Научная статья
УДК 004.27+004.056
https://doi.org/10.31854/1813-324X-2024-10-4-110-125

Обеспечение информационной безопасности интегрируемых информационных систем на базе доверия

Виталий Владимирович Грызунов[1] ✉, viv1313r@mail.ru
Александр Сергеевич Крюков[2], steelrat76@mail.ru
Александр Викторович Шестаков[1], alexander.shestakov@yandex.ru
Игорь Алексеевич Зикратов[3], zikratov.ia@sut.ru

[1]Санкт-Петербургский университет ГПС МЧС России,
Санкт-Петербург, 196105, Российская Федерация
[2]Российский государственный университет правосудия,
Москва, 117418, Российская Федерация
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация

Актуальность. *Информационные системы интегрируются между собой, что приводит к необходимости обеспечить доверие к интегрированной системе. Обеспечение доверия требует формализовать понятие доверия, изучить его природу и структуру.*

Цель работы: *снять противоречие между потребностями, предоставить доступ к ресурсам результирующей интегрированной системы и обеспечить выполнение требований информационной безопасности каждой из интегрируемых систем за счет формулировки понятия доверия с позиции информационной безопасности. Для чего были использованы* ***методы*** *системного анализа, теории управления рисками, резолюций, синтеза операторного уравнения iSOFT.*

Результаты. *Выявлены основные недостатки существующих подходов к формализации понятия «доверие». На базе модели FIST информационной системы разработана функциональная структура доверия и оформлена в нотации IDEF0 для всех уровней интегрируемых информационных систем: обеспечивающего уровня, уровня персонала, уровней аппаратного и программного обеспечений. Приведены примеры нарушения доверия и примеры инструментов создания доверия для каждого уровня информационной системы. Адекватность модели проиллюстрирована на примере реальной интеграции информационных систем. Применение предложенной модели доверия позволило выявить особенности, которые увеличивают риски информационной безопасности для интегрированной информационной системы из примера.*

Новизна. *Предложена трактовка доверия как меры информационной безопасности в отличие от «риска» как меры опасности, а также – инструмент количественного оценивания доверия. Сформулировано и доказано методом резолюций необходимое и достаточное условие создания максимального доверия в информационной системе.*

Практическая значимость. *Предлагаемая модель доверия может использоваться при разработке руководящих документов, регламентирующих процесс интеграции информационных систем, при выдвижении требований к обслуживающему персоналу и созданию программ его обучения, для разработки средств защиты информации и методик их применения.*

Ключевые слова: *риск информационной безопасности, доверие, аргумент доверия, интеграция информационных систем*

Ссылка для цитирования: Грызунов В.В., Крюков А.С., Шестаков А.В., Зикратов И.А. Обеспечение информационной безопасности интегрируемых информационных систем на базе доверия // Труды учебных заведений связи. 2024. Т. 10. № 4. С. 110–125. DOI:10.31854/1813-324X-2024-10-4-110-125. EDN:MZMYXF

Original research
https://doi.org/10.31854/1813-324X-2024-10-4-110-125

Ensuring Information Security of Information Systems to be Integrated Based on Trust

Vitaliy V. Gryzunov[1] ✉, viv1313r@mail.ru
Alexandr S. Krjukov[2], steelrat76@mail.ru
Alexander V. Shestakov[1], alexander.shestakov@yandex.ru
Igor A. Zikratov[3], zikratov.ia@sut.ru

[1]Saint Petersburg University of State Fire Service of Emercom of Russia,
St. Petersburg, 196105, Russian Federation
[2]Russian State University of Justice,
Moscow, 117418, Russian Federation
[3]The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

Relevance. *Information systems are integrated with each other, which leads to the need to ensure the protection of the integrated system. The level of trust requires formalizing the concept of trust and studying its nature and structure.*
The purpose of the article *is to remove the contradiction between the needs to provide access to the resources of the resulting integrated system and ensure compliance with the information security requirements of each of the integrated systems by formulating the concept of trust from the information security perspective.*
Methods used*: systems analysis, risk management theory, resolutions, iSoft operator equation synthesis method.*
Results. *Main shortcomings of existing approaches to the formalization of the concept of "trust" are identified. Based on the FIST information system model, a functional trust structure has been developed and formalized in IDEF0 notation for all levels of integrated information systems: supporting level, personnel level, hardware and software levels. Examples of violation of trust and examples of tools for creating trust for each level of the information system are given. The adequacy of the model is illustrated by the example of real integration of information systems. Application of the proposed trust model made it possible to identify features that increase information security risks for the integrated information system from the example.*
Novelty. *An interpretation of trust as a measure of information security is proposed, in contrast to "risk" as a measure of danger. A tool for quantitative assessment of trust is proposed. A necessary and sufficient condition for creating maximum trust in an information system is formulated and proven by the resolution method*

Practical significance. *The proposed trust model can be used in the development of guidance documents regulating the process of integration of information systems, in setting requirements for service personnel and creating training programs for them, for developing information security tools and methods for their application.*

Keywords: *information security risk, trust, assurance argument, information systems integration*

For citation: Gryzunov V.V., Krjukov A.S., Shestakov A.V., Zikratov I.A. Ensuring Information Security of Information Systems to be Integrated Based on Trust. *Proceedings of Telecommunication Universities.* 2024;10(4):110–125. (in Russ.) DOI:10.31854/1813-324X-2024-10-4-110-125. EDN: MZMYXF

1. Введение

Информационные системы с каждым годом все больше интегрируются друг с другом. Это происходит как в рамках локальной бизнес-сферы: Сбер, Яндекс, электронные торговые площадки и т. д., так и на международном уровне, согласно решению Коллегии евразийской экономической комиссии (ЕЭК). На практике, под интеграцией информационных систем (ИС) понимают процесс установки связей между информационными системами для получения единого информационного пространства, организации поддержки сквозных бизнес-процессов. Под интегрированной системой (*от англ.* Integrated System) понимается «система, в которой все входящие в нее подсистемы работают по

единому алгоритму, т. е. имеет единую точку управления» (ГОСТ Р 55062–2021).

В России действует «Стратегия развития информационного общества на 2017–2030 годы», утвержденная указом Президента Российской Федерации от 9 мая 2017 г. № 203. Целью данной стратегии является улучшение взаимодействия бизнеса и общества с государственными органами власти за счет решения «задачи интеграции федеральных государственных информационных систем (ФГИС) и инфраструктуры пространственных данных на уровне среды (создающей условия для развития платформ и технологий их эффективного взаимодействия с субъектами органов власти) различных сфер деятельности» [1].

Для кардинального улучшения взаимодействия между государством и обществом необходимо устойчивое функционирование информационной инфраструктуры Российской Федерации. Информационная инфраструктура страны в данный момент насчитывает более 50 государственных информационных систем, которые взаимодействуют между собой тем или иным способом.

Интеграция ИС на международном, государственном и корпоративном уровнях позволяет в полной мере раскрыть преимущества, которые дает цифровизация: снижение издержек, связанных с информационной безопасностью (ИБ), как указано в G20 Ministerial in Tsukuba, Japan: Statement on Trade and Digital (https://www.economy.gov.ru/material/file/d53673906a29de7bde82260e21ebcd8b/G20.pdf), повышение эффективности эксплуатации ИС, согласно докладу корпорации PricewaterhouseCoopers «Building Digital Trust The confidence to take risks» (https://www.pwc.com.cy/en/technology-consulting-services/assets/building-digital-trust-january-2016.pdf), создание уверенности в предоставляемых цифровых услугах [2–3], упрощение адаптации ИС к действию деструктивных факторов [4].

В ходе интеграции образуются новые связи между ИС, поэтому возникает проблема согласования целей ИБ, моделей угроз, требований к обеспечению безопасности интегрируемых систем. На интуитивном уровне согласование вопросов ИБ обычно описывается понятием «доверие». То есть ИС могут интегрироваться, если они доверяют друг другу.

Для решения проблемы интеграции информационных систем принят ГОСТ Р 55062-2021 «Информационные технологии. Интероперабельность. Основные положения». Данный документ описывает единый подход к созданию интероперабельных ИС, создание которых позволит полноценно интегрировать информационные системы, но документ не затрагивает вопросы обеспечения ИБ интегрируемых систем. Действующие нормативные документы по ИБ информационных систем определяют требования к ее обеспечению посредством аттестации отдельного экземпляра ИС, а также в ходе эксплуатации этого экземпляра [5, 6]. Обеспечение безопасности интегрированных ИС при этом не рассматривается.

Таким образом, в настоящий момент наблюдается противоречие между необходимостью интегрировать информационные системы и обеспечить их ИБ. Цель настоящего исследования – снять обозначенное противоречие за счет разработки модели обеспечения ИБ интегрируемых ИС, в которой согласуются цели ИБ, модели угроз, требования к обеспечению ИБ интегрируемых систем. Модель является продолжением исследования [7] и базируется на понятии «доверие».

Понятие доверия относится к области ИБ, и понимается научными исследователями по-разному.

2. Обзор современных исследований

Так, например, в работе [8] авторы затрагивают только аспект управления доступом в сложных, территориально распределенных ИС и определяют доверие как меру готовности стороны A с некоторой относительной уверенностью предоставить стороне B запрашиваемый доступ, несмотря на возможные негативные последствия, т. е., принимая в расчет возможный ущерб от действий стороны B, не согласующихся с заявленной ролью. Поскольку под интегрированной системой понимается система, в которой все входящие в нее подсистемы работают по единому алгоритму (см. выше), можно утверждать, что интеграция сегментов сложной, территориально распределенной ИС и отдельных ИС носит идентичный характер.

В качестве развития предыдущей идеи можно рассматривать работу [9], где авторы определяют доверие как меру готовности стороны A положиться на кого-то или что-то в данной ситуации с некоторой относительной уверенностью, несмотря на возможные негативные последствия. В работе отмечается, что в это же определение входит учет потерь в случае обмана. Доверие выражается через риск, преддоверие (репутацию) и канал передачи информации:

$$D = \frac{PD \cdot X}{R + \mu},$$

где D – доверие; PD – преддоверие; X – канал передачи данных; μ – роль (ответственность) абонента; R – риск.

Достоинство данной модели состоит в том, что она предполагает количественную оценку доверия. Однако вызывают вопросы единицы измерения

как элементов доверия, так и самого доверия. В работе [9] не приведены измерения единицы, не указано, чему соответствует доверие, если R и μ равны нулю.

В исследовании [10] доверие к информационной системе управления (ИСУ) определяется как готовность зависеть от нее и быть уязвимым перед ней, не имея возможности отслеживать или контролировать ее функционирование, т. е. в условиях неопределенности и риска. Авторы рассматривают доверие к ИСУ как пережитое состояние отдельного пользователя, которое включает в себя как когнитивные, так и аффективные аспекты. Доверие возникает и изменяется как функция воспринимаемой надежности ИСУ и склонности человека доверять технологиям в целом. Авторы определяют воспринимаемую надежность ИСУ в качестве ее когнитивной оценки пользователем, имеющей положительные свойства в ситуациях, когда пользователи сталкиваются с потенциальными негативными последствиями. Воспринимаемая надежность включает в себя восприятие пользователями надежности, функциональности, полезности и достоверности ИСУ. Кроме того, авторы предполагают, что испытанное доверие влияет на поведенческие намерения пользователей, которые, в свою очередь, предсказывают фактическое использование ИСУ в рабочих процессах и решениях. В работе рассматривается доверительное использование ИСУ не как «наивное», а, скорее как рефлексивное и преднамеренное использование, не ощущая необходимости в дополнительных обходных путях.

В данной работе доверие устанавливается между пользователем (одним человеком) и информационной системой. Представленная в работе «теоретическая модель доверия» в информационных системах управления не отображает составные части ИСУ, и предполагает доверие сразу ко всей системе. Способы получения количественной оценки доверия опущены.

В работе [11] авторы рассматривают фактор доверия как фактор продолжения работы пользователей в социальной сети Facebook, что только косвенно относится к ИБ. Аналогично предыдущей работе доверие рассматривается между пользователем и информационной системой. Пользователь имеет самую низкую компетенцию в ИБ.

Научные изыскания авторов в [12] касаются доверительных отношений двух технологических ядер фирмы: информационных технологий (ИТ) и исследований и разработок. В статье показано, что отношение доверия между технологическими ядрами не зарегулированы документально и больше строятся на доверии между работниками фирмы. Сам термин «доверие» не формализован и не может быть измерен количественно.

В работе [13] делается вывод, что в широком смысле «доверие к технологии» означает готовность зависеть от конкретной технологии в конкретной ситуации, в которой возможны негативные последствия. Подобно доверию к людям, доверие к конкретной технологии формируется двумя отдельными компонентами – доверительным намерением и доверительными убеждениями. Доверие к технологии, ориентированной на конкретные намерения, означает готовность людей зависеть от конкретной технологии. Когда доверие высоко, люди выражают готовность зависеть от конкретной технологии в неопределенных и рискованных ситуациях. Данный подход описывает доверие качественно, и ограничен к применению на практике, где требуется количественное измерение.

В источнике [14] доверие к ИБ рассматривается как услуга. Основой доверия выступает «готовность стороны (доверителя) быть уязвимой для действий другой стороны (доверительного управляющего) на основе ожидания того, что другой (доверительный управляющий) выполнит определенное действие, важное для доверителя, независимо от возможности мониторить или контролировать эту другую сторону (доверенного управляющего)». Приведены семь предположений по взаимосвязи и на их основе предложена концептуальная модель доверия, в которой сервис-провайдер услуг безопасности интегрирует свои сервисы в корпоративную инфраструктуру заказчика. Однако данная модель не в полной мере позволяет понять, как формируется доверие, и как оно может быть измерено.

В работе [15] авторы приводят «конструкт доверия» к интеллектуальным роботам в сфере туризма. В этой работе предлагается модель многогранного доверия к сервисным роботам, состоящая из трех конструктов – производительность, процесс и цель. Само доверие понимается как «установка, что агент поможет достичь целей человека в ситуации, характеризующейся неопределенностью и уязвимостью». Т. е. можно сказать, что в работе рассматривается только один аспект ИБ – доступность.

Исследование [16–17] посвящено доверию пользователей к мобильному банкингу. Выдвинуто предположение, что доверие, влекущее за собой использование мобильного банкинга, включает в себя: осведомленность, инновационность, конфиденциальность, безопасность, полезность, простоту в использовании. В такой постановке ИБ характеризуется понятиями «конфиденциальность» и «безопасность». Но не приводятся инструменты, позволяющие измерить данные понятия количественно.

В исследовании [18] представлено определение отношения доверия между информационными системами. Отношением доверия между системами A

и B – подмножество $T_{a,b} \subset S(A) \times S(B)$. Если пара ($a$, b) принадлежит $T_{a,b}$, то субъект a может получить доступ к объектам системы B посредством субъекта b. В этом случае автор считает, что субъект b доверяет субъекту a. Данное определение доверия касается только получения доступа. В приведенной формулировке доверие – бинарная величина, поэтому невозможно выделить уровни доверия для более гибкого применения данного термина. Некоторые исследователи не формализуют понятие доверия, но подразумевают его существование, и описывают только состав доверия и/или порядок применения. Так, например, авторы [2] приводят главные факторы установления доверия: уверенность, риск, честность, законность, безопасность.

В работе [19] утверждается, что доверие должно быть реализовано с помощью корпоративного WEB–портала, обеспечивающего единую точку входа в информационное пространство корпоративной сети со всеми необходимыми атрибутами – межсетевыми экранами, VPN, системами обнаружения вторжений, антивирусной защитой, системой фильтрации спама и т. д., Доверием может управлять корпоративный удостоверяющий центр с разными режимами доступа, желательно с разной криптографией – западной и отечественной, с различной длиной ключа и т. д.

В своем докладе «Building digital trust into better experiences» компания IBM указывает, что цифровое доверие состоит из нескольких элементов: пользователь и его уникальные атрибуты; аутентификация устройства и конечной точки; деятельность, связанная с данными, приложением и пользователем; среда пользователя, а также сеть; поведение пользователя, при использовании информации; надежность; прозрачность; честность; безопасность. В докладе IBM высказывается мнение, что целью построения доверия должно быть создание безопасного функционала для пользователей. Вопросы количественного измерения доверия отсутствуют.

PricewaterhouseCoopers в своем докладе «Building Digital Trust The confidence to take risks» указывает, что для построения доверия нужна уверенность в:

– безопасности (системы безопасны для защиты данных и нет проблем с идентификацией пользователей);

– данных (в целостности данных и способность извлекать выгоду для развития и получения прибыли);

– системах (ИС осуществляется контроль и мониторинг, позволяющие гарантировать, что они выполняют то, что от них требуется, независимо от того, являются ли они собственными системами или предоставляются в виде облачных сервисов);

– рисках (технологические риски понятны и хорошо управляются, а цифровые платформы будут доступны при необходимости круглосуточно);

– программе цифровой трансформации (в информационной системе можно начать и реализовать следующую комплексную программу цифровой трансформации так, чтобы обеспечить ожидаемые выгоды, в срок и в рамках бюджета).

В данном докладе не уточняется, что такое «уверенность», как ее измерить и как быть, если доверие целенаправленно атакуется [20].

В решении Совета ЕЭК от 05.12.2018 г. № 96 «О требованиях к созданию, развитию и функционированию трансграничного пространства доверия» идет речь о пространстве доверия при межгосударственном обмене данными, выдвигаются требования к созданию, развитию и функционированию трансграничного пространства доверия, требования к архитектуре, обеспечивающей пространство доверия. Однако само определение «пространства доверия» отсутствует.

Согласно ГОСТ Р 54581-2011 доверие (*от англ.* Assurance): выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности. Здесь стоит отметить следующие моменты:

1) налицо неудачный перевод «assurance», более точным является слово «гарантия», «доверию» соответствует английское слово «trust»;

2) доверие является процессом, что немного не согласуется с дальнейшим текстом документа;

3) данный ГОСТ базируется на международном стандарте, который в 2012 г. утратил силу и заменен на ISO/IEC TR 15443-1:2012, где assurance – это основания для обоснованной уверенности в том, что объект оценки соответствует функциональным требованиям безопасности.

ГОСТ Р 54581-2011 касается безошибочной работы IT-систем, а не вопросов обеспечения ИБ.

Аналогичная ситуация с определением доверия в ГОСТ Р ИСО/МЭК 15408-1-2012, где под доверием (assurance) понимается «основание для уверенности в том, что объект оценки отвечает конкретным функциональным требованиям безопасности». Суть стандарта в том, чтобы доказать, что для конкретного типа объекта оценки, в роли которого в настоящей статье выступают интегрируемые информационные системы, применяемые средства защиты позволят гарантировать достижение одного из оценочных уровней доверия [21–23].

На каждый тип объекта оценки составляется профиль защиты – «независимое от реализации изложение потребностей в безопасности для некоторого типа объекта оценки». Применение ГОСТ 15408 для интегрируемых ИС ограничено тем, что:

1) в ходе их интеграции гарантированно возникают особенности, которые сложно типизировать и предусмотреть заранее; 2) интегрированная ИС изменяется во времени, что требует периодического пересмотра профиля защиты и самой системы, а также нового запуска всех оценочных процедур.

Обозначенная ситуация, когда информационная система изменяется во времени, и применение нормативного подхода для обеспечения ее безопасности не вполне достаточное, привело к появлению новой концепции нулевого уровня доверия (Zero Trust Architecture) в NIST Special Publication 800-207 (https://doi.org/10.6028/NIST.SP.800-207). В стандарте речь идет именно о доверии (trust), а не о гарантии (assurance). Нулевое доверие (ZT) «представляет собой набор концепций и идей, предназначенных для минимизации неопределенности при обеспечении точных решений о доступе с наименьшими привилегиями для каждого запроса в информационных системах и службах в условиях сети, которая считается скомпрометированной», т. е. фактически говорится о том, как действовать в ИС, если никакому элементу доверять нельзя [24–26]. Сам термин «доверие» оставлен за скобками стандарта.

Таким образом можно утверждать, что термин «доверие» понимается интуитивно, нуждается в формализации и введении соответствующей метрики. Предложенные в статье определение доверия и количественный показатель для его измерения базируются на модели FIST [27]. FIST разработана в ходе исследования геоинформационных систем. Поскольку геоинформационные системы являются самым сложным типом информационных систем, то любые другие ИС могут рассматриваться как упрощенные версии геоинформационных систем. Следовательно, модель FIST, описывающая произвольные геоинформационные системы, применима для описания произвольной ИС.

3. Доверие в информационной системе согласно модели FIST

Обобщая опыт исследователей, продиктованный в первую очередь требованиями практического применения, можно сделать вывод, что доверие является некоторым антиподом риска. Если считать риск мерой опасности, то *доверие является мерой безопасности*. Когда доверие максимально, то риск минимален. Когда риск максимален, то о доверии говорить не приходится.

Риск – влияние неопределенности на достижение поставленных целей (ГОСТ Р 51897-2021. Менеджмент риска. Термины и определения). Риск ИБ (*по англ.* Information Security Risk) – «возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации. Измеряется, исходя из комбинации вероятности события и его последствия» (ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности). Далее под риском понимается риск ИБ.

Специалисты ИБ выполняют обеспечивающие, а не целевые функции, поэтому обычно не вмешиваются в соответствующие процессы. Поскольку ущерб рассчитывается именно по результатам целевых процессов, то специалисты ИБ не могут его уменьшить, но могут влиять на вероятность возникновения ущерба (далее – вероятность риска P_{risk}) за счет применения средств защиты информации, которые нейтрализуют угрозы.

Взаимосвязь вероятности риска и доверия аналогична связи вероятности отказа и вероятности безотказной работы: если доверия нет, то вероятность риска равна единице, если доверие максимально и равно единице, то вероятность риска равна нулю:

$$D = 1 - R, \qquad (1)$$

где D – доверие ϵ [0; 1]; R – вероятность риска ϵ [0; 1].

Следует отметить, что на практике доверие не может быть равно 1, потому что всегда существует остаточный риск.

Практическое использование формулы (1) будет представлено в дальнейших исследованиях, связанных непосредственно с расчетом количественного значения доверия в рамках модели доверия интегрируемых ИС.

Согласно модели FIST, все ИС имеют «вложенные друг в друга уровни»: уровень программного обеспечения (УПО) «вложен» в уровень аппаратного обеспечения (УАО), УАО «вложен» в уровень персонала (УП), УП «вложен» в обеспечивающий уровень (рисунок 1). Другими словами – обеспечивающим является метауровень для УП, который является метауровнем для УАО, представляющийся, в свою очередь, метауровнем для УПО. Метауровень задает требуемые пространственно-временны́е состояния «вложенного» уровня, т. е. предъявляет требования к его функционированию, накладывает ограничения [27]. На каждом уровне иерархии к доверию предъявляются свои требования, существуют свои особенности его создания; доверие имеет свой состав.

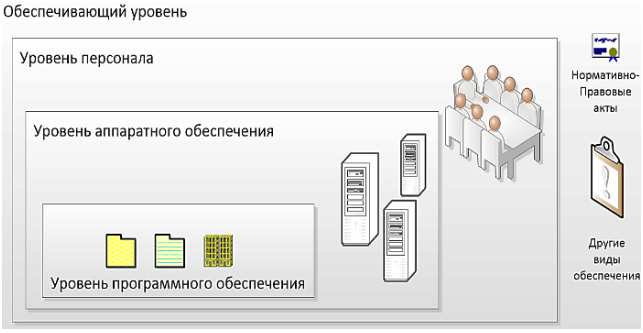

Рис. 1. Модель FIST

Fig. 1. Model FIST

На уровне программного обеспечения доверие связано с программными средствами ИС. Здесь оказывают деструктивное влияние незашифрованный трафик, вредоносное программное обеспечение, эксплойты и т. д. Пример инструмента создания доверия на данном уровне – внедрение протокола https.

На уровне аппаратного обеспечения доверие касается аппаратных средств ИС. Его нарушают аппаратные закладки, подслушивающие устройства, средства радиоэлектронной борьбы и т. д. На данном уровне доверия формируется при помощи модулей доверенной загрузки.

На уровне персонала доверие создается посредством работы с людьми. Действия, совершаемые социальными инженерами, халатными сотрудниками, болтунами и т. д. приводят к снижению доверия к организации [28]. Пример инструмента создания доверия на данном уровне – обучение персонала, проверка его лояльности компании.

На обеспечивающем уровне доверие связано с организационными, правовыми, финансовыми и другими видами обеспечения интеграции ИС [29]. Доверие нарушается за счет сокращения финансирования, ослабления или чрезмерного ужесточения требований к персоналу, программно-аппаратным средствам, необязательностью выполнения регламентов работы ИС и т. д. Пример инструментов создания доверия – создание регламентов, оформление требований к ИБ, разделение сфер ответственности персонала, обслуживающего интегрируемые ИС, и т. п.

Управление доверием непосредственно связано с бизнес-процессами и может быть построено аналогично системе управления адаптацией ИС к деструктивным воздействиям [18–20]. Деструктивные воздействия могут быть детерминированными, стохастическими или агрессивными, целенаправленными [27–30]. Одним наиболее удобных инструментов моделирования в этом случае выступает нотация IDEF0, так как он специально разработан для функциональной декомпозиции и моделирования управленческих процедур [31].

4. Функциональная структура доверия

Функциональная структура модели доверия интегрируемых ИС в нотации IDEF0 представлена на рисунках 2 и 3. Точка зрения – специалист ИБ. Элементы структуры доверия выделены различными цветами для облегчения визуального восприятия. Представленная модель доверия отличается своей функциональной структурой, охватывающей все уровни информационной системы согласно модели FIST.

Цель моделирования – выявление и формулировка условия существования доверия, показателей эффективности создания доверия для интегрируемых информационных систем. Для достижения целей моделирования достаточен первый уровень детализация модели доверия в нотации IDEF0. Более глубокая детализация будет приведена в методике построения пространства доверия.

Цель создания доверия – снизить риск интегрируемых информационных систем до величины остаточного риска. Для этого необходимо знать, какие риски есть, какими активами располагают интегрируемые информационные системы (блок A0). Под активами ИС понимаются информационные ресурсы и средства, а также системы информатизации [32–33], имеющие существенное значение для интегрируемых ИС. Наличие доверия подтверждается аргументом доверия ИС.

Согласно ГОСТ Р ИСО/МЭК 21827-2010:

– аргумент доверия (*от англ.* Assurance Argument): совокупность структурированных заявлений о доверии, подтвержденных доказательствами и аргументацией, четко демонстрирующих, каким образом были удовлетворены потребности в доверии;

– заявление о доверии (*от англ.* Assurance Claim): утверждение или поддержка утверждения того, что система удовлетворяет требованиям безопасности;

– свидетельство обеспечения доверия (*от англ.* Assurance Evidence): результаты анализа обеспечения доверия к объекту (включая итоговые отчеты или другие обоснования), поддерживающие утверждение о доверии.

Формирование доверия обусловлено экономическими, физическими и правовыми ограничениями, а также требованиями бизнеса (целевых процессов). Доверие охватывает все уровни иерархии, согласно модели FIST, и создается организационными мероприятиями, персоналом, аппаратными и программными средствами.

Снижение рисков включает в себя четыре блока функций (см. рисунок 3): снижение рисков обеспечивающего уровня (блок A1), снижение рисков на уровне персонала (блок A2), снижение рисков на аппаратном уровне (блок A3), снижение рисков на программном уровне (блок A4).

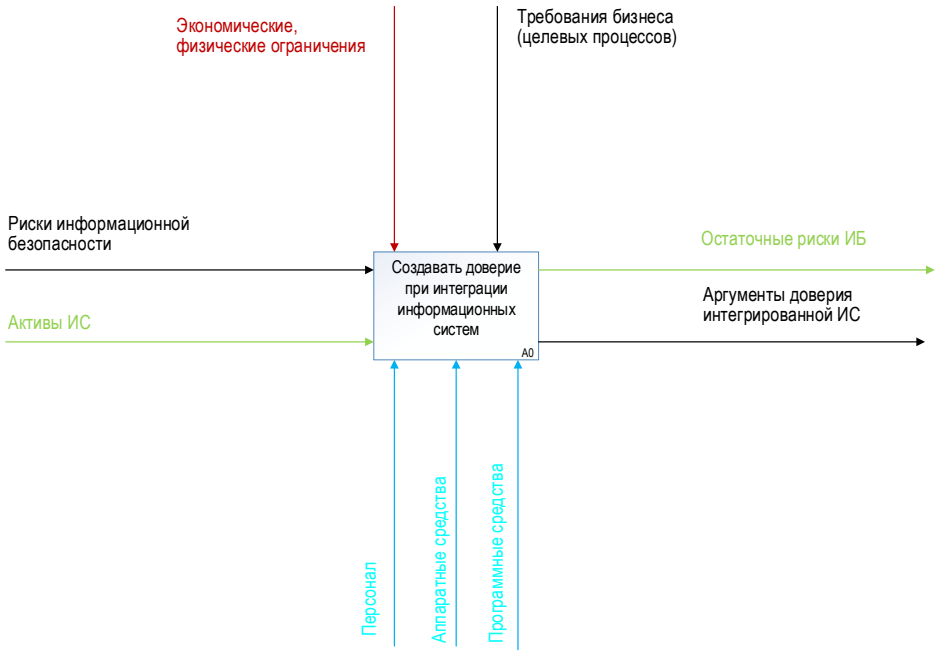

Рис. 2. Доверие в интегрируемых ИС

Fig. 2. Trust in Integrated IS

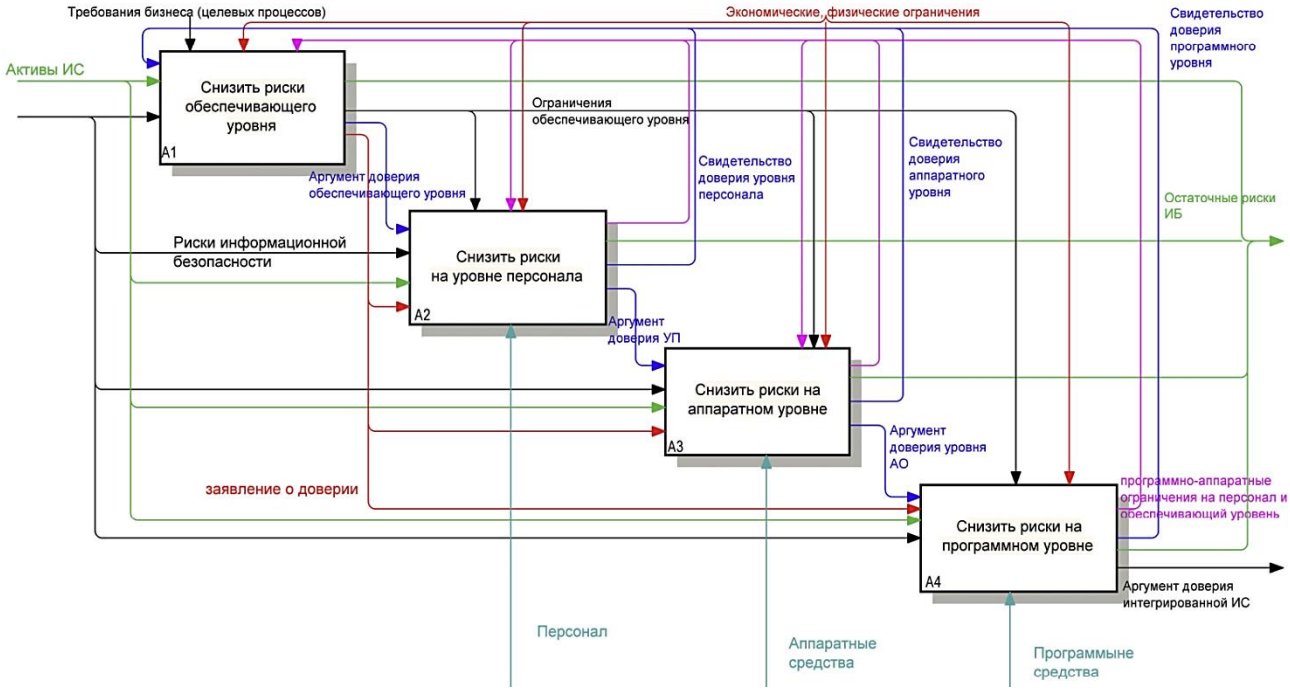

Рис. 3. Функциональная структура доверия в интегрируемых ИС согласно модели FIST

Fig. 3. The Functional Structure of Trust in Integrated IS According to the FIST Model

Снижение риска при создании доверия на обеспечивающем уровне (блок А1) подразумевает подготовку соответствующих организационно-правовых документов, выделение финансирования, предъявление требований ИБ к «вложенным» уровням персонала, аппаратного и программного обеспечения. Разработка документов и финансирование производится для существующих активов интегрируемых информационных систем и рисков этим активам с учетом действующих требований бизнеса (целевых процессов) и экономических и физических ограничений. При этом принимается во внимание обратная связь от «вложенных» уровней в виде ограничений, накладываемых этими уровнями. Например, в качестве требования обеспечивающего уровня может выступать применение сертифицированного программного, аппаратного или программно-аппаратного обеспечения.

Однако, если такого обеспечения не существует, то это является ограничением «вложенных» уровней, накладываемым на обеспечивающий уровень.

Результатом работы обеспечивающего уровня выступают заявление о доверии и аргумент доверия, подтверждающий, что на обеспечивающем уровне вопросы ИБ решены. Аргумент доверия может содержать доказательство того, что правовая экспертиза документов пройдена, документы составлены и утверждены должным образом, запланированное финансирование поступит в требуемом объеме.

Заявление о доверии относится к разряду формальных требований, являющихся видом обеспечения, поэтому заявления о доверии для всех уровней формируются на обеспечивающем уровне.

Снижение риска на уровне персонала (блок А2) выполняется для существующих активов интегрируемых информационных систем, рисков для этих активов. Снижение выполняется на основе заявлений о доверии и аргумента доверия, сформированных на обеспечивающем уровне, с учетом его ограничений, а также ограничений уровней аппаратного и программного обеспечения. Например, для организации выдвигается требование к подтвержденной квалификации персонала (ограничение обеспечивающего уровня). При этом в интегрируемых информационных системах используется платформа Wintel, что выдвигает дополнительные требования к квалификации персонала со стороны «вложенных» уровней аппаратного и программного обеспечения. В свою очередь уровень персонала выдвигает ограничения, обусловленные персоналом. Например, способность усваивать информацию в процессе обучения.

Аргумент доверия, созданный на уровне персонала, содержит элементы аргумента доверия обеспечивающего уровня, дополненные доказательствами того, что на уровне персонала доверие может быть сформировано: персонал прошел аттестационные испытания, участвовал в киберучениях и т. д.

Снижение риска на уровне аппаратного обеспечения (блок А3) выполняется на основе аргумента доверия, сформулированного на уровне персонала, включающего в себя элементы аргумента доверия обеспечивающего уровня, заявления о доверии защищаемых активов информационных систем и рисков для защищаемых активов.

Снижение риска на уровне аппаратного обеспечения выполняется с учетом ограничений, накладываемых другими уровнями информационных систем, требованиями бизнеса (целевых процессов) и экономических и физических ограничений. Например, если необходимо сформировать доверие к распределенной мобильной информационной системе, то требования к весу и энергопотреблению являются ограничениями бизнеса (целевых процессов), минимально возможные габариты и стоимость – физическими и экономическими ограничениями, требования к эргономичности – ограничениями уровня персонала, к безопасности эксплуатации – ограничениями обеспечивающего уровня, применение специального программного обеспечения – ограничениями уровня программного обеспечения.

Ограничения, рождаемые на уровне аппаратного обеспечения, касаются возможностей аппаратуры: пропускная способность линии связи, производительность, емкость накопителей и т. д.

Генерируемый аргумент доверия содержит элементы метауровней, плюс подтверждение того, что доверие сформировано на уровне аппаратного обеспечения. Например, аппаратное обеспечение прошло проверки на отсутствие недекларированных возможностей.

Доверие, создаваемое на уровне программного обеспечения (блок А4), охватывает активы информационной системы, риски для этих активов, использует заявление о доверии и аргумент доверия, поступающий с уровня аппаратного обеспечения.

В процессе формирования доверия учитываются ограничения внешних систем и остальных уровней информационной системы. Например, требование к лицензионной чистоте или наличие антивируса – это ограничения обеспечивающего уровня, способности пользователей запомнить сложные пароли – ограничения уровня персонала, использование процессоров RISC – ограничения уровня аппаратного обеспечения, требование к стоимости разработки программного обеспечения – требование внешней системы.

Уровень программного обеспечения аналогично другим уровням интегрированной информационной системы формирует свои ограничения. Пусть на обеспечивающем уровне выдвинуто требование использовать антивирус марки *X*. Однако этот антивирус работает только под управлением операционной системы *Y*. Операционная система *Y* разработана только для архитектуры CISC. В этом случае требования к архитектуре CISC – ограничение, накладываемое уровнем программного обеспечения на уровень аппаратного обеспечения, требования к квалификации персонала работать с архитектурой CISC и операционной системой *Y* – ограничения для уровня персонала, необходимость сертифицировать операционную систему *Y* – ограничение для обеспечивающего уровня.

По итогам создания доверия на уровне программного обеспечения формируется аргумент до-

верия для интегрированной системы, включающий элементы доверия метауровней и элементы уровня программного обеспечения. Например, подтверждение того, что применение сканера уязвимостей не выявило уязвимостей.

Аргумент доверия содержит структурированные заявления о доверии, которые, в свою очередь, утверждают, что система соответствует требованиям безопасности, и учитывают и прямые, и косвенные угрозы (ГОСТ Р ИСО/МЭК 21827-2010). Поэтому можно сказать, что заявление о доверии учитывает риск, или, другими словами, риск входит в заявление о доверии. Риски информационной системы, которые не могут быть нейтрализованы, формируют остаточный риск интегрированной информационной системы.

Вычисление конкретного значения доверия требует разработки соответствующей методики. На основе предложенных определений и модели доверия необходимое и достаточное условие создания максимального доверия в ИС формулируется следующим образом (результатом интеграции информационных систем является также информационная система, поэтому утверждение сформулировано к ИС как к таковой):

Утверждение. Чтобы в информационной системе доверие было максимальным, необходимо и достаточно, чтобы каждый риск ИБ входил в заявление о доверии и аргумент доверия интегрированной ИС включал каждое заявление о доверии.

Ограничение. Каждый риск ИБ можно нейтрализовать посредством защиты до величины остаточного риска.

Доказываемое утверждение в виде резолюций записывается в следующем виде:

$$\{J\} \Leftrightarrow \{R \wedge S\},$$

где в фигурные скобки {} берется система формул или множество дизъюнктов; $\{J\} \rightarrow \{R \wedge S\}$ - необходимость; $\{R \wedge S\} \rightarrow \{J\}$ - достаточность.

Доказательство непротиворечивости выражения $\{J\} \Rightarrow \{R \wedge S\}$.

Докажем необходимость методом резолюций. Согласно методу, чтобы доказать истинность утверждения F1 ⇒ F2, необходимо и достаточно убедиться, что формула F1 → F2 является тавтологией, где F1, F2 – это посылки. Для этого необходимо и достаточно убедиться, что система формул $\{F1, \overline{F2}\}$ содержит в себе тождественно ложный дизъюнкт 0 ∨ 0.

Система формул утверждения в случае доказательства необходимости примет вид:

$$\left\{J, \overline{(R \wedge S)}\right\} = \left\{J, \overline{R} \vee \overline{S}\right\}.$$

Добавим в систему формул неявно существующие утверждения (таблица 1).

ТАБЛИЦА 1. Неявно существующие утверждения

TABLE 1. Implicitly Existing Statements

Обозначение	Высказывание	Формула
F	Каждый риск ИБ можно нейтрализовать средством защиты до величины остаточного риска (ограничение 1)	
$F \rightarrow M$	Если каждый риск ИБ можно нейтрализовать, то он нейтрализуется	$\overline{F} \vee M$
R	Каждый риск ИБ входит в заявление о доверии	
J	Доверие максимально	
M	Каждый риск ИБ нейтрализован до величины остаточного риска	
S	Каждое заявление о доверии входит в аргумент доверия	
$R \wedge M \rightarrow S$	Если каждый риск ИБ входит в заявление о доверии, и он нейтрализован до величины остаточного риска, то каждое заявление о доверии входит в аргумент доверия (требование утверждения)	$\overline{R} \vee (\overline{M} \vee S)$
$S \rightarrow M \wedge R$	Если каждое заявление о доверии входит в аргумент доверия, значит, каждый риск ИБ нейтрализован до величины остаточного риска (следует из определения аргумента доверия)	$\overline{S} \vee (R \wedge M) = = \overline{S} \vee \overline{R} \vee \overline{M}$

Используем подстановки для представления выражения $\overline{R} \vee (\overline{M} \vee S)$ через совокупность тождественных выражений, являющихся бинарными операциями:

$$\left(\overline{M} \vee S\right) = X,$$
$$\left(\overline{R} \vee \overline{M}\right) = Y,$$
$$\left(\overline{R} \vee S\right) = Z,$$
$$\overline{R} \vee \left(\overline{M} \vee S\right) = \left\{\overline{R} \vee X, Y \vee S, Z \vee \overline{M}\right\}.$$

Используем подстановки для представления выражения $\overline{S} \vee \overline{R} \vee \overline{M}$ через совокупность тождественных выражений, являющихся бинарными операциями:

$$\overline{S} \vee \overline{R} = X2,$$
$$\overline{R} \vee \overline{M} = Y2,$$
$$\overline{S} \vee \overline{M} = Z2,$$
$$\overline{S} \vee \overline{R} \vee \overline{M} = X2 \vee \overline{M}, \ \vee Y2, \ Z2 \vee \overline{R}.$$

В этом случае система формул утверждения для доказательства необходимости примет вид:

$$J, \overline{R} \vee \overline{S}, \overline{R} \vee X, Y \vee S, Z \vee \overline{M}, \overline{F} \vee M, X2 \vee \overline{M}, \overline{S} \vee Y2,$$
$$Z2 \vee \overline{R}, F, R.$$

Если R – контрарный литерал, то для дизъюнктов $\{R, \overline{R} \vee X\}$ резольвентой будет $X = \overline{M} \vee S$.

Добавим резольвенту в систему формул:

$$J, \overline{R} \vee \overline{S}, \overline{R} \vee X, Y \vee S, Z \vee \overline{M}, \overline{F} \vee M, X2 \vee \overline{M}, \overline{S} \vee Y2,$$
$$Z2 \vee \overline{R}, F, R, X, \overline{M} \vee S.$$

Если S – контрарный литерал, то для дизъюнктов $\{\overline{R} \vee \overline{S}, \overline{M} \vee S\}$ резольвентой будет $\overline{M} \vee \overline{R}$.

Добавим резольвенту в систему формул:

$$J, \overline{R} \vee \overline{S}, \overline{R} \vee X, Y \vee S, Z \vee \overline{M}, \overline{F} \vee M, X2 \vee \overline{M}, \overline{S} \vee Y2,$$
$$Z2 \vee \overline{R}, F, R, X, \overline{M} \vee S, \overline{M} \vee \overline{R}.$$

Если R – контрарный литерал, то $R, \overline{M} \vee \overline{R} \Rightarrow \overline{M}$. Если M – контрарный литерал, то $\overline{M}, \overline{F} \vee M \Rightarrow \overline{F}$. Если F – контрарный литерал, то $F \vee 0, \overline{F} \vee 0 \Rightarrow \underline{\mathbf{0 \vee 0}}$ тождественно ложный дизъюнкт. Следовательно, утверждение истинно.

Доказательство непротиворечивости достаточности:

$$\{R \wedge S\} \Rightarrow \{J\} = \{R \wedge S, \overline{J}\}.$$

Система формул утверждения в случае доказательства достаточности методом резолюций примет следующий вид (согласно методу резолюций, конъюнкции должны быть удалены):

$$\{R \wedge S, \overline{J}\} = \{R, S, \overline{J}\}.$$

С учетом неявных закономерностей:

$$R, S, J, \overline{R} \vee X, Y \vee S, Z \vee \overline{M}, X2 \vee \overline{M}, \overline{S} \vee Y2, Z2 \vee \overline{R},$$
$$\overline{F} \vee M, F.$$

Если R – контрарный литерал, то $R, Z2 \vee \overline{R} \Rightarrow$ $\Rightarrow Z2 = \overline{S} \vee \overline{M}$. Если F и M – контрарные литералы, то $F, \overline{F} \vee M \Rightarrow M$ $M, \overline{S} \vee \overline{M} \Rightarrow \overline{S}$, соответственно Если S – контрарный литерал, то $S \vee 0, \overline{S} \vee 0 \Rightarrow \underline{\mathbf{0 \vee 0}}$ – тождественно ложный дизъюнкт. Следовательно, утверждение истинно.

Следствие 1. Если доверие максимально, то вероятность риска минимальна (1).

Следствие 2. Чтобы создать доверие в интегрированной ИС, необходимо описать активы и риски интегрируемых информационных систем.

Рассмотрим работу предложенной модели доверия на примере интеграции информационной системы персональных данных Петербургского государственного университета путей сообщения (далее – ИСПДн ПГУПС) и Государственной информационной системы «Современная цифровая образовательная среда» (далее – ГИС СЦОС), созданной согласно постановлению правительства от 16.11.2020 г. № 1836 «О государственной информационной системе «Современная цифровая образовательная среда».

5. Контрольный пример применения предложенной модели доверия

При интеграции обозначенных ИС требованиями бизнеса (целевых процессов) являются установленные в регламенте требования по подключению к ГИС СЦОС, такие как: приказ о назначении ответственных лиц образовательной организации на подключение к ГИС СЦОС, обеспечение требований к ИБ, заключающиеся в установке определенных средств защиты согласно регламенту. Минимальный класс – КС1 – является ограничением целевых процессов. Сведения об ИС образовательной организации, требования к составу отправляемых данных, минимальные требования к автоматизированному рабочему месту (далее – АРМ) операторов являются ограничениями блока А4.

Требование по наличию лицензии ФСТЭК России и ФСБ России для установки средств криптографической защиты информации (СКЗИ) является правовым ограничением на блок А1. Стоимость установки средств защиты организацией, имеющей лицензии на проведение установочных работ СКЗИ, является экономическим ограничением на блоки А3 и А4. Удовлетворение требований к пропускной способности сети представляется проблематичным, потому что подразумевает прокладку нового сетевого кабеля в культурно-охраняемом здании ПГУПС. Это физическое ограничение от блоков А3 и А4.

Рисками ИБ для двух информационных систем при интеграции являются те риски, которые описаны в актуальной модели угроз информационных систем. Например, в настоящий момент актуальными угрозами для ИСПДн ПГУПС являются: утечка акустической (речевой) информации, НСД с применением стандартных функций операционной системы, утечка информации путем преднамеренного копирования защищаемой информации на неучтенные (в том числе съемные) носители.

Активами информационной системы выступают:

1) данные, которые необходимо передавать в ходе интеграции (персональные данные студентов, информация о направлении подготовки и успеваемости);

2) АРМ, на которых производится обработка данных;

3) программное обеспечение, с помощью которого реализуется взаимодействие.

Заявлением доверия является сообщение о готовности к подключению, а аргументом доверия – совокупность структурированных заявлений о доверии, подтвержденных актами установки средств защиты информации (СЗИ), защите сведений об организации и ответственных сотрудниках.

Инструменты для создания доверия в ходе интеграции:

– персонал информационной системы: операторы и специалисты по ИБ (блок А2);

– аппаратные СЗИ: модули доверенной загрузки на АРМ оператора (блок А3);

– программные СЗИ: Secret Net Studio с дополнительным модулем межсетевого экрана, Kaspersky Endpoint Security для Windows, Континент TLS. Версия 2 (блок А4).

Остаточным риском ИБ являются риски от новых угроз и возможных инсайдеров в ИС. Свидетельством доверия в данном примере выступает закрывающий документ (акт установления интеграции) об успешной интеграции с ГИС СЦОС.

Пример формирования доверия по уровням

Блок А1, обеспечивающий уровень. Данные формируются и движутся между уровнями ИС согласно инструкции по эксплуатации ГИС СЦОС, утвержденной в ПГУПС (требования блока для А1). Активами ИС на данном уровне являются передаваемые данные и АРМ оператора. Свидетельствами доверия с блоков А2–А4 будет информация о конфигурации, настройке СКЗИ и уровень образования сотрудников. Аргументом доверия обеспечивающего уровня (выходным параметром блока А1) являются листы ознакомления операторов с нормативными документами (инструкциями по взаимодействию с ГИС СЦОС, моделью угроз ПГУПС и т. д.), а заявлением о доверии для блоков А2–А4 будет требование о наличии обозначенных документов.

Блок А2, уровень персонала. Предполагается, что квалифицированный оператор несет меньше рисков, чем неквалифицированный, поэтому оператор должен иметь навыки работы с программными и аппаратными средствами (требования для блока А2). Свидетельством доверия уровня персонала (выходной параметр блока А2) выступает результат сдачи зачета на допуск к самостоятельной работе.

Блок А3, уровень аппаратного обеспечения. Требования бизнеса (целевых процессов) на данном уровне (ограничения для блока А3) – стоимость аппаратного обеспечения. Свидетельством доверия на данном уровне является аттестат АРМ оператора, который выдает испытательная лаборатория, имеющая лицензии ФСТЭК России и ФСБ России (выходной параметр блока А3). Ограничением, накладываемым блоком А3 на блок А2, является требование к квалификации оператора работать с данными аппаратными средствами. Ограничения, накладываемые блоком А4 на блок А3: процессор не ниже *i*-10, оперативная память не меньше 16 ГБ и т. д.

Блок А4, уровень программного обеспечения. Оператор формирует пакет данных для передачи из базы данных ИСПДн ПГУПС. Данные из БД ИСПДн ПГУПС через защищенное соединение (TLS) передаются в ГИС СЦОС. Свидетельством доверия будет сообщение об успешной доставке информации до ГИС СЦОС. Ограничения для блока А4 от блока А1 состоят в требованиях настроить парольную политику ПГУПС (например, в парольной политике установлено требование для пароля не менее 8 символов, а программное средство устанавливает максимум пароль из 7 символов), а также программные СЗИ (например, включить межсетевой экран в Secret Net Studio). Ограничениями блока А4 на блок А2 является осведомленность оператора об особенностях работы с данными программными средствами. Аргументом доверия блока А4, который является аргументом доверия ко всей интегрированной ИС, выступает акт об успешном выполнении всех требований ИБ, результаты периодического контроля безопасности.

Если по результатам внедрения СЗИ вероятность риска стала R = 0,002, то, согласно (1), доверие в интегрированной ИС будет D = 0,998.

В ходе практической эксплуатации и, исходя из моделирования, установлено, что необходимое и достаточное условия существования доверия интегрируемых систем (ИСПДн ПГУПС и ГИС СЦОС) не выполнены. Необходимое и достаточное условие, сформулированное в Утверждении, связано с элементами структуры доверия (см. рисунок 3): J – цель создания доверия (на рисунке 3 не отражено явно); R – говорит о том, что каждой стрелке, обозначающей риск ИБ, ставится в соответствие стрелка, обозначающая заявление о доверии; S – требует, чтобы результирующая стрелка «Аргумент доверия интегрированной ИС» включала в себя все стрелки, описывающие аргументы доверия других уровней, которые, в свою очередь, включают в себя все стрелки, описывающие заявления о доверии. Следовательно, необходимое и достаточное условие существования доверия (см. Утверждение) на рисунке 3 выглядит как наличие всех «стрелочек» в структуре доверия, т. е. выполнение и наличие всех ограничений, аргументов, заявления доверия и т. д. По причине отсутствия некоторых ограничений существуют следующие возможности нарушения ИБ:

– удаленный доступ на АРМ оператора при подключении к ГИС СЦОС (нарушает аргумент доверия уровня персонала, что может привести нарушению ИБ ИС);

– подключения другим оператором / посторонним лицом с помощью действующего сертификата оператора (управление ИС оператором, не ознакомленным с инструкцией по ее эксплуатации, является нарушением аргумента доверия уровня персонала);

– перемещение АРМ операторов в другие кабинеты (нарушает аргумент доверия обеспечивающего уровня, что может привести к утечке информации по визуальным каналам утечки);

– эксплуатация системы даже в случае увольнения работников, ответственных за интеграцию ИС (нарушает аргумент доверия уровня персонала, что приводит приведет к сложностям при расследовании инцидента);

– подключение съемных носителей к АРМ оператора (возможен перенос вирусов и различной вредоносной информации, в том числе и такой, что ее не обнаружит последняя версия антивируса, т. е. нарушены аргументы доверия программного и аппаратного уровней.

Кроме того, выявлено отсутствие в нормативных документах (блок А1):

– ответственности за передачу неверных данных и / или вредоносной информации, что повышает риски нарушения ИБ на уровне персонала (блок А2);

– обоснование необходимости применения средств защиты и разъяснение последствий инцидентов ИБ; в результате персонал не видит необходимости в использовании СЗИ и может их отключить для более комфортной работы в ИС.

6. Заключение

В работе на основе анализа литературы сформулировано определение доверия как меры ИБ, дополняющей риск безопасности до полной группы событий и распространяющееся на каждый уровень иерархии ИС согласно модели FIST. На каждом уровне иерархии ИС доверие имеет свою специфику, но цель доверия, заключающаяся в снижении риска ИБ, возникающего при интеграции ИС, остается неизменной.

Разработана модель доверия, отличающаяся охватом всех уровней интегрируемых информационных систем и позволяющая оценить доверие количественно. Согласно предложенной модели доверия, на каждом уровне иерархии ИС существует остаточный риск ИБ, из которого состоит остаточный риск интегрированной ИС. Расчет остаточного риска и доверия требует разработки соответствующих методик.

С продвижением от уровня (см. рисунок 3) с меньшим номером (А1) к уровню с большим номером (А4) появляется все больше ограничений, однако каждый последующий уровень в некоторых случаях может снизить остаточный риск других уровней ИС.

Необходимым и достаточным условием максимизации доверия в ИС при некоторых ограничениях является формирование аргумента доверия, включающего в себя все заявления о доверии интегрируемых ИС.

Адекватность модели продемонстрирована на контрольном примере интеграции ИСПДн ПГУПС и ГИС СЦОС. Данного примера достаточно для демонстрации адекватности модели, т. к. он отражает все связи в структуре модели и варианты использования модели.

Поскольку доверие по определению (см. выше) строится, исходя из удовлетворения целей безопасности, риски и активы формулируются согласно целям безопасности и моделям угроз, то можно утверждать, что предложенная модель доверия дает возможность обеспечить ИБ интегрируемых ИС, и значит, цель исследования достигнута.

Дальнейшим направлением исследований выступит разработка методики практического применения разработанной модели доверия.

Список источников

1. Черных А.М. Основные направления интеграции федеральных государственных информационных систем и пространственных данных // Правовая информатика. 2018. № 2. С. 47–56. EDN: XRPRMT

2. Yan Z., Holtmanns S. Trust Modeling and Management: From Social Trust to Digital Trust // Computer Security, Privacy and Politics: current Issues, Challenges and Solutions. 2008. PP. 290–323. DOI:10.4018/978-1-59904-804-8.ch013

3. Chahal R.K., Kumar N., Batra S. Trust management in social Internet of Things: A taxonomy, open issues, and challenges // Computer Communications. 2020. Vol. 150. PP. 13–46. DOI:10.1016/j.comcom.2019.10.034

4. Burlov V.G., Gryzunov V.V. Evaluation of the effectiveness of geographic information systems adaptation to destabilizing factors // Journal of Physics: Conference Series. 2020. Vol. 1703. P. 012016. DOI:10.1088/1742-6596/1703/1/012016

5. Селифанов В.В., Гордеев А.С., Карманов И.Н. Требования по защите информации при межсетевом взаимодействии государственных информационных систем с иными информационными системами // Интерэкспо Гео-Сибирь. 2018. № 7. С. 277–282. EDN:YORFLV

6. Прокушев Я.Е., Пономаренко С.В., Пономаренко С.А. Моделирование процессов проектирования систем защиты информации в государственных информационных системах // Computational nanotechnology. 2021. Т. 8. № 1. С. 26–37. DOI:10.33693/2313-223X-2021-8-1-26-37. EDN:XJMNND

7. Грызунов В.В., Корниенко А.А., Глухарев М.Л., Крюков А.С. Выбор моделей доверия при интеграции распределенных информационных систем критического применения // Проблемы информационной безопасности. Компьютерные системы. 2021. № 4. С. 79–90. DOI:10.48612/jisp/ev3e-fmtu-x25h. EDN:VMALWC

8. Кругликов С.В., Дмитриев В.А., Степанян А.Б., Максимович Е.П. Информационная безопасность информационных систем с элементами централизации и децентрализации // Вопросы кибербезопасности. 2020. № 1(35). С. 2–7. DOI:10.21681/2311-3456-2020-01-02-07. EDN:HVFMFK

9. Шиверов П.К., Бондаренко В.В. Понятие доверия в контексте информационной безопасности // Международная конференция и молодёжной школы «Информационные технологии и нанотехнологии» (ИТНТ-2016, Самара, Российская Федерация, 17–19 мая 2016). Самара: Самарский государственный аэрокосмический университет, 2016. С. 414–418. EDN:WMPXCP

10. Meeßen S.M., Thielsch M.T., Hertel G. Trust in Management Information Systems (MIS) // Zeitschrift für Arbeits-und Organisationspsychologie A&O. 2019. № 64. Iss. 1. PP. 6–16. DOI:10.1026/0932-4089/a000306

11. Maqableh M., Hmoud H.Y., Jaradat M., Masadeh R. Integrating an information systems success model with perceived privacy, perceived security, and trust: the moderating role of Facebook addiction // Heliyon. 2021. Vol. 7. Iss. 9. PP. 1–15. DOI:10.1016/j.heliyon.2021.e07899

12. Ettlie J.E., Tucci C., Gianiodis P.T. Trust, integrated information technology and new product success // European Journal of Innovation Management. 2017. Vol. 20. Iss. 3. PP. 406–427. DOI:10.1108/EJIM-12-2015-0128

13. McKnight H., Carter M., Clay P. Trust in technology: Development of a set of constructs and measures // DIGIT 2009 Proceedings. 2009. URL: https://aisel.aisnet.org/digit2009/10 (Accessed 10.06.2024)

14. Ngo-Ye T.L., Nazareth D.L., Choi J.J. Trust in security as a service: a theoretical model // Issues in Information Systems. 2020. Vol. 21. Iss. 2. PP 64–74.

15. Park S. Multifaceted trust in tourism service robots // Annals of Tourism Research. 2020. Vol. 81. P. 102888. DOI:10.1016/j.annals.2020.102888

16. Ramos F.L., Ferreira J.B., Freitas A.S., Rodrigues J.W. The Effect of Trust in the Intention to Use *m*-banking // BBR. Brazilian Business Review. 2018. Vol. 15. Iss. 2. PP. 175–191. DOI:10.15728/bbr.2018.15.2.5

17. Putra G.C., Astiti N.P.Y., Gunadi G.N.B. The Exploring of Trust that Influences Customer's Intention to Use FinnTech M-Banking Application on Regional Banks // International Journal of Economics and Business Administration. 2020. Vol. 8. Iss. 4. PP. 407–421.

18. Иткес А.А. Объединение моделей логического разграничения доступа для сложноорганизованных распределенных информационных систем // Проблемы информатики. 2010. № 1(5). С. 85–94. EDN:NBRZPN

19. Глухова Л.В., Губанова С.Е. Некоторые аспекты менеджмента информационной безопасности промышленных комплексов // Вестник Волжского университета им. В.Н. Татищева. 2015. №3(34). С. 135–144. EDN:VBWJDX

20. Gryzunov V.V. Conceptual Model for Adaptive Control of a Geographic Information System under Conditions of Destabilization // Automatic Control and Computer Sciences. 2021. Vol. 55. Iss. 8. PP. 1222–1227. DOI:10.3103/S0146411621080381

21. Покровский И.А. Разобраться в понятиях // Безопасность информационных технологий. 2023. Т. 30. №. 2. С. 21–22.

22. Калашников А.О., Бугайский К.А., Бирин Д.С., Дерябин Б.О., Цепенда С.О., Табаков К.В. Применение логико-вероятностного метода в информационной безопасности (часть 1) // Вопросы кибербезопасности. 2023. №. 4(56). С. 23–32. DOI:10.21681/2311-3456-2023-4-23-32. EDN:GIHSBN

23. Zefferer T., Prunster B., Kollmann C., Corici A.A. A Security-Evaluation Framework for Mobile Cross-Border e-Government Solutions // Proceedings of the 24th Annual International Conference on Digital Government Research (Gdansk, Poland, 11–14 July 2023). New York: Association for Computing Machinery, 2023. PP. 536–543. DOI:10.1145/3598469. 359852

24. Phiayura P., Teerakanok S. A Comprehensive Framework for Migrating to Zero Trust Architecture // IEEE Access. 2023. Vol. 11. PP. 19487–19511. DOI:10.1109/ACCESS.2023.3248622

25. Ahmadi S. Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities // Journal of Engineering Research and Reports. 2024. Vol. 26. Iss. 2. PP. 215–228. DOI:10.9734/jerr/2024/v26i21083

26. Khan M.J. Zero trust architecture: Redefining network security paradigms in the digital age // World Journal of Advanced Research and Reviews. 2023. Vol. 19. Iss. 3. PP. 105–116. DOI:10.30574/wjarr.2023.19.3.1785

27. Грызунов В.В. Модель геоинформационной системы FIST, использующей туманные вычисления в условиях дестабилизации // Вестник Дагестанского государственного технического университета. Технические науки. 2021. Т. 48. № 1. С. 76–89. DOI:10.21822/2073-6185-2021-48-1-76-89. EDN:IDEYPX

28. Gryzunov V.V. Model of Purpose Aggressive Actions on the Information-Computing System // Proceedings of the 3rd International Conference on Human Factors in Complex Technical Systems and Environments (ERGO, St. Petersburg, Russia, 04–07 July 2018). IEEE, 2018. PP. 119–121. DOI:10.1109/ERGO.2018.8443814

29. Gryzunov V.V., Bondarenko I.Yu. A Social Engineer in Terms of Control Theory // Proceedings of the 3rd International Conference on Human Factors in Complex Technical Systems and Environments (ERGO, St. Petersburg, Russia, 04–07 July 2018). IEEE, 2018. PP. 202–204. DOI:10.1109/ERGO.2018.8443835

30. Gryzunov V., Gryzunova D. Problems of Providing Access to a Geographic Information System Processing Data of Different Degrees of Secrecy // Khanna K., Estrela V.V., Rodrigues J.J.P.C. (eds.) Cyber Security and Digital Forensics. Lecture Notes on Data Engineering and Communications Technologies. Singapore: Springer, 2022. Vol. 73. PP. 191–198. DOI:10.1007/978-981-16-3961-6_17

31. Ананьев И.В., Серова Е.Г. Области эффективного применения нотации IDEF0 для задач описания бизнес-процессов // Вестник Санкт-Петербургского университета. Менеджмент. 2008. № 2. С. 161–172. EDN:JUBTXH

32. Канев С.А. Акцент на эффект. Определение характеристик эффективности использования информационных активов компаний // Креативная экономика. 2010. № 8(44). С. 42–47. EDN:MSVWFV

33. Манжосов А.В., Болодурина И.П., Сабуров В.С., Долгушев Н.А. Разработка специальной классификации информационных активов в сфере информационной безопасности // Вестник Пермского университета. Математика. Механика. Информатика. 2022. № 4(59). С. 54–60. DOI:10.17072/1993-0550-2022-4-54-60. EDN:ZHZWNB

References

1. Chernykh A. The main directions of federal state information systems and classified data. *Legal Informatics*. 2018;2: 47–56. (in Russ.) EDN:XRPRMT
2. Yan Z., Holtmanns S. Trust Modeling and Management: From Social Trust to Digital Trust. *Computer Security, Privacy and Politics: current Issues, Challenges and Solutions*. 2008:290–323. DOI:10.4018/978-1-59904-804-8.ch013
3. Chahal R.K., Kumar N., Batra S. Trust management in social Internet of Things: A taxonomy, open issues, and challenges. *Computer Communications*. 2020;150:13–46. DOI:10.1016/j.comcom.2019.10.034
4. Burlov V.G., Gryzunov V.V. Evaluation of the effectiveness of geographic information systems adaptation to destabilizing factors. Journal of Physics*: Conference Series*. 2020;1703:012016. DOI:10.1088/1742-6596/1703/1/012016
5. Selifanov V.V., Gordeev A.S., Karmanov I.N. Requirements for information sequrity in cross-network interaction of the state information systems with other information systems. *Interexpo GEO-Sibiria.* 2018;7:277–282. (in Russ.) EDN:YORFLV
6. Prokushev Ya.E., Ponomarenko S.V., Ponomarenko S.A. The Modeling of information security system design processes in state information systems. Computational Nanotechnology. 2021;1:26–37. (in Russ.) DOI:10.33693/2313-223X-2021-8-1-26-37. EDN:XJMNND
7. Gryzunov V.V Kornienko A.A., Glukharev M.L., Kryukov A.S. Selection of trust models when integrating distributed information systems of critical application. *Information Security Problems. Computer Systems.* 2021;479–90. (in Russ.) DOI:10.48612/jisp/ev3e-fmtu-x25h. EDN:VMALWC
8. Kruglikov S., Dmitriev V., Stepanian A., Maksimovich E. Information security of information systems with elements of centralization and decentralization. Voprosy kiberbezopasnosti. 2022;1(35):2–7. (in Russ.) DOI:10.21681/2311-3456-2020-01-02-07. EDN:HVFMFK
9. Shiverov P.K., Bondarenko V.V. The concept of trust in the context of information security. *Proceedings of the International Conference and Youth School on Information Technologies and Nanotechnologies, ITNT-2016, 17–19 May 2016, Samara, Russian Federation.* Samara: Samara State Aerospace University Publ.; 2016. p.414–418. (in Russ.) EDN:WMPXCP
10. Meeßen S.M., Thielsch M.T., Hertel G. Trust in Management Information Systems (MIS). *Zeitschrift für Arbeits-und Organisationspsychologie A&O.* 2019;64(1):6–16. DOI:10.1026/0932-4089/a000306
11. Maqableh M., Hmoud H.Y., Jaradat M., Masadeh R. Integrating an information systems success model with perceived privacy, perceived security, and trust: the moderating role of Facebook addiction. *Heliyon*. 2021;7(9):1–15. DOI:10.1016/j.heliyon.2021.e07899
12. Ettlie J.E., Tucci C., Gianiodis P.T. Trust, integrated information technology and new product success. *European Journal of Innovation Management*. 2017;20(30):406–427. DOI:10.1108/EJIM-12-2015-0128
13. McKnight H., Carter M., Clay P. Trust in technology: Development of a set of constructs and measures. *DIGIT 2009 Proceedings*. 2009. URL: https://aisel.aisnet.org/digit2009/10 [Accessed 10.06.2024]
14. Ngo-Ye T.L., Nazareth D.L., Choi J.J. Trust in security as a service: a theoretical model. *Issues in Information Systems*. 2020;21(2);64–74.
15. Park S. Multifaceted trust in tourism service robots. *Annals of Tourism Research*. 2020;81:102888. DOI:10.1016/ j.annals.2020.102888
16. Ramos F.L., Ferreira J.B., Freitas A.S., Rodrigues J.W. The Effect of Trust in the Intention to Use *m*-banking. *BBR. Brazilian Business Review*. 2018;15(2):175–191. DOI:10.15728/bbr.2018.15.2.5
17. Putra G.C., Astiti N.P.Y., Gunadi G.N.B. The Exploring of Trust that Influences Customer's Intention to Use FinnTech M-Banking Application on Regional Banks. *International Journal of Economics and Business Administration*. 2020;8(4):407–421.
18. Itkes A.A. Combining logical access control models for complex distributed information systems. *Problemy informatiki*. 2010;3:85–94. (in Russ.) EDN:NBRZPN
19. Glukhova L.V., Gubanova S.E. Some aspects of information security management of industrial complexes. Vestnik of Volzhsky University named after V.N. Tatishchev. 2015;3(34):135–144. (in Russ.) EDN:VBWJDX
20. Gryzunov V.V. Conceptual Model for Adaptive Control of a Geographic Information System under Conditions of Destabilization. *Automatic Control and Computer Sciences.* 2021;55(8):1222–1227. DOI:10.3103/S0146411621080381
21. Pokrovskij I.A. To understand the concepts. IT Security. 2023;2:21–22. (in Russ.).
22. Kalashnikov A.O., Bugajskij K.A., Birin D.S., Dereabin B.O., Tsependa S.O., Tabakov K.V. Application of the logical-probabilistic method in information security (part 1). *Voprosy kiberbezopasnosti.* 2023;4(56):23–32. (in Russ.) DOI:10.21681/2311-3456-2023-4-23-32. EDN:GIHSBN
23. Zefferer T., Prunster B., Kollmann C., Corici A.A. A Security-Evaluation Framework for Mobile Cross-Border e-Government Solutions. *Proceedings of the 24th Annual International Conference on Digital Government Research, 11–14 July 2023, Gdansk, Poland*. New York: Association for Computing Machinery; 2023. p.536–543. DOI:10.1145/3598469. 359852
24. Phiayura P., Teerakanok S. A Comprehensive Framework for Migrating to Zero Trust Architecture. *IEEE Access*. 2023;11:19487–19511. DOI:10.1109/ACCESS.2023.3248622
25. Ahmadi S. Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. *Journal of Engineering Research and Reports*. 2024;26(2):215–228. DOI:10.9734/jerr/2024/v26i21083
26. Khan M.J. Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*. 2023;19(3):105–116. DOI:10.30574/wjarr.2023.19.3.1785
27. Gryzunov V.V. FIST geoinformation system model using fog computing in destabilization. *Herald of Dagestan State Technical University. Technical Sciences*. 2021;48(1):76–89. (in Russ.) DOI:10.21822/2073-6185-2021-48-1-76-89. EDN:IDEYPX
28. Gryzunov V.V. Model of Purpose Aggressive Actions on the Information-Computing System. *Proceedings of the 3rd International Conference on Human Factors in Complex Technical Systems and Environments, ERGO, 04–07 July 2018, St. Petersburg, Russia*. IEEE; 2018. p.119–121. DOI:10.1109/ERGO.2018.8443814

29. Gryzunov V.V., Bondarenko I.Yu. A Social Engineer in Terms of Control Theory. *Proceedings of the 3rd International Conference on Human Factors in Complex Technical Systems and Environments, ERGO, 04–07 July 2018, St. Petersburg, Russia*. IEEE; 2018. p.202–204. DOI:10.1109/ERGO.2018.8443835

30. Gryzunov V., Gryzunova D. Problems of Providing Access to a Geographic Information System Processing Data of Different Degrees of Secrecy. *In: Khanna K., Estrela V.V., Rodrigues J.J.P.C. (eds.) Cyber Security and Digital Forensics. Lecture Notes on Data Engineering and Communications Technologies, vol.73*. Singapore: Springer; 2022. p.191–198. DOI:10.1007/978-981-16-3961-6_17

31. Anan'ev I.V., Serova E.G. Areas of effective application of IDEF0 notation for tasks of describing business processes. *Vestnik of Saint Petersburg University. Management.* 2008;2:161–172. (in Russ.) EDN:JUBTXH

32. Kanev S.A. Determination of characteristics of a company's informational assets use efficiency. *Creative Economy.* 2010;8(44):42–47. (in Russ.) EDN:MSVWFV

33. Manzhosov A.V., Bolodurina I.P., Saburov V.S., Dolgushev N.A. Development of a special classification of information assets in the information security field. *Bulletin of Perm University. Mathematics. Mechanics. Computer Science.* 2022;4(59):54–60. (in Russ.) DOI:10.17072/1993-0550-2022-4-54-60. EDN:ZHZWNB

Статья поступила в редакцию 14.06.2024; одобрена после рецензирования 15.07.2024; принята к публикации 25.07.2024.
The article was submitted 14.06.2024; approved after reviewing 15.07.2024; accepted for publication 25.07.2024.

Информация об авторах:

ГРЫЗУНОВ Виталий Владимирович
доктор технических наук, доцент, профессор кафедры прикладной информатики и информационных технологий Санкт-Петербургского университета ГПС МЧС России
https://orcid.org/0000-0003-4866-217X

КРЮКОВ Александр Сергеевич
преподаватель кафедры информационного и интеллектуального права, цифровых технологий и инноватики Российского государственного университета правосудия
https://orcid.org/0000-0002-4633-8635

ШЕСТАКОВ Александр Викторович
доктор технических наук, старший научный сотрудник, ведущий научный сотрудник отдела информационного обеспечения населения и технологий информационной поддержки РСЧС и пожарной безопасности Санкт-Петербургского университета ГПС МЧС России
https://orcid.org/0000-0002-8462-6515

ЗИКРАТОВ Игорь Алексеевич
доктор технических наук, профессор, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0009-0000-2939-1971

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.