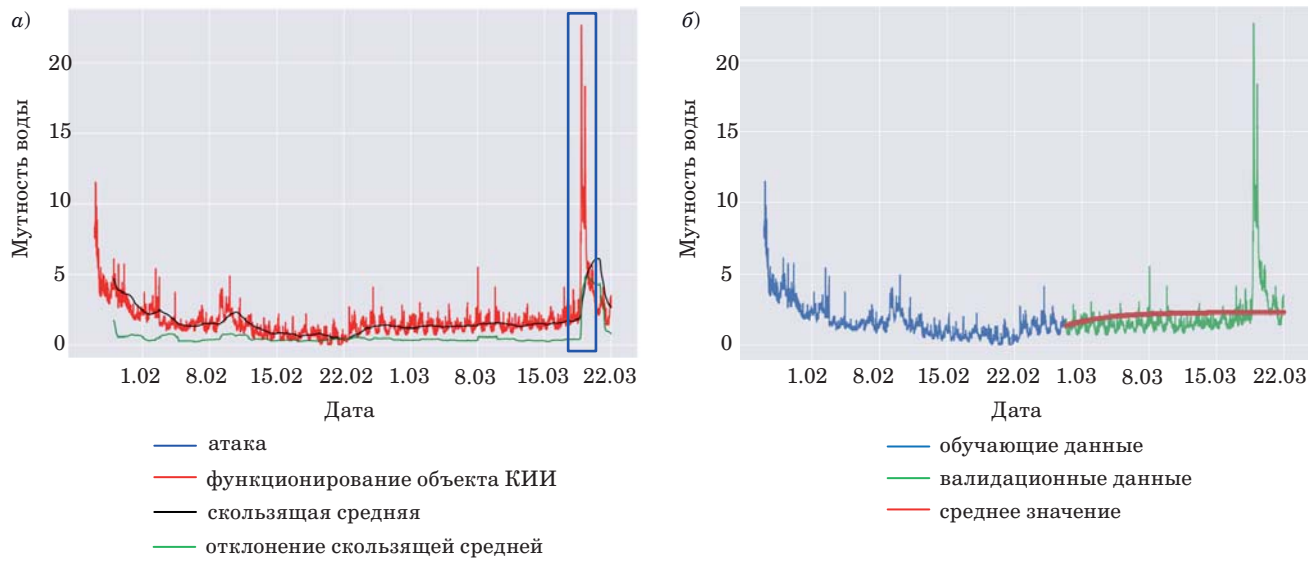
Эксперимент

Для выбора из рассмотренных путей повышения результативности выявления атак на объекты КИИ был проведен эксперимент. Целью эксперимента была проверка гипотезы, что не оптимизированные алгоритмы машинного обучения будут иметь разный результат и могут быть проранжированы по метрикам качества.

Данные

Отсутствие надежных и общедоступных наборов данных функционирования объектов КИИ является фундаментальной проблемой для исследователей, изучающих защищенность таких объектов от различного типа атак и других воздействий. Персонал реальных объектов КИИ не может предоставлять точные наборы данных, поскольку ошибки или атаки в лучшем случае можно только предполагать.

Для проведения эксперимента вместо объекта КИИ были использованы данные испытательного стенда системы очистки воды (SWaT) [53]. SWaT представляет собой уменьшенную версию реальной городской водоочистной станции, производящей 25 литров воды в минуту с помощью мембранных установок и обратного осмоса. Стенд функционировал в двух состояниях: нормальном и при атаке на информационную инфраструктуру.



■ ***Рис. 4.*** Пример функционирования системы очистки воды (SWaT) после атаки: *а* — атака; *б* — разделение на выборки данных

■ ***Fig. 4.*** Example of the functioning of the water treatment system (SWaT) after attack: *а* — attack; *б* — data sampling

Для атаки на систему очистки воды использовался системный подход. Входом атаки может быть физический элемент или коммуникационная сеть, соединяющая датчики или исполнительные механизмы с контроллерами и системой SCADA. SWaT состоит из шести уровней, каждый из которых содержит разное количество датчиков и исполнительных механизмов. Набор данных содержит сетевой трафик и все значения, полученные от 51 датчика и исполнительных механизмов в течение 11 дней непрерывной работы (семь дней в обычном режиме и четыре дня с 41 атакой). Данные помечены в соответствии с нормальным и аномальным функционированием.

Результирующее действие на функционирование — качество очистки воды — представлено на рис. 4, *а*. Набор данных содержит физические характеристики, связанные с процессом водоподготовки, а также сетевой трафик на испытательном стенде. Для проведения эксперимента данные были разделены на обучающую и валидационные части (рис. 4, *б*), содержащие результаты проведения атак.

Оценивание качества выявления нарушения функционирования объектов КИИ

Для оценки эффективности различных подходов из-за (сильно) несбалансированного распределения классов общие показатели качества, такие как точность, недостаточно информативны. Поэтому метриками качества для сравнения было принято использовать метрики пропуска и ошибки выявления нового (аномального) функционирования объекта КИИ, а также F-меру.

F-мера была рассчитана путем рассмотрения двух других метрик: полноты и точности. Все показатели перечислены в следующих уравнениях.

Показатель точности

$$FE = \frac{z_{g'} \to z_g}{z_g + z_{g'} \to z_g},$$

где z_g — количество экземпляров, правильно классифицированных как старый класс; $z_{g'} \to z_g$ — количество экземпляров из нового класса, классифицированных как старый класс.

Далее оценили метрику полноты, которая представляет количество правильно определенных объектов из общего числа объектов в наборе данных.

Показатель пропуска нового (аномального) функционирования объекта КИИ

$$MN = \frac{z_g \to z_{g'}}{z_{g'} + (z_g \to z_{g'})},$$

где $z_{g'}$ — количество экземпляров, правильно классифицированных как новый класс; $z_g \to z_{g'}$ — количество экземпляров из старого класса, классифицированных как новый класс.

Наконец, F-мера может быть вычислена на основе полученных значений:

$$F_1 = 2\frac{MN \cdot FE}{MN + FE}.$$

Валидации эксперимента

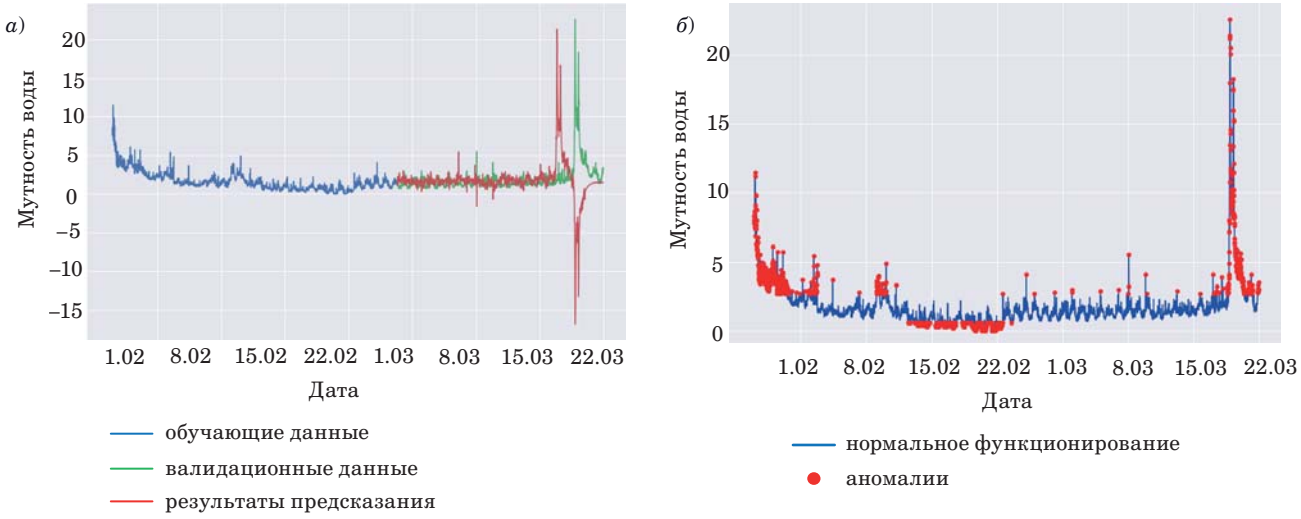
Результаты эксперимента представлены на рис. 5 и в табл. 4. Стоит отметить, что для статистического выявления новизны характерно отклонение результатов по времени (рис. 5, *а*), а для выявления редкого события (рис. 5, *б*) — ложноположительные результаты и низкая точность выявления начальной фазы атаки.

Проведенный эксперимент показал, что из-за ограниченного времени выявить можно только ограниченное количество атак, поэтому качество их выявления для любых алгоритмов должно быть крайне высоким. При динамическом выявлении качество (F-мера) повышается. Связано это с адаптацией под различные изменения функционирования из-за 41 атаки.

Стоит отметить, что для детекторов (автоэнкодеров и нейронных сетей) характерна зависимость от длины данных, взятых для обучения. Лучшие результаты были получены при размере пакетов 22 записи. Качество обнаружения сильно различается для разных размеров пакета, даже при небольших изменениях (21 или 23 записи). В целом оба детектора дают многообещающие результаты.

Заключение

В статье представлены основные данные сравнения путей повышения результативности выявления атак на объекты КИИ: редкого собы-



■ ***Рис. 5.*** Результаты выявления атак на объект КИИ: *а* — статистическое выявление новизны; *б* — выявление редкого события

■ ***Fig. 5.*** Representation of the results of detecting an attacks on the CII object: *а* — statistical novelty identification; *б* — identification of a rare event

■ ***Таблица 4.*** Результаты сравнения алгоритмов

■ ***Table 4.*** Algorithm comparison results

Редкое событие		Аномалия		Новизна (статическое выявление)		Новизна (динамическое выявление)	
Подход	F-мера	Подход	F-мера	Подход	F-мера	Подход	F-мера
Идеальный детектор	1	Идеальный детектор	1	Идеальный детектор	1	Идеальный детектор	1
Нейронные сети	0,8446	Автоэнкодеры	0,8301	Нейронные сети	0,8598	Автоэнкодеры	0,9045
Байесовские сети	0,8275	*k*-средних	0,8046	Случайный лес	0,8234	Нейронные сети	0,8687
Логистическая регрессия	0,7657	Нейронные сети	0,7945	Логистическая регрессия	0,7963	Логистическая регрессия	0,8174
Нулевой детектор	0	Нулевой детектор	0	Нулевой детектор	0	Нулевой детектор	0

тия, аномалии и новизны. Для этого были рассмотрены характеристики процесса выявления, исходных данных и наиболее репрезентативные методы.

Выявление известных сигнатур компьютерных атак по-прежнему критически важно, но оно не обеспечивает достаточной защищенности в ландшафте угроз безопасности КИИ. Данная технологическая отрасль должна избегать проблемы с изменяющимися атаками с помощью решений последнего поколения, применяя новые подходы, которые устраняют пробелы в разработке и функционировании сервисов и систем защиты.

Принцип работы предлагаемого подхода заключается в выявлении и отделении аномалий от нормальных наблюдений с использованием концепции динамического изменения меток для переменного класса с течением времени. Динамическое обнаружение новизны сравнили с другими подходами по показателю F1-меры. Для данных SWaT, который представляет собой макет объекта КИИ — автоматизированной системы управления, было установлено, что выявление атак с использованием динамического обнаружения новизны улучшилось на 7 %.

Дальнейшие исследования, на наш взгляд, должны быть направлены на:

1) повышение производительности подхода к обнаружению атак посредством сокращения признакового пространства функционирования объектов КИИ;

2) расширение предлагаемого подхода на гибридную систему обнаружения, использующую как данные процесса, так и данные сетевого трафика системы, чтобы улучшить качество обнаружения скрытых атак.

Финансовая поддержка

Работа выполнена в рамках гранта Президента Российской Федерации для государственной поддержки молодых российских ученых — кандидатов наук МК-2485.2022.4.

Литература

1. **Petrenko S. A.** Cyber resilient platform for Internet of Things (IIoT/IoT) ed systems: survey of architecture patterns. *Вопросы кибербезопасности*, 2021, № 2, с. 81–91. doi:10.21681/2311-3456-2021-2-81-91
2. **Maynard P., McLaughlin K., Sezer S.** Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure control systems. *Journal of Cybersecurit*, 2020, vol. 6, iss. 1, pp. 1–20. doi:10.1093/cybsec/tyaa020
3. **Langner R.** Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 2011, vol. 6, iss. 3, pp. 49–51. doi:10.1109/MSP.2011.67
4. **Miller B., Rowe D.** A survey SCADA of and critical infrastructure incidents. *Proc. of the 1st Annual Conf. on Research in Information Technology*, New York, Oct. 2012, NY, United States, 2012, pp. 51–56. doi:10.1145/2380790.2380805
5. **Assante M. J., Lee R. M.** *The Industrial Control System Cyber Kill Chain*. SANS Institute InfoSec Reading Room, 2015. Vol. 1. 24 p.
6. **Rrushi J., Farhangi H., Howey C., Carmichael K., Dabell J.** A quantitative evaluation of the target selection of havex ics malware plugin. *Industrial Control System Security (ICSS) Workshop*, Los Angeles, California, USA, 2015, pp. 1–5.
7. *ICS-CERT A. Ongoing sophisticated malware campaign compromising ICS*. http://www.ics-cert.uscert.gov/alerts/ICS-ALERT-14-281-01B (дата обращения: 12.01.2022).
8. **Rrushi J. L.** Multi-range Decoy I/O defense of electrical substations against industrial control system malware. *Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction*. F. Flammini (eds). Springer, Cham., 2019. Pp. 151–175. doi:10.1007/978-3-319-95597-1_7
9. **Lee R. M., Assante M. J., Conway T.** German steel mill cyber attack. *Industrial Control Systems*, 2014, vol. 30, iss. 62, pp. 1–15.
10. **Bencsáth B., Pék G., Buttyán L., Félegyházi M.** *Duqu: A Stuxnet-like malware found in the wild*. CrySyS Lab Technical Report, 2011. Vol. 14. 60 p.
11. **Zetter K.** *A cyberattack has caused confirmed physical damage for the second time ever*. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ (дата обращения: 12.01.2022).
12. **Alladi T., Chamola V., Zeadally S.** Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, 2020, vol. 155, pp. 1–8. doi:10.1016/j.comcom.2020.03.007
13. **Саенко И. Б., Лаута О. С., Карпов М. А., Крибель А. М.** Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры. *Электросвязь*, 2021, № 1, с. 36–44. doi:10.34832/ELSV.2021.14.1.004
14. **Рыбкина О. В.** Построение модели угроз безопасности информации на основе математической модели Ланкастера. *Научно-техническое и экономическое сотрудничество стран АТР в XXI веке: тр. Всерос. науч.-практ. конф.*, Хабаровск, 20–23 апреля 2021 г., 2021, т. 1, с. 252–257.
15. **Бражук А. И.** Методика моделирования угроз компьютерных систем на основе предметно-ориентированных моделей. *Всерос. науч. конф. «Информационные технологии в моделировании и управле-*

нии: подходы, методы, решения», Тольятти, 20–22 апреля 2021 г., 2021, с. 94–101.

16. **Суханов И. Д., Рыбкина О. В.** Новые подходы к моделированию угроз безопасности информации. *Научно-техническое и экономическое сотрудничество стран АТР в XXI веке: тр. Всерос. науч.-практ. конф.*, Хабаровск, 20–23 апреля 2021 г., 2021, т. 1, с 277–282.
17. **Caldwell M., Andrews J. T. A., Tanay T., Griffin L. D.** AI-enabled future crime. *Crime Science*, 2020, vol. 9, no. 1, pp. 1–13. doi:10.1186/s40163-020-00123-8
18. **Schneier B.** Attack trees. *Dr. Dobb's Journal*, 1999, vol. 24, no. 12, pp. 21–29.
19. **Hutchins E. M., Cloppert M. J., Amin R. M**. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*. Academic Publishing International Limited, 2011. Vol. 1. Pp. 80–106.
20. *MITRE. 2017. ATT & CK Matrix for Enterprise*. https://attack.mitre.org/matrices/enterprise/ (дата обращения: 21.05.2022).
21. **Bu Z.** *Zero-day attacks are not the same as zero-day vulnerabilities*. www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html (дата обращения: 12.01.2022).
22. **Di Pinto A., Dragoni Y., Carcano A.** *TRITON: The first ICS cyber attack on safety instrument systems*. Black Hat, USA, 2018. 26 p.
23. **Găitan V. G., Zagan I.** Experimental implementation and performance evaluation of an IoT access gateway for the modbus extension. *Sensors*, 2021, vol. 21, 246, iss. 1, pp. 1–24. doi:10.3390/s21010246
24. **Radoglou-Grammatikis P., Sarigiannidis P., Efstathopoulos G., Karipidis P., Sarigiannidis A.** DIDEROT: an intrusion detection and prevention system for DNP3-based SCADA systems. *Proc. of the 15th Intern. Conf. on Availability, Reliability and Security*, 2020, pp. 1–8. doi:10.1145/3407023.3409314
25. **Ustun T. S., Hussain S. M. S.** IEC 61850 Modeling of UPFC and XMPP communication for power management in microgrids. *IEEE Access*, 2020, vol. 8, pp. 141696–141704. doi:10.1109/ACCESS.2020.3013264
26. **Saranya T., Sridevi S., Deisy C., Tran Duc Chung, Ahamed Khan M. K. A.** Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*, 2020, vol. 171, pp. 1251–1260. doi:10.1016/j.procs.2020.04.133
27. **Kumar I., Mohd N., Bhatt C., Sharma S. K.** Development of IDS using supervised machine learning. *Soft computing: Theories and applications*. M. Pant et al (eds.). Springer, 2020. Pp. 565–577. doi:10.1007/978-981-15-4032-5_52
28. **Sudar K. M., Deepalakshmi P.** Comparative study on IDS using machine learning approaches for software defined networks. *Intern. Journal of Intelligent Enterprise*, 2020, vol. 7, iss. 1–3, pp. 15–27. doi:10.1504/IJIE.2020.104642
29. **Leichtnam L., Totel E., Prigent N., Me L.** Sec-2graph: Network attack detection based on novelty detection on graph structured data. *Intern. Conf. on Detection of Intrusions and Malware, and Vulnerability Assessment*, Lisboa, Portugal, 2020, pp. 238–258. doi:10.1007/978-3-030-52683-2_12
30. **Ковтун Л. И., Крюков О. В., Саушев А. В., Антоненко С. И.** Аналитико-статистический метод оценки состояния и прогнозирования рисков сложных технических систем. *Надежность и качество: тр. Междунар. симп.*, Пенза, 25–31 мая 2020 г., 2020, т. 1, с. 264–269.
31. **Murray J. F., Hughes G. F., Kreutz-Delgado F.** Machine learning methods for predicting failures in hard drives: A multiple-instance application. *Journal of Machine Learning Research*, 2005, vol. 6, pp. 783–816. doi:10.5555/1046920.1088699
32. **Gnidko K. O., Dudkin A. S., Ivanov O. S., Lokhvitsky V. A., Pilkevich S. V., Sabirov T. R.** The Unconscious response of multimedia content consumers to emociogenic visual symbols: Experimental study and oculometry dataset. *Solid State Technology*, 2020, vol. 63, no. 6, pp. 4549–4558.
33. **Zhang S., Bahrampour S., Ramakrishnan N., Schott L., Shah M.** Deep learning on symbolic representations for large-scale heterogeneous time-series event prediction. *42nd Intern. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 5–9, 2017, IEEE, 2017, pp. 5970–5974. doi:10.1109/ICASSP.2017.7953302
34. **Khreich W., Khosravifar B., Hamou-Lhadj A., Talhib C.** An anomaly detection system based on variable N-gram features and one-class SVM. *Information and Software Technology*, 2017, vol. 91, pp. 186–197. doi:10.1016/j.infsof.2017.07.009
35. **Timoneda J. C.** Estimating group fixed effects in panel data with a binary dependent variable: how the LPM outperforms logistic regression in rare events data. *Social Science Research*, 2021, vol. 93, Article 102486. doi:10.1016/j.ssresearch.2020.102486
36. **Cafiso S., Pappalardo G.** Safety effectiveness and performance of lane support systems for driving assistance and automation — Experimental test and logistic regression for rare events. *Accident Analysis & Prevention*, 2020, vol. 148, Article 105791. doi:10.1016/j.aap.2020.105791
37. **Xu J., Denman S., Fookes C., Sridharan S.** Detecting rare events using Kullback — Leibler divergence. *40th Intern. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, April 19–24, 2015, IEEE, 2015, pp. 1305–1309. doi:10.1109/ICASSP.2015.7178181
38. **Cheon S. P., Kim S., Lee S-Y., Lee C-B.** Bayesian networks based rare event prediction with sensor data. *Knowledge-Based Systems*, 2009, vol. 22, iss. 5, pp. 336–343. doi:10.1016/j.knosys.2009.02.004

39. **Bourinet J. M.** Rare-event probability estimation with adaptive support vector regression surrogates. *Reliability Engineering & System Safety*, 2016, vol. 150, pp. 210–221. doi:10.1016/j.ress.2016.01.023
40. **Gong D., Liu L., Le V., Saha B., Mansour M. R., Venkatesh S., Hengel A.** Memorizing normality to detect anomaly: Memory-augmented deep autoencoder for unsupervised anomaly detection. *The IEEE/CVF Intern. Conf. on Computer Vision*, 2019, pp. 1705–1714. doi:10.48550/arXiv.1904.02639
41. **Han L. I.** Using a dynamic K-means algorithm to detect anomaly activities. *Seventh Intern. Conf. on Computational Intelligence and Security*, Dec. 3–4, 2011, Sanya, China, IEEE, 2011, pp. 1049–1052. doi:10.1109/CIS.2011.233
42. **Pradhan M., Pradhan S. K., Sahu S. K.** Anomaly detection using artificial neural network. *International Journal of Engineering Sciences & Emerging Technologies*, 2012, vol. 2, no. 1, pp. 29–36. doi:10.23919/FRUCT.2017.8071288
43. **Naseer S., Saleem Y., Khalid S., Bashir M. K., Han J., Iqbal M. M., Han K.** Enhanced network anomaly detection based on deep neural networks. *IEEE Access*, 2018, vol. 6, pp. 48231–48246. doi:10.1109/ACCESS.2018.2863036
44. **Lindemann B., Maschler B., Sahlab N., Weyrich M.** A survey on anomaly detection for technical systems using LSTM networks. *Computers in Industry*, 2021, vol. 131, Article 103498. doi:10.1016/j.compind.2021.103498
45. **Aguayo L., Barreto G. A.** Novelty detection in time series using self-organizing neural networks: A comprehensive evaluation. *Neural Processing Letters*, 2018, vol. 47, pp. 717–744. doi:10.1007/s11063-017-9679-2
46. **Jodelka O., Anagnostopoulos C., Kolomvatsos K.** Adaptive novelty detection over contextual data streams at the edge using one-class classification. *12th Intern. Conf. on Information and Communication Systems (ICICS)*, May 24–26, 2021, Valencia, Spain, IEEE, 2021, pp. 213–219. doi:10.1109/ICICS52457.2021.9464585
47. **Kulkarni P. G., Praneet S. Y., Bongole R., Das B.** Deep detection of anomalies in static attributed graph. *Intern. Conf. on Machine Learning, Image Processing, Network Security and Data Sciences*, Singapore, Springer, 2020, pp. 627–640. doi:10.1007/978-981-15-6318-8_50
48. **Li L., Yan J., Wang H., Jin Y.** Anomaly detection of time series with smoothness-inducing sequential variational auto-encoder. *IEEE Transactions on Neural Networks and Learning Systems*, 2020, vol. 32, iss. 3, pp. 1177–1191. doi:10.48550/arXiv.2102.01331
49. **Chalapathy R., Chawla S.** Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407, 2019.
50. **Yuan Y., Kaklamanos G., Hogrefe D**. A novel semi-supervised adaboost technique for network anomaly detection. *Proc. of 19th ACM Intern. Conf. on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2016, pp. 111–114. doi:10.1145/2988287.2989177
51. **Alippi C., Roveri M., Trovo F.** A self-building and cluster-based cognitive fault diagnosis system for sensor networks. *IEEE Transactions on Neural Networks and Learning Systems*, 2014, vol. 25, iss. 6, pp. 1021–1032. doi:10.1109/TNNLS.2014.2303651
52. *База угроз безопасности информации ФСТЭК*. https://bdu.fstec.ru/threat (дата обращения: 21.05.2022).
53. **Goh J., Adepu S., Junejo K. N., Mathur A.** A dataset to support research in the design of secure water treatment systems. *Intern. Conf. "Critical Information Infrastructures Security"*, Springer, Cham, 2016, pp. 88–99. doi:10.1007/978-3-319-71368-7_8

UDC 004.89
doi:10.31799/1684-8853-2022-4-29-43

A study of ways and solutions to increase the efficiency of detecting computer attacks on the objects of critical information infrastructure

V. N. Kuzmin[a], Dr. Sc., Mil., Professor, orcid.org/0000-0002-6411-4336, vka@mil.ru
A. B. Menisov[a], PhD, Tech., Researcher, orcid.org/0000-0002-9955-2694
[a]A. F. Mozhaiskiy Military Space Academy, 13, Zhdanovskaia Emb., 197198, Saint-Petersburg, Russian Federation

Introduction: In the era of information technology almost all organizations face a wide range of automated and rapidly spreading cyber threats. This is due not only to the growing complexity, diversity and scale of digitalization, but also to the enlargement of cyber threats and the area of their possible implementation. **Purpose:** To compare possible ways of improving the effectiveness of attack detection for the objects of critical information infrastructure (CII): to detect a rare event, anomaly or novelty in the functions of the objects of CII. **Results:** The principle of operation of the proposed (effective) approach to cyberattack detection is to identify and separate anomalies from normal functioning of objects with the use of the concept of dynamic change of labels for a variable class over time. Dynamic novelty detection is compared to other approaches in terms of F1-score. For SWaT data, which is a layout of a critical information infrastructure object as an automated control system, it was determined that attack detection improved by up to 7% using the proposed approach. **Practical relevance:** The results of the research have shown a reduction in the risk of conducting (developing) a computer attack on critical information infrastructure objects. A possible targeted application of the dynamic novelty detection approach is to optimize the

means of protecting information at critical information infrastructure facilities, as well as to integrate the proposed approach into the information security system as an intelligent detector.

Keywords — information security, artificial intelligence technologies, critical information infrastructure, neural networks.

For citation: Kuzmin V. N., Menisov A. B. A study of ways and solutions to increase the efficiency of detecting computer attacks on the objects of critical information infrastructure. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 4, pp. 29–43 (In Russian). doi:10.31799/1684-8853-2022-4-29-43

Financial support

The work was carried out within the framework of the grant of the President of the Russian Federation for state support of young Russian scientists — candidates of sciences MK-2485.2022.4.

References

1. Petrenko S. A. Cyber resilient platform for Internet of Things (IIoT/IoT) ed systems: survey of architecture patterns. *Voprosy kiberbezopasnosti*, 2021, no. 2, pp. 81–91. doi:10.21681/2311-3456-2021-2-81-91
2. Maynard P., McLaughlin K., Sezer S. Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure control systems. *Journal of Cybersecurit*, 2020, vol. 6, iss. 1, pp. 1–20. doi:10.1093/cybsec/tyaa020
3. Langner R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 2011, vol. 6, iss. 3, pp. 49–51. doi:10.1109/MSP.2011.67
4. Miller B., Rowe D. A survey SCADA of and critical infrastructure incidents. *Proc. of the 1st Annual Conference on Research in Information Technology*, New York, Oct. 2012, NY, United States, 2012, pp. 51–56. doi:10.1145/2380790.2380805
5. Assante M. J., Lee R. M. *The Industrial Control System Cyber Kill Chain*. SANS Institute InfoSec Reading Room, 2015. Vol. 1. 24 p.
6. Rrushi J., Farhangi H., Howey C., Carmichael K., Dabell J. A quantitative evaluation of the target selection of havex ics malware plugin. *Industrial Control System Security (ICSS) Workshop*, Los Angeles, California, USA, 2015, pp. 1–5.
7. *ICS-CERT A. Ongoing sophisticated malware campaign compromising ICS*. Available at: http://www.ics-cert.uscert.gov/alerts/ICS-ALERT-14-281-01B (accessed 12 January 2022).
8. Rrushi J. L. *Multi-range Decoy I/O defense of electrical substations against industrial control system malware*. In: *Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction*. F. Flammini (eds). Springer, Cham., 2019. Pp. 151–175. doi:10.1007/978-3-319-95597-1_7
9. Lee R. M., Assante M. J., Conway T. German steel mill cyber attack. *Industrial Control Systems*, 2014, vol. 30, iss. 62, pp. 1–15.
10. Bencsáth B., Pék G., Buttyán L., Félegyházi M. *Duqu: A Stuxnet-like malware found in the wild*. CrySyS Lab Technical Report, 2011. Vol. 14. 60 p.
11. Zetter K. *A cyberattack has caused confirmed physical damage for the second time ever*. Available at: https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ (accessed 12 January 2022).
12. Alladi T., Chamola V., Zeadally S. Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, 2020, vol. 155, pp. 1–8. doi:10.1016/j.comcom.2020.03.007
13. Saenko I. B., Lauta O. S., Karpov M. A., Kribel A. M. Model of threats to information and telecommunication network resources as a key asset of critical infrastructure. *Electrosvyaz*, 2021, no. 1, pp. 36–44 (In Russian). doi:10.34832/ELSV.2021.14.1.004
14. Rybkina O. V. Building a model of information security threats based on the Lancaster mathematical model. *Trudy Vserossijskoj nauchno-prakticheskoj konferencii "Nauchno-tekhnicheskoe i ekonomicheskoe sotrudnichestvo stran ATR v XXI veke"* [Proc. of the All-Russian Scient. and Pract. Conf. "Scientific, technical and economic cooperation of the Asia-Pacific countries in the 21st century"]. Khabarovsk, 2021, vol. 1, pp. 252–257 (In Russian).
15. Brazhuk A. I. Technique of threat modeling of computer systems based on subject-oriented models. *Trudy Vserossijskoj nauchnoj konferencii "Informacionnye tekhnologii v modelirovanii i upravlenii: podhody, metody, resheniya"* [Proc. of the All-Russian Scient. Conf. "Information technologies in modeling and management: approaches, methods, solutions"]. Tolyatti, 2021, pp. 94–101 (In Russian).
16. Sukhanov I. D., Rybkina O. V. New approaches to modeling information security threats. *Trudy Vserossijskoj nauchno-prakticheskoj konferencii "Nauchno-tekhnicheskoe i ekonomicheskoe sotrudnichestvo stran ATR v XXI veke"* [Proc. of the All-Russian Scient. and Pract. Conf. "Scientific, technical and economic cooperation of the Asia-Pacific countries in the 21st century"]. Khabarovsk, 2021, vol. 1, pp. 277–282 (In Russian).
17. Caldwell M., Andrews J. T. A., Tanay T., Griffin L. D. AI-enabled future crime. *Crime Science*, 2020, vol. 9, no. 1, pp. 1–13. doi:10.1186/s40163-020-00123-8
18. Schneier B. Attack trees. *Dr. Dobb's Journal*, 1999, vol. 24, no. 12, pp. 21–29.
19. Hutchins E. M., Cloppert M. J., Amin R. M. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. In: *Leading Issues in Information Warfare & Security Research*. Academic Publishing International Limited, 2011. Vol. 1. Pp. 80–106.
20. *MITRE. 2017. ATT & CK Matrix for Enterprise*. Available at: https://attack.mitre.org/matrices/enterprise/ (accessed 21 May 2022).
21. Bu Z. *Zero-day attacks are not the same as zero-day vulnerabilities*. Available at: www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html (accessed 12 January 2022).
22. Di Pinto A., Dragoni Y., Carcano A. *TRITON: The first ICS cyber attack on safety instrument systems*. Black Hat, USA, 2018. 26 p.
23. Găitan V. G., Zagan I. Experimental implementation and performance evaluation of an IoT access gateway for the modbus extension. *Sensors*, 2021, vol. 21, 246, iss. 1, pp. 1–24. doi:10.3390/s21010246
24. Radoglou-Grammatikis P., Sarigiannidis P., Efstathopoulos G., Karipidis P., Sarigiannidis A. DIDEROT: an intrusion detection and prevention system for DNP3-based SCADA systems. *Proc. of the 15th Intern. Conf. on Availability, Reliability and Security*, 2020, pp. 1–8. doi:10.1145/3407023.3409314
25. Ustun T. S., Hussain S. M. S. IEC 61850 Modeling of UPFC and XMPP communication for power management in microgrids. *IEEE Access*, 2020, vol. 8, pp. 141696–141704. doi:10.1109/ACCESS.2020.3013264
26. Saranya T., Sridevi S., Deisy C., Tran Duc Chung, Ahamed Khan M. K. A. Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*, 2020, vol. 171, pp. 1251–1260. doi:10.1016/j.procs.2020.04.133
27. Kumar I., Mohd N., Bhatt C., Sharma S. K. *Development of IDS using supervised machine learning*. In: *Soft computing: Theories and applications*. M. Pant et al (eds.). Springer, 2020. Pp. 565–577. doi:10.1007/978-981-15-4032-5_52
28. Sudar K. M., Deepalakshmi P. Comparative study on IDS using machine learning approaches for software defined networks. *International Journal of Intelligent Enterprise*, 2020, vol. 7, iss. 1–3, pp. 15–27. doi:10.1504/IJIE.2020.104642
29. Leichtnam L., Totel E., Prigent N., Me L. Sec2graph: Network attack detection based on novelty detection on graph structured data. *Intern. Conf. on Detection of Intrusions and Malware, and Vulnerability Assessment*, Lisboa, Portugal, 2020, pp. 238–258. doi:10.1007/978-3-030-52683-2_12
30. Kovtun L. I., Kryukov O. V., Saushev A. V., Antonenko R. P. I. Analytical and statistical method for assessing the state and predicting the risks of complex technical systems. *Trudy Mezhdunarodnogo simpoziuma "Nadezhnost i kachestvo"* [Proc. Int. Symp. "Reliability and quality"], Penza, 2020, vol. 1, pp. 264–269 (In Russian).

31. Murray J. F., Hughes G. F., Kreutz-Delgado F. Machine learning methods for predicting failures in hard drives: A multiple-instance application. *Journal of Machine Learning Research*, 2005, vol. 6, pp. 783–816. doi:10.5555/1046920.1088699
32. Gnidko K. O., Dudkin A. S., Ivanov O. S., Lokhvitsky V. A., Pilkevich S. V., Sabirov T. R. The unconscious response of multimedia content consumers to emociogenic visual symbols: Experimental study and oculometry dataset. *Solid State Technology*, 2020, vol. 63, no. 6, pp. 4549–4558.
33. Zhang S., Bahrampour S., Ramakrishnan N., Schott L., Shah M. Deep learning on symbolic representations for large-scale heterogeneous time-series event prediction. *42nd Intern. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2017, pp. 5970–5974. doi:10.1109/ICASSP.2017.7953302
34. Khreich W., Khosravifar B., Hamou-Lhadj A., Talhib C. An anomaly detection system based on variable N-gram features and one-class SVM. *Information and Software Technology*, 2017, vol. 91, pp. 186–197. doi:10.1016/j.infsof.2017.07.009
35. Timoneda J. C. Estimating group fixed effects in panel data with a binary dependent variable: how the LPM outperforms logistic regression in rare events data. *Social Science Research*, 2021, vol. 93, Article 102486. doi:10.1016/j.ssresearch.2020.102486
36. Cafiso S., Pappalardo G. Safety effectiveness and performance of lane support systems for driving assistance and automation — Experimental test and logistic regression for rare events. *Accident Analysis & Prevention*, 2020, vol. 148, Article 105791. doi:10.1016/j.aap.2020.105791
37. Xu J., Denman S., Fookes C., Sridharan S. Detecting rare events using Kullback — Leibler divergence. *40th Intern. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2015, pp. 1305–1309. doi:10.1109/ICASSP.2015.7178181
38. Cheon S. P., Kim S., Lee S-Y., Lee C-B. Bayesian networks based rare event prediction with sensor data. *Knowledge-Based Systems*, 2009, vol. 22, iss. 5, pp. 336–343. doi:10.1016/j.knosys.2009.02.004
39. Bourinet J. M. Rare-event probability estimation with adaptive support vector regression surrogates. *Reliability Engineering & System Safety*, 2016, vol. 150, pp. 210–221. doi:10.1016/j.ress.2016.01.023
40. Gong D., Liu L., Le V., Saha B., Mansour M. R., Venkatesh S., Hengel A. Memorizing normality to detect anomaly: Memory-augmented deep autoencoder for unsupervised anomaly detection. *The IEEE/CVF Intern. Conf. on Computer Vision*, 2019, pp. 1705–1714. doi:10.48550/arXiv.1904.02639
41. Han L. I. Using a dynamic K-means algorithm to detect anomaly activities. *Seventh Intern. Conf. on Computational Intelligence and Security*, Dec. 3–4, 2011, Sanya, China, IEEE, 2011, pp. 1049–1052. doi:10.1109/CIS.2011.233
42. Pradhan M., Pradhan S. K., Sahu S. K. Anomaly detection using artificial neural network. *International Journal of Engineering Sciences & Emerging Technologies*, 2012, vol. 2, no. 1, pp. 29–36. doi:10.23919/FRUCT.2017.8071288
43. Naseer S., Saleem Y., Khalid S., Bashir M. K., Han J., Iqbal M. M., Han K. Enhanced network anomaly detection based on deep neural networks. *IEEE Access*, 2018, vol. 6, pp. 48231–48246. doi:10.1109/ACCESS.2018.2863036
44. Lindemann B., Maschler B., Sahlab N., Weyrich M. A survey on anomaly detection for technical systems using LSTM networks. *Computers in Industry*, 2021, vol. 131, Article 103498. doi:10.1016/j.compind.2021.103498
45. Aguayo L., Barreto G. A. Novelty detection in time series using self-organizing neural networks: A comprehensive evaluation. *Neural Processing Letters*, 2018, vol. 47, pp. 717–744. doi:10.1007/s11063-017-9679-2
46. Jodelka O., Anagnostopoulos C., Kolomvatsos K. Adaptive novelty detection over contextual data streams at the edge using one-class classification. *12th Intern. Conf. on Information and Communication Systems (ICICS)*, 2021, pp. 213–219. doi:10.1109/ICICS52457.2021.9464585
47. Kulkarni P. G., Praneet S. Y., Bongole R., Das B. Deep detection of anomalies in static attributed graph. *Intern. Conf. on Machine Learning, Image Processing, Network Security and Data Sciences*, Singapore, Springer, 2020, pp. 627–640. doi:10.1007/978-981-15-6318-8_50
48. Li L., Yan J., Wang H., Jin Y. Anomaly detection of time series with smoothness-inducing sequential variational auto-encoder. *IEEE Transactions on Neural Networks and Learning Systems*, 2020, vol. 32, iss. 3, pp. 1177–1191. doi:10.48550/arXiv.2102.01331
49. Chalapathy R., Chawla S. Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407, 2019.
50. Yuan Y., Kaklamanos G., Hogrefe D. A novel semi-supervised adaboost technique for network anomaly detection. *19th ACM Intern. Conf. on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2016, pp. 111–114. doi:10.1145/2988287.2989177
51. Alippi C., Roveri M., Trovo F. A self-building and cluster-based cognitive fault diagnosis system for sensor networks. *IEEE Transactions on Neural Networks and Learning Systems*, 2014, vol. 25, iss. 6, pp. 1021–1032. doi:10.1109/TNNLS.2014.2303651
52. *Baza ugroz bezopasnosti informacii FSTEK* [FSTEC information security threat database]. Available at: https://bdu.fstec.ru/threat (accessed 21 May 2022).
53. Goh J., Adepu S., Junejo K. N., Mathur A. A dataset to support research in the design of secure water treatment systems. *Intern. Conf. "Critical Information Infrastructures Security"*, Springer, Cham, 2016, pp. 88–99. doi:10.1007/978-3-319-71368-7_8