УДК 004.056 Вестник УрФО № 2(60) / 2026, с. 59–67

Лукоянов А.А.

DOI: 10.14529/secur260206

МОДЕЛЬ СБОРА ВЕРИФИЦИРОВАННЫХ ДАННЫХ ДЛЯ ИНТЕГРАЛЬНОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В статье рассматривается задача сбора и проверки исходных данных, используемых для интегральной оценки защищенности распределенной информационной системы. Достоверность итогового показателя зависит не только от выбранной математической модели, но и от качества данных, поступающих из средств мониторинга информационной безопасности, систем инвентаризации, средств анализа уязвимостей, подсистем управления доступом, журналов приложений, средств резервного копирования и систем регистрации инцидентов. В работе обоснована необходимость отдельной проверки исходных данных до их использования в автоматизированном расчете. Проверка включает оценку полноты, актуальности, согласованности, доверия к источнику и целостности данных. Предложена модель сбора верифицированных данных и введен показатель качества исходной информационной базы, который используется совместно с интегральным показателем защищенности.

Ключевые слова: *информационная безопасность, распределенная информационная система, интегральная оценка, мониторинг, верификация данных, качество данных.*

Lukoyanov A.A.

MODEL FOR COLLECTING VERIFIED DATA FOR INTEGRAL SECURITY ASSESSMENT OF A DISTRIBUTED INFORMATION SYSTEM

The paper considers the problem of collecting and verifying source data used for integral security assessment of a distributed information system. It is shown that the reliability of the fi-

nal security indicator depends not only on the selected mathematical model, but also on the quality of data received from information security monitoring tools, asset inventory systems, vulnerability scanners, access management subsystems, application logs, backup systems and incident registration systems. The need to introduce a separate verification layer is substantiated. This layer checks completeness, relevance, consistency, source trustworthiness and data integrity before the data are admitted to calculation. A verified data collection model is proposed, a data verification algorithm is developed, and a source data quality indicator is introduced for joint use with the integral security indicator.

Keywords: *information security, distributed information system, integral assessment, monitoring, data verification, data quality.*

Введение. Интегральная оценка защищенности информационной системы используется для обобщенного представления состояния защиты, сопоставления объектов, контроля динамики изменений и поддержки управленческих решений. Для распределенных информационных систем такая оценка важна, поскольку прикладные сервисы, базы данных, сетевые компоненты, средства защиты, пользовательские рабочие места и внешние интеграции могут находиться в различных сегментах инфраструктуры.

Расчет интегрального показателя рассматривается как преимущественно математическая задача: выбирается набор частных показателей, каждому показателю назначается вес, после чего выполняется агрегирование. Достоверность результата зависит не только от выбранной расчетной формулы, но и от качества исходных данных: их полноты, актуальности, взаимной согласованности и доверия к используемым источникам.

В работе О.В. Казарина, С.Е. Кондакова и И.И. Троицкого обоснован переход от качественного описания состояния защищенности информационных систем к его количественной оценке [1]. С.Е. Кондаков отдельно рассматривал вопросы количественной оценки защищенности информации от несанкционированного доступа [2]. Д.А. Рыленков и Д.С. Карпов предложили интегральный метод оценки уровня защищенности серверной инфраструктуры организации [3], а Е.В. Бурькова исследовала особенности оценки защищенности информационных систем персональных данных [4]. В работах И.И. Лившица и А.С. Бакшеева данная проблематика рассматривается применительно к контролю уровня защищенности информации на объектах критической информационной инфраструктуры [5, 6]. В документах NIST SP 800-55, NIST SP 800-137, NIST Cybersecurity Framework 2.0 и ISO/IEC 27004 отмечается, что метрики безопасности должны быть связаны с источниками данных, процессами мониторинга, оценкой состояния защиты и принятием управленческих решений [7–9, 13, 14]. ГОСТ Р 59547-2021 также определяет мониторинг информационной безопасности как процесс получения и анализа данных, характеризующих состояние защищенности [10]. Современные исследования показывают, что при анализе уязвимостей и оценке защищенности необходимо учитывать не только значения отдельных показателей, но и качество данных, на которых основан расчет [15, 17]. Отдельные работы посвящены количественной и интегральной оценке защищенности компонентов информационной инфраструктуры [3, 16].

Существующие подходы к построению метрик информационной безопасности в основном ориентированы на выбор показателей, их измерение и последующее агрегирование, тогда как предварительная проверка качества исходных данных перед расчетом интегрального показателя защищенности рассматривается недостаточно подробно. Для распределенных информационных систем эта проблема имеет особое значение, поскольку данные поступают из разных источников: SIEM, CMDB, сканеров уязвимостей, IAM, EDR/XDR, систем резервного копирования и журналов приложений. Эти источники различаются форматами, периодичностью обновления, задержками передачи данных и степенью доверия. В результате без отдельной проверки в расчет могут попадать неполные, устаревшие или несогласованные данные, а также записи, которые невозможно надежно соотнести с конкретным сервером, сервисом, учетной записью или сетевым сегментом.

Целью статьи является разработка модели и алгоритма сбора верифицированных данных для интегральной оценки защищенности распределенной информационной системы.

Научная новизна. Научная новизна исследования состоит в том, что в интегральную оценку защищенности распределенной информационной системы включена предварительная проверка качества исходных данных. В отличие от подходов, где основное внимание уделяется выбору показателей и формуле их объединения, в данной работе отдельно рассматривается достоверность данных, поступающих из разных источников. Предложенная модель проверяет данные по пяти критериям: полнота, актуальность, согласованность, доверие к источнику и целостность. Результат оценки предлагается представлять в виде двух показателей: уровня защищенности и качества данных, на которых основан расчет.

Постановка задачи. Распределенную информационную систему представим как множество активов:

$$A = \{a_1, a_2, \ldots, a_n\}, \quad (1)$$

где A_i – отдельный актив или компонент системы: сервер, рабочая станция, сетевое устройство, база данных, прикладной сервис, средство защиты, API-компонент, учетная запись или сегмент сети.

Для каждого актива могут оцениваться несколько направлений защищенности:

$$R = \{r_1, r_2, \ldots, r_m\}, \quad (2)$$

где r_j – направление оценки: управление доступом, управление уязвимостями, защищенность конфигураций, мониторинг событий информационной безопасности, реагирование на инциденты, резервное копирование и восстановление, защита внешних взаимодействий.

Первичная запись, поступающая от средств мониторинга или управления информационной безопасностью, может быть представлена в виде:

$$D = <a, s, t, p, v, r>, \quad (3)$$

где a – актив, к которому относится запись; s – источник данных; t – время получения данных; p – измеряемый параметр; v – значение параметра; r – направление оценки защищенности. Такая запись не должна автоматически включаться в расчет, поскольку она может быть устаревшей, неполной, противоречивой или неподтвержденной.

Задача состоит в преобразовании первичных записей в верифицированные данные, пригодные для расчета частных и интегрального показателей защищенности.

Состав данных для оценки защищенности. Для интегральной оценки защищенности распределенной информационной системы необходимо учитывать события информационной безопасности, данные о составе активов, уязвимостях, конфигурациях, доступах, инцидентах, резервном копировании и внешних взаимодействиях. События информационной безопасности отражают зарегистрированные факты функционирования системы, а данные об активах, настройках и уязвимостях позволяют учитывать потенциальные слабые места ее защиты.

Для распределенной системы принципиальное значение имеет связь данных с акти-

Таблица 1

Основные группы данных для оценки защищенности распределенной ИС

Группа данных	Возможные источники	Применение к оценке
Состав активов	CMDB, инвентаризация активов, сетевое сканирование	Определение границ системы и полноты охвата
Инциденты	IRP/SOAR, журналы регистрации инцидентов, отчеты реагирования	Оценка выявления, классификации и устранения инцидентов
Уязвимости	Сканеры уязвимостей, отчеты анализа защищенности	Оценка технической уязвимости компонентов
Конфигурации	Средства контроля конфигураций, эталонные профили	Оценка соответствия безопасным настройкам
Доступы	IAM, AD/LDAP, журналы привилегированных действий	Оценка управления доступом
События информационной безопасности	SIEM, EDR/XDR, IDS/IPS, WAF	Оценка мониторинга, обнаружения и реагирования
Восстановление	Backup-системы, отчеты тестового восстановления	Оценка устойчивости восстановления

вами. Значение показателя, не привязанное к конкретному серверу, сервису, учетной записи или сетевому сегменту, трудно использовать в расчете. Поэтому модель должна обеспечивать нормализацию идентификаторов и сопоставление данных из разных источников с единым перечнем активов.

Модель сбора верифицированных данных. Предлагаемая модель технологического контура сбора и обработки данных включает шесть функциональных уровней: уровень источников данных, уровень сбора и доставки, уровень нормализации, уровень привязки к активам и направлениям оценки, уровень верификации данных и уровень расчета показателей защищенности.

Общая структура модели представлена на рис. 1.

Рис. 1. Модель сбора верифицированных данных для оценки защищенности распределенной информационной системы

Первичные данные о состоянии системы поступают из средств мониторинга, инвентаризации, анализа уязвимостей, управления доступом и иных подсистем. На уровне сбора и доставки обеспечивается их получение с использованием агентов, коннекторов, API, Syslog, файловых выгрузок или регламентированных отчетов. На этапе нормализации данные преобразуются к единой структуре представления, что позволяет сопоставлять записи из разных источников. В предлагаемой модели исходные данные не передаются непосредственно в расчетный модуль. Их предварительная проверка выполняется в самостоятельном контуре верификации, который обеспечивает исключение из расчетной выборки записей, не отвечающих установленным требованиям к полноте, актуальности, согласованности, доверию к источнику и целостности.

Критерии верификации данных. Для оценки качества исходных данных предлагается использовать пять критериев: полнота, актуальность, согласованность, доверие к источнику и целостность. Выбор этих критериев согласуется с общими подходами к оценке качества данных, в которых подчеркивается значение полноты, точности, своевременности и соответствия данных задачам последующего анализа [11, 12].

Коэффициент полноты показывает, достаточно ли данных для расчета:

$$C = \frac{N_{пол}}{N_{тр}}, \qquad (4)$$

где $N_{пол}$ – количество полученных обязательных значений; $N_{тр}$ – количество значений, необходимых для расчета.

Коэффициент актуальности характеризует соответствие данных установленному интервалу их обновления:

$$F = \max\left(0, 1 - \frac{\Delta t}{T_{доп}}\right), 0 \le F \le 1, \qquad (5)$$

где Δt – время, прошедшее с момента получения или последнего обновления данных; $T_{доп}$ – максимально допустимый интервал времени для соответствующего типа данных.

Все частные коэффициенты качества исходных данных принимают значения на отрезке [0; 1]. Если данные устарели настолько, что значение Δt превышает $T_{доп}$, коэффициент актуальности принимается равным нулю.

Коэффициент согласованности опреде-

Таблица 2

Критерии верификации исходных данных

Критерий	Обозначение	Содержание	Пример проверки
Полнота	C	Наличие необходимых данных по активам и направлениям	Все ли серверы охвачены сканированием
Актуальность	F	Данные получены или обновлены в пределах установленного интервала времени	Не устарел ли отчет сканера
Согласованность	G	Отсутствие существенных противоречий между источниками	Совпадает ли статус актива в CMDB и SIEM
Доверие к источнику	S	Уровень доверия к источнику и способу получения данных	Источник входит в утвержденный перечень доверенных источников данных
Целостность	I	Контроль целостности данных	Используется ли защищенный канал или контрольная сумма

ляется как доля контрольных сопоставлений, по результатам которых не выявлены противоречия между данными из разных источников:

$$G = 1 - \frac{N_{пр}}{N_{пров}}, \quad (6)$$

где $N_{пр}$ – количество выявленных противоречий; $N_{пров}$ – количество выполненных проверок согласованности. При этом $N_{пров} > 0$.

Коэффициент доверия к источнику S задается на основе утвержденного перечня источников данных. Коэффициент целостности I принимает значение 1 при подтвержденной целостности, 0,5 при частичном подтверждении и 0 при отсутствии подтверждения.

Итоговый показатель качества исходных данных рассчитывается по формуле:

$$Q_D = C \cdot F \cdot G \cdot S \cdot I; \quad (7)$$

Мультипликативная форма агрегирования позволяет ограничить взаимное замещение критериев: высокое значение одного критерия качества данных не должно полностью устранять влияние существенных отклонений по другим критериям, включая полноту, доверие к источнику и целостность данных.

Параметры модели задаются на основании регламентов эксплуатации информационной системы, состава контролируемых активов, утвержденных источников данных и требований к периодичности мониторинга. Количество обязательных значений для расчета коэффициента полноты определяется перечнем данных, необходимых для соответствующего направления оценки. Максимально допустимый интервал актуальности устанавливается с учетом типа данных и частоты их обновления: для событий информационной безопасности – по времени поступления в SIEM, для данных об уязвимостях – по периодичности сканирования, для данных об активах – по регламенту актуализации CMDB, для резервного копирования – по периодичности формирования отчетов и проверок восстановления.

Значение коэффициента доверия к источнику определяется по утвержденной шкале: 1 – основной доверенный источник, данные которого формируются автоматически и передаются по защищенному каналу; 0,75 – дополнительный доверенный источник; 0,5 – косвенный или периодически актуализируемый источник; 0 – источник, не включенный в утвержденный перечень или не обеспечивающий подтверждение происхождения данных. Коэффициент целостности определяется по результатам проверки отсутствия искажений при передаче, хранении и обработке данных. Минимально допустимый порог качества данных определяется владельцем информационной системы или подразделением информационной безопасности с учетом допустимого риска принятия решений на основе неполных, устаревших или противоречивых данных. Весовые коэффициенты направлений оценки устанавливаются с учетом критичности соответствующих направлений защищенности и нормируются таким образом, чтобы их сумма была равна единице.

Алгоритм сбора и проверки данных. Предлагаемый алгоритм описывает последовательность преобразования первичных

данных мониторинга в набор верифицированных данных, используемых при расчете интегрального показателя защищенности. Общая логика алгоритма представлена на рис. 2. На первом этапе формируется множество активов распределенной информационной системы и определяются направления оценки. Для каждого направления назначаются источники данных: SIEM, EDR/XDR, сканеры уязвимостей, системы управления учетными записями и правами доступа, CMDB, системы резервного копирования и журналы прикладных сервисов. Полученные данные приводятся к единому формату: актив, источник, время, параметр, значение и направление оценки. Записи сопоставляются с активами из сформированного перечня. Данные, не имеющие связи с конкретным активом, направляются на дополнительную проверку и не включаются в расчет. Ключевым этапом является расчет обобщенного показателя качества данных Q_D и его сравнение с минимально допустимым порогом Q_{min}. При выполнении условия $Q_D \geq Q_{min}$ данные включаются в верифицированный набор и используются для расчета частных показателей и интегрального показателя защищенности $K_{зи}$. Если условие не выполняется, данные уточняются, собираются повторно либо исключаются из расчетной выборки.

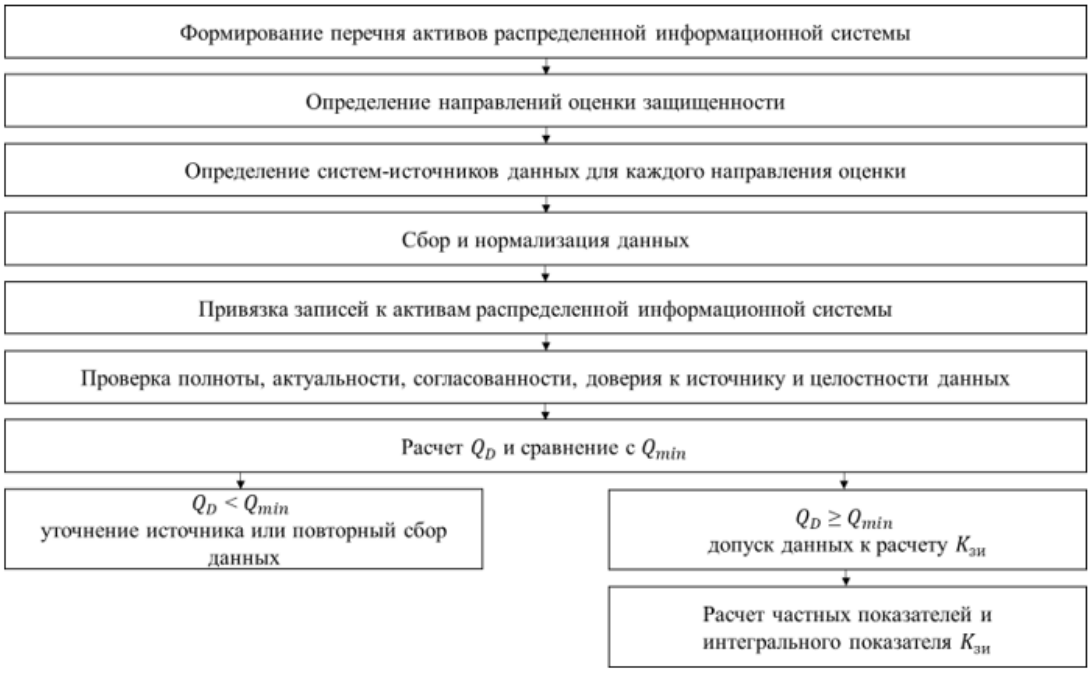

Рис. 2. Алгоритм сбора и верификации данных для расчета интегрального показателя защищенности

Использование верифицированных данных при интегральной оценке. Пусть частные показатели защищенности по направлениям оценки имеют вид K_1, K_2, ..., K_m. Для их агрегирования может использоваться взвешенное геометрическое среднее, позволяющее учитывать существенное снижение защищенности по отдельному направлению даже при высоких значениях остальных частных показателей:

$$K_{зи} = \prod_{j=1}^{m} K_j^{w_j}, \quad (8)$$

где $K_{зи}$ – интегральный показатель защищенности; K_j – частный показатель по j-му направлению; w_j — вес j-го направления, при этом сумма весов равна 1.

Каждому направлению оценки может быть сопоставлен собственный показатель качества данных Q_{Dj}. Используются те же веса w_j, что и для направлений защищенности. Обобщенный показатель качества исходных данных определяется аналогично:

$$Q_{Dобщ} = \prod_{j=1}^{m} Q_{Dj}^{w_j}; \quad (9)$$

Результат оценки предлагается представлять в виде пары:

$$<K_{зи}; Q_{Dобщ}>; \quad (10)$$

Первый элемент характеризует расчетный уровень защищенности, второй – качество исходных данных, на которых основан расчет. В отдельных случаях может использоваться скорректированная оценка защищенности, учитывающая качество исходных данных:

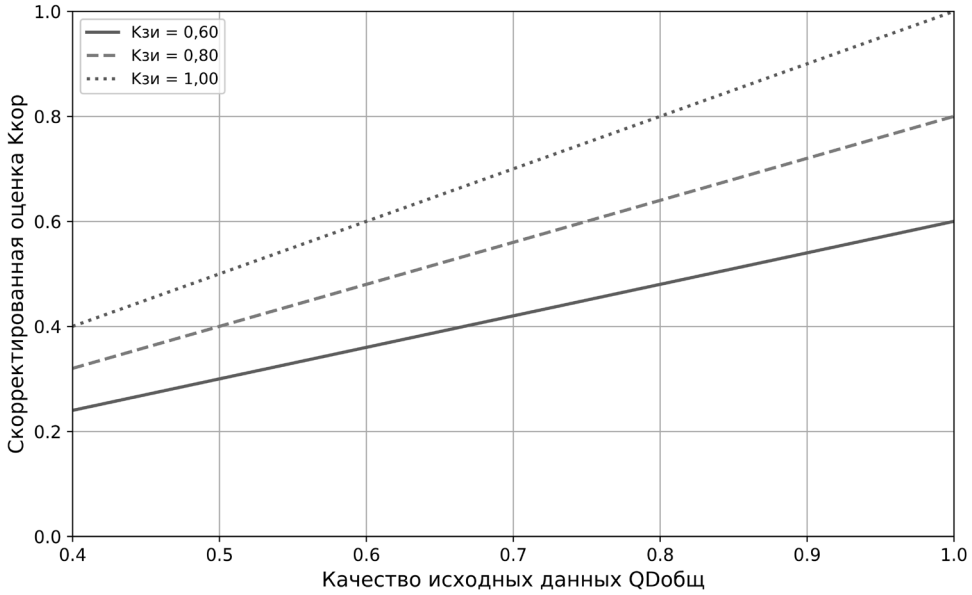

Рис. 3. Зависимость скорректированной оценки защищенности от качества исходных данных

$$K_{кор} = K_{зи} \cdot Q_{Добщ}; \quad (11)$$

Показатель $K_{кор}$ не заменяет $K_{зи}$, а служит для управленческой интерпретации результата, когда необходимо учитывать риск принятия решения на основе неполной или недостаточно проверенной информации.

На рис. 3 показана зависимость скорректированной оценки защищенности от качества исходных данных при нескольких фиксированных значениях расчетного показателя защищенности.

Пример расчета. Рассмотрим пример, в котором оцениваются четыре направления защищенности: управление уязвимостями, управление доступом, мониторинг событий ИБ, резервное копирование и восстановление.

Таблица 3

Пример оценки защищенности и качества исходных данных

Направление оценки	K_j	Q_{Dj}	Вес w_j
Управление уязвимостями	0,72	0,80	0,30
Управление доступами	0,85	0,90	0,25
Мониторинг событий информационной безопасности	0,78	0,70	0,25
Резервное копирование и восстановление	0,88	0,75	0,20

По формуле (8) интегральный показатель защищенности составляет $K_{зи} \approx 0{,}80$. По формуле (9) обобщенный показатель качества исходных данных составляет $Q_{Добщ} \approx 0{,}79$. Следовательно, результат оценки может быть представлен как <0,80; 0,79>.

Если используется скорректированная оценка защищенности, то по формуле (11) получаем $K_{кор} = 0{,}80 \cdot 0{,}79 = 0{,}63$. Следовательно, без учета качества исходных данных система могла бы быть охарактеризована как имеющая достаточно высокий уровень защищенности, однако с учетом качества данных скорректированная оценка защищенности оказывается ниже. Это указывает на необходимость повышения полноты, актуальности или согласованности исходной информационной базы.

Заключение. Предложена модель сбора верифицированных данных для интегральной оценки защищенности распределенной информационной системы. В отличие от подходов, ориентированных преимущественно на выбор частных показателей и способ их агрегирования, модель включает самостоятельный контур проверки качества исходных данных до выполнения расчета.

Разработан алгоритм сбора и верифика-

ции данных, предусматривающий формирование перечня активов, определение направлений оценки, назначение источников, нормализацию, привязку записей к активам, проверку полноты, актуальности, согласованности, доверия к источнику и целостности данных. Предложено представлять результат оценки в виде пары $<K_{зи}; Q_{Добщ}>$, где $K_{зи}$ характеризует расчетный уровень защищенности, а $Q_{Добщ}$ отражает качество исходных данных. Такой подход повышает интерпретируемость результата и снижает риск принятия управленческих решений на основе неполных, устаревших или противоречивых данных.

Практическая значимость работы заключается в возможности применения модели при построении подсистем мониторинга информационной безопасности, автоматизированной оценке защищенности, подготовке отчетности для владельца информационной системы и контроле качества данных, используемых для принятия решений в области защиты информации.

Литература

1. Казарин О.В., Кондаков С.Е., Троицкий И.И. Подходы к количественной оценке защищенности ресурсов автоматизированных систем // Вопросы кибербезопасности. 2015. № 2(10). С. 31–35.

2. Кондаков С.Е. К вопросу о количественной оценке защищенности информации от несанкционированного доступа в информационных системах // Вопросы кибербезопасности. 2015. № 4(12). С. 28–35.

3. Рыленков Д.А., Карпов Д.С. Разработка интегрального метода оценки уровня защищенности серверной инфраструктуры организации // Инженерный вестник Дона. 2025. № 1.

4. Бурькова Е.В. Задача оценки защищенности информационных систем персональных данных // Вестник Чувашского университета. 2016. № 1. С. 112–118.

5. Лившиц И.И., Бакшеев А.С. Исследование методик контроля уровня защищенности информации на объектах критической информационной инфраструктуры // Вопросы кибербезопасности. 2022. № 6(52). С. 40–52. DOI: 10.21681/2311-3456-2022-6-40-52.

6. Бакшеев А.С., Лившиц И.И. Разработка методики контроля уровня защищенности информации объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2023. № 2(54). С. 85–98. DOI: 10.21681/2311-3456-2023-2-85-98.

7. Schroeder K., Trinh H., Pillitteri V.Y. Measurement Guide for Information Security: Volume 1 – Identifying and Selecting Measures. NIST Special Publication 800-55 Vol. 1. National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.SP.800-55v1.

8. Dempsey K., Chawla N.S., Johnson A., Johnston R., Jones A.C., Orebaugh A., Scholl M., Stine K. Information Security Continuous Monitoring for Federal Information Systems and Organizations. NIST Special Publication 800-137. National Institute of Standards and Technology, 2011. DOI: 10.6028/NIST.SP.800-137.

9. ISO/IEC 27004:2016. Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation.

10. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения.

11. Wang R.Y., Strong D.M. Beyond Accuracy: What Data Quality Means to Data Consumers // Journal of Management Information Systems. 1996. Vol. 12. No. 4. P. 5–33. DOI: 10.1080/07421222.1996.11518099.

12. Pipino L.L., Lee Y.W., Wang R.Y. Data Quality Assessment // Communications of the ACM. 2002. Vol. 45. No. 4. P. 211–218. DOI: 10.1145/505248.506010.

13. Schroeder K., Trinh H., Pillitteri V.Y. Measurement Guide for Information Security: Volume 2 – Developing a Measurement Program. NIST Special Publication 800-55 Vol. 2. National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.SP.800-55v2.

14. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.CSWP.29.

15. Croft R., Babar M.A., Kholoosi M.M. Data Quality for Software Vulnerability Datasets // Proceedings of the 45th International Conference on Software Engineering. 2023. P. 121–133. DOI: 10.1109/ICSE48619.2023.00022.

16. Янгиров А.И., Янгиров И.М., Рогозин Е.А., Ахлюстин С.Б. Методический подход к количественной оценке защищенности открытых операционных систем АС ОВД // Вестник Дагестанского государственного технического университета. Технические науки. 2024. Т. 51, № 3. С. 72–85.

17. Кучкарова Н.В. Оценка актуальных угроз и уязвимостей объектов критической информаци-

онной инфраструктуры с использованием технологий интеллектуального анализа текстов // СИИТ. 2024. Т. 6, № 2(17). С. 50–65. DOI: 10.54708/2658-5014-SIIT-2024-no2-p50. EDN NLDWBE.

References

1. Kazarin O.V., Kondakov S.E., Troitskii I.I. Podkhody k kolichestvennoy otsenke zashchishchennosti resursov avtomatizirovannykh sistem // Voprosy kiberbezopasnosti. 2015. № 2(10). S. 31–35.

2. Kondakov S.E. K voprosu o kolichestvennoy otsenke zashchishchennosti informatsii ot nesanktsionirovannogo dostupa v informatsionnykh sistemakh // Voprosy kiberbezopasnosti. 2015. № 4(12). S. 28–35.

3. Rylenkov D.A., Karpov D.S. Razrabotka integral'nogo metoda otsenki urovnya zashchishchennosti servernoy infrastruktury organizatsii // Inzhenernyy vestnik Dona. 2025. № 1.

4. Burkova E.V. Zadacha otsenki zashchishchennosti informatsionnykh sistem personal'nykh dannykh // Vestnik Chuvashskogo universiteta. 2016. № 1. S. 112–118.

5. Livshits I.I., Baksheev A.S. Issledovanie metodik kontrolya urovnya zashchishchennosti informatsii na obektakh kriticheskoy informatsionnoy infrastruktury // Voprosy kiberbezopasnosti. 2022. № 6(52). S. 40–52. DOI: 10.21681/2311-3456-2022-6-40-52.

6. Baksheev A.S., Livshits I.I. Razrabotka metodiki kontrolya urovnya zashchishchennosti informatsii obektov kriticheskoy informatsionnoy infrastruktury // Voprosy kiberbezopasnosti. 2023. № 2(54). S. 85–98. DOI: 10.21681/2311-3456-2023-2-85-98.

7. Schroeder K., Trinh H., Pillitteri V.Y. Measurement Guide for Information Security: Volume 1 – Identifying and Selecting Measures. NIST Special Publication 800-55 Vol. 1. National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.SP.800-55v1.

8. Dempsey K., Chawla N.S., Johnson A., Johnston R., Jones A.C., Orebaugh A., Scholl M., Stine K. Information Security Continuous Monitoring for Federal Information Systems and Organizations. NIST Special Publication 800-137. National Institute of Standards and Technology, 2011. DOI: 10.6028/NIST.SP.800-137.

9. ISO/IEC 27004:2016. Information Technology — Security Techniques — Information Security Management — Monitoring, Measurement, Analysis and Evaluation.

10. GOST R 59547-2021. Zashchita informatsii. Monitoring informatsionnoy bezopasnosti. Obshchie polozheniya.

11. Wang R.Y., Strong D.M. Beyond Accuracy: What Data Quality Means to Data Consumers // Journal of Management Information Systems. 1996. Vol. 12. No. 4. P. 5–33. DOI: 10.1080/07421222.1996.11518099.

12. Pipino L.L., Lee Y.W., Wang R.Y. Data Quality Assessment // Communications of the ACM. 2002. Vol. 45. No. 4. P. 211–218. DOI: 10.1145/505248.506010.

13. Schroeder K., Trinh H., Pillitteri V.Y. Measurement Guide for Information Security: Volume 2 – Developing a Measurement Program. NIST Special Publication 800-55 Vol. 2. National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.SP.800-55v2.

14. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.CSWP.29.

15. Croft R., Babar M.A., Kholoosi M.M. Data Quality for Software Vulnerability Datasets // Proceedings of the 45th International Conference on Software Engineering. 2023. P. 121–133. DOI: 10.1109/ICSE48619.2023.00022.

16. Yangirov A.I., Yangirov I.M., Rogozin E.A., Akhlyustin S.B. Metodicheskiy podkhod k kolichestvennoy otsenke zashchishchennosti otkrytykh operatsionnykh sistem AS OVD // Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskie nauki. 2024. T. 51, № 3. S. 72–85.

17. Kuchkarova N.V. Otsenka aktual'nykh ugroz i uyazvimostey obektov kriticheskoy informatsionnoy infrastruktury s ispol'zovaniem tekhnologiy intellektual'nogo analiza tekstov // SIIT. 2024. T. 6, № 2(17). S. 50–65. DOI: 10.54708/2658-5014-SIIT-2024-no2-p50. EDN NLDWBE.

ЛУКОЯНОВ Алексей Александрович, специалист по информационной безопасности. RUSSPASS — Московская цифровая туристская платформа. Автономная некоммерческая организация «Проектный офис по развитию туризма и гостеприимства Москвы». 125009, г. Москва, ул. Тверская, д. 5А. E-mail: 9261781233@mail.ru

LUKOYANOV Aleksey Aleksandrovich, Information Security Specialist, RUSSPASS — Moscow Digital Tourism Platform. Autonomous Non-profit Organization "Project Office for the Development of Tourism and Hospitality of Moscow". 125009, Moscow, 5A Tverskaya St. E-mail: 9261781233@mail.ru.