ПРОБЛЕМЫ ОЦЕНКИ ДОВЕРИЯ К ПРОЦЕССАМ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Иванов А. В.[1], Огнев И. А.[2]

DOI: 10.21681/2311-3456-2024-3-40-50

Цель исследования: *формирование алгоритма оценки доверия к процессу аудита информационной безопасности, состоящего из последовательного многоэтапного анализа доказательств доверия по иерархической модели «объект-критерии-метрики».*

Методы исследования *базируются на анализе отечественного и зарубежного нормативно-правового поля, научных публикаций, а также на применении функции желательности Харрингтона.*

Результат: *был сформирован алгоритм проведения оценки доверия, состоящий из последовательного многоэтапного анализа доказательств доверия по иерархической модели «объект-критерии-метрики». В соответствии с данной иерархической моделью метрики вычисляются на основе анализа доказательств доверия, критерии – на основе значений метрик, а уровень доверия – на основе значений критериев. Были определены метрики и критерии оценки доверия. Расчет доверия к процессу аудита информационной безопасности базируется на функции желательности Харрингтона и ГОСТ Р 57580.2–2018. В данном случае метрики, как числовой результат оценки доказательств доверия, выступают частными признаками желательности, критерии – как частные функции желательности, а уровень доверия к процессу аудита информационной безопасности – как обобщенная функция желательности.*

Полученный алгоритм оценки доверия к процессам аудита информационной безопасности будет интегрирован в общий алгоритм оценки доверия к субъектам информационного обмена, который включает в себя анализ ряда процессов информационной безопасности, одним из которых является аудит.

Научная новизна *заключается в предложении динамического метода контроля процесса аудита информационной безопасности, основанного на анализе объективных свидетельств и подлежавшего автоматизации. Оценка доверия, как динамическая мера контроля процессов информационной безопасности, призвана минимизировать трудо- и времязатраты при контроле процессов информационной безопасности.*

Ключевые слова: *доверие, оценка доверия, оценка соответствия, доверие к аудиту, оценка процессов, доверенное взаимодействие, информационная безопасность, кибербезопасность.*

PROBLEMS OF ASSESSING TRUST IN INFORMATION SECURITY AUDIT PROCESSES

Ivanov A. V.[3], Ognev I. A.[4]

The purpose of the study: *the formation of an algorithm for assessing trust in the information security audit process, consisting of a sequential multi-stage analysis of evidence of trust according to the hierarchical model «object-criteria-metrics».*

The research methods *are based on the analysis of the domestic and foreign regulatory framework, scientific publications, as well as on the application of Harrington's desirability function.*

Result: *an algorithm for assessing trust was formed, consisting of a sequential multi-stage analysis of evidence of trust according to the hierarchical model «object-criteria-metrics». In accordance with this hierarchical*

1 Иванов Андрей Валерьевич, кандидат технических наук., доцент, заведующий кафедрой защиты информации, Новосибирский государственный технический университет (НГТУ), Новосибирск, РФ. E mail: andrej.ivanov@corp.nstu.ru

2 Огнев Игорь Александрович, аспирант, ассистент кафедры защиты информации, Новосибирский государственный технический университет (НГТУ), Новосибирск, РФ. E-mail: i.ognev.2016@corp.nstu.ru

3 Andrey V. Ivanov, Ph.D., Associate Professor, Head of the Department of Information Security, Novosibirsk State Technical University (NSTU), Novosibirsk, Russian Federation. E-mail: andrej.ivanov@corp.nstu.ru

4 Igor A. Ognev, graduate student, assistant at the Department of Information Security, Novosibirsk State Technical University (NSTU), Novosibirsk, Russian Federation. E-mail: i.ognev.2016@corp.nstu.ru

model, metrics are calculated based on the analysis of evidence of trust, criteria are calculated based on the values of the metrics, and the level of trust is calculated based on the values of the criteria. Metrics and criteria for assessing trust were defined. The calculation of trust in the information security audit process is based on the Harrington desirability function and GOST R 57580.2–2018. In this case, metrics, as a numerical result of assessing evidence of trust, act as partial signs of desirability, criteria – as partial functions of desirability, and the level of confidence in the information security audit process – as a generalized function of desirability.

The resulting algorithm for assessing trust in information security audit processes will be integrated into the general algorithm for assessing trust in subjects of information exchange, which includes an analysis of a number of information security processes, one of which is audit.

***The scientific novelty** lies in the proposal of a dynamic method for monitoring the information security audit process, based on the analysis of objective evidence and subject to automation. Trust assessment, as a dynamic measure of control of information security processes, is designed to minimize labor and time costs when monitoring information security processes.*

***Keywords:** trust, methodology, conformity assessment, audit trust, process assessment, trusted interaction, information security, cybersecurity.*

Введение

Текущая ситуация в сфере информационной безопасности явно указывает на то, что организациям необходимо постоянно повышать свой уровень защищенности, как от внешних, так и от внутренних угроз. Positive Technologies, ведущая компания-разработчик в сфере информационной безопасности[5], основываясь на статистике, полученной от более чем 2300 организаций в России, отмечает постоянный рост количества киберугроз. В 2020 г. по сравнению с 2019 г. рост составил 51%, при этом 70% атак носили целенаправленный характер[6]; в 2021 г. по сравнению с 2020 г. рост составил 6,5%, при этом доля целевых атак возросла на 4% и составила 74% от общего количества атак[7]. Эксперты «Лаборатории Касперского» отмечают резкий рост количества сложных кибератак в 4 раза в первом квартале 2022 г. по сравнению с аналогичным периодом в 2021 г[8]. Основой для построения сложных атак являются небольшие бреши в системе безопасности организации [1]. Для планирования векторов проведения атаки злоумышленники используют результаты нелегитимного исследования, оценивая уязвимости – как известные, так и еще необнародованные, так называемые уязвимости нулевого дня (0-day). Из-за технической сложности обнаружения таких брешей стандартными средствами защиты информации необходимо выстроить непрерывный процесс анализа и контроля систем защиты информации и процессов информационной безопасности.

В современных условиях функционирования информационных систем вопрос о подтверждении состояния защищенности субъектов информационного обмена становится актуальным. Под субъектом информационного обмена понимается юридическое лицо или орган государственной власти, которому на праве владения, аренды или ином законном основании принадлежат информационные системы (государственные информационные системы, информационные системы персональных данных, автоматизированные системы управления технологическими процессами, объекты критической информационной инфраструктуры). Существующие статические методы[9] [2, 3] оценки защищенности субъектов информационного обмена не дают актуальную информацию о состоянии системы защиты, что приводит к необходимости использовать динамические методы оценки состояния систем защиты информации. Разрабатываемая технология оценки уровня доверия к субъектам информационного обмена [4, 5] позволит оперативно оценивать состояние систем безопасности участников информационного обмена и реагировать на изменение этого состояния. Данная технология позволит обеспечить высокую скорость реагирования на нарушения состояния безопасности, возникающие при взаимодействии участников информационного обмена, и своевременное принятие необходимых мер по их устранению.

5 О компании // Positive Technologies [Электроный ресурс]. 2022 – URL: https://www.ptsecurity.com/ru-ru/about/ (дата обращения: 12.02.2023).

6 Актуальные киберугрозы: итоги 2020 года // Positive Technologies [Электроный ресурс]. 2021 – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020 (дата обращения: 12.02.2023).

7 Positive Technologies: число кибератак в 2021 году выросло на 6,5% // Positive Technologies [Электронный ресурс]. 2022 – URL: https://www.ptsecurity.com/ru-ru/about/news/chislo-kiberatak-v-2021-godu-vyroslo-na-6-5-procentov/ (дата обращения: 12.02.2023)

8 «Лаборатория Касперского»: количество киберинцидентов в российских компаниях увеличилось в 4 раза // Лаборатория Касперского [Электронный ресурс]. 2022 – URL: https://www.kaspersky.ru/about/press-releases/2022_laboratoriya-kasperskogo-kolichestvo-kiberincidentov-v-rossijskih-kompaniyah-uvelichilos-v-4-raza (дата обращения: 12.02.2023).

9 ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 г. № 17 // https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17. – 2013 г. – с изм. и допол. в ред. от Приказов ФСТЭК России от 15.02.2017 № 27, от 28.05.2019 № 106.

Технология оценки доверия к субъектам информационного обмена включает в себя комплексный анализ ряда процессов информационной безопасности. В рамках настоящего исследования разрабатывается алгоритм проведения оценки доверия к процессу аудита информационных систем, включая экспертный (экспертно-аналитический) и активный (инструментальный) аудит. Будут рассмотрены вопросы трактовки термина доверие применительно к процессу оценки доверия, описания процесса аудита, как объекта оценки доверия, формирования алгоритма оценки доверия к процессу аудита информационной безопасности, включая описание выходных данных процесса, логику анализа и обработки входных данных, описание выходных данных для принятия решении о возможности построения доверенного взаимодействия с контрагентами.

1. Вопросы оценки доверия

В настоящее время термин доверия не имеет единой трактовки, что является одной из первостепенных проблем исследования. В различных источниках (отечественное и зарубежное нормативно-правовое поле, отечественные и зарубежные научные публикации) можно найти трактовку доверия в качестве:

1) доверия к техническим или программным средствам:
   a. как процесс оценки соответствия средств защиты информации требованиям по безопасности, включающих требования к разработке и производству средства, к проведению испытаний средства, к поддержке безопасности средства[10,11];
   b. как доверие к устройствам IoT [6] или узлам сетей типа Bode Area Network [7];
2) доверия к субъекту информационных систем (пользователь, программа и т.д.) – архитектура нулевого доверия, смысл которой заключается в формировании правил идентификации и аутентификации пользователей на основе отсутствия неявного доверия к активам и учетным записям организации, основанного на их физическом или сетевом местоположении, а также на основе владельца активов[12] [8, 9, 10];
3) доверия к информации – алгоритмы оценки доверия к информации на основе происхождения информации и (или) источника информации [11, 12, 13].

В рамках настоящего исследования будем трактовать процесс оценки доверия как процесс оценки соответствия субъектов информационного обмена требованиям доверия, путем оценки процессов информационной безопасности, которые будут рассмотрены далее по тексту.

Цель оценки уровня доверия заключается в создании объективных доказательств, которые позволяют в произвольный момент времени убедиться в невозможности реализации неприемлемых рисков злоумышленником. Это также включает в себя риски, которые оператор или владелец информационной системы принял без учета информационного взаимодействия. Такая оценка помогает обеспечить безопасность информационных систем и минимизировать возможные угрозы.

Например, аттестат соответствия[13], как статическая мера контроля, свидетельствует о том, что система защиты информации правильно организована и соответствует всем необходимы требованиям по защите информации, но процесс аттестации проводится перед вводом системы защиты информации в эксплуатацию, и аттестат действует бессрочно. Исходя из этого аттестат не дает уверенности в том, система защиты информации правильно и исправно функционирует спустя некоторое время (например, через 3 месяца или через год). Для формирования уверенности контрагентов в том, что система защиты информации и процессы информационной безопасности правильно функционируют, можно использовать динамический метод контроля, который за короткий промежуток времени на основе объективных показателей даст заключение о состоянии информационной безопасности контрагента.

Общая оценка уровня доверия к субъекту информационного обмена состоит из оценки ряда внутренних процессов и процедур информационной безопасности субъекта информационного обмена:

1) системы управления рисками;
2) системы управления угрозами и уязвимостями;
3) процессов аудита;
4) системы управления информационной безопасностью;
5) процедур эксплуатации средств защиты информации;
6) процедур создания системы управления информационной безопасностью;
7) информационных технологий.

В данной работе объектом исследования является процесс аудита. Под процессом аудита будем понимать процесс получения свидетельств о состоянии информационной безопасности объекта аудита

10 Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76.

11 ГОСТ Р ИСО/МЭК 15408–3–2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

12 NIST SP 800–207 Zero Trust Architecture

13 ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 г. № 17 // https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17. - 2013 г. - с изм. и допол. в ред. от Приказов ФСТЭК России от 15.02.2017 № 27, от 28.05.2019 № 106.

и процесс оценки свидетельств с целью установления степени соответствия критериям аудита. В данное понятие включаются экспертный, нормативный аудит, а также технический аудит (оценка защищенности).

2. Оценка доверия к процессу аудита информационной безопасности

Анализ научных и нормативных источников по тематике аудита информационной безопасности показал, что обобщенно процесс аудита представляет собой ряд последовательных шагов[14,15] [14]:

1. Формирование команды аудита;
2. Предварительное обследование объекта аудита;
3. Формирование программы аудита, включающую определение методов аудита и критериев аудита;
4. Обследование объекта аудита и сбор свидетельств аудита;
5. Оценка свидетельств аудита полностью или выборочно на соответствие критериям аудита;
6. Формирование итогового заключения аудита с указанием замечаний.

Оценку уровня доверия к аудиту предлагается проводить в соответствии с линейной моделью оценки «критерий–метрика», которая основана на модели «фактор–критерий–метрика»[16] (рис. 1).

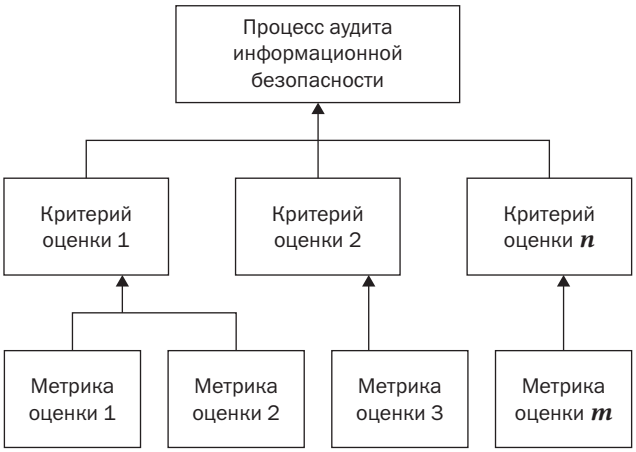

Рис. 1. Оценка процессов по модели «критерий-метрика»

Под объектом оценки будем понимать процесс аудита, под критериями – оцениваемые свойства процесса аудита, под метриками – конкретные свидетельства аудита, подлежащие оценке.

Оценка уровня доверия к процессу аудита информационной безопасности заключается в ряде последовательных шагов (рис. 2):

1) формирование и передача доказательств доверия – самостоятельный сбор доказательств доверия к процессу аудита информационной безопасности субъектом информационного обмена;
2) анализ доказательств доверия на предмет соответствия требованиям доверия – расчет значений метрик доверия на основе анализа доказательств доверия;
3) оценка свойств процесса аудита информационной безопасности – расчет значений критериев доверия на основе значений метрик доверия;
4) расчет значения уровня доверия к процессу аудита информационной безопасности субъекта информационного обмена на основе значений критериев доверия.

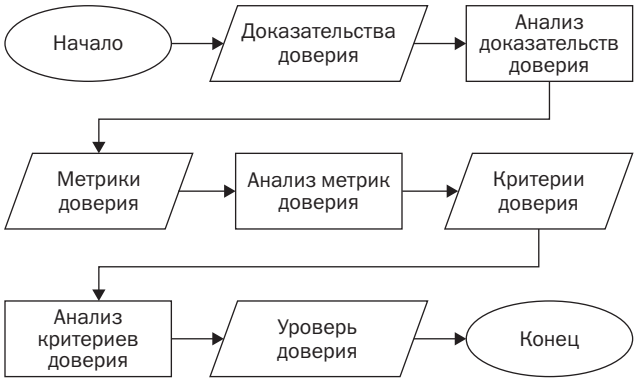

Рис. 2. Оценка доверия к процессу аудита

В данном случае доказательства доверия являются входными данными процесса оценки доверия к процессу аудита информационной безопасности, вычисление метрик, критериев доверия и уровня доверия являются логикой обработки доказательств доверия, уровень доверия – является выходным значением процесса оценки доверия к процессу аудита информационной безопасности. Более подробно доказательства доверия, критерии и метрики доверия рассмотрим далее.

Данный алгоритм проведения процесса оценки уровня доверия базируется на процессе проведения оценки соответствия по ряду ГОСТов.[17,18,19]

2.1. Доказательства доверия

При проведении оценки уровня доверия к аудиту субъекта информационного обмена необходимо осуществить сбор доказательств доверия (таблица 1).

14 ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»

15 ГОСТ Р ИСО 19011–2021. Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента качества. – М.: Стандартинформ, 2021. – 35 с

16 ГОСТ 28195–89 Оценка качества программных средств. Общие положения.

17 ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. Методика оценки соответствия».

18 ГОСТ Р ИСО/МЭК 27007–2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности».

19 ГОСТ Р ИСО 19011–2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента».

Таблица 1

Доказательства доверия

№ п/п	Наименование доказательства	Обозначение
1	Акт приема-передачи (на средства контроля защищенности)	P_1
2	Программа аудита	P_2
3	Заключение аудита	P_3
4	Приказ о формировании комиссии (отдела) внутреннего аудита	P_4
	Договор (соглашение) о проведении внешнего аудита	
5	План мероприятий по обеспечению безопасности информации	P_5
6	План мероприятий по актуализации состава информационной системы и (или) подсистемы безопасности	P_6
7	Наличие в плане мероприятий по обеспечению безопасности информации сведений о проведении аудита	P_7
8	Отчеты об устранении замечаний из заключений аудита	P_8
9	Сведения о составе информационной системы и подсистемы защиты информации	P_9
10	Сведения о делах Арбитражных судов в отношении поставщиков услуг аудита в связи с невыполнением или недобросовестным выполнением обязательств (при наличии поставщика услуг аудита)	P_{10}
11	Выписка из личных дел сотрудников, входящих в состав комиссии (отдела) аудита	P_{11}
12	Сертификаты о повышении квалификации сотрудников, входящих в состав комиссии (отдела) аудита	P_{12}
13	Лицензия ФСТЭК России на предоставление услуг по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации	P_{13}

Эти доказательства субъект информационного обмена собирает и передает самостоятельно. Набор доказательств сформирован на основе нормативного сопровождения процесса аудита информационной безопасности[20,21,22], а также на основе возможности подтверждения ряда фактов, свидетельствующих о качестве и добросовестности подхода к организации и проведению аудита информационной безопасности [15].

Каждое доказательство имеет свое уникальное обозначение для формирования формул расчета метрик доверия на основе анализа доказательств доверия. Данные вопросы будут рассмотрены далее.

Точные наименования документов могут отличаться от указанных в таблице 1 в соответствии с устоявшимися в субъектах информационного обмена наименованиями. Обозначения доказательств P_n введены для их упрощенного обозначения далее по тексту.

Оценка соответствия доказательств доверия требованиям доверия осуществляется в виде расчета метрик доверия. Числовое значение соответствия доказательства доверия требованиям доверия является метрикой доверия.

2.2. Расчет метрик доверия

Оценка доказательств доверия (расчет метрик доверия) необходима для получения численных показателей – метрик доверия. Анализ доказательств доверия заключается в выявлении ряда фактов [16, 17]:

1. Факт наличия доказательства доверия или факт наличия иных признаков доверия, содержащихся в доказательствах доверия;
2. Отношения количественных показателей какого-либо из свойств системы, полученных из доказательств доверия, к общему номинальному значению уникальному для каждого изучаемого объекта (например, отношение числа процессов или систем, попавших под аудит, к общему числу процессов или систем).

Метрики сгруппированы в 4 критерия доверия, каждый из которых является каким-либо свойством

20 ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»

21 ГОСТ Р ИСО 19011–2021. Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента качества. – М.: Стандартинформ, 2021. – 35 с

22 Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. — 2018. — № 1. — С. 1–29.

оцениваемого процесса информационной безопасности – процесса аудита информационной безопасности:

1) доверие к полноте аудита;
2) доверие к качеству аудита;
3) доверие к своевременности аудита;
4) доверие к поставщику услуг аудита.

Значения метрик лежат в промежутке [0, 1], где 0 – самая низкая оценка, а 1 – самая высокая. Более конкретные формулы приведены далее.

Для обозначения критериев и метрик примем обозначения M_n для критериев и M_{nm} для метрик. Соответственно критерий доверия к полноте аудита будет иметь обозначение M_1, а метрики данного критерия – M_{1m}. Критерий доверия к качеству аудита и его метрики будут иметь обозначения M_2 и M_{2m} соответственно, критерий доверия к своевременности и его метрики – M_3 и M_{3m}, критерий доверия к поставщику услуг и его критерии – M_4 и M_{4m}.

2.2.1. Оценка метрик доверия к полноте аудита

В качестве исходных данных для вычисления метрик для оценки доверия к полноте процесса аудита информационной безопасности предлагается использовать следующие доказательства доверия:

1) акт приема – передачи (на средства контроля защищенности);
2) программа аудита;
3) заключение аудита;
4) приказ о формировании комиссии (отдела) внутреннего аудита или договор (соглашение) о проведении внешнего аудита;
5) сведения о составе информационной системы и подсистемы защиты информации.

Состав метрик оценки доверия к полноте аудита (таблица 2) и формулы для их вычисления приведены ниже.

Таблица 2

Метрики оценки полноты аудита

Номер метрики	Наименование
M_{11}	Наличие программных средств контроля защищенности
M_{12}	Наличие программы аудита
M_{13}	Наличие заключения аудита
M_{14}	Наличие временной или постоянной группы аудита
M_{15}	Отношение процессов/систем, попадающих под аудит к общему числу процессов/систем
M_{16}	Наличие замечаний в заключении аудита

Метрики вычисляются по следующим формулам:

$$M_{11} = \begin{cases} 0, \nexists P_1 \\ 1, \exists P_1 \end{cases} \quad (1)$$

$$M_{12} = \begin{cases} 0, \nexists P_2 \\ 1, \exists P_2 \end{cases} \quad (2)$$

$$M_{13} = \begin{cases} 0, \nexists P_3 \\ 1, \exists P_3 \end{cases} \quad (3)$$

$$M_{14} = \begin{cases} 0, \nexists P_4 \\ 1, \exists P_4 \end{cases} \quad (4)$$

$$M_{15} = \begin{cases} 0, \nexists P_2 \vee \nexists P_9 \\ \dfrac{N_{ауд}}{N_{общ}}, \exists P_4 \wedge \exists P_9 \end{cases} \quad (5)$$

где $N_{ауд}$ – количество процессов/систем, в отношении которых проводится аудит, $N_{общ}$ – общее количество процессов/систем.

$$M_{15} = \begin{cases} 0, \nexists Z_{крит} \wedge \nexists Z_{нс} \\ 0.5, \nexists Z_{крит} \wedge \exists Z_{нс} \\ 1, \exists Z_{крит} \end{cases} \quad (6)$$

где $Z_{крит}$ – критические замечания, выявленные при аудите и требующие устранения, $Z_{нс}$ – несущественные замечания, выявленные при аудите и требующие устранения, при этом $(Z_{крит} \cap Z_{нс}) \subseteq P_3$ [15].

По результатам оценки метрик полноты аудита информационной безопасности можно, во-первых, выявить недостатки процесса аудита информационной безопасности, а во-вторых, рассчитать числовое значение доверия к полноте аудита. Данные расчеты приведены далее в пп. 2.3.

Далее рассмотрим вопросы расчета метрик доверия к качеству процесса аудита информационной безопасности.

2.2.2. Оценка метрик доверия к качеству аудита

В качестве исходных данных для вычисления метрик оценки доверия к качеству процесса аудита информационной безопасности предлагается использовать следующие доказательства доверия:

1) акт приема-передачи (на средства контроля защищенности);
2) программа аудита;
3) заключение аудита;
4) план мероприятий по обеспечению безопасности информации;
5) отчеты об устранении замечаний из заключений аудита.

Состав метрик оценки доверия к качеству аудита (таблица 3) и формулы их вычисления приведены ниже.

Таблица 3

Метрики оценки качества аудита

Номер метрики	Наименование
M_{21}	Наличие программных средств контроля защищенности
M_{22}	Соответствие аудита одной из методологий проведения аудита или оценки защищенности
M_{23}	Наличие замечаний в заключении аудита
M_{24}	Наличие отчета о проведении мероприятий по устранению замечаний в заключении аудита
M_{25}	Отношение времени, затраченного на устранение замечаний, к допустимому времени устранения замечаний

Аналогично метрикам оценки доверия к полноте процесса аудита информационной безопасности проводится расчет метрик доверия к качеству аудита: метрика M_{21} рассчитывается по формуле (1), метрика M_{22} – по формуле (2), метрика M_{23} – по формуле (6). Расчет остальных метрик приведен ниже.

$$M_{24} = \begin{cases} 0, \nexists P_5 \\ 1, \exists P_5 \end{cases} \quad (7)$$

$$M_{25} = \begin{cases} 0, \nexists P_8 \vee t_y > 1.5 t_д \\ 0.5, t_y \le 1.5 t_д \\ 1, t_y \le t_д \end{cases} \quad (8)$$

где t_y – время, затраченное на исправление замечаний, выявленных при аудите, $t_д$ – допустимое время устранения замечаний, устанавливаемое регулятором, командой проведения аудита или планом по устранению замечаний.

Расчет числового значения доверия к качеству процесса аудита информационной безопасности приведен далее в пп. 2.3.

Далее рассмотрим вопросы расчета метрик доверия к своевременности процесса аудита информационной безопасности.

2.2.3. Оценка метрик доверия к своевременности аудита

В качестве исходных данных для вычисления метрик оценки доверия к своевременности процесса аудита информационной безопасности предлагается использовать следующие доказательства доверия:

1) план мероприятий по актуализации состава информационной системы и (или) подсистемы безопасности;
2) наличие сведений о проведении аудита в плане мероприятий по обеспечению безопасности информации;
3) сведения о составе информационной системы и подсистемы защиты информации.

Состав метрик оценки доверия к своевременности аудита (таблица 4) и формулы их вычисления приведены ниже.

Таблица 4

Метрики оценки своевременности аудита

Номер метрики	Наименование
M_{31}	Наличие фактов проведения инвентаризации компонентов ИС и периодичность проведения инвентаризации
M_{32}	Наличие фактов проведения аудита информационной безопасности и периодичность проведения аудита
M_{33}	Наличие факта обновления сведений об инвентаризации при изменениях в ИС

Приведенные метрики вычисляются по следующим формулам:

$$M_{31} = \begin{cases} 0, \nexists P_6 \vee t_u > 5 \\ \dfrac{0.5}{T_u}, 0 < T_u \le 5 \end{cases} \quad (9)$$

где T_u – периодичность проведение инвентаризации в годах (0,5–5)

$$M_{32} = \begin{cases} 0, \nexists P_7 \vee t_A > 5 \\ \dfrac{0.5}{T_A}, 0 < T_A \le 5 \end{cases} \quad (10)$$

где ТА – периодичность проведение аудита в годах (0,5; 5)

$$M_{24} = \begin{cases} 0, \nexists P_9 \\ 1, \exists P_9 \end{cases} \quad (11)$$

Расчет числового значения доверия к своевременности процесса аудита информационной безопасности приведен далее в пп. 2.3.

Далее рассмотрим расчет метрик доверия к поставщику услуг процесса аудита информационной безопасности.

2.2.4. Оценка доверия к поставщику услуг аудита

В качестве исходных данных для вычисления метрик оценки доверия к поставщику услуг процесса аудита информационной безопасности предлагается использовать следующие доказательства доверия:

1) сведения о делах арбитражных судов в отношении поставщиков услуг аудита в связи с невыполнением или недобросовестным выполнением обязательств (при наличии внешнего поставщика услуг аудита);
2) выписка из личных дел сотрудников, входящих в состав комиссии (отдела) аудита;
3) сертификаты о повышении квалификации сотрудников, входящих в состав комиссии (отдела) аудита;

4) лицензия ФСТЭК России на предоставление услуг по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
5) акт приема – передачи (на средства контроля защищенности);
6) приказ о формировании комиссии (отдела) внутреннего аудита или договор (соглашение) о проведении внешнего аудита.

Состав метрик оценки доверия к поставщику услуг аудита (таблица 5) и формулы их вычисления приведены ниже.

Таблица 5

Метрики оценки поставщика услуг аудита

Номер метрики	Наименование
M_{41}	Наличие фактов недобросовестности поставщика услуг аудита (только при привлечении внешнего поставщика услуг)
M_{42}	Подтверждение опыта работы специалистов команды аудита в области аудита информационной безопасности
M_{43}	Наличие фактов повышения квалификации специалистов команды аудита в области аудита информационной безопасности и периодичности прохождения курсов повышения квалификации
M_{44}	Наличие программных средств контроля защищенности
M_{45}	Соответствие процедур аудита и оценки защищенности одной из методологий проведения аудита/оценки защищенности
M_{46}	Наличие лицензий на выполнение работ по аудиту/оценке защищенности (пп. б п. 4 ПП РФ 79) (только при привлечении внешнего поставщика услуг)

Аналогично метрикам оценки доверия к полноте процесса аудита информационной безопасности проводится расчет метрик доверия к качеству аудита: метрика M_{44} рассчитывается по формуле (1), метрика M_{45} – по формуле (4). Расчет остальных метрик приведен ниже.

$$M_{41} = \begin{cases} \frac{1}{N_c}, N_c \geq 1 \\ 1, \nexists P_{10} \vee N_c = 0 \end{cases} \quad (12)$$

где N_c – количество удовлетворительных исков о неисполнении или ненадлежащем исполнении обязательств в Арбитражном суде за последние 3 года, в которых поставщик услуг ответчик.

$$M_{42} = \begin{cases} 0, \nexists P_{11} \vee O < 3 \\ 1, O \geq 3 \end{cases} \quad (13)$$

где O – стаж работы в годах специалистов, входящих в команду аудита, в области аудита или оценки защищенности.

$$M_{43} = \begin{cases} 0, \nexists P_{12} \vee T\kappa < 3 \\ 1, T\kappa \geq 3 \end{cases} \quad (14)$$

где $T\kappa$ – периодичность проведения повышения квалификации в годах.

$$M_{46} = \begin{cases} 0, \nexists P_{13} \\ 1, \exists P_{13} \end{cases} \quad (15)$$

По результатам оценки метрик доверия к поставщику услуг аудита информационной безопасности можно, во-первых, выявить недостатки в команде аудита информационной безопасности, а во-вторых, рассчитать числовое значение доверия к поставщику услуг аудита.

Далее перейдем к расчету критериев доверия к качеству процесса аудита информационной безопасности, а именно к расчету доверия к полноте, качеству, своевременности аудита и доверия к поставщику услуг, на основе значений метрик доверия, описанных ранее в пп. 2.2.1–2.2.4.

2.3. Расчет критериев доверия и уровня доверия к процессу аудита информационной безопасности

Для проведения оценки доверия предлагается использование функции желательности Харрингтона, которая позволяет проводить однозначное соответствие количественных и качественных показателей произвольного процесса. Функция желательности (с односторонним ограничением задаётся уравнением,[23,24] [20]:

$$d = e^{-e^{-y'}} \quad (16)$$

где d – значение желательности в промежутке (0, 1), y' – значение частного признака, приведенное к промежутку [0, 7].

Ось координат Y называется шкалой частных показателей. Ось d – шкалой желательности. Промежуток эффективных значений на шкале частных показателей – [2, +5]. Для сдвига промежутка частных показателей в значения [0, 7] предлагается воспользоваться формулой:

$$d = e^{-e^{-(y'-2)}} \quad (17)$$

Шкала желательности содержит в себе ряд числовых промежутков, которым соответствует какой-либо лингвистический показатель желательности, который

23 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.
24 Пичкалев А. В. Обобщенная функция желательности Харрингтона для сравнительного анализа технических средств // Космические аппараты и технологии. – 2012. – №1 (1). – С. 25–28.

является качественной оценкой количественных значений желательности и несет в себе смысловую нагрузку, касающуюся значения желательности. В нашем случае лингвистические значения желательности будут обозначать степень зрелости процесса аудита информационной безопасности в качественной величине, а числовые значения желательности – степень зрелости процесса аудита в количественной величине.

Также функцию Харрингтона можно использовать при вычислениях значений желательности в несколько этапов. В таком случае финальное значение желательности называется обобщенной функцией желательности D, а промежуточные – частными функциями желательности d_i. Обобщенная функция желательности определяется как среднее арифметическое частных функций желательности:

$$D = \sqrt[n]{(d_1 * d_2 * ... * d_n)} \quad (18)$$

где n – число используемых показателей параметров сравнения для данной системы, причем число этих показателей может быть разным для разных систем.

За основу лингвистических показателей и промежутков показателей желательности (таблица 6) была взята процедура оценки соответствия по ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. Методика оценки соответствия», как самая проработанная процедура оценки соответствия, содержащая методику оценки и расчета степени соответствия мер защиты информации требования по защите информации.

Далее перейдем к расчету критериев доверия. Расчет критериев доверия основан на расчете частной функции желательности по формуле (17), где в качестве частных признаков желательности выступают соответствующие критерию метрики доверия M_{nm}.

2.3.1. Критерии доверия как частные функции желательности

Описанные в пп. 2.2.1–2.2.4 метрики доверия сгруппированы по 4 критериям доверия для многоступенчатой оценки процесса аудита информационной безопасности (рисунок 1). В данном пункте рассмотрим расчет числовых значений критериев доверия.

Исходя из формулы (16) для расчета значения каждого критерия необходимо определить вычисление приведенного значения y':

$$y_i' = k_i * \sum_{j=1}^{m} M_{ij}, \quad (19)$$

где m – количество измеряемых величин (метрики), j – порядковый номер величины, M_{ij} – j-ая измеряемая величина (метрика) i-ого критерия, k_i – корректирующий коэффициент, для приведенного значения в промежуток [0, 7].

$$k_i = \frac{y'_{max}}{y_{i\,max}}, \quad (20)$$

где y'_{max} – максимальное значение эффективного промежутка значений частного признака, $y_{i\,max}$ – максимальное значение суммы метрик i-ого критерия.

Получив из 20 значений метрик доверия 4 значения критерия доверия, можно перейти к финальному этапу расчета доверия к процессу аудита информационной безопасности. Уровень доверия к процессу аудита информационной безопасности основан на расчете обобщенной функции желательности по формуле (23).

2.3.2. Уровень доверия как обобщенная функция желательности

Общий уровень доверия к процессу аудита информационной безопасности рассчитывается из значений критериев доверия, рассчитываемых по пп. 2.3.1.

Исходя из формулы (18) приведения частных функций желательности к обобщенной сформирована

Таблица 6

Лингвистические значения оценки доверия

Обобщенный уровень доверия к аудиту, D	Уровень соответствия	Интерпретация
$D = 0$	Нулевой	Процедура аудита не выполняется
$0 < D \le 0{,}5$	Базовый	Процедура аудита выполняется на нерегулярной основе
$0{,}5 < D \le 0{,}7$	Базовый повышенный	Процедура аудита выполняется на регулярной основе и результат выполнения процесса задокументирован
$0{,}7 < D \le 0{,}85$	Средний	Процедура аудита выполняется, планируется, управляется и контролируется
$0{,}85 < D \le 1$	Высокий	Процедура аудита выполняется, планируется, управляется, измеряется при помощи количественных показателей (метрик) и постоянно совершенствуется

формула (21) для расчета уровня доверия к процессу аудита информационной безопасности исходя из значений критериев доверия:

$$D = \sqrt[4]{(d_1 * d_2 * d_3 * d_4)}, \quad (21)$$

где D – обобщенная функция желательности (уровень доверия к процессу аудита информационной безопасности), d_1 – частная функция желательности оценки доверия к полноте аудита, d_2 – частная функция желательности оценки доверия к качеству аудита, d_3 – частная функция желательности оценки доверия к своевременности аудита, d_4 – частная функция желательности оценки доверия к поставщику услуг аудита.

Итого, общий алгоритм оценки доверия к процессу аудита информационной безопасности выглядит следующим образом (рис. 3).

Смысл числового значения D базируется на таблице 6 – уровень контроля за состоянием системы защиты информации, означающий степень зрелости процессов аудита информационной безопасности. Уровень доверия к процессу аудита информационного обмена является одним из факторов доверия[25] к субъекту информационного обмена. Смысл показателя доверия к субъекту информационного обмена также базируется на таблице 6 – уровень злоумышленника, которому субъект информационного обмена способен противостоять в процессе информационного обмена с контрагентами.

25 ГОСТ 28195–89 Оценка качества программных средств. Общие положения.

Заключение

В ходе исследования был сформирован алгоритм проведения оценки доверия к процессу аудита информационной безопасности. Определены входные данные для процесса оценки доверия к процессу аудита информационной безопасности – 13 доказательств доверия из нормативно-правового обеспечения субъекта информационного обмена. Для расчета уровня доверия к процессу аудита информационной безопасности была использована функция желательности Харрингтона, а лингвистические показатели желательности сформированы на основе ГОСТ Р 57580.2–2018. ГОСТ Р 57580.2–201 взят за основу как самая проработанная методика проведения процедуры оценки соответствия. Определены 20 метрик и 4 критерия для оценки доверия как результаты оценки доказательств доверия. Описан метод расчета доверия к процессу аудита информационной

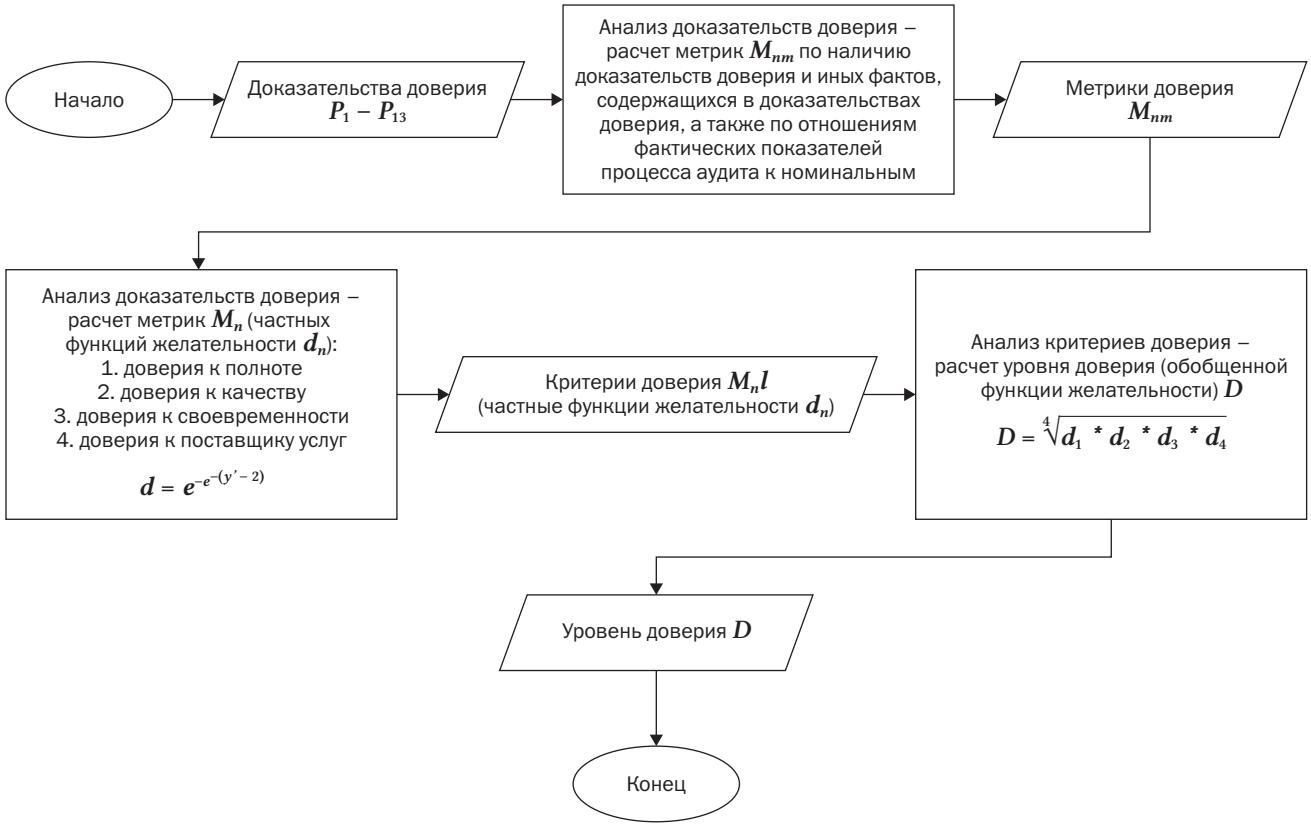

Рис. 3. Алгоритм оценки доверия к процессу аудита

безопасности на основе значений метрик и критериев доверия.

Сформированный алгоритм проведения оценки доверия к процессу аудита информационной безопасности является одной из составляющих процесса оценки доверия к субъектам информационного обмена и содержит объективные доказательства оценки уровня контроля за системой защиты информации информационных систем. Добросовестный подход к реализации процессов системы защиты информации и процессов информационной безопасности является одним из залогов способности субъекта информационного обмена противостоять злоумышленникам.

Алгоритм оценки доверия к процессу аудита информационной безопасности является одним из составляющих процесса оценки доверия к субъекту информационного обмена, охватывающего основные процессы информационной безопасности, включая процессы управления рисками, угрозами, уязвимостями, процессы аудита и менеджмента информационной безопасности. Далее в исследованиях планируется формирование имитационных моделей изучаемых процессов для оценки эффективности этих процессов, разработка методик оценки уровня доверия в различных условиях, разработка платформы доверенного взаимодействия, включающую модули оценки доверия.

Данная работа выполнена при финансовой поддержке Фонда поддержки проектов Национальной технологической инициативы (НТИ) в рамках реализации Программы Центра компетенций НТИ «Технологии доверенного взаимодействия» (договор от «14» декабря 2021 г. № 70-2021-00246).

Литература

1. *Кузнецова Н. М. Решение задачи автоматизации процессов защиты стратегически важных ресурсов предприятия от комплексных кибератак на основе анализа тактик злоумышленников / Н. М. Кузнецова, Т. В. Карлова, А. В. Бекмешов // Вестник Брянского государственного технического университета. 2020. №7 (92). URL: https://cyberleninka.ru/article/n/reshenie-zadachi-avtomatizatsii-protsessov-zaschity-strategicheski-vazhnyh-resursov-predpriyatiya-ot-kompleksnyh-kiber-atak-na-osnove (дата обращения: 12.02.2023).*
2. *Макаренко С. И. Тестирование на проникновение на основе стандарта NIST SP 800–115 // Вопросы кибербезопасности. – 2022. – №3 (49). – С. 44–57. DOI:10.21681/2311-3456-2022-3-44-49*
3. *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.*
4. *Селифанов В. В. Вопросы оценки доверия к системе управления рисками / В. В. Селифанов, В. В. Аникеева, И. А. Огнев // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 69–82. – DOI: 10.17212/2782–2230–2023–1–69–82.*
5. *Построение адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры / А. С. Голдобина, Ю. А. Исаева, В. В. Селифанов, А. М. Климова, П. С. Зенкин // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2018. – №21. – С. 51–58.*
6. *Roy S. S. Enhanced trust management for building trustworthy social internet of things network / S.S. Roy, B.J.R. Sahu, S. Dash // IET Networks. – 2024. – № . – С. 1–11.*
7. *Access Control, Key Management, and Trust for Emerging Wireless Body Area Networks / A. S. Shahraki, H. Lauer, M. Grobler, A. Sakzad, C. Rudolph // Sensors. – 2023. – № 23 (24). – С. 1–32.*
8. *Брызгалов А. А. Применение концепции «нулевого доверия» для защиты коммерческой тайны на предприятии в условиях цифровизации / А. А. Брызгалов, П. А. Козырев, В. В. Ульянов // Вызовы цифровой экономики: технологический суверенитет и экономическая безопасность. – Брянск: ФГБОУ ВО «Брянский государственный инженерно-технологический университет» Инженерно–экономический институт, 2023. – С. 70–77.*
9. *Букирева Ю. М. Стратегия доступа к корпоративным сетям с применением модели нулевого доверия // Инновационные технологии: теория, инструменты, практика. – 2021. – №1. – С. 136–141.*
10. *Security of Zero Trust Networks in Cloud Computing: A Comparative Review / S. Sarkar, G. Choudhary, Sh. K. Shandilya, A. Hussain, H. Kim // Sustainability. – 2022. – №14. – С. 1–22.*
11. *Atencia M. Trust in networks of ontologies and alignments / M. Atencia, M. Al-Bakri, M.-C. Rousset // Knowledge and Information Systems. — 2013. — № 2 (42). — С. 1–27.*
12. *W. Al-shadood Enhancement the Security by Creating Ontology-Based Trust Management Using Semantic Web Tools // AlKadhum Journal of Science. — 2023. — № 2 (1). — С. 11–16.*
13. *Implementation of a Multi-Approach Fake News Detector and of a Trust Management Model for News Sources / C. Marche, I. Cabiddu, C. G. Castangia, L. Serreli // IEEE Transactions on Services Computing. – 2023. – № 6 (16). – С. 1–14.*
14. *Ан В. Р. Разработка алгоритма проведения аудита кибербезопасности / В. Р. Ан, В. А. Табакаева // МНСК-2021. Информационные технологии: материалы 59-й Международной научной студенческой конференции, Новосибирск, 12–23 апреля 2021 г. – Новосибирск, 2021. – С. 5. – EDN CAYHXE.*
15. *Макаренко С. И. Критерии и показатели оценки качества тестирования на проникновение // Вопросы кибербезопасности. – 2021. – №3 (43). – С. 43–57. DOI:10.681/2311-3456-2021-3-43-57*
16. *Ситская А. В. Вопросы аудита информационной безопасности / А. В. Ситская, В. В. Селифанов, П. А. Звягинцева // Безопасность цифровых технологий. – 2023. – № 3 (110). – С. 67–82.*
17. *Захахатнов В. Г. Функция желательности Харрингтона как критерий оптимального выбора зерносушилки / В. Г. Захахатнов, В. М. Попов, В. А. Афонькина // Известия Оренбургского государственного аграрного университета. – 2022. №2 (94). С. 110–114.*