УДК 004.056.5:681.518.5 EDN: AOYHDJ

МЕТОДОЛОГИЯ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И УПРАВЛЕНИЯ

С.Ю. Тырышкин service.vip-spe@yandex.ru
Е.В. Шарлаев sharlaev@mail.ru

АлтГТУ, г. Барнаул, Российская Федерация

Аннотация

Рассмотрены вопросы эффективного использования информационных технологий в химической промышленности. Актуальность данного направления обусловлена необходимостью повышения производительности и конкурентоспособности предприятий химической промышленности путем активного внедрения передовых цифровых решений. Основное внимание уделено преимуществам и особенностям применения современных информационных систем и программных продуктов, таких как SCADA-системы, корпоративные ERP-платформы, специальные аналитические и расчетные пакеты для моделирования и оптимизации химических процессов. Подробно проанализированы возможные пути интеграции ИТ-инструментов в производственные процессы, методики оценки экономической целесообразности и эффективности внедрения таких систем. Приведены примеры реализации проектов по автоматизации химических производств. Описаны реальные кейсы внедрения цифровых решений, позволяющие снижать издержки, повышать качество продукции и обеспечивать безопасность на предприятиях. Отмечена необходимость непрерывного обучения и переобучения специалистов-химиков, которым предстоит осваивать и эффективно применять современные информационные технологии в своей повседневной практике. Приведены подходы к формированию и развитию необходимых профессиональных компетенций в условиях перехода к цифровым методам проектирования, анализа и управления химико-

Ключевые слова

Промышленность, автоматизация, угрозы, риски, защита, оценка, когнитивная карта

технологическими предприятиями. Результаты апробации методологии являются эффективным инструментом, который переводит требования нормативной базы в плоскость измеряемых показателей и позволяет принимать обоснованные решения по управлению рисками информационной безопасности

Поступила 10.09.2025
Принята 16.05.2026

Введение. В настоящее время промышленность вступает в новую эру интеллектуальной трансформации, обусловленную активным переходом к цифровой экономике и растущим спросом на высокопроизводительные и надежные автоматизированные системы управления. Современная промышленная парадигма основана на широком внедрении цифровых решений, создании «умных» фабрик и повсеместном распространении концепции Индустрии 4.0, основные принципы которой заключаются в ведущей роли информации и коммуникационных технологий в поддержании конкурентоспособности предприятий [1, 2].

Разработка и внедрение современных систем автоматизации имеют решающее значение для устойчивого развития всей экономики, предлагая организациям возможность радикально трансформировать традиционные производственные процессы и цепочки создания добавочной стоимости. Так постепенная цифровая интеграция локальных промышленных объектов создает предпосылки для существенного повышения операционной эффективности, точности выполнения заданий и управляемости технологических процессов. Одновременно с этим возрастает необходимость в формировании безопасной и надежной ИТ-инфраструктуры, отвечающей высоким стандартам кибербезопасности и удовлетворяющей потребности как самого производства, так и административного управления системой [3].

Важным аспектом является взаимопроникновение внутренних производственных сетей и внешних систем коммуникаций, в частности через подключение к интернету. Производственная инфраструктура давно стала неотъемлемой частью всемирной паутины, что обеспечивает компаниям значительные удобства для удаленных настройки, обслуживания и обновления своего оборудования, однако одновременно порождает дополнительные риски и новые вызовы в плане информационной безопасности. Многие устройства внутри промышленных систем оказываются доступны внешним пользователям, например, разработчикам программного обеспечения (ПО), интеграторам, сторонним подрядчикам и консультантам, что открывает новые потенциальные точки проникновения злоумышленников [3].

Значимость указанной проблемы подтверждает статистика масштабных киберинцидентов последнего десятилетия, связанных с промышленными объектами. Ярким примером является массированная атака вируса-шифровальщика WannaCry в мае 2017 г., в результате которой пострадало огромное число организаций и предприятий в различных секторах экономики, включая крупнейшие заводы, объекты городской инфраструктуры и энергосети [4, 5].

Результаты анализа текущего состояния дел свидетельствуют о наличии острой необходимости в разработке универсальной методологии оценки киберугроз и идентификации рисков для систем промышленной автоматизации. В связи с этим необходим целостный подход, позволяющий учитывать уникальные особенности каждой конкретной системы, оценивать типы угроз и потенциальных рисков, их вероятность и последствия компрометации. Такая задача остается крайне сложной из-за разнообразия архитектур промышленных систем, различий в уровнях защищенности и широты спектра возможных угроз. Более подробно с решениями научно-технических задач такого рода можно ознакомиться в [6–9].

Несмотря на значительное число выполненных исследований и предложений по совершенствованию методов анализа и тестирования промышленной инфраструктуры, в настоящее время отсутствует единый стандартизированный подход, пригодный для любой системы автоматизации и управления. Большинство предлагаемых методик недостаточно полно раскрывают картину возможных угроз и ограничиваются лишь поверхностным описанием действий злоумышленника, не отражая полной картины потенциального ущерба [10–12].

Международные стандарты в области кибербезопасности системы автоматизации и управления технологическими процессами, например, такие как ГОСТ, ISO и IEC, разрабатываются ведущими организациями и институтами. Однако разработчики ПО и другие специалисты, использующие предлагаемые документы, не способны обеспечить исчерпывающего решения при оценке всех уровней риска и уязвимостей промышленных систем [13–15].

Цель настоящей работы — анализ подходов к разработке методологии оценки рисков информационной безопасности для промышленных систем автоматизации и управления (ПСАиУ).

Материалы и методы исследования. Методологическую основу настоящего исследования составили авторитетные публикации и международные стандарты в области информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП), например,

руководство Национального института стандартов и технологий США (NIST SP 800–82), спецификация Международной электротехнической комиссии (ISA/IEC 62443), классификация атак CAPEC™ (Common Attack Pattern Enumeration and Classification), а также признанные инструментарии анализа угроз, в числе которых модель STRIDE и структура обмена индикаторами угроз STIX. Основополагающим этапом исследования стал углубленный систематический обзор экспертной литературы, посвященной различным подходам к моделированию угроз и оценке рисков в киберфизических системах.

Результаты и их обсуждение. Первый шаг исследования заключается в выделении характерных признаков систем автоматизации и управления промышленной средой. Подобные системы осуществляют непосредственное управление физическими процессами производства, включающими в себя эксплуатацию оборудования и инфраструктурных компонентов, тогда как классические информационные технологии занимаются обработкой данных и функционированием информационных сетей. Поломка такой системы способна повлечь материальный ущерб, длительные остановки оборудования и даже серьезные опасности для здоровья людей. Нарушения функций ПСАиУ могут приводить к катастрофическим последствиям вроде взрывов, токсичных разливов либо массовых отключений электроэнергии, резко отличающихся их от обычных нарушений в традиционном секторе ИТ-безопасности [16].

Эти обстоятельства предопределяют специфику подходов, которые используются при оценке рисков информационной безопасности в ПСАиУ, что отличает их от оценки рисков в традиционных ИТ-системах.

Описание особенностей оценок рисков информационной безопасности в ПСАиУ приведены ниже.

Приоритет последствий — главный фокус смещен с потери данных на физический ущерб; в приоритете обеспечение безопасности персонала, защита окружающей среды и непрерывность технологического процесса.

Киберфизическая природа систем — кибератака имеет прямые и ощутимые последствия в реальном мире, такие как остановка производственной линии, авария на химическом заводе или отключение электроэнергии.

Расширенная поверхность атаки — растущая интеграция промышленных сетей с корпоративными сетями и интернетом создает новые, ранее не существовавшие векторы атак.

Комплексный анализ угроз — оценка рисков должна выходить за рамки технических уязвимостей и включать в себя анализ рисков цепочек поста-

вок (например, зараженное оборудование от поставщика) и угроз несанкционированного удаленного доступа.

Специализированные стандарты — для адекватной оценки рисков применяют профильные международные стандарты (IEC 62443), которые учитывают уникальные характеристики промышленных сред.

Защита систем автоматизации и управления охватывает физическую инфраструктуру производственных мощностей наряду с цифровыми активами, поскольку любая угроза может оказать негативное воздействие на безопасность производственного цикла и стабильность функционирования предприятий. Информация, циркулирующая в таких системах, влияет не только на целостность данных, но и на физическое состояние оборудования, функционирование которого регулируется этими системами. Таким образом, обеспечение информационной безопасности в данном контексте выходит далеко за пределы стандартных мер ИТ-защиты и требует особых подходов к оценке рисков и устранению угроз.

Однако наиболее острой проблемой, характерной для большинства систем автоматизации и управления, является широкое распространение устаревшего оборудования и ПО, которое изначально создавалось без должного внимания к вопросам информационной безопасности. Устаревшие системы широко применяют в действующих производственных линиях, а замена или обновление такого оборудования сопряжено с высокими финансовыми затратами и сложностью интеграции обновленного ПО в действующую инфраструктуру. Многие предприятия предпочитают избегать частых обновлений из-за опасности возможного ухудшения стабильности производственного процесса, задержки и временной остановки производства [17].

Расширение интеграции технологий промышленного интернета вещей (IIoT) заметно увеличивает сложность обеспечения информационной безопасности на уровне производства. Несмотря на то, что IIoT приносит значительную пользу, улучшая эффективность, облегчая мониторинг и управление производством, он же формирует дополнительную угрозу, увеличивая площадь потенциальной атаки. Каждое новое устройство, входящее в состав IIoT-инфраструктуры, потенциально способно стать объектом взлома и источником для более крупной кибератаки.

В результате анализа соответствующих научных трудов и экспертных заключений выделено несколько актуальных методологических подходов, используемых для выявления угроз и оценки рисков в области информационной безопасности систем автоматизации и управления. Наиболее

распространенные методические подходы к оценке рисков информационной безопасности ПСАиУ приведены в табл. 1 (составлена авторами на основе полученных данных в ходе исследования).

Таблица 1

Методические подходы к оценке рисков информационной безопасности ПСАиУ

Методологическое решение	Метод моделирования угроз	Система, к которой обращается	Подход
Моделирование угроз кибербезопасности для организационных сред цепочки поставок	Сочетание графического и формального с ручным процессом моделирования угроз	Моделирование кибератак на цепочку поставок	С использованием инструмента STIX
Разработка сценариев злоупотребления на основе моделирования угроз и шаблонов атак	Графическое с ручным процессом моделирования угроз	Случаи нарушения безопасности в системе технической информации	STRIDE и CAPEC™
Моделирование угроз в киберфизических системах		Архитектура безопасности для общих систем	
Структурированное моделирование угроз системы и анализ мер по их снижению для систем промышленной автоматизации		Энергетические сети и системы управления	Количественный
Моделирование угроз на основе STRIDE для киберфизических систем		Моделирование безопасности общей системы и отдельных элементов	STRIDE

Инструмент STIX предназначен для описания характеристик киберугроз и способов противодействия им. Этот фреймворк фиксирует наблюдаемые события, индикаторы, профили субъектов угроз, а также сценарии атак и техники, используемые злоумышленниками для осуществления нападения.

Методология STRIDE представляет собой классификацию шести категорий угроз информационной безопасности, широко применяемую для анализа уязвимостей в системах автоматизации и управления промышленными процессами. Данный метод выделяет следующие категории угроз: спуфинг (подделка личности), манипулирование данными (фальсификация), отказ от ответственности, нарушение конфиденциальности, блокировка доступа (DoS-атаки) и эскалация прав пользователей (повышение привилегий) [18].

Методология CAPECE™ — систематизированная база данных, содержащая описание известных шаблонов атак, ранжированных по уровню опасности, с рекомендациями по снижению негативных последствий вторжения хакеров.

Вместе с тем основным недостатком многих существующих методологий оценки рисков информационной безопасности ПСАиУ является отсутствие надежных, формализованных подходов к количественному анализу и вычислению объективных метрик рисков. Растущие объемы собранных данных, прогресс в математическом моделировании рисков и угроз создают повышенные требования к качеству методологий и алгоритмов оценки уровня угроз. Огромный массив накапливаемой статистики настоятельно требует создания четко сформулированных и научно обоснованных подходов, позволяющих точно определить приоритеты защитных мер и обоснованно выбрать меры реагирования на инциденты [19].

Отдельного внимания заслуживают отечественные наработки, например [20], в которых приведен алгоритм оценки рисков информационной безопасности АСУ ТП. Преимуществом алгоритма является, во-первых, его согласованность с существующей нормативно-правовой базой (приказы Федеральной службы по техническому и экспортному контролю (ФСТЭК) России, ГОСТ Р ИСО/МЭК 18045–2013), международными стандартами CVSS (Common Vulnerability Scoring System), которые устанавливают требования и регламентируют меры по обеспечению информационной безопасности. Во-вторых, предложенный подход является гибридным, сочетающим в себе методы количественной и качественной оценок рисков, что позволяет провести детальную оценку угроз и уязвимостей в условиях неопределенности видов возможных злоумышленников и их целей.

В то же время подход [20] не лишен определенных недостатков. Представляется, что главный недостаток заключается в том, что процесс оценки основан на анализе уже идентифицированных уязвимостей. Это делает

методику в большей степени реактивной, чем проактивной. Она менее эффективна для оценки рисков, связанных с совершенно новыми векторами атак или еще не известными угрозами, которые не задокументированы в базах данных. Кроме того, алгоритм сфокусирован главным образом на технических аспектах, при этом из виду упускаются нетехнические риски, такие как социальная инженерия, непреднамеренные ошибки персонала или сбои в организационных процессах, которые также могут привести к серьезным последствиям.

Целесообразно отметить предложение [21] рассматривать риски информационной безопасности и меры по управлению ими через призму жизненного цикла АСУ ТП. Заслуживает внимания составленная карта реализуемых функций подсистемы мониторинга состояния информационной безопасности в различных режимах функционирования. Практическую ценность имеют составные элементы системы анализа и мониторинга состояния информационной безопасности, из числа которых выделены: подсистемы мониторинга состояния информационной безопасности, анализа и корреляции событий информационной безопасности, оценки соответствия требованиям по информационной безопасности. С учетом отмеченных элементов в [21] описано соответствие мероприятий информационной безопасности и функций соответствующих подсистем.

В настоящее время в России наработана широкая нормативно-правовая база, которая регламентирует вопросы, связанные с информационной безопасностью объектов критической информационной инфраструктуры (КИИ). Существующими документами устанавливаются требования к методологии оценки рисков, определяются полномочия регулирующих органов и технические меры защиты объектов. Отдельный акцент необходимо сделать на том, что используемые стандарты гармонизированы с международными. Детальная информация о регуляторной базе приведена в табл. 2.

Таблица 2

Нормативная база по оценке рисков информационной безопасности для АСУ ТП на объектах КИИ

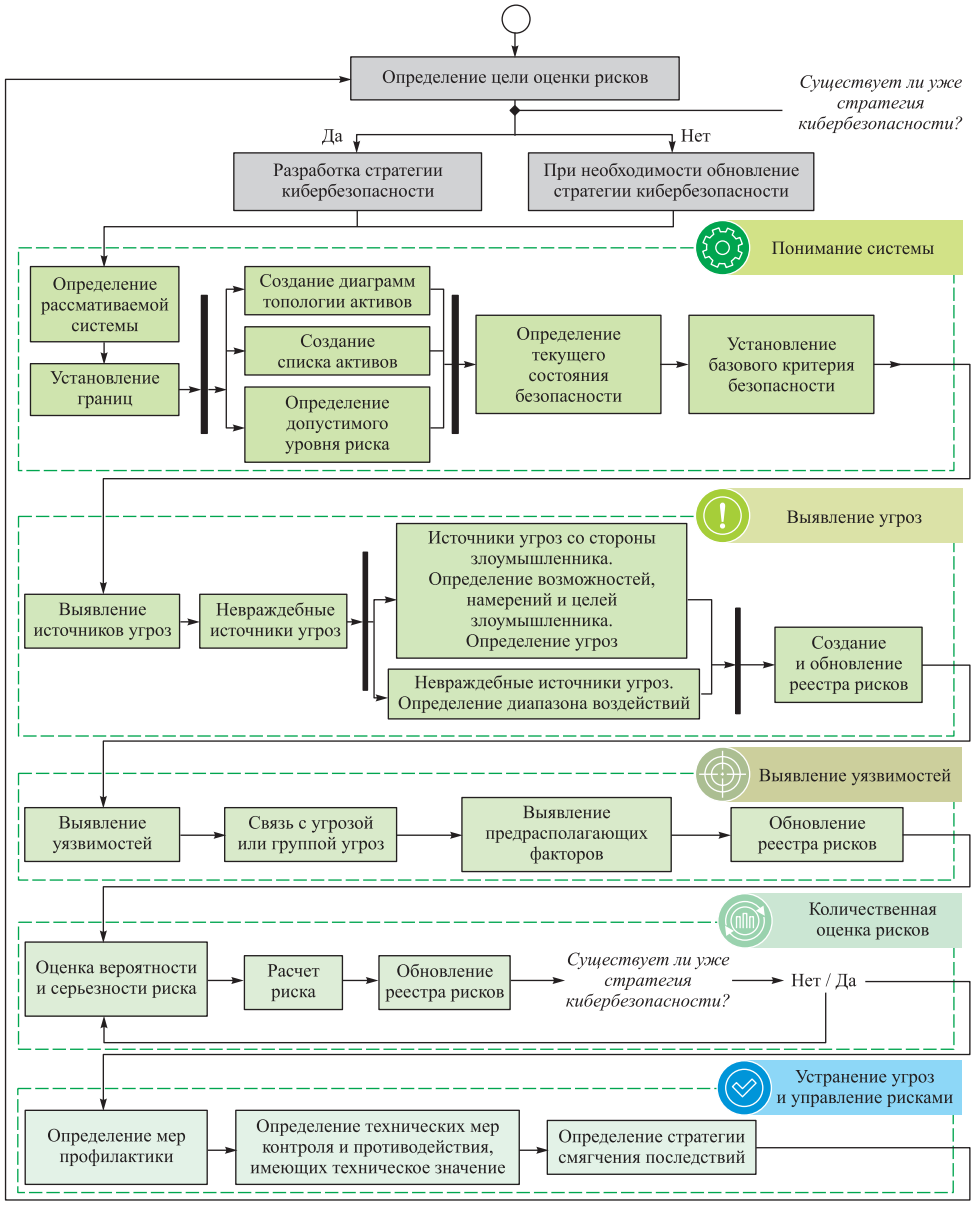
Название документа	Ключевая роль и содержание
Закон	
Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	Вводятся понятия КИИ, определяются права, обязанности и ответственность субъектов КИИ

Окончание табл. 2

Название документа	Ключевая роль и содержание
Постановления Правительства	
Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации»	Устанавливаются критерии и показатели значимости для присвоения объектам КИИ одной из трех категорий
Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры»	Определяется порядок проведения проверок и надзора за обеспечением безопасности значимых объектов КИИ
Приказы ФСТЭК	
Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»	Детализируются состав и содержание организационных и технических мер защиты, обязательных для каждой категории значимости объектов КИИ
Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры»	Регулируются процессы проектирования, создания и ввода в эксплуатацию систем безопасности на объектах КИИ
Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»	Устанавливаются правила включения объектов в реестр значимых объектов КИИ
Национальные стандарты	
ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности	Предоставляется руководство по процессам идентификации, анализа, оценки и обработки рисков информационной безопасности

По мнению авторов настоящей работы, одно из перспективных направлений решения проблемы заключается в применении технологий когнитивного моделирования, основанных на методике построения и анализа нечетких («серых») когнитивных карт. Такой подход продемонстрировал результативность при изучении сложных многомерных сценариев, характеризуемых наличием неопределенностей и вероятностных факторов. В соот-

ветствии с изложенным на рисунке приведена разработанная авторами оригинальная методология оценки рисков информационной безопасности ПСАиУ.



Методология оценки рисков информационной безопасности ПСАиУ

Предлагаемая методология предусматривает деление всех составляющих элементов ПСАиУ на три класса, исходя из степени доступности сведений об их внутренней структуре и характеристиках.

1. Белые системы — системы, чьи внутренние компоненты, архитектура и функциональные свойства полностью раскрыты и детально изучены.

2. Серые системы характеризуются лишь фрагментарной осведомленностью исследователя об устройстве и особенностях работы.

3. Черные системы представляют собой объект полного незнания, где сведения о внутреннем строении и параметрах функционирования отсутствуют.

Более глубокая лексическая интерпретация и математическое представление упомянутых концепций белых, серых и черных систем, а также методов их когнитивного моделирования приведены в [6, 22].

Отдельно следует отметить, что, в отличие от традиционного представления нечетких когнитивных карт, веса связей нечетких серых когнитивных карт устанавливаются с использованием серых (интервальных) чисел $\otimes W_{ij}$, определяемых как $\otimes W_{ij} \in \left[\underline{W_{ij}},\ \overline{W_{ij}}\right]$, где $\underline{W_{ij}}$ и $\overline{W_{ij}}$ — нижняя и верхняя границы серого числа, $\underline{W_{ij}} < \overline{W_{ij}}$, $\left[\underline{W_{ij}},\ \overline{W_{ij}}\right] \in [-1,1]$. Таким образом, вес связи между i-м и j-м понятиями $(C_i \to C_j)$ может принимать любое значение в заданном диапазоне изменения.

Несомненно, что для приведенной методологии оценки рисков требуется автоматизация, которая может обеспечить реализацию стратегии упреждающего выявления слабых мест в ПСАиУ. Разнообразие сегодняшних промышленных сред и приложений чрезвычайно велико. В табл. 3, составленной на основе полученных данных в ходе исследования, приведены разнообразные аспекты автоматизации оценки рисков. Здесь учтены уровень сложности каждой задачи, достигнутые промежуточные результаты и комментарии, относящиеся ко всем этапам комплексного подхода, предназначенного для промышленных сред SCADA и ICS.

В целях демонстрации работоспособности предложенной методики проведем ее апробацию на практическом примере. Для расчетов используем модель АСУ ТП насосной станции. Ключевые понятия (концепты) информационной безопасности включают в себя:

– C1: уязвимость программно-логического контроллера (ПЛК);

– C2: надежность межсетевого экрана;

– C3: осведомленность персонала;

– C4: состояние риска для АСУ ТП (целевой показатель).

Таблица 3

Требования к системе автоматизации оценки рисков информационной безопасности для ПСАиУ

Задача	Сложность	Достижения	Примечание
Обнаружение устройств	Низкая	Легкое обнаружение изменений в сети	Широкий спектр методов
Сканирование уязвимостей		Повторяемость	Различные базы данных, в том числе статические
Непрерывный мониторинг		Информация в режиме реального времени и автоматическое реагирование	Различные базы данных, в том числе динамические
Интеграция с системой анализа угроз	Высокая	Проактивность	Не все системы диспетчерского контроля, сбора данных и ПСАиУ имеют открытый API для управления конфигурацией
Управление конфигурацией и проверка соответствия		Быстрая и простая перенастройка	Не все системы диспетчерского контроля, сбора данных и ПСАиУ имеют открытый API; тесты могут вывести из строя рабочую систему
Автоматизация тестирования на проникновение		Повторяемость	Не все системы диспетчерского контроля, сбора данных и ПСАиУ имеют открытый API; ложные срабатывания могут вывести систему из строя
Автоматизация плана реагирования на инциденты		Автоматическое реагирование	

Оценка рисков и определение приоритетов	Умеренная	Быстрое устранение наиболее серьезных уязвимостей	–
Интеграция с системами управления задачами	Низкая	Простое отслеживание	
Машинное обучение для обнаружения аномалий	Высокая	Проактивность	
Интеграция с платформой для совместной работы		Простое отслеживание	

Расчет итогового риска ($\otimes X_4$) проводился на основе начальных оценок состояния концептов и весов их взаимосвязей, представляющих собой серые (интервальные) числа для моделирования неопределенности. Полученные результаты приведены в табл. 4.

Таблица 4

Результаты апробации методологии оценки рисков информационной безопасности АСУ ТП насосной станции

Параметр	Обозначение	Начальное значение (интервал)	Описание
Уязвимость ПЛК	$\otimes X_1$ (0)	[0,8; 1,0]	Известна критическая, неисправленная уязвимость
Надежность экрана	$\otimes X_2$ (0)	[–0,6; –0,4]	Экран настроен, но есть сомнения в актуальности правил
Осведомленность персонала	$\otimes X_3$ (0)	[0,3; 0,5]	Персонал обучен, но фиксировались попытки фишинга
Итоговый риск	$\otimes X_4$ (1)	[0,92; 1,0]	Рассчитанный уровень риска для системы

Полученный результат [0,92; 1,0] указывает на критически высокий уровень риска. Этот количественный показатель позволяет перейти от общих оценок к конкретным действиям, предписанным регуляторами.

1. Обоснование адаптации мер защиты: в соответствии с Приказом ФСТЭК России от 25.12.2017 № 239, базовый набор мер защиты должен быть адаптирован, если он не позволяет обеспечить блокирование (нейтрализацию) всех угроз безопасности информации. Полученный высокий количественный показатель риска является числовым обоснованием для проведения такой адаптации. На практике это может означать включение в набор мер защиты для насосной станции отдельных мероприятий, которые установлены Приказом № 239 для более высоких категорий значимости.

2. Приоритизация действий: в соответствии с ГОСТ Р ИСО/МЭК 27005–2010 методика позволяет не только измерить риск, но и выявить его главный источник (уязвимость ПЛК). Это дает возможность приоритизировать меры по обработке риска, например, немедленно установить обновления безопасности для контроллера.

Отметим, что предложенная методология является инструментом выполнения регламентированных в России требований к защите и обеспечению информационной безопасности ПСАиУ.

Заключение. Переход к реалиям Индустрии 4.0 стимулирует предприятия формировать современную производственную экосистему, базирующуюся на обработке больших объемов данных, развертывании информационных систем и осуществлении удаленных управляющих воздействий. Такая среда оказывает положительное влияние как на общий экономический эффект функционирования предприятия, так и на качественные характеристики выпускаемого продукта. Тем не менее активное внедрение систем автоматизации и управления промышленными процессами сопровождается значительным увеличением спектра информационных рисков и угроз. Их реализация чревата негативными последствиями в виде повреждений оборудования, аварийных остановок производства, финансовой нестабильности, убытков от утечек конфиденциальных данных, разрушения целостности системы, задержек в выпуске продукции, а также правовых претензий и нанесения вреда деловой репутации предприятия.

Исходя из актуальности указанной проблематики, предложено оригинальное решение вопроса оценки рисков информационной безопасности ПСАиУ. Разработанная авторами методология направлена на проведение полноценного анализа и моделирования возможных вариантов реализации угроз посредством метода топологического анализа и использования инструмента нечетких серых когнитивных карт. Приведенный подход направлен на развитие механизма автоматического оценивания рисков, который позволяет адекватно учитывать многообразие сценариев угроз и вариабельность протекающих процессов в реальных условиях эксплуатации промышленных систем.

Апробация методологии проведена на примере АСУ ТП насосной станции. Полученные результаты позволяют утверждать, что предлагаемая методология дает инструмент, который переводит требования нормативной базы в плоскость измеряемых показателей, позволяя принимать обоснованные решения по управлению рисками информационной безопасности на объектах КИИ.

ЛИТЕРАТУРА

[1] Паршин Р.Г. Новая эра информационной безопасности в промышленности: вызовы, угрозы, решения. *Управление качеством*, 2024, № 10, с. 36–40.
DOI: https://doi.org/10.33920/pro-01-2410-06

[2] Мельников Н.М., Никишкин А.В., Ветрова Е.В. и др. Системы охраны с искусственным интеллектом стратегически важных инфраструктурных объектов. *Информатизация и связь*, 2023, № 1, с. 44–50.
DOI: https://doi.org/10.34219/2078-8320-2023-14-1-44-50

[3] Журавлев С.И., Сидак А.А., Кадомкин В.В. и др. Нормативно-методические аспекты мониторинга безопасности автоматизированных информационных систем в промышленности. *Автоматизация в промышленности*, 2022, № 10, с. 44–50. DOI: https://doi.org/10.25728/avtprom.2022.10.09

[4] Малиев Д.А., Миськов Д.В., Назаренко М.А. Управление рисками информационной безопасности на предприятии электронной промышленности. *Нелинейный мир*, 2022, т. 20, № 4, с. 51–59. DOI: https://doi.org/10.18127/j20700970-202204-05

[5] Шарлаев Е.В., Ткаченко Д.М. Исследование подходов к контролю состояний защищенности программной среды автоматизированных систем и разработка методики комплексного подхода к обеспечению защищенности программной среды и инфраструктуры организации. *Наукосфера*, 2022, № 7-1, с. 167–171.
EDN: DQXXTK

[6] Tiwari P.K., Pandey S.K., Meshach W.T., et al. Improved data security in cloud environment for test automation framework and access control for Industry 4.0. *Wirel. Commun. Mob. Comput.*, 2022, art. 3242092. DOI: https://doi.org/10.1155/2022/3242092

[7] Vangala A., Das A.K, Kumar N., et al. Designing access control security protocol for Industry 4.0 using Blockchain-as-a-Service. *Secur. Priv.*, 2024, vol. 7, no. 2, art. e362.
DOI: https://doi.org/10.1002/spy2.362

[8] Тырышкин С.Ю. Информационная безопасность при использовании технологий нейронных сетей. *Международный журнал гуманитарных и естественных наук*, 2025, № 4-1, с. 226–230.
DOI: https://doi.org/10.24412/2500-1000-2025-4-1-226-230

[9] Чернышова Т.В., Чернышова Е.А., Титков А.А. Внедрение информационных технологий и автоматизации в промышленность: проблемы и пути решения. *Современная наука: актуальные проблемы теории и практики. Сер. Естественные и технические науки*, 2024, № 3, с. 130–134. EDN: BQATUO

[10] Краснов А.Е., Чеканов И.Р., Козочкин И.Д. Автоматизация поддержки принятия управленческих решений в области информационной безопасности на основе технологии экспертных систем. *Информатизация образования и науки*, 2023, № 2, с. 81–89. EDN: TKLBEM

[11] Jiang Y., Wang B. Analysis on network information security protection technology of intelligent terminal power monitoring system of substation under the support of multimodal multimedia information. *Adv. Multimed.*, 2023, art. 8607305.
DOI: https://doi.org/10.1155/2023/8607305

[12] Егоров И.В., Щавелев П.А. Несанкционированный доступ к промышленной инфраструктуре: инциденты и решения. *Перспективные технологии для систем безопасности*, 2023, № 2, с. 32–43. EDN: OBLERC

[13] Степанов Е.В. Цифровая трансформация промышленных предприятий на основе интеллектуальных решений концепции «Промышленность 4.0». *Вестник Самарского университета. Экономика и управление*, 2022, т. 13, № 1, с. 49–55.
DOI: https://doi.org/10.18287/2542-0461-2022-13-1-49-55

[14] He J., Sun Y. Information security countermeasures for big data platforms based on cloud computing. *Mob. Inf. Syst.*, 2022, art. 3981775.
DOI: https://doi.org/10.1155/2022/3981775

[15] Shubham J., Audumbar P.A., Manish S., et al. Adoption of blockchain technology for privacy and security in the context of Industry 4.0. *Wirel. Commun. Mob. Comput.*, 2022, art. 4079781. DOI: https://doi.org/10.1155/2022/4079781

[16] Филяк П.Ю., Тырин И.А., Пажинцев Д.А. Информационная безопасность киберфизических систем. *Информация и безопасность*, 2022, т. 25, № 3, с. 433–452.
DOI: https://doi.org/10.36622/VSTU.2022.25.3.012

[17] Lampropoulos G., Siakas K. Enhancing and securing cyber-physical systems and Industry 4.0 through digital twins: a critical review. *J. Softw. Evol. Proc.*, 2023, vol. 35, no. 7, art. e2494. DOI: https://doi.org/10.1002/smr.2494

[18] Sun H., Bai S. Enterprise information security management using internet of things combined with artificial intelligence technology. *Comput. Intell. Neurosc.*, 2022, art. 7138515. DOI: https://doi.org/10.1155/2022/7138515

[19] Ребро И.В., Шарлаев Е.В. Построение системы обнаружения сетевых вторжений на базе искусственных иммунных систем и нейронных сетей. *Ползуновский альманах*, 2016, № 2, с. 145–147. EDN: XHVZWL

[20] Иваненко В.Г., Иванова Н.Д. Оценка рисков информационной безопасности автоматизированных систем управления технологическим процессом. *Вопросы кибербезопасности*, 2024, № 1, с. 116–123.
DOI: https://doi.org/10.21681/2311-3456-2024-1-116-123

[21] Комаров А.В. Обеспечение информационной безопасности при эксплуатации АСУ ТП. *Защита информации. INSIDE*, 2016, № 2, с. 50–53. EDN: VSBKNL

[22] Тырышкин С.Ю. Эмуляция квантовых вычислительных процессов для автоматизированных систем управления на классическом ПК. *Современная наука: актуальные проблемы теории и практики. Сер. Естественные и технические наук*и, 2024, № 12, с. 130–134.

Тырышкин Сергей Юрьевич — канд. техн. наук, доцент, доцент кафедры «Информатика, вычислительная техника и информационная безопасность» АлГТУ (Российская Федерация, 656000, г. Барнаул, пр-т Ленина, д. 46 Б).

Шарлаев Евгений Владимирович — канд. техн. наук, доцент кафедры «Информатика, вычислительная техника и информационная безопасность» АлГТУ (Российская Федерация, 656000, г. Барнаул, пр-т Ленина, д. 46 Б).

Просьба ссылаться на эту статью следующим образом:

Тырышкин С.Ю., Шарлаев Е.В. Методология оценки рисков информационной безопасности для систем промышленной автоматизации и управления. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*, 2026, № 2 (155), с. 107–127.
EDN: AOYHDJ

METHODOLOGY FOR ASSESSING INFORMATION SECURITY RISKS FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS

S.Yu. Tyryshkin service.vip-spe@yandex.ru
E.V. Sharlaev sharlaev@mail.ru

AltSTU, Barnaul, Russian Federation

Abstract

The article discusses the effective use of information technology in the chemical industry. The relevance of this area stems from the necessity to enhance productivity and competitiveness of enterprises within the chemical industry through active integration of advanced digital solutions. Special emphasis is placed on advantages and specifics of modern information systems and software products: SCADA systems, corporate ERP platforms, specialized analytical tools for modeling and optimization of chemical processes. The article analyzes possible ways of integrating IT tools into production processes and discusses methods for assessing the economic feasibility and effectiveness of implementing such systems. The article provides examples of implementing projects for the automation of chemical production and describes real-life cases of implementing digital solutions that help reduce costs, improve product quality, and ensure safety at enterprises. There is a need for continuous education and retraining of chemical specialists who will have to master and effectively apply modern information technologies in their daily practice. Approaches to developing and enhancing professional competencies under conditions of transition towards digital methods of design, analysis, and management of chemical-technology enterprises are discussed in detail. The results of the methodology's testing will serve as an effective tool that translates the requirements of the regulatory framework into measurable indicators, allowing for informed decisions on managing information security risks

Keywords

Industry, automation, threats, risks, protection, assessment, cognitive map

Received 10.09.2025
Accepted 16.05.2026

REFERENCES

[1] Parshin R.G. New era of information security in industry: challenges, threats, solutions. *Upravlenie kachestvom* [Quality Management], 2024, no. 10, pp. 36–40 (in Russ.). DOI: https://doi.org/10.33920/pro-01-2410-06

[2] Melnikov N.M., Nikishkin A.V., Vetrova E.V., et al. Security systems with artificial intelligence strategically important infrastructural facilities. *Informatizatsiya i svyaz* [Informatization and Communication], 2023, no. 1, pp. 44–50 (in Russ.). DOI: https://doi.org/10.34219/2078-8320-2023-14-1-44-50

[3] Zhuravlev S.I., Sidak A.A., Kadomkin V.V., et al. Regulatory and methodological aspects of security monitoring of automated information systems in industry. *Avtomatizatsiya v promyshlennosti*, 2022, no. 10, pp. 44–50 (in Russ.). DOI: https://doi.org/10.25728/avtprom.2022.10.09

[4] Maliev D.A., Miskov D.V., Nazarenko M.A. Information security risk management in the electronics industry. *Nelineynyy mir* [Nonlinear World], 2022, vol. 20, no. 4, pp. 51–59 (in Russ.). DOI: https://doi.org/10.18127/j20700970-202204-05

[5] Sharlaev E.V., Tkachenko D.M. Research of approaches to control the security conditions of the software environment of automated systems and development of a methodology for an integrated approach to ensuring the security of the software environment and infrastructure of the organization. *Naukosfera*, 2022, no. 7-1, pp. 167–171 (in Russ.). EDN: DQXXTK

[6] Tiwari P.K., Pandey S.K., Meshach W.T., et al. Improved data security in cloud environment for test automation framework and access control for Industry 4.0. Wirel. *Commun. Mob. Comput*., 2022, art. 3242092. DOI: https://doi.org/10.1155/2022/3242092

[7] Vangala A., Das A.K., Kumar N., et al. Designing access control security protocol for Industry 4.0 using Blockchain-as-a-Service. *Secur. Priv*., 2024, vol. 7, no. 2, art. e362. DOI: https://doi.org/10.1002/spy2.362

[8] Tyryshkin S.Yu. Information security using neural network technologies. *Mezhdunarodnyy zhurnal gumanitarnykh i estestvennykh nauk* [International Journal of Humanities and Natural Sciences], 2025, no. 4-1, pp. 226–230 (in Russ.). DOI: https://doi.org/10.24412/2500-1000-2025-4-1-226-230

[9] Chernyshova T.V., Chernyshova E.A., Titkov A.A. Introduction of information technologies and automation in industry: problems and solutions. *Sovremennaya nauka: aktualnye problemy teorii i praktiki. Ser. Estestvennye i tekhnicheskie nauki* [Modern Science: Actual Problems of Theory and Practice. Ser. Natural and Technical Sciences], 2024, no. 3, pp. 130–134 (in Russ.). EDN: BQATUO

[10] Krasnov A.E., Chekanov I.R., Kozochkin I.D. Automation of management decision support in the field of information security based on expert systems technology. *Informatizatsiya obrazovaniya i nauki* [Informatization of Education and Science], 2023, no. 2, pp. 81–89 (in Russ.). EDN: TKLBEM

[11] Jiang Y., Wang B. Analysis on network information security protection technology of intelligent terminal power monitoring system of substation under the support of multimodal multimedia information. *Adv. Multimed.*, 2023, art. 8607305.
DOI: https://doi.org/10.1155/2023/8607305

[12] Egorov I.V., Shchavelev P.A. Information security incidents in industry: challenges and solutions. *Perspektivnye tekhnologii dlya sistem bezopasnosti* [Promising Technologies for Security Systems], 2023, no. 2, pp. 32–43 (in Russ.). EDN: OBLERC

[13] Stepanov E.V. Digital transformation of industrial enterprises based on intelligent solutions of the Industry 4.0 concept. *Vestnik Samarskogo universiteta. Ekonomika i upravlenie* [Vestnik of Samara University. Economics and Management], 2022, vol. 13, no. 1, pp. 49–55 (in Russ.). DOI: https://doi.org/10.18287/2542-0461-2022-13-1-49-55

[14] He J., Sun Y. Information security countermeasures for big data platforms based on cloud computing. *Mob. Inf. Syst.*, 2022, art. 3981775.
DOI: https://doi.org/10.1155/2022/3981775

[15] Shubham J., Audumbar P.A., Manish S., et al. Adoption of blockchain technology for privacy and security in the context of Industry 4.0. *Wirel. Commun. Mob. Comput.*, 2022, art. 4079781. DOI: https://doi.org/10.1155/2022/4079781

[16] Filyak P.Yu., Tyrin I.A., Pazhintsev D.A. Information security of cyber-physical systems. *Informatsiya i bezopasnost* [Information & Security], 2022, vol. 25, no. 3, pp. 433–452 (in Russ.). DOI: https://doi.org/10.36622/VSTU.2022.25.3.012

[17] Lampropoulos G., Siakas K. Enhancing and securing cyber-physical systems and Industry 4.0 through digital twins: a critical review. *J. Softw. Evol. Proc.*, 2023, vol. 35, no. 7, art. e2494. DOI: https://doi.org/10.1002/smr.2494

[18] Sun H., Bai S. Enterprise information security management using internet of things combined with artificial intelligence technology. *Comput. Intell. Neurosc.*, 2022, art. 7138515. DOI: https://doi.org/10.1155/2022/7138515

[19] Rebro I.V., Sharlaev E.V. Building a network intrusion detection system based on artificial immune systems and neural networks. *Polzunovskiy almanakh*, 2016, no. 2, pp. 145–147 (in Russ.). EDN: XHVZWL

[20] Ivanenko V.G., Ivanova N.D. Information security risk assessment of industrial control systems. *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2024, no. 1, pp. 116–123 (in Russ.). DOI: https://doi.org/10.21681/2311-3456-2024-1-116-123

[21] Komarov A.V. Information security in the SCADA. *Zashchita informatsii. INSIDE*, 2016, no. 2, pp. 50–53 (in Russ.). EDN: VSBKNL

[22] Tyryshkin S.Yu. Emulation of quantum computing processes for automated control systems on a classical PC. *Sovremennaya nauka: aktualnye problemy teorii i praktiki. Ser. Estestvennye i tekhnicheskie nauki* [Modern Science: Actual Problems of Theory and Practice. Ser. Natural and Technical Sciences], 2024, no. 12, pp. 130–134 (in Russ.).

Tyryshkin S.Yu. — Cand. Sc. (Eng.), Assoc. Professor, Department of Computer Science and Information Security, AltSTU (Lenina prospekt 46B, Barnaul, 656000 Russian Federation).

Sharlaev E.V. — Cand. Sc. (Eng.), Assoc. Professor, Department of Computer Science and Information Security, AltSTU (Lenina prospekt 46B, Barnaul, 656000 Russian Federation).

Please cite this article in English as:

Tyryshkin S.Yu., Sharlaev E.V. Methodology for assessing information security risks for industrial automation and control systems. *Herald of the Bauman Moscow State Technical University, Series Instrument Engineering*, 2026, no. 2 (155), pp. 107–127 (in Russ.). EDN: AOYHDJ