Научная статья/Scientific article
УДК 004.056.5:681.5:622
https://dx.doi.org/10.26583/bit.2026.1.03
https://elibrary.ru/wjwlra

АДАПТАЦИЯ МЕТОДИКИ ФСТЭК РОССИИ ДЛЯ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ЗАЩИЩЁННОСТИ НЕФТЕГАЗОВОГО ПРЕДПРИЯТИЯ

Всеволод А. Буркин
РГУ нефти и газа (НИУ) им. И.М. Губкина, Ленинский пр–кт, 65, к. 1, Москва, 119991, Россия
murashkin.v@gubkin.ru

Аннотация. В статье представлен подход к адаптации «Методики оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утверждённой ФСТЭК России 2 мая 2024 г., для предприятий нефтегазового комплекса. Проведённый анализ показал, что базовый набор показателей, предложенный регулятором, недостаточно полно отражает отраслевую специфику, связанную с непрерывностью производственных процессов и критичностью автоматизированных систем управления технологическими процессами (АСУ ТП). Предложена расширенная система количественных и качественных показателей, учитывающих не только технические характеристики систем защиты, но и организационные аспекты управления информационной безопасностью, такие как уровень подготовки и вовлечённости персонала, своевременность обновления программного обеспечения, относительное время простоя критически важных объектов вследствие киберинцидентов, а также полноту реализации плановых мероприятий. Разработанные показатели позволяют комплексно и объективно оценивать текущее состояние защищенности, своевременно выявлять проблемные зоны и приоритизировать ресурсы на наиболее уязвимых направлениях. В работе приведены рекомендации по практическому внедрению и развитию предложенной системы показателей, включая формирование интегрированной инфраструктуры сбора данных, автоматизацию вычисления показателей и использование современных инструментов мониторинга. Применение предложенного подхода позволит предприятиям нефтегазовой отрасли перейти от формальной проверки требований регулятора к эффективному управлению информационной безопасностью на основе объективных и измеримых критериев, минимизировать риски возникновения киберинцидентов и снизить возможный экономический ущерб от остановки производства.

Ключевые слова: *информационная безопасность, оценка защищённости, топливно-энергетический комплекс, критическая информационная инфраструктура, нефтегазовая отрасль, автоматизированные системы управления, интегральный показатель, метрики безопасности*

Для цитирования: Буркин, В. (2026). Адаптация методики ФСТЭК России для количественной оценки защищённости нефтегазового предприятия. *Безопасность информационных технологий,* 33(1), 29-39. doi: http://dx.doi.org/10.26583/bit.2026.1.03

ADAPTATION OF THE FSTEC METHODOLOGY FOR QUANTITATIVE ASSESSMENT OF CYBERSECURITY AT AN OIL AND GAS ENTERPRISE

Vsevolod A. Burkin
Gubkin University, Leninsky Ave., 65, Bldg. 1, Moscow, 119991, Russia
murashkin.v@gubkin.ru

Abstract. The article presents an approach to adapting the methodology for assessing the security status of information systems, approved by the FSTEC of Russia on May 2, 2024, for oil and gas enterprises. The analysis showed that the basic set of indicators proposed by the regulator does not fully reflect the industry specifics related to the continuity of production processes and the criticality of Industrial Control Systems (ICS). The author propose an expanded system of quantitative and qualitative indicators that take into account not only the technical characteristics of security systems, but also organizational aspects of information security management, such as the level of training and involvement of personnel, timely software updates, relative downtime of critical facilities due to cyber incidents, as well as the completeness of planned measures. The developed indicators allow for a comprehensive and objective assessment of the current state of security,

timely identification of problem areas and prioritization of resources in the most vulnerable areas. The paper provides recommendations for the practical implementation and development of the proposed system of indicators, including the formation of an integrated data collection infrastructure, automation of the calculation of indicators and the use of modern monitoring tools. The application of the proposed approach will allow oil and gas industry enterprises to move from formal verification of regulatory requirements to effective information security management based on objective and measurable criteria, minimize the risks of cyber incidents and reduce possible economic damage from production shutdowns.

Keywords: *information security, protection assessment, fuel and energy complex, critical information infrastructure, oil and gas sector, automated control systems, integral index, security metrics*

For citation: Burkin, V. (2026). Adaptation of the FSTEC methodology for quantitative assessment of cybersecurity at an oil and gas enterprise. *IT Security (Russia),* 33(1), 29-39. doi: http://dx.doi.org/10.26583/bit.2026.1.03

Введение

Обеспечение информационной безопасности (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) является одной из приоритетных задач предприятий нефтегазового комплекса. Это обусловлено высокой критичностью таких систем для стабильного функционирования объектов отрасли и потенциально значительным экономическим ущербом от киберинцидентов [1–3]. В настоящее время существуют требования по информационной безопасности, установленные регуляторами, в первую очередь ФСТЭК России. Однако общие подходы, предложенные регуляторами, зачастую недостаточно учитывают специфику предприятий нефтегазовой отрасли. Это связано с необходимостью непрерывности технологических процессов, высокой степенью распределенности объектов и спецификой архитектуры АСУ ТП, что требует особого подхода к оценке состояния информационной безопасности [2, 4].

В связи с этим актуальной задачей является адаптация методик количественной оценки защищенности информационных систем с учётом отраслевых особенностей, что позволит повысить точность и объективность оценки уровня защищённости предприятий. Целью данной работы является разработка адаптированной системы показателей состояния защищённости, обеспечивающей количественное и качественное отражение уровня защиты АСУ ТП на предприятиях нефтегазового комплекса, а также формулирование практических рекомендаций по внедрению и развитию такой системы.

1. Методические подходы к оценке состояния защищённости

Показатель состояния защищённости не сводится к одной-единственной цифре: он формируется на основе комплекса показателей, связанных с технологическими, организационными и человеческими факторами [1, 2]. Однако для удобства управления и сравнения объектов на практике используют интегральный индекс [5, 6], отражающий совокупный уровень безопасности.

Существуют различные подходы к оценке защищённости объектов:

1. Стандарты серии ISO/IEC 27000.

Данные стандарты содержат комплекс требований к организации системы управления ИБ (СУИБ)[1], включая технические, организационные и кадровые аспекты. Основное преимущество – комплексный подход, но недостатком является отсутствие учёта отраслевой специфики [1].

2. Методика ФСТЭК России (от 02.05.2024).

Данный документ устанавливает комплексный подход к оценке состояния технической защиты информации и применим к значимым объектам КИИ, в том числе к нефтегазовым предприятиям. Предлагает конкретные критерии и показатели оценки защищённости, позволяющие оценить соответствие установленным требованиям безопасности и уровень риска, однако методика носит универсальный характер и не учитывает специфики

[1]ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. URL: https://www.iso.org/contents/data/standard/05/45/54534.html (дата обращения: 12.07.2025).

предприятий ТЭК, особенно особенностей автоматизированных систем управления технологическими процессами (АСУ ТП)[2].

3. Риск-ориентированный подход

Позволяет учитывать угрозы и возможные последствия, оценивая вероятность и ущерб от их реализации. Недостаток подхода – сложность оценки и субъективность, зависящая от опыта аналитиков [7].

Риск-ориентированная модель базируется на том, что каждое предприятие определяет критичные активы и оценивает для них угрозы и уязвимости [8]. Риск R зачастую выражают формулой:

$$R = P \times C,$$

где P – вероятность реализации угрозы, C – последствия (ущерб) при реализации угрозы.

Для нефтегазовых объектов ущерб может включать как прямой финансовый урон (простой оборудования, штрафы регуляторов), так и косвенный (экологические последствия, потеря репутации, угрозы для жизни и здоровья персонала) [6].

4. Непрерывный мониторинг (SIEM, SOC).

Позволяет отслеживать события ИБ в режиме реального времени, но требует высокой степени автоматизации и квалифицированного персонала [9].

Современные инструменты (SIEM, SOC, системы IDS/IPS) позволяют вести сбор событий ИБ в реальном времени, отслеживая аномалии в сети, несанкционированные действия пользователей, попытки вторжения. Информация о количестве и критичности инцидентов, времени их обнаружения и устранения (MTTD, MTTR) используется для расчёта динамического компонента показателя защищённости.

5. Серия IEC 62443 «Industrial Automation and Control Systems Security»

Международная серия стандартов IEC 62443 [3]формирует целостную методическую основу кибербезопасности промышленных автоматизированных систем, охватывая все этапы их жизненного цикла – от проектирования и интеграции до эксплуатации и вывода из эксплуатации. Центральным элементом является модель зон и каналов, предписывающая сегментацию OT-инфраструктуры по критичности и отдельную оценку рисков для коммуникационных путей. Для каждой зоны могут устанавливаться уровни безопасности SL1–SL4, определяющие стойкость к противнику заданной квалификации и конкретизирующие требования к аутентификации, контролю потоков данных, целостности, своевременности отклика и другим функциям защиты. Стандарты вводят ролевую модель «поставщик – системный интегратор – владелец актива», распределяя обязанности по управлению уязвимостями, испытаниям и сопровождению; кроме того, предусмотрена процедура оценки соответствия с возможностью сертификации как отдельных компонентов, так и всей системы, что особенно востребовано на глобальном рынке нефтегазового оборудования.

Для нефтегазовых предприятий достоинством IEC 62443 является строгая увязка требований с уровнем риска, позволяющая точечно повышать уровень безопасности наиболее критичных участков, таких как насосные станции магистрального трубопровода, равно как и встроенная совместимость с нормативами функциональной безопасности IEC 61508/61511. Однако применение серии сопровождается существенными ограничениями. Полноценное внедрение требует комплексной инвентаризации активов, переработки архитектуры распределённых месторождений и регулярной валидации зон и каналов, что серьёзно усложняет проект и увеличивает сроки. На российском рынке пока недостаточно устройств и программных решений с подтверждённым соответствием IEC 62443, поэтому компаниям

[2]Методический документ «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» Утвержден ФСТЭК России 2 мая 2024 г. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-2-maya-2024-g (дата обращения: 12.07.2025).

[3]ISA/IEC 62443 Series of Standards URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (дата обращения: 12.07.2025).

приходится формировать собственные доказательства или комбинировать контрольные процедуры с национальными регуляторными актами. Терминология и структура требований стандарта не полностью совпадают с положениями ФЗ-187[4] и методиками ФСТЭК России, что порождает необходимость двойных аудитов и усложняет отчётность. Наконец, достижение уровней SL3–SL4 для оборудования во взрывоопасных зонах требует дорогих аппаратных доработок и иногда ведёт к росту задержек в сетях реального времени, что критично для управляющих контуров.

6. Национальные стандарты РФ, применимые к АСУ ТП

К адаптации требований кибербезопасности на нефтегазовых предприятиях чаще всего привлекают четыре базовых национальных стандарта. Во-первых, ГОСТ Р МЭК 62443-2-1-2015 и ГОСТ Р МЭК 62443-3-3-2016 – российские издания международной серии IEC 62443, регулирующие соответственно создание программы управления кибербезопасностью IACS[5] и системные требования безопасности с уровнями SL1–SL4[6]. Во-вторых, ГОСТ Р 51583-2014 задаёт порядок создания автоматизированных систем в защищённом исполнении и детализирует содержание документации на этапах жизненного цикла[7]; а ГОСТ Р ИСО/МЭК 27019-2021 переносит принципы ISO/IEC 27002 на управление технологическими процессами энергетической (неатомной) отрасли, что позволяет единообразно выстраивать систему менеджмента информационной безопасности от корпоративного уровня до полевых контроллеров[8].

Комплекс этих документов обеспечивает прямое соответствие национальным регуляторным требованиям ФСТЭК России и охватывает как процессные, так и технические аспекты защиты АСУ ТП. Тем не менее, внедрение стандартов сопряжено с важными ограничениями. Российское издание IEC 62443 опирается на риск-ориентированную модель зон и каналов, требующую трудоёмкой инвентаризации активов и постоянной валидации, а наличие на рынке сертифицированных решений, отвечающих требованиям SL3–SL4, остаётся ограниченным. ГОСТ Р 51583-2014 акцентируется на документарных процедурах, что усложняет поддержание актуальных отчётов для распределённых месторождений, а пересечение его терминологии с ФЗ-187 вносит неоднозначность в трактовку обязанностей ответственных лиц. ГОСТ Р ИСО/МЭК 27019-2021, будучи адаптацией для энергетики, формулирует меры на относительно абстрактном уровне и недостаточно учитывает взрывоопасные зоны и специфику непрерывных технологических процессов нефтепереработки. Как следствие, предприятия вынуждены дополнительно уточнять профили защитных мер и разрабатывать компенсирующие процедуры, чтобы избежать избыточных вложений и конфликтов с требованиями промышленной безопасности.

7. NIST SP 800-82 «Guide to Industrial Control Systems Security»

NIST SP 800-82 остаётся наиболее детальным открытым руководством по защите технологических сетей. Документ последовательно описывает архитектуру современных OT-сегментов, характерные уязвимости контроллеров, сенсоров и промежуточных шлюзов, а также методику оценки киберрисков, основанную на влиянии атак на безопасность персонала, окружающую среду и непрерывность технологических процессов. Отдельный акцент сделан на том, что переход АСУ ТП к IP-стеку и растущая интеграция с корпоративными ИТ-сервисами увеличивают площадь атаки: IoT-устройства, собирающие данные с датчиков

[4]Федеральный закон от 26.07.2017 №187-ФЗ – «О безопасности критической информационной инфраструктуры Российской Федерации».

[5]ГОСТ Р МЭК 62443-2-1-2015 «Сети коммуникационные промышленные. Защищённость (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищённости (кибербезопасности) системы управления и промышленной автоматики».

[6]ГОСТ Р МЭК 62443-3-3-2016 «Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности».

[7]ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения».

[8]ГОСТ Р ИСО/МЭК 27019-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Меры обеспечения информационной безопасности в энергетике (неатомной)».

и актюаторов, выводят полевые сети в Интернет и тем самым повышают вероятность успешной эксплуатации уязвимостей [10].

Руководство предлагает базовую трёхзонную модель «корпоративная сеть – DMZ – зона управления», формализует подход к сегментации и определяет перечень технических мер (сегментация, whitelisting команд, защищённый удалённый доступ, резервное копирование прошивок) в увязке с каталогом техник атак на Modbus, OPC UA и DNP3. Для нефтегазовых объектов приведены примеры создания буферной DMZ между ЦОД и удалёнными SCADA-станциями добычи, а также рекомендации по защите контроллеров, расположенных во взрывоопасных зонах. Использование NIST SP 800-82 в составе интегрального показателя позволяет количественно учесть долю сегментированных узлов, частоту обновлений прошивок и степень покрытия сетевого трафика мониторингом, что даёт объективную картину защищённости.

В то же время прямое перенесение требований NIST SP 800-82 на российские нефтегазовые предприятия сталкивается с несколькими ограничениями. Во-первых, документ ориентирован на нормативную базу США и не учитывает процедур лицензирования ФСТЭК России, а терминология его контролей требует соотнесения с национальными стандартами, прежде всего с ГОСТ Р МЭК 62443-2-1-2015, ГОСТ Р МЭК 62443-3-3-2016, ГОСТ Р 51583-2014 и ГОСТ Р ИСО/МЭК 27019-2021. Во-вторых, многие рекомендации предполагают высокую зрелость процессов OT-мониторинга и наличие специализированного персонала, что значительно повышает стоимость внедрения на удалённых кустовых площадках и морских платформах. В-третьих, требование к регулярным обновлениям прошивок ПЛК или тотальному журналированию трафика порой противоречит режиму непрерывной эксплуатации и нормам промышленной безопасности, где критичнее минимизировать простои и исключить непредсказуемое поведение оборудования. Поэтому NIST SP 800-82 следует рассматривать как источник лучших практик, которые нуждаются в адаптации к российским регулятивным реалиям и производственным ограничениям нефтегазовой отрасли.

Критический анализ методик показывает, что они универсальны и требуют адаптации под специфику нефтегазовых объектов. В этой связи актуальна задача разработки специализированной методики оценки защищённости, учитывающей уникальные особенности отрасли: технологические процессы, распределённость инфраструктуры и специфические угрозы.

2. Математическая модель интегрального показателя

Для формализованного учёта различных факторов (технических, организационных, кадровых) вводится интегральный показатель I, задав ему структуру взвешенной суммы из нескольких групп метрик:

$$I = \sum_{k=1}^{n} w_k \times K_k,$$

где K_k – оценка по k-й группе показателей (техническая защищённость, уровень соответствия регламентам, время реагирования на инциденты, уровень обучения персонала); w_k – весовой коэффициент для k-й группы, отражающий важность соответствующих факторов; n – общее количество групп метрик.

В рамках каждой группы K_k можно выделять множество подметрик. Например, для технической составляющей учитываются:

$$K_{\text{тех}} = f(\text{число уязвимостей, динамика их устранения, } \dots).$$

Для организационной составляющей:

$$K_{\text{орг}} = f(\text{наличие актуальных политик ИБ, результат аудитов, } \dots).$$

Аналогично для человеческой составляющей:

$$K_{\text{люди}} = f(\text{сотрудников, прошедших обучение; результат фишинг} - \text{тестов, } \dots).$$

При агрегировании данных каждая подметрика нормируется в диапазон от 0 до 1, а итоговая сумма умножается на заданные коэффициенты значимости w_k.

Предприятия ТЭК характеризуются высокой степенью автоматизации и использования специализированных систем управления технологическими процессами, таких как SCADA/ICS. Атаки на эти системы имеют серьёзные последствия, включая аварии, экологические катастрофы и экономические потери. Это требует специфических метрик, учитывающих особенности отрасли.

3. Частные показатели безопасности по методике ФСТЭК России и обоснование их адаптации для предприятий ТЭК

Методический документ ФСТЭК России от 2 мая 2024 г. формирует интегральную оценку за счёт совокупности «частных показателей» по группам, в том числе по группе «Защита информационных систем»[9]. В её составе предусмотрены семь базовых индикаторов, ориентированных на универсальные требования к ИТ-средам и критической инфраструктуре: 1) доля систем, охваченных средствами антивирусной защиты; 2) доля систем с своевременно установленными обновлениями безопасности; 3) доля систем, в которых резервное копирование организовано в соответствии с требованиями; 4) доля сегментированных сетевых интерфейсов, защищённых межсетевыми экранами; 5) наличие централизованного мониторинга и реагирования на инциденты (SIEM/SOC); 6) доля применяемых средств защиты с действующими сертификатами соответствия; 7) доля защищённого сетевого трафика. Эти индикаторы задают нормативно выверенный «минимальный профиль» зрелости процессов и технических мер в организациях, эксплуатирующих значимые объекты КИИ.

Вместе с тем прямое применение перечисленных индикаторов без отраслевой настройки ограничивает качество оценки для нефтегазовых предприятий. Во-первых, для АСУ ТП критичны непрерывность технологического цикла и цена простоев: классические измерители «наличия» мер (например, доля сертифицированных СЗИ или факт резервного копирования) слабо коррелируют с реальной устойчивостью к инцидентам и восстановительной способностью производственных узлов [1–3]. Во-вторых, архитектура OT-сетей и используемые промышленные протоколы требуют иных ориентиров: доля «защищённого трафика» в терминах ИТ (сквозное шифрование) не всегда является подходящим прокси-показателем для сегментированных детерминированных сетей с jump-host-доступом и строгими политиками межсетевого экранирования [11]. В-третьих, в условиях распределённости активов и удалённой эксплуатации определяющее значение приобретает оперативность обнаружения и устранения инцидентов (MTTD/MTTR), а также подготовка и вовлечённость персонала, что прямо поддерживается как международными стандартами управления измерениями (ISO/IEC 27004), так и риск-ориентированным подходом NIST CSF [9, 12].

Поэтому в настоящей работе сохраняются ключевые технические индикаторы методики ФСТЭК России, но ряд частных показателей заменяется (или дополняется) метриками, непосредственно отражающими производственный риск: относительное время простоя технологических систем, оперативность реагирования, охват критичных OT-узлов средствами защиты, доля выполненных мероприятий и коэффициент финансирования функций ИБ. Такая адаптация согласуется с требованиями регулятора и профильными стандартами (ISO/IEC 27001, ISO/IEC 27019, серия ISA/IEC 62443), повышает валидность интегральной оценки для объектов нефтегаза и создаёт основу для управленческих решений, увязанных с технологическими и экономическими эффектами [2, 13].

[9]Методический документ «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» Утвержден ФСТЭК России 2 мая 2024 г. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-2-maya-2024-g (дата обращения: 12.07.2025).

4. Предлагаемая адаптация методики для предприятий ТЭК

Методический документ ФСТЭК России формально задаёт семь базовых показателей безопасности информационных систем. Для нефтегазовой отрасли сохранены четыре из них; три заменены отраслевыми метриками, отражающими специфику АСУ ТП, непрерывность технологических процессов и высокую стоимость простоев.

1. Доля АСУ ТП и ИТ-систем, охваченных средствами антивирусной защиты

Показатель полностью соответствует оригиналу ФСТЭК России; уточняется перечень защищаемых объектов (контроллеры, инженерные рабочие станции, сервера реального времени) с учётом требований ISA/IEC 62443.

2. Доля систем, для которых обновления безопасности устанавливаются своевременно

Без изменений по отношению к методике; при расчёте учитываются не только классические OS-патчи, но и микропрограммы ПЛК/RTU.

3. Время простоя защищаемой технологической системы.

Будет являться базовым критерием оценки эффективности системы обеспечения информационной безопасности. Учитывая, что для различных предприятий и, соответственно, различных технологических процессов абсолютное время простоя будет сильно разниться, для нормирования введем показатель относительного времени простоя, соотнесенный с временем, заранее запланированным для обслуживания технологических систем

$$К_{\text{простоя}} = \frac{Т_{\text{простоя}}}{Т_{\text{техно}}},$$

где $Т_{\text{простоя}}$ – суммарное время простоя, вызванного инцидентами информационной безопасности; $Т_{\text{техно}}$ – заданное время заранее запланированного технологического перерыва [3].

Для объектов различной критичности используется взвешенная формула:

$$К_{\text{простоя}-\text{взв}} = \frac{\sum_i Т_{\text{простоя},i} w_i}{\sum_i Т_{\text{техно},i} w_i},$$

в которой коэффициент $w_i \in [1;5]$ устанавливается по методикам ISA/IEC 62443-3-3 и ГОСТ Р ИСО/МЭК 27019.

Целевые значения, подтверждённые отраслевой практикой, находятся в пределах 0,2–0,5 % (добыча ≤ 0,5 %, транспорт ≤ 0,3 %, переработка ≤ 0,2 %); превышение порогов на 1,0–1,5 % сигнализирует о необходимости пересмотра стратегии обнаружения и реагирования [1, 2, 4].

Расчёт выполняется ежеквартально на основании отметок журнала о начале/завершении аварийных остановок и регистрации простоев. Полученное значение включается в сводный KPI-дашборд в соответствии с рекомендациями ISO/IEC 27004 и анализируется совместно с метриками эффективности реагирования [8].

Заменяя показатель резервного копирования из методики ФСТЭК России, данный коэффициент напрямую отражает убытки от остановок технологических процессов нефтегазового предприятия и тем самым обеспечивает более релевантную оценку уровня защищённости отраслевых объектов.

4. Доля сетевых интерфейсов, сегментированных и защищённых межсетевыми экранами

Сохраняется без изменений; оценка проводится относительно изолирования уровней OT и IT в соответствии с моделью ISA-95 и требованиями ISA/IEC 62443-3-3.

5. Наличие централизованного мониторинга и реагирования (SIEM/SOC)

Показатель сохранён; для отрасли уточняется обязательное покрытие событий ПЛК/SCADA [11], что коррелирует с рекомендациями NIST CSF[10].

6. Коэффициенту финансирования подразделений ИБ предприятия.

Отношение расходов на службу информационной безопасности предприятия к общим расходам на предприятии ($К_{фин}$). Данный коэффициент позволяет оценить распределение ресурсов, выделяемых на информационную безопасность в рамках годового бюджета и эффективность их применения

$$К_{фин} = \frac{P_{фин}}{P_{общ}},$$

где $P_{фин}$ – расходы на финансирование информационной безопасности предприятия, руб.; $P_{общ}$ – совокупные операционные расходы предприятия.

Значение 0,05–0,15 свидетельствуют о тенденции роста коэффициента [3, 6].

Метрика заменяет долю сертифицированных СЗИ, так как устойчивое финансирование напрямую определяет возможность продлевать сертификаты и внедрять отраслевые решения.

7. Оперативность реагирования

$$t_{реакц} = t_{обн} + t_{устр},$$

где $t_{обн}$ – среднее время обнаружения инцидента; $t_{устр}$ – среднее время реакции и устранения инцидента [8, 15].

8. Готовность персонала

$$U_{вовл} = \frac{N^{уч}}{N} \times 100\%, U_{осв} = \frac{N^{обуч}}{N} \times 100\%,$$

где $N^{уч}$ – число сотрудников, обеспечивающих информационную безопасность; $N_{обуч}$ – число сотрудников, прошедших обучение, N – общее число сотрудников [5, 8];

9. Процент охвата АСУ ТП средствами защиты.

$$U_{покр} = \frac{N_{покр}}{N} \times 100\%,$$

где $N_{покр}$ – количество систем, оснащённых защитными средствами, N – общее количество критических систем [11].

10. Процент выполнения мероприятий по улучшению безопасности АСУ ТП

$$P_{улуч} = \frac{P_{вып}}{P} \times 100\%,$$

где $P_{вып}$ – реально завершённые мероприятия за отчётный период; P – количество мероприятий плана развития ИБ [5, 10].

Значение $Р_{улуч} \geq 80\%$ свидетельствует о высокой дисциплине исполнения программ непрерывного совершенствования, предусмотренных ISO/IEC 27001 и национальными рекомендациями для ТЭК-сектора [3].

Представленная расширенная адаптация из девяти метрик сохраняет преемственность методики ФСТЭК России, но учитывает критически важные для нефтегазового предприятия факторы, объединяя технические и управленческие аспекты.

5. Рекомендации по внедрению и развитию системы показателей

Эффективное внедрение предложенной адаптированной системы показателей должно осуществляться в рамках единого цикла управления информационной безопасностью предприятия, базирующегося на рекомендациях стандартов ISO/IEC 27001, ISO/IEC 27004 и NIST Cybersecurity Framework. Первоначальным шагом является разработка методических

[10]NIST (National Institute of Standards and Technology). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1, 2018. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (дата обращения: 12.07.2025).

документов, закрепляющих перечень показателей, способы их вычисления, периодичность мониторинга и ответственность за сбор и обработку данных. Каждому показателю необходимо назначить ответственного сотрудника из профильных подразделений: службы информационной безопасности, SOC, производственных служб и финансового блока предприятия.

Важнейшим условием является построение интегрированной инфраструктуры сбора и обработки данных на основе систем мониторинга и управления информационной безопасностью (SIEM/SOC, CMDB, CMMS, ERP). Это позволит обеспечить регулярный и автоматизированный расчёт показателей с минимальной трудоёмкостью. При этом необходима обязательная автоматическая верификация данных по ключевым индикаторам (например, фиксация начала и завершения инцидентов в журнале событий и регистрация простоев).

Внедрение адаптированной модели следует реализовывать поэтапно. На начальном этапе рекомендуется запуск базовых технических показателей, связанных с покрытием АСУ ТП средствами защиты, своевременностью обновлений и контролем времени простоев. На следующем этапе вводятся управленческие показатели, связанные с финансированием мероприятий по информационной безопасности и контролем реализации плановых улучшений. Завершающим этапом является интеграция всей группы показателей в централизованную систему визуализации (дашборд ИБ), обеспечивающую наглядное представление текущего уровня защищённости и динамики его изменения.

Сформированная система показателей должна регулярно анализироваться с точки зрения выполнения целей по безопасности АСУ ТП и соответствия регуляторным требованиям. Итоговые значения показателей и их динамика должны становиться основой принятия решений на уровне руководства предприятия, включая корректировку бюджетов и программ развития информационной безопасности [1, 3, 9]. Регулярное проведение внутреннего аудита ИБ позволяет дополнительно оценить зрелость процессов и эффективность мер защиты, выявить проблемные зоны и скорректировать подходы к развитию информационной безопасности [12, 13]. Такой подход обеспечивает не только прозрачность оценки состояния защищённости критически важных объектов нефтегазового предприятия, но и непрерывное повышение общей эффективности защиты технологических процессов.

Заключение

В статье предложен подход к адаптации методики оценки состояния защищенности информационных систем, утвержденной ФСТЭК России в 2024 г., к специфике предприятий нефтегазовой отрасли. На основе существующих российских и международных стандартов разработан расширенный перечень показателей, позволяющий учитывать не только техническое состояние автоматизированных систем управления технологическими процессами, но и организационные аспекты информационной безопасности, включая уровень подготовки персонала и эффективность реализации плановых мероприятий.

Предложенные показатели образуют систему, ориентированную на количественную оценку, что позволяет перейти от формальных проверок требований регуляторов к измерению реального уровня защищённости объектов отрасли. Внедрение разработанных показателей на практике позволит сократить риски инцидентов информационной безопасности и снизить связанные с ними экономические потери за счет своевременного обнаружения и устранения угроз, рационального распределения ресурсов и приоритезации мероприятий по защите критических производственных.

Дальнейшие исследования целесообразно направить на практическую апробацию предложенных показателей на реальных объектах нефтегазовой отрасли, уточнение весовых коэффициентов для интегральной оценки защищённости, а также разработку механизмов прогнозирования и предупреждения киберугроз на основе современных методов анализа данных и машинного обучения.

СПИСОК ЛИТЕРАТУРЫ/REFERENCES:

1. Правиков Д.И. Подходы к количественной оценке информационной безопасности на предприятии ТЭК. Д.И. Правиков, В.А. Мурашкин. Проблемы управления безопасностью сложных систем: Материалы XXXII международной конференции, посвященной памяти Владимира Васильевича Кульбы, Заслуженного деятеля науки РФ, д-ра техн. наук, профессора, Москва, 13 ноября 2024 г. Москва: Институт проблем управления им. В.А. Трапезникова РАН. 2024, с. 212-217. URL: https://elibrary.ru/item.asp?id=79446201 (дата обращения: 12.07.2025).
   Pravikov D.I., Murashkin V.A. Approaches to Quantitative Assessment of Information Security at Energy Enterprises. In: Proceedings of the XXXII International Conference “Security Management of Complex Systems”, in memory of Vladimir Vasilievich Kulba, Honored Scientist of the Russian Federation, Doctor of Technical Sciences, Professor. Moscow: Trapeznikov Institute of Control Sciences of RAS. 2024, pp. 212-217. URL: https://elibrary.ru/item.asp?id=79446201 (accessed: 12.07.2025) (in Russian).
2. Правиков Д.И. Показатель состояния защищенности на объектах нефтегазовой отрасли. Д.И. Правиков, В.А. Мурашкин. Кибернетика и информационная безопасность «КИБ-2024»: Сборник научных трудов Второй Всероссийской научно-технической конференции, Москва, 22–23 октября 2024 г. Москва: НИЯУ МИФИ 2024, с. 26-27. URL: https://elibrary.ru/item.asp?id=75062623 (дата обращения: 12.07.2025).
   Pravikov D.I., Murashkin V.A. Indicator of Security Status at Oil and Gas Industry Facilities. In: Cybernetics and Information Security “KIB-2024”: Proceedings of the 2nd All-Russian Scientific and Technical Conference, Moscow, October 22–23, 2024. Moscow: National Research Nuclear University MEPhI. 2024, pp. 26-27. URL: https://elibrary.ru/item.asp?id=75062623 (accessed: 12.07.2025) (in Russian).
3. Мурашкин В.А. Эффективность процессов управления информационной безопасностью на предприятии ТЭК. В.А. Мурашкин, А.А. Пырьева. Актуальные проблемы развития нефтегазового комплекса России: Сборник трудов XVII Всероссийской научно-технической конференции, Москва, 25 апреля 2024 г. Москва: Российский государственный университет нефти и газа (национальный исследовательский университет) им. И.М. Губкина. 2024, с. 416-423. URL: https://elibrary.ru/item.asp?id=69218515 (дата обращения: 12.07.2025).
   Murashkin V.A., Pyrieva A.A. Effectiveness of Information Security Management Processes at Energy Sector Enterprises. In: Actual Problems of Development of the Oil and Gas Industry: Proceedings of the XVII Russian Scientific and Technical Conference. Eds. Kalashnikov P.K., Komkov A.N., Dubinov Yu.S., Dubinova O.B., Vanchugov I.M. Moscow: Gubkin Russian State University of Oil and Gas (NRU). 2024, pp. 416-423. URL: https://elibrary.ru/item.asp?id=69218515 (accessed: 12.07.2025) (in Russian).
4. Правиков, Д.И. Оценка комплексной безопасности производственных объектов нефтегазовой отрасли. Д.И. Правиков, Г.Д. Потапов. Кибернетика и информационная безопасность «КИБ-2024»: Сборник научных трудов Второй Всероссийской научно-технической конференции, Москва, 22–23 октября 2024 г. Москва: НИЯУ МИФИ 2024, с. 30-31. URL: https://elibrary.ru/item.asp?id=75062625 (дата обращения: 12.07.2025).
   Pravikov, D.I. Assessment of the integrated safety of production facilities in the oil and gas industry. D.I. Pravikov, G.D. Potapov. Cybernetics and information security "KIB-2024": Proceedings of the Second All-Russian Scientific and Technical Conference, Moscow, October 22–23, 2024. Moscow: National Research Nuclear University "MEPhI". 2024, p. 30-31. URL: https://elibrary.ru/item.asp?id=75062625 (accessed: 12.07.2025) (in Russian).
5. Милославская Н.Г., Толстой А.И. Управление информационной безопасностью. Москва: НИЯУ МИФИ, 2020. – 536 с.
   Miloslavskaya, N.G.; Tolstoy, A.I. Upravlenie informatsionnoy bezopasnost'yu [Information Security Management]. Moscow: National Research Nuclear University MEPhI, 2020. 536 p. (in Russian).
6. Остапчук Т.А. Методы оценки эффективности систем информационной безопасности. Москва: РТ-Софт, 2019. – 192 с.
   Ostapchuk, T.A. Metody otsenki effektivnosti sistem informatsionnoy bezopasnosti [Methods for Assessing the Effectiveness of Information-Security Systems]. Moscow: RT-Soft, 2019. 192 p. (in Russian).
7. MTE Cyber**.** Риск-ориентированный подход к информационной безопасности. URL: https://mte-cyber.by/mte-blog/risk-based-approach-to-information-security/ (дата обращения: 12.07.2025).
   MTE Cyber. Risk-based approach to information security. URL: https://mte-cyber.by/mte-blog/risk-based-approach-to-information-security/ (accessed: 12.07.2025) (in Russian).
8. Рахметов Р. Измерение эффективности процессов кибербезопасности. Security Vision Blog. 2021. URL: https://www.securityvision.ru/blog/izmerenie-effektivnosti-protsessov-kiberbezopasnosti-metriki-ib-chast-1/ (дата обращения: 12.07.2025).
   Rahmetov, R. Measuring cybersecurity-process efficiency. Security Vision Blog. 2021. URL: https://www.securityvision.ru/blog/izmerenie-effektivnosti-protsessov-kiberbezopasnosti-metriki-ib-chast-1/ (accessed: 12.07.2025) (in Russian).
9. Александров А.В. Методика комплексной оценки состояния информационной безопасности предприятия. А.В. Александров, А.В. Велигура, Я.В. Соколова. Экономический вектор. 2016, № 2(5), с. 104–112. URL: https://www.elibrary.ru/item.asp?id=26255560 (дата обращения 12.07.2025).
   Aleksandrov A.V., Veligura A.V., Sokolova Ya.V. A Methodology for Comprehensive Assessment of the Information Security Status of an Enterprise. In: Economic Vector. 2016, no. 2(5), pp. 104–112. URL: https://www.elibrary.ru/item.asp?id=26255560 (accessed: 12.07.2025) (in Russian).

10. Рахметов Р. Обзор специальных публикаций NIST по информационной безопасности. Часть 1. URL: https://habr.com/ru/articles/662353/ (дата обращения: 12.07.2025).
Rakhmetov R. Overview of NIST Special Publications on Information Security. Part 1. URL: https://habr.com/ru/articles/662353/ (accessed: 12.07.2025) (in Russian).
11. Knapp E.D., Langill J. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 2nd ed. Syngress/Elsevier, 2014. 384 p.
12. Милославская Н.Г., Сенаторов М.Ю. Проверка и оценка деятельности по управлению ИБ. 2-е изд. Москва: Горячая линия – Телеком, 2022. – 166 с.
Miloslavskaya, N.G.; Senatorov, M.Yu. Proverka i otsenka deyatel'nosti po upravleniyu IB [Audit and Assessment of Information-Security Management Activities]. 2nd ed. Moscow: Goryachaya Liniya – Telekom, 2022. 166 p. (in Russian).
13. Герасимов А.В., Смирнов П.О. Аудит информационной безопасности: методология и практика. Москва: Инфотропик Медиа, 2023. – 210 с.
Gerasimov A.V., Smirnov P.O. Information Security Audit: Methodology and Practice. Moscow: Infotropik Media, 2023. 210 p. (in Russian).
14. Cherdantseva A., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems. Computers & Security. 2016, v. 56, pp. 1-27. DOI: https://doi.org/10.1016/j.cose.2015.09.009.
15. Freund J., Jones J. Measuring and Managing Information Risk: A FAIR Approach. Elsevier, 2014. 408 p.

Конфликт интересов. *Автор заявляет об отсутствии конфликта интересов.*
Conflict of interest. *The author declares no conflict of interest.*

ИНФОРМАЦИЯ ОБ АВТОРАХ:

Всеволод Алексеевич Буркин, *старший преподаватель, РГУ нефти и газа (НИУ) им. И.М. Губкина.*
e-mail: murashkin.v@gubkin.ru,
https://orcid.org/0009-0008-6327-8022.

INFORMATION ABOUT THE AUTHORS:

Vsevolod Alekseevich Burkin, *Senior Lecturer, Gubkin University.*
e-mail: murashkin.v@gubkin.ru,
https://orcid.org/0009-0008-6327-8022.

Статья поступила в редакцию 05.05.2025; одобрена после рецензирования 20.12.2025; принята к публикации 20.01.2026
The article was submitted 05.05.2025; approved after reviewing 20.12.2025; accepted for publication 20.01.2026