БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2025. – № 2 (117). – 25–39

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2025-2-25-39

ВОПРОСЫ ОЦЕНКИ ДОВЕРИЯ К ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ*

Л.Е. СВИРИДОВА[1], И.А. ОГНЕВ[2]

[1] *630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: l.sviridova.2021@stud.nstu.ru*

[2] *630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: i.ognev@corp.nstu.ru*

Целью исследования является применение формализованного подхода к оценке уровня доверия к информационной системе персональных данных (ИСПДн) с использованием существующих моделей и нормативных требований. В работе проводится анализ действующей нормативно-правовой базы, включая требования ФСТЭК и ФСБ России, а также Федерального закона № 152-ФЗ. В качестве методологической основы использована линейная модель «фактор – критерий – метрика», которая позволяет проводить всестороннюю количественную и качественную оценку защищенности ИСПДн. Рассмотрены основные метрики, отражающие степень соответствия требованиям безопасности, эффективность проведения аудитов, скорость реагирования на инциденты и полноту устранения уязвимостей. Применяется функция желательности Харрингтона для расчета обобщенного уровня доверия. Особое внимание уделено влиянию среды функционирования системы (доверенной или недоверенной) на интерпретацию результатов. Научная новизна работы заключается в практическом применении многоуровневой модели оценки доверия в реальных условиях функционирования ИСПДн. Практическое значение исследования заключается в возможности использовать полученные результаты для аудита и модернизации информационных систем персональных данных, повышения прозрачности процессов обеспечения безопасности, а также для подготовки к аттестации и контролю со стороны регуляторов.

Ключевые слова: доверие, информационная безопасность, ИСПДн, оценка доверия, метрики безопасности, нормативное соответствие, управление рисками, доверенная среда, защита персональных данных

* Статья получена 30 января 2025 г.

ВВЕДЕНИЕ

Современное общество всё больше зависит от информационных систем, обрабатывающих персональные данные. Эти системы используются в различных сферах, начиная от государственных услуг и заканчивая коммерческими организациями. Однако с ростом объемов обрабатываемой информации и числа киберугроз возрастает потребность в надежных механизмах обеспечения безопасности. Оценка доверия к информационным системам персональных данных (ИСПДн) становится ключевым элементом управления информационной безопасностью.

В условиях стремительного развития технологий и усложнения киберугроз недостаточно полагаться на статические меры защиты [1, 2]. Необходим динамический подход к обеспечению безопасности, который включает постоянный мониторинг и регулярную оценку уровня доверия к системе. Целью данной статьи является исследование методов и критериев оценки доверия к ИСПДн, анализ существующих подходов, а также описание моделей и показателей, позволяющих формировать объективную оценку безопасности системы. Рассматриваются как технические, так и организационные аспекты обеспечения доверия, включая управление рисками, аудиты безопасности и соответствие нормативным требованиям.

1. НОРМАТИВНЫЕ РЕГУЛИРОВАНИЯ И ТРЕБОВАНИЯ

Оценка доверия к информационным системам персональных данных играет ключевую роль в обеспечении информационной безопасности и соответствия нормативным требованиям. Доверие в данном контексте означает уверенность в том, что ИСПДн защищает данные от утечек, несанкционированного доступа и других угроз, что достигается через комплексную проверку их соответствия требованиям безопасности.

При оценке доверия к информационным системам персональных данных ключевым аспектом является соблюдение нормативных требований [3–6].

Федеральный закон № 152 регулирует обработку персональных данных, включая их сбор, хранение, передачу и уничтожение. Одним из обязательных этапов в процессе оценки доверия является проверка соблюдения процедур категорирования ИСПДн. Категорирование представляет собой процесс определения уровня защищенности системы в зависимости от типа и объема обрабатываемых данных, а также потенциальных последствий утраты или утечек этих данных. Закон требует составления акта категорирования, который должен быть утвержден ответственным лицом в организации. Кроме того, оценивается соответствие политик организации, таких как политика обработки персональных данных, которая должна быть разработана и актуализирована

в соответствии с требованиями законодательства. Важным аспектом является проверка наличия согласий субъектов данных на обработку их персональных данных, а также правильности ведения журналов учета и контроля (например, журналов регистрации доступа к персональным данным и их носителям).

Требования ФСТЭК России регламентируют технические и организационные меры защиты персональных данных, которые должны быть реализованы в ИСПДн. Одним из обязательных этапов является разработка и утверждение модели угроз. Эта модель описывает потенциальные угрозы безопасности данных и определяет меры защиты, которые должны быть реализованы для минимизации рисков. Модель угроз разрабатывается в соответствии с методическими рекомендациями ФСТЭК и должна быть согласована с регулятором.

Еще одним важным этапом является аттестация ИСПДн. Аттестация предполагает проверку системы на соответствие установленным требованиям безопасности, что включает анализ документации, тестирование системы на уязвимости и проведение проверки на соответствие использованным сертифицированным средствам защиты [7]. Также важным элементом является сертификация средств защиты информации (СЗИ). Используемые СЗИ, такие как криптографические средства или системы защиты от несанкционированного доступа, должны быть сертифицированы ФСТЭК для обеспечения их соответствия требованиям безопасности, установленным для ИСПДн.

Кроме того, ФСБ России регулирует использование криптографических методов защиты информации в ИСПДн. В частности, средства криптографической защиты информации (СКЗИ) должны быть сертифицированы ФСБ, что подтверждает их способность обеспечивать защиту данных в соответствии с требованиями безопасности. Также проверяется правильность использования криптографических алгоритмов и управления ключами шифрования.

2. МОДЕЛЬ И КРИТЕРИИ ДОВЕРИЯ

Линейная модель «фактор – критерий – метрика» представляет собой системный подход к оценке уровня доверия информационным системам персональных данных. В этой модели структура анализа строится по иерархической схеме, начиная с факторов, которые охватывают ключевые аспекты доверия, такие как управление рисками, угрозами и уязвимостями, процедуры аудита, система управления информационной безопасностью (СУИБ), средства защиты информации и процедуры их создания, а также используемые технологии. Каждый фактор детализируется через критерии, которые формализуют конкретные аспекты оценки (например, полноту управления

рисками, качество процедур аудита или степень покрытия процессов в СУИБ). Эти критерии измеряются с помощью метрик, предоставляющих количественные или качественные показатели, такие как процент устраненных уязвимостей, время реакции на инциденты или доля выполненных требований нормативных актов [8].

Процесс оценки включает сбор доказательств доверия, таких как результаты аудитов, протоколы тестирования и аттестационные документы, их сопоставление с критериями и последующий расчет метрик. Итоговый уровень доверия определяется как взвешенное среднее всех факторов с учетом их значимости. Эта модель позволяет объективно оценить соответствие информационной системы требованиям безопасности и установить уровень доверия в рамках нормативных актов [9–12]. Применение модели «фактор – критерий – метрика» обеспечивает стандартизацию процессов оценки доверия, прозрачность и возможность интеграции динамического анализа для постоянного мониторинга состояния системы.

Процесс сбора доказательств доверия автоматизируется, включая мониторинг процедур защиты данных, эксплуатационной документации и соответствующих протоколов. Это позволяет минимизировать влияние человеческого фактора и ускоряет процесс проверки.

3. БАЗОВЫЕ ФОРМУЛЫ

Для расчета уровня доверия предлагается использовать функцию желательности Харрингтона [13, 14]. Конечный уровень доверия к субъекту информационного обмена будет являться обобщенной функцией желательности и рассчитываться по формуле

$$D = \sqrt[i+1]{D_{12} D_{22} \dots D_{i2} W_э}, \quad (1)$$

где D – общий уровень доверия (обобщенная функция желательности); i – порядковый номер величины (количество факторов доверия); d_{i2} – i-й показатель 2-й категории (факторы); $W_э$ – показатель эффективности системы управления, учитывающий вес каждого из семи сегментов (факторов).

Факторы доверия будут выступать частными функциями желательности и будут рассчитываться по формуле

$$D_{i2} = \sqrt[N_j]{d_{i11} d_{i12} \dots d_{i1N_j}}, \quad (2)$$

где D_{i2} – i-й показатель 2-й категории (факторы); N_j – количество измеряемых величин (критерии) в i-м показателе 2-й категории (частная функция жела-

тельности); j – порядковый номер величины; d_{i1N_j} – j-й показатель 1-й категории (критерии) для вычисления i-го показателя 2-й категории (факторы).

Критерии доверия будут также выступать частными функциями желательности и рассчитываться по формуле

$$d_{i1j} = e^{-e^{-\left(y'_{i1j}-2\right)}}, \tag{3}$$

где y' – частные признаки желательности, т. е. метрики доверия.

Метрики доверия являются частными признаками желательности и рассчитываются по формуле

$$y'_{i1j} = F_{i1j} \sum_{m=1}^{N_j} K_{i1jm}, \tag{4}$$

где N_j – количество измеряемых величин (метрики) в j-м показателе 1-й категории; m – порядковый номер величины; K_{i1jm} – m-я измеряемая величина (метрика) в j-м показателе 1-й категории (критерии) для вычисления i-го показателя 2-й категории (факторы); F_{i1j} – нормализующий коэффициент для получения приведенного значения y'_{i1j} в промежутке (0…7).

4. ВЛИЯНИЕ СРЕДЫ НА ДОВЕРИЕ

Доверенная среда – это система, в которой запуск и функционирование программного обеспечения контролируются через список проверенных объектов. К таким объектам относятся приложения, библиотеки и скрипты, для которых определено, что они безопасны. Система принимает решения о доверенности объектов на основе их электронно-цифровой подписи (ЭЦП), подтверждающей, что объект создан доверенным разработчиком и не изменен. Однако не все программы имеют ЭЦП, и злоумышленники могут использовать украденные сертификаты. Для решения этой проблемы используются базы знаний, содержащие информацию о легитимном ПО, а также облачные технологии и динамические списки разрешенных приложений, позволяющие оперативно проверять файлы. Доверенная среда сохраняет свое свойство доверенности даже при создании новых объектов внутри нее, если исключен контакт с недоверенными внешними источниками [15].

Недоверенная среда, напротив, представляет собой систему, где нет уверенности в безопасности взаимодействующих объектов. В такой среде допол-

нительно проверяется защита каналов связи и взаимодействия с внешними системами, так как они могут быть потенциальными источниками угроз.

Доверие к информационной системе, включая ИСПДн, зависит от статуса среды ее функционирования. В доверенной среде фокус проверок сосредоточен на внутренних механизмах безопасности, тогда как в недоверенной среде требуется усиленный контроль взаимодействий с внешними системами и защитой каналов связи.

5. МЕТРИКИ ДЛЯ ОЦЕНКИ ИСПДн

Для подробного анализа метрик оценки ИСПДн можно рассмотреть несколько ключевых аспектов, которые помогут в проведении всесторонней оценки уровня доверия.

Метрики для оценки информационных систем персональных данных являются ключевым инструментом для определения уровня защищенности таких систем и их соответствия нормативным требованиям. Эти метрики позволяют объективно измерить эффективность применяемых мер безопасности, выявлять слабые стороны системы и принимать обоснованные решения для их устранения. Важной метрикой является доля выполненных требований нормативной базы. Этот показатель рассчитывается как процент успешно реализованных мер защиты от общего числа предписанных, что помогает снизить риски несоответствия и юридической ответственности.

Эффективность аудитов также является значимой метрикой. Она оценивается через частоту проведения проверок и их результаты. Регулярность аудитов обеспечивает своевременное выявление уязвимостей, а их устранение указывает на уровень защиты системы. Время реакции на инциденты безопасности определяет готовность системы оперативно отвечать на угрозы. Быстрое реагирование уменьшает ущерб и снижает вероятность дальнейших атак, демонстрируя высокий уровень управления рисками [16–22].

Процент уязвимостей, устраненных в установленные сроки, отражает способность системы эффективно справляться с выявленными проблемами. Эта метрика подтверждает наличие налаженных процессов управления уязвимостями, что минимизирует риск повторных инцидентов. Наконец, соответствие систем управления информационной безопасностью аттестационным требованиям показывает, насколько полно реализованы процессы обеспечения безопасности в системе. Это включает проверку процедур, их документальное подтверждение и соответствие стандартам.

Использование перечисленных метрик позволяет сформировать комплексное представление о текущем состоянии защищенности ИСПДн, выявить критически важные зоны для улучшения и усилить защитные механизмы.

Такие показатели способствуют не только обеспечению соответствия нормативным требованиям, но и повышению доверия со стороны пользователей и регуляторов.

6. РАСЧЕТ ИТОГОВОГО УРОВНЯ ДОВЕРИЯ

В качестве примера будет приведен расчет итогового уровня доверия информационной системы персональных данных. При проведении оценки используются 8 факторов доверия, 31 критерий и 224 метрики.

После анализа и сбора доказательств можно сформировать значения метрик, которые должны лежать в диапазоне (0…1). Так, метрики $K_{1111} - K_{1114}$ имеют общее значение «3», так как отсутствует акт, подтверждающий проведение первичной оценки рисков (классификации / категорирования).

Частные признаки желательности рассчитываются по формуле (4), где интерес представляет нормализующий коэффициент. К примеру, частный признак желательности, получаемый из значений метрик критерия доверия «соответствие требованиям нормативных правовых актов» фактора «система управления рисками», будет рассчитываться по следующей формуле:

$$y'_{111} = F_{111} \sum_{m=1}^{N_j} K_{111m} = \frac{7}{4} \sum_{m=1}^{4} K_{111m} = 1,75 \sum_{m=1}^{4} K_{111m} = 1,75 \cdot 2 = 3,5. \qquad (5)$$

Возьмем еще один пример – критерий доверия «соответствие требованиям нормативных правовых актов» фактора «процедуры создания СУИБ»:

$$y'_{611} = F_{611} \sum_{m=1}^{N_j} K_{611m} = \frac{7}{49} \sum_{m=1}^{49} K_{611m} = 0,14 \sum_{m=1}^{49} K_{611m} = 0,14 \cdot 30 = 4,2. \qquad (6)$$

Соответственно частные показатели желательности рассчитываются аналогично для всех критериев доверия.

Для оценки критериев доверия необходимо воспользоваться формулой (3). Например, для критерия доверия «соответствие требованиям нормативных правовых актов» фактора «система управления рисками» расчет будет выглядеть следующим образом:

$$d_{111} = e^{-e^{-(y'_{111}-2)}} = e^{-e^{-(3,5-2)}} \approx 0,8, \qquad (7)$$

где y'_{111} – частный признак желательности, получаемый из значений метрик доверия.

Остальные критерии рассчитываются аналогичным образом.

Согласно формуле (2) значение доверия к факторам рассчитывается как среднее геометрическое значений соответствующих критериев доверия. Например, расчет значения фактора доверия «система управления рисками» выполняется по формуле

$$D_{12} = \sqrt[4]{d_{111}d_{112}d_{113}d_{114}} = \sqrt[4]{0,8 \cdot 0,8 \cdot 0,75 \cdot 0,6} \approx 0,73. \quad (8)$$

Для расчета итогового уровня доверия воспользуемся формулой (1):

$$D = \sqrt[9]{D_{12}D_{22}D_{32}D_{42}D_{52}D_{62}D_{72}D_{82}W_э} =$$

$$= \sqrt[9]{0,73 \cdot 0,83 \cdot 0,56 \cdot 0,77 \cdot 0,58 \cdot 0,66 \cdot 0,95 \cdot 0,64 \cdot 0,8} = 0,71. \quad (9)$$

Полученное значение итогового уровня доверия оцениваемой ИСПДн свидетельствует о среднем уровне соответствия. Это говорит о том, что процессы информационной безопасности в ИСПДн реализованы, но требуют дальнейшего развития. Они выполняются, планируются и контролируются, но еще не достигли стадии, при которой эффективность этих процессов оценивается количественно и проводится постоянное улучшение. Такой уровень не гарантирует устойчивой защиты от современных угроз, особенно в условиях повышенных рисков. Для повышения уровня доверия необходимо перейти к более зрелой модели управления безопасностью, в которой обеспечивается количественная оценка эффективности каждого процесса, проводится регулярный аудит и реализуется цикл постоянного улучшения, например, по модели PDCA. Требуется автоматизация сбора доказательств доверия, а также анализ текущих слабых сторон по факторам доверия, таких как управление рисками, управление угрозами и уязвимостями, аудиторские процедуры, защита информации и используемые информационные технологии. Повышение метрик по этим направлениям позволит увеличить итоговый показатель доверия. Кроме того, важно обеспечить своевременное обновление документов, аттестатов соответствия и внедрение современных методов защиты, включая сертифицированные средства защиты информации. Внедрение указанных улучшений позволит достичь высокого уровня доверия (значение итогового уровня доверия выше 0,85), при котором процессы безопасности не только формализованы, но и управляются на основе объективных, измеримых показателей.

ЗАКЛЮЧЕНИЕ

Оценка доверия к ИСПДн является важным инструментом обеспечения информационной безопасности и соответствия нормативным требованиям. Использование линейной модели «фактор – критерий – метрика» позволяет формализовать процесс оценки и обеспечить объективность и прозрачность. Метрики, такие как доля выполненных требований нормативной базы, эффективность аудитов, время реакции на инциденты и процент устраненных уязвимостей, помогают выявлять слабые стороны системы и усиливать механизмы защиты. Влияние среды функционирования, доверенной или недоверенной, требует применения различных подходов к оценке, что обеспечивает гибкость и адаптивность систем управления информационной безопасностью. Представленные в статье подходы и рекомендации могут быть использованы для создания надежных и устойчивых систем, способных эффективно противостоять современным угрозам.

СПИСОК ЛИТЕРАТУРЫ

1. *Макаренко С.И.* Тестирование на проникновение на основе стандарта NIST SP 800–115 // Вопросы кибербезопасности. – 2022. – № 3 (49). – С. 44–57.

2. К вопросу анализа нормативно-правовых документов по информационной безопасности автоматизированных систем органов внутренних дел Российской Федерации для оценки уровня их защищенности / Е.А. Рогозин, И.Г. Дровникова, А.О. Ефимов, В.Р. Романова // Вестник Дагестанского государственного технического университета. Технические науки. – 2022. – № 4 (49). – С. 97–103. – DOI: 10.21822/2073-6185-2022-49-4-97-103.

3. Разработка методики оценки уровня доверия к субъекту информационного обмена в доверенной среде / А.В. Иванов [и др.]. – Новосибирск: Изд-во НГТУ, 2024.

4. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – № 31, ч. 1–2. – Ст. 3448.

5. Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6. Приказ ФСТЭК России от 14.05.2020 № 68 «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

7. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

8. *Янсюкевич А.В.* К вопросу об аттестации объектов информационных систем персональных данных // Устойчивое развитие: исследования, инновации, трансформация: материалы XVIII Международного конгресса с элементами научной школы для молодых ученых. В 2 т. Т. 1. – М.: Моск. ун-т им. С.Ю. Витте, 2022. – С. 560–565.

9. ГОСТ Р ИСО/МЭК 27001–2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Рос. ин-т стандартизации, 2021. – 23 с.

10. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 46 с.

11. ГОСТ Р 54581–2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Ч. 1. Обзор и основы. – М.: Стандартинформ, 2012. – 26 с.

12. ГОСТ Р 54582–2011. Основы доверия к безопасности информационных технологий. Ч. 2. Методы доверия. – М.: Стандартинформ, 2013. – 46 с.

13. *Юсупова Г.Ф.* Использование функции желательности в оценке уровня техносферной безопасности территории // Социально-экономические и технические системы: исследование, проектирование, оптимизация. – 2017. – № 3 (76). – С. 67–81.

14. *Пичкалев А.В.* Обобщенная функция желательности Харрингтона для сравнительного анализа технических средств // Исследования наукограда. – 2012. – № 1 (1). – С. 25–28.

15. *Мазепин П.С., Гришин Н.А., Бочаров М.В.* Принцип работы концепции доверенной среды // Инновации. Наука. Образование. – 2021. – № 35. – С. 644–648.

16. *Иванов А.В., Огнев И.А.* Проблемы оценки доверия к процессам аудита информационной безопасности // Вопросы кибербезопасности. – 2024. – № 3 (61). – С. 40–50.

17. *Иванов А.В., Селифанов В.В., Огнев И.А.* Некоторые вопросы оценки доверия к субъектам информационного обмена // Защита информации. Инсайд. – 2025. – № 1 (121). – С. 34–40.

18. *Иванов А.В., Огнев И.А., Селифанов В.В.* Вопросы оценки эффективности аудита информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. – 2024. – № 4 (54). – С. 37–48.

19. *Мартыненко К.К., Ценина А.В., Селифанов В.В.* Моделирование процесса управления рисками и оценка его эффективности // Интеллектуальный потенциал Сибири: 32-я региональная научная студенческая конференция, Новосибирск, 20–25 мая 2024 года. В 5 ч. Ч. 3. – Новосибирск: НГТУ, 2024. – С. 506–508.

20. *Солдатов А.Ю., Иванов А.В., Селифанов В.В.* Вопросы построения модели системы управления угрозами информационной безопасности // Интерэкспо Гео-Сибирь. – 2024. – Т. 6. – С. 248–255. – DOI: 10.33764/2618-981X-2024-6-248-255.

21. Метод оценивания рисков в системах принятия решений с учетом защиты информации / В.В. Селифанов, А.Ю. Солдатов, Е.Ю. Солдатов, Подлегаев А.П., Скориков В.С. // Вестник СибГУТИ. – 2023. – Т. 17, № 2. – С. 84–92. – DOI: 10.55648/1998-6920-2023-17-2-84-92.

22. *Селифанов В.В., Аникеева В.В., Огнев И.А.* Вопросы оценки доверия к системе управления рисками // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 69–82. – DOI: 10.17212/2782-2230-2023-1-69-82.

Свиридова Любовь Евгеньевна, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – оценка доверия к информационной системе обработки персональных данных. E-mail: l.sviridova.2021@stud.nstu.ru

Огнев Игорь Александрович, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – оценка доверия к субъектам информационного обмена, информационная безопасность, кибербезопасность. E-mail: i.ognev@corp.nstu.ru

DOI: 10.17212/2782-2230-2025-2-25-39

Questions of trust assessment in information systems of personal data*

L.E. Sviridova[1], I.A. Ognev[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of Information Security Department. E-mail: l.sviridova.2021@stud.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Senior Lecturer of Information Security Department. E-mail: i.ognev@corp.nstu.ru*

The aim of the study is to apply a formalized approach to assessing the level of trust in a personal data information system (PDIS) using existing models and regulatory requirements. The paper analyzes the current legal and regulatory framework, including the requirements of FSTEC and the FSB of Russia, as well as Federal Law No. 152-FZ. The methodological basis is the linear "factor – criterion – metric" model, which enables a comprehensive quantitative and qualitative evaluation of the security of PDIS. The study examines key metrics reflecting the degree of compliance with security requirements, audit effectiveness, incident response time, and the completeness of vulnerability remediation. The Harrington desirability function is applied to calculate the generalized trust level. Special attention is given to the influence of the system's operational environment (trusted or untrusted) on the interpretation of the results. The scientific novelty lies in the practical application of a multi-level trust assessment model under real-world operating conditions of PDIS. The practical significance of the research is in the potential use of the results for auditing and modernizing personal data information systems, improving transparency in security assurance processes, and preparing for system certification and regulatory inspections.

Keywords: trust, information security, PDIS, trust assessment, security metrics, regulatory compliance, risk management, trusted environment, personal data protection

REFERENCES

1. Makarenko S.I. Testirovanie na proniknovenie na osnove standarta NIST SP 800–115 [Penetration Testing Based on NIST SP 800–115 Standard]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2022, no. 3 (49), pp. 44–57.

2. Rogozin E.A., Drovnikova I.G., Yefimov A.O., Romanova V.R. [On the analysis of regulatory legal documents on information security of automated systems of the internal affairs bodies of the Russian Federation for assessing their security level]. *Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskie nauki = Herald of Dagestan State Technical University. Tech-*

* *Received 30 January 2025.*

nical Sciences, 2023, no. 49 (4), pp. 97–103. DOI: 10.21822/2073-6185-2022-49-4-97-103. (In Russian).

3. Development of a Methodology for Assessing the Level of Trust in Information Exchange Subjects in a Trusted Environment. A.V. Ivanov [et al.], Novosibirsk: Novosibirsk State Technical University, 2024.

4. Federal Law of the Russian Federation of July 27, 2006 No. 152 "On Personal Data". *Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the Legislation of the Russian Federation*, 2006, no. 31, art. 3448. (In Russian).

5. FSTEC of Russia Order No. 21 February 18, 2013 "On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data during their Processing in Personal Data Information Systems". (In Russian).

6. FSTEC of Russia Order No. 68 May 14, 2020 "On Amendments to the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data During Their Processing in Personal Data Information Systems". (In Russian).

7. Order of Federal Security Service of the Russian Federation of July 10, 2014 No. 378 "About statement of structure and content of organizational and technical measures for safety of personal data in case of their processing in personal data information systems with use of the means of cryptographic information protection necessary for accomplishment of the security requirements of personal data established by the Government of the Russian Federation for each of security levels". (In Russian).

8. Yansyukevic A.V. [On the Issue of certification of objects of personal data information systems]. *Ustoichivoe razvitie: issledovaniya, innovatsii, transformatsiya* [Sustainable development: research, innovations, transformation]. Proceedings of the XVIII International Congress with Elements of a Scientific School for Young Scientists. Moscow, Moscow Witte University Publ., 2022, pp. 560–565. (In Russian).

9. State Standard R ISO/IEC 27001–2021. *Information technology. Security techniques. Information security management systems. Requirements*. Moscow, Russian Standardization Institute Publ., 2021. 23 p.

10. State Standard R ISO/IEC 27005–2010. *Information technology. Security techniques. Information security risk management*. Moscow, Standartinform Publ., 2011. 45 p. (In Russian).

11. State Standard R 54581–2011. *Information technology. Security techniques. A framework for IT security assurance*. Pt. 1. *Overview and framework*. Moscow, Standartinform Publ., 2012. 26 p.

12. State Standard R 54582–2011 *Information technology. Security techniques. Aframework for IT security assurance*. Pt. 2. *Assurance methods*. Moscow, Standartinform Publ., 2013. 46 p.

13. Yusupova G.F. Ispol'zovanie funktsii zhelatel'nosti v otsenke urovnya technosfernoi bezopasnosti territorii [Using the desirability function in assessment of level of technospheric safety of the territory]. *Sotsial'no-ekonomicheskie i tekhnicheskie sistemy: issledovanie, proektirovanie, optimizatsiya = Social-Economic and Technical Systems: Research, Design and Optimization*, 2017, no. 3 (76), pp. 67–81.

14. Pichkalev A.V. Obobshchennaya funktsiya zhelatel'nosti Kharringtona dlya sravnitel'nogo analiza tekhnicheskikh sredstv [Generalized Harrington's desirability function for the comparative analysis of technical facilities]. *Issledovaniya naukograda = Research of the Science Cities*, 2012, no. 1 (1), pp. 25–28.

15. Mazepin P.S., Grishin N.A., Bocharov M.V. Printsip raboty kontseptsii doverennoi sredy [The principle of operation of the trusted environment concept]. *Innovatsii. Nauka. Obrazovanie = Innovations. Science. Education*, 2021, no. 35, pp. 644–648.

16. Ivanov A.V., Ognev I.A. Problemy otsenki doveriya k protsessam audita informatsionnoi bezopasnosti [Problems of assessing trust in information security audit processes]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2024, no. 3 (61), pp. 40–50.

17. Ivanov A.V., Selifanov V.V., Ognev I.A. Nekotorye voprosy otsenki doveriya k sub"ektam informatsionnogo obmena [Some issues of assessing trust in the subjects of information interaction]. *Zashchita informatsii. Insaid*, 2025, no. 1 (121), pp. 34–40. (In Russian).

18. Ivanov A.V., Ognev I.A., Selifanov V.V. Voprosy otsenki effektivnosti audita informatsionnoi bezopasnosti [Issues of assessing the effectiveness of information security audit]. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere = Journal of the Ural Federal District. Information Security*, 2024, no. 4 (54), pp. 37–48.

19. Martynenko K.K., Tsenina A.V., Selifanov V.V. [Modeling of the risk management process and evaluation of its effectiveness]. *Intellektual'nyi potentsial Sibiri* [Intellectual potential of Siberia]. The 32nd Regional Scientific Student Conference. In 5 pt. Pt. 3. Novosibirsk, NSTU Publ., 2024, pp. 506–508. (In Russian).

20. Soldatov A.Yu., Ivanov A.V., Selifanov V.V. Voprosy postroeniya modeli sistemy upravleniya ugrozami informatsionnoi bezopasnosti [Issues of building a model of information security threat management system]. *Interekspo Geo-Sibir' = Interexpo Geo-Siberia*, 2024, vol. 6, pp. 248–255. DOI: 10.33764/2618-981X-2024-6-248-255.

21. Selifanov V.V., Soldatov A.Yu., Soldatov E.Yu., Podlegaev A.P., Skorikov V.S. Metod otsenivaniya riskov v sistemakh prinyatiya reshenii s uchetom

zashchity informatsii [Risk assessment method in decision-making systems taking into account information protection]. *Vestnik SibGUTI = The Herald of the Siberian State University of Telecommunications and Information Science*, 2023, vol. 17 (2), pp. 84–92. DOI: 10.55648/1998-6920-2023-17-2-84-92.

22. Selifanov V.V., Anikeeva V.V., Ognev I.A. Voprosy otsenki doveriya k sisteme upravleniya riskami [Issues of assessing the credibility of the risk management system]. Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security, 2023, no. 1 (108), pp. 69–82. DOI: 10.17212/2782-2230-2023-1-69-82.

Для цитирования:

Свиридова Л.Е., Огнев И.А. Вопросы оценки доверия к информационной системе персональных данных // Безопасность цифровых технологий. – 2025. – № 2 (117). – С. 25–39. – DOI: 10.17212/2782-2230-2025-2-25-39.

For citation:

Sviridova L.E., Ognev I.A. Voprosy otsenki doveriya k informatsionnoi sisteme personal'nykh dannykh [Questions of trust assessment in information systems of personal data]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2025, no. 2 (117), pp. 25–39. DOI: 10.17212/2782-2230-2025-2-25-39.