УДК 004.056 Вестник УрФО № 4(54) / 2024, с. 37–48

Иванов А. В., Огнев И. А., Селифанов В. В. DOI: 10.14529/secur240405

ВОПРОСЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Актуальность исследования: в настоящее время вопросы оценки доверия к субъектам информационного обмена повышают свою актуальность. Такая оценка основывается на оценке доверия к процессам информационной безопасности, принадлежащим субъекту информационного обмена. Среди процессов информационной безопасности, подвергающихся оценке доверия, присутствует процесс аудита информационной безопасности. Оценка доверия к процессу аудита информационной безопасности заключается в вычислении трех показателей – показателя структурной целостности, показателя эффективности и показателя зрелости. Целью работы является разработка методики оценки эффективности процесса аудита информационной безопасности на основе анализа функционирования процесса аудита. Используемые методы и технологии: в работе использованы методы математической статистики, имитационного моделирования. Результат: в результате исследования была сформирована методика оценка эффективности процесса аудита информационной безопасности на базе следующих показателей: коэффициента выявления свидетельств аудита, коэффициента соответствия запланированных ресурсов аудита в программе аудита фактически использованным, коэффициента достаточности времени для проведения аудита. Данные показатели были выбраны в силу того, что из всех возможных составляющих процесса аудита только они зависимы от самого процесса аудита, в то время как часть аспектов регулируется за рамками аудита. Практическая значимость: такой подход позволяет провести оценку эффективности процесса аудита информационной безопасности, основываясь на эффективности использования выделенных временных и человеческих ресурсов для достижения целей аудита с наибольшей вероятностью. Полученный результат является частью методики оценки доверия к процессам аудита информационной безопасности и служит в данной методике характеристикой работы процесса аудита во времени.

Ключевые слова: *эффективность, эффективность процесса, эффективность аудита, аудит, доверие, оценка доверия, доверенное взаимодействие, информационная безопасность*

ISSUES OF ASSESSING THE EFFECTIVENESS OF INFORMATION SECURITY AUDIT

Relevance of the study: currently, the issues of assessing trust in the subjects of information exchange are increasing their relevance. Such an assessment is based on the assessment of trust in the information security processes belonging to the subject of information exchange. Among the information security processes subject to trust assessment, there is the information security audit process. Assessing trust in the information security audit process consists in calculating three indicators - the structural integrity indicator, the efficiency indicator and the maturity indicator. The purpose of the work is to develop a methodology for assessing the effectiveness of the information security audit process based on the analysis of the audit process. Methods and technologies used: the work uses the methods of mathematical statistics, simulation modeling. Result: as a result of the study, a methodology for assessing the effectiveness of the information security audit process was formed based on the following indicators: the coefficient of detection of audit evidence, the coefficient of compliance of the planned audit resources in the audit program with those actually used, the coefficient of sufficiency of time for the audit. These indicators were chosen due to the fact that of all the possible components of the audit process, only they depend on the audit process itself, while some aspects are regulated outside the audit. Practical significance: this approach allows for an assessment of the effectiveness of the information security audit process based on the effectiveness of the use of allocated time and human resources to achieve the audit objectives with the greatest probability. The result obtained is part of the methodology for assessing trust in information security audit processes and serves in this methodology as a characteristic of the audit process over time.

Keywords: *efficiency, process efficiency, audit efficiency, audit, trust, trust assessment, trusted interaction, information security*

Введение

Аудит информационной безопасности представляет собой процесс сбора свидетельств деятельности определенного процесса или группы процессов и проверку этих свидетельств на соответствие требованиям, выдвигаемых к исследуемым процессам или группам процессов [1]. В рамках области информационной безопасности объектом процесса аудита зачастую являются системы защиты информации, процессы управления информационной безопасностью, а также иные процессы или их части, связанные с деятельностью по защите информации [2; 3]. То есть процесс аудита информационной безопасности является методом контроля других процессов информационной безопасности [4].

Построение эффективного процесса аудита информационной безопасности напрямую влияет на общий уровень безопасности информации в силу того, что своевременное и качественное выявление отклонений в системах защиты информации и соответствующих процессов от эталонных показателей закладывает начало своевременному устранению таких отклонений, что снижает вероятность реализации угроз безопасности информации из-за различного рода ошибок [5; 6]. Помимо прочего эффективность процесса аудита влияет на использование и планирование использования сил и времени для снижения количества издержек при выполнении аудита и повышения эффективности процесса как такового.

Целью данного исследования является формирование методики оценки эффективности процесса аудита информационной безопасности. В рамках текущей работы были рассмотрены следующие вопросы: формирование объекта и предмета исследования, формальная постановка задачи исследования, формирование показателей эффективности процесса аудита, формирование функции оценки эффективности процесса аудита, демонстрация работы функции оценки эффективности процесса аудита с использованием средств имитационного моделирования.

Описание процесса аудита информационной безопасности

Цель процесса аудита информационной безопасности – выявление несоответствий (нарушений) реализованных мер по защите информации требованиям регуляторов в области информационной безопасности или стандартов [7–10]. В ходе процесса аудита проводится поиск свидетельств аудита, которые касаются реализации или отсутствия реализации мер по защите информации. Затем осуществляется оценка этих свидетельств, направленная на проверку их соответствия установленным требованиям и стандартам относительно каждой отдельной меры, по итогу чего выявляются отклонения от требований или стандартов [11; 12]. Формальное описание процесса аудита информационной безопасности сводится к формированию определенных наборов входных и выходных данных в соответствии с определенными правилами.

В качестве выходных данных процесса аудита информационной безопасности должен появиться набор замечаний Z (обнаружений аудита):

$$Z = \{z_1..z_j\} \quad (1)$$

где j – количество замечаний аудита.

В процессе проведения аудита информационной безопасности экспертная комиссия анализирует ряд свидетельств аудита C, связанных с каждой мерой защиты информации:

$$C = \{c_1..c_M\} \quad (2)$$

где M – количество свидетельств аудита.

Замечания по аудиту (обнаружения аудита) выявляются на основе анализа свидетельств аудита путем выявления нарушений в реализации мер по защите информации $z(c_i)$:

$$z(c_i) = \begin{cases} 0, \exists c_i \wedge c_i \in Y^{mp} \\ 1 \end{cases} \quad (3)$$

где i – порядковый номер требования ЗИ,

c_i – свидетельство аудита, относящееся к i-му требованию ЗИ, $c_i \in C$,

$Y^{тр}$ – набор требований ЗИ:

$$Y^{mp} = \{Y_1^{mp}..Y_i^{mp}\} \quad (4)$$

То есть в случае, если существуют свидетельство аудита, подтверждающее реализацию i-й меры ЗИ и соответствующие требованию ЗИ $Y^{тр}$, то нарушения в реализации меры ЗИ не обнаружено. В иных случаях, если свидетельств аудита не существует или обнаруженные свидетельства аудита не соответствуют эталонным, то считаем, что нарушение в реализации меры ЗИ обнаружено, соответственно появляется замечание, касающееся i-й меры ЗИ, которое должно быть включено в заключение аудита.

Формально создание и наполнение аудиторского заключения (отчета по аудиту) W можно выразить как составной оператор [13]:

$$\psi = U^c \times C \times \Pi \times R \times Y^{mp} \rightarrow W \quad (5)$$

где U^c – множество актуальных (существенных) угроз безопасности информации,

C – множество свидетельств аудита,

Π – множество программ аудита, применимых для текущего объекта аудита,

R – ресурс, выделенный для проведения аудита,

Y^{mp} – проверяемые требования по ЗИ,

При этом аудиторское заключение содержит ряд обнаружений аудита, основанных на выявленных нарушениях в реализации мер ЗИ:

$$W = Z(C) \quad (6)$$

Зависимость выявления замечаний по аудиту от нарушений в реализации мер ЗИ приведено в формуле (3).

Задача исследования

На сегодняшний день не определен единый формат оценки эффективности процесса аудита информационной безопасности [14], а существующие методы оценки эффективно-

сти процесса аудита информационной безопасности представлены следующими группами методов [15]:

- методы, направленные на оценку достаточности обеспечения аудита ресурсами [16–18];
- методы, направленные на оценку зрелости аудита [6; 19; 20];
- методы, направленные на удовлетворенности результатами аудита [16; 21].

Методы первого типа (оценка достаточности обеспечения аудита ресурсами) направлены на оценку достаточности времени, финансов, людей, выделяемых для реализации процессов аудита. В таком виде оценка носит ограниченный характер из-за того, что объект оценки – ресурсы. Как следствие такие методы оценки могут опосредовано свидетельствовать об эффективности непосредственно процесса аудита информационной безопасности.

Методы основанные на оценке зрелости в первую очередь за объект оценки принимают уровень развития процесса аудита и его составляющих: подпроцесса планирования, подпроцесса исполнения, подпроцесса отчетности и ликвидации нарушений. Здесь зачастую идет экспертная оценка с усреднением результатом, что является основным недостатком таких методов. Такая оценка не позволяет сократить время оценки процесса аудита и подвержена влиянию человеческого фактора.

Последний тип методов, направленный на оценку удовлетворенности результатами аудита за основу оценки берет отзывы различных групп людей различных подразделений различного уровня с их мнением по поводу проведенного аудита. Такая оценка является также опосредованной в отношении эффективности аудита и при этом также являются сугубо субъективной оценкой порой без определенных критериев оценки.

Итого существующие методы оценки эффективности процесса аудита, в том числе процесса аудита информационной безопасности за объект оценки принимают узкий набор аспектов аудита, основаны на экспертной оценке с уравновешиваем результатов и не пригодны для автоматизации в целях сильного снижения времени оценки процесса аудита. В данной работе предлагается способ оценки эффективности процесса аудита информационной безопасности на основе оценки критериев, непосредственно зависимых от самого процесса. При этом предлагается аппарат оценки с четко определенными показателями, влияющими на эффективность процесса аудита, с возможностью автоматизации и проведении оценки в срок менее 24 часов.

В рамках настоящего исследования предлагается решение вопроса формирования показателей эффективности процесса аудита, то есть нахождение такого $f(x)$, которое будет демонстрировать эффективность процесса аудита информационной безопасности A:

$$A = f\left(x\right) \tag{7}$$

где $f(x)$ – функция оценки эффективности процесса аудита информационной безопасности.

Количество свидетельств аудита и длительность их оценки напрямую влияют на вероятность достижения цели аудита – выявления всех нарушений требований или стандартов. Недостаточное количество свидетельств аудита, как и малое время их оценки могут являться причинами неполного выявления нарушений требований или стандартов, или же будет достигнута недостаточная достоверность результатов аудита [22; 23].

Итого для достижения цели аудита – формирование заключения по аудиту, содержащего замечания по реализации мер по ЗИ. Формируется данная цель, исходя из ряда параметров:

1. Множества актуальных угроз безопасности информации (УБИ);
2. Множества выявленных свидетельств аудита;
3. Программы аудита;
4. Множества ресурсов, выделенных для аудита;
5. Количества мер по защите информации (ЗИ), подлежащих оценке.

Результаты исследований

Множества, связанные с актуальными угрозами безопасности информации, содержанием программы аудита, количеством проверяемых мер по защиты информации считаются независимыми от непосредственно процесса аудита и членов команды аудита, в силу того, что программа формируется исходя из целей и задач аудита, формируемых совместно с заказчиком или руководством организации, множество актуальных УБИ и мер ЗИ, формируется на этапе создания системы

ЗИ и в процессе аудита происходит лишь верификация УБИ и мер ЗИ, а иногда верификация вообще отсутствует в зависимости от типа и целей аудита.

Далее отдельно остановимся на оставшихся пунктах, которые напрямую зависят от действий, производимых непосредственно на этапе сбора и анализа информации в процессе аудита [15].

Коэффициент нахождения всех свидетельств аудита

Множество выявленных свидетельств аудита является в свою очередь тем самым, что появляется и анализируется в процессе аудита ИБ. От полноты нахождения элементов множества зависит достижение цели аудита. Соответственно коэффициент нахождения элементов в множестве является одним из основных показателей эффективности аудита.

Коэффициенты заполнения вышеуказанных множеств рассчитываются как отношение фактически найденных элементов к максимально возможному количеству:

$$C = \frac{C_m}{M} \tag{8}$$

где C – коэффициент нахождения всех свидетельств аудита,

C_m – количество обнаруженных свидетельств аудита, $c_m \in C,\ m < M$.

Коэффициент соответствия ресурсов запланированным показателям

Программа аудита в составе своем содержит ряд параметров аудита, необходимых для проведения последнего [24]:

- цель аудита;
- границы аудита;
- критерии аудита;
- дорожная карта аудита;
- команда аудита.

В нашем случае интерес представляют последний и предпоследний пункты. Достаточность и избыточность данных параметров на аудит разобрано далее по тексту, здесь остановимся на ином показателе – коэффициент отклонения от программы аудита [25]:

$$O_L = \frac{\left|L_ф - L_n\right|}{L_n} \tag{9}$$

где O_L – коэффициент отклонения по показателю человеческих ресурсов,

$L_ф$ – фактическое количество аудиторов, $0<L_ф \le 2L_п$,

$L_п$ – запланированное количество аудиторов.

$$O_T = \frac{\left|T_ф - T_n\right|}{T_n} \tag{10}$$

где $P(O_T)$ – коэффициент отклонения по показателю временных ресурсов,

$T_ф$ – фактическое количество времени, затраченного на аудит, $0<T_ф \le 2T_п$,

$T_п$ – запланированное количество времени на аудит.

Далее можно определить общую величину коэффициент отклонений от программы аудита:

$$O = O_L * O_T \tag{11}$$

Соответственно показатель отклонения процесса аудита от запланированных объемов сил и времени фиксирует процент отклонений в каждом процессе непосредственно. Применение данного показателя на статистических данных позволит по смыслу перейти на частоту и размер отклонений от программы аудита и коэффициент придерживания запланированным объемам сил и времени в рамках проведения аудита информационной безопасности.

Показатель коэффициент соответствия ресурсов запланированным показателям обеспечения аудита S будет рассчитываться следующим образом:

$$S = 1 - O \tag{12}$$

Коэффициент достаточности временных ресурсов на аудит

Множество ресурсов, выделенных для аудита, можно интерпретировать по-разному, например, как совокупность ресурсов для сбора свидетельств аудита и для реализации анализа свидетельств аудита [13], как совокупность временных ресурсов [23; 26] или совокупность ресурсов человеческих [27; 28]. В данном исследовании аудиторские ресурсы будем интерпретировать как совокупность временных и человеческих ресурсов. В таком виде можно ответить на два вопроса:

1) является ли достаточным выделенное количество времени на проведение аудита?

2) является ли достаточным выделенное количество людей на проведение аудита?

Таким образом данные показатели достаточности ресурсов также являются одними из основных компонент вероятности достижения целей аудита.

Вопрос достаточности времени может быть сформирован как 2 вариации, зависящих от детерминированности времени проведения каждого этапа аудита. В первом случае, если время каждого этапа является детерминированным (известным и точным), то задача выявления времени, достаточного для проведения аудита, достаточно проста:

$$T_{mp} = \sum_{j=1}^{J} T_j \qquad (13)$$

где T_{mp} – время, требуемое для проведения аудита,

T_j – время проведения j-ого этапа аудита,

J – количество этапов аудита.

Такая формула может применяться, если заранее определены наборы времени для проведения каждого этапа аудита. Например, такие наборы времени могут быть прописаны в (типовой) программе аудита, регламентироваться требованиями по ЗИ или стандартами, выведены эмпирическим путем командой по аудиту и т.п. В таком случае физический смысл формулы также достаточно прост – если команда аудита знает количество времени, требуемое для проведения этапов аудита, то, суммируя это время, можно сказать об известности времени, требуемого для проведения полного аудита (что и является целью аудита).

Иногда можно встретить вторую ситуацию – время каждого этапа аудита строго не определено. Тогда примем, что время проведения каждого i-ого этапа аудита Ti является случайной величиной, подчиняющаяся закону нормального распределения. Тогда время, требуемое для аудита, является также случайной величиной с нормальным распределением, при этом математическое ожидание и дисперсия этой величины будет являться суммой математических ожиданий и дисперсий каждого этапа аудита соответственно. Тогда время $T_{тр}$ будет рассчитываться как:

$$T_{mp} = \arg\left(f\left(\frac{T_{ф} - \sum_{j=1}^{J} M\left(T_j\right)}{\sqrt{\sum_{j=1}^{J} \sigma^2\left(T_j\right)}} \right) \middle| f\left(T\right) = P\left(A\right)_{треб} \right) \qquad (14)$$

где *arg()* – аргумент функции *f(T)*,

f(T) – функция вероятности нормального распределения,

$T_{ф}$ – время проведения аудита,

T_j – время проведения этапа аудита,

$M(T_j)$ – математическое ожидание времени проведения j-ого этапа аудита,

$\sigma^2(T_j)$ – дисперсия времени проведения j-ого этапа аудита,

$P(A)_{треб}$ – требуемое значения вероятности достижения целей аудита.

Здесь для расчета необходимо при помощи лица, принимающего решения, определить требуемую вероятность достижения целей аудита и далее путем анализа графика функции нормального распределения определить значение времени, необходимого для достижения целей аудита с заданной вероятностью.

Формулу (13) можно использоваться в 2 целях:

• ретроспективный анализ, на основе прошлых аудитов (требуемая вероятность аудита становится фактической рассчитанной на основе уже имеющихся данных);

• прогнозирование (лицо, принимающее решение, может задать желаемую вероятность и тогда на базе этого можно провести анализ достаточности времени).

Коэффициент достаточности времени D_T здесь уже рассчитывается как коэффициент, основанный на разности фактического времени аудита и достаточного:

$$D_T = 1 - \frac{\left|T_{ф} - T_{mp}\right|}{T_{mp}} \qquad (15)$$

При этом $0 < T\text{ф} \leq 2T_{тр}$.

Здесь знак разницы неважен для расчета эффективности аудита. Если разница принимает положительный знак, то речь идет об избыточности, в ином случае – о недостаточности. При избыточности времени выделенные

ресурсы для проведения аудита задействованы в неполную силу, а также возможна перегрузка основных бизнес-процессов. При недостатке времени будет цель аудита может быть достигнута с недостаточной достоверностью (формула (13).

Человеческий ресурс имеет влияние на время проведения аудита ИБ, часть задач можно делать параллельно, что снижает общее время проведения аудита и наоборот увеличивает, если количество людей ниже. Количество аудиторов имеет влияние на этапе сбора свидетельства аудита и выявления обнаружений аудита, так как данные 2 этапа являются основными в ходе процесса аудита ИБ. Остальные этапы по большей части независимы от количества аудиторов, поэтому здесь пренебрежем зависимостью времени аудита от человеческих ресурсов в силу значительно малой величины.

Вербально влияние может быть описано следующим образом: если можно выполнять часть независимых этапов (подэтапов) аудита параллельно, то можно сгруппировать время, необходимое для выполнения этих этапов, по принципу максимального значения. Математически мы переходим от суммирования времени этапов аудита к поиску максимального значения:

$$T_{j1-jk} = \begin{cases} T_{j1} + T_{j2} + \ldots + T_{jk}, \text{у} V \vee L < 2 \\ \max\left(T_{j1}, T_{j2}, \ldots, T_{jk}\right), \exists V \wedge L \geq 2 \end{cases} \quad (16)$$

где $T_{j1\text{-}jk}$ – общее время, требуемое для проведения этапов аудита j_1-j_k,

T_{jk} – время, требуемое для проведения j_k-ого этапа аудита,

V – факт возможности распараллеливания проведения этапов аудита,

L – количество аудиторов.

Таким образом человеческий ресурс влияет на временной ресурс аудита, необходимый для достижения целей аудита с требуемой вероятностью.

Коэффициент эффективности аудита

Учитывая все вышесказанное коэффициент эффективности аудита А будет находиться как произведение коэффициент нахождения свидетельств аудита, соответствия ресурсов аудита запланированным показателям и достаточности времени:

$$A = C \times S \times D_T \quad (17)$$

В результате разработанной методики оценки эффективности аудита информационной безопасности появляется возможность получить следующие результаты:

– статистические характеристики оцениваемых показателей (текущее, минимальное, максимальное, среднее значение);

– графики текущих и средних значений оцениваемых показателей;

– гистограммы и статистические функции распределения значений оцениваемых показателей, которые позволят провести опосредованную оценку следующих вопросов:

• управления временными и человеческими ресурсами;

• формирования ретроспективной оценки процесса аудита в течение длительного времени;

• скорости реакции процесса аудита на изменения в процессе аудита.

Имитационное моделирование

На основе сформированной эталонной модели процесса аудита информационной безопасности [5] можно сформировать модель (рис. 1) для расчета показателей эффективности аудита. В качестве среды имитационного моделирования используется программный комплекс AnyLogic, который предоставляет возможность имитации и анализа процессов информационной безопасности.

Здесь реализованы все основные процедуры процесса аудита информационной безопасности, отвечающие за сбор и анализ свидетельств аудита. Далее сформируем ряд экспериментов, касающихся реализации оценки эффективности. Примем следующие показатели за постоянные:

1) планируемое количество аудиторов $L_{\text{п}} = 5$ (чел.);

2) планируемое количество времени $T_{\text{п}} = 19$ (дней);

3) требуемое количество времени $T_{mp} = 20$ (дней);

4) максимальное количество свидетельств аудита $M = 30$ (шт.).

Далее на сымитированных статистических данных проведем оценку процесса аудита информационной безопасности на базе нескольких прогонов системы:

1) фактическое количество свидетельств аудита $C_m = [20..30]$;

2) фактическое количество аудиторов $L_{\text{ф}} = [3..7]$;

3) фактическое количество времени $T_{\text{ф}} = [14..28]$.

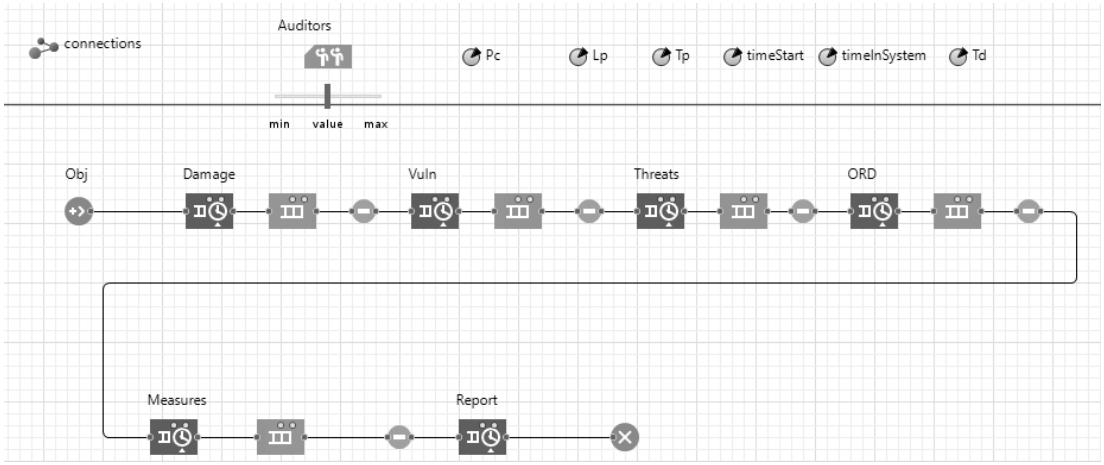

Рис. 1. Имитационная модель процесса аудита

Результаты прогона модели представлены на рисунке 2.

Анализ представленных графиков зависимости эффективности процесса аудита от таких ключевых показателей, как коэффициент нахождения всех свидетельств аудита, коэффициент соответствия ресурсов аудита запланированному количеству в программе аудита и коэффициент достаточности времени, выделенного для аудита, свидетельствует о критической важности поддержания баланса этих факторов. Отклонения любого из указанных показателей в любую сторону ведут к снижению общей эффективности процесса аудита. Например, недостаточное количество обнаруженных свидетельств аудита или избыточное отклонение от запланированной программы аудита могут приводить к пропуску важных нарушений или к нецелевому расходу ресурсов. С другой стороны, как недостаточное, так и избыточное время, выделенное на аудиторские процедуры, приводит либо к поверхностному анализу, либо к растрате ресурсов, не влияя на улучшение качества процесса аудита информационной безопасности. Таким образом, поддержание баланса между этими показателями является решающим для достижения оптимальной эффективности аудита информационной безопасности.

Заключение

В результате проведенного исследования были рассмотрены вопросы проведения оценки эффективности процесса аудита информационной безопасности. За показатели эффективности были приняты следующие аспекты аудита – коэффициент нахождения всех свидетельств аудита, коэффициент соответствия использованных временных и человеческих ресурсов запланированным в программе аудита, коэффициент достаточности времени, выделенного для проведения аудита информационной безопасности.

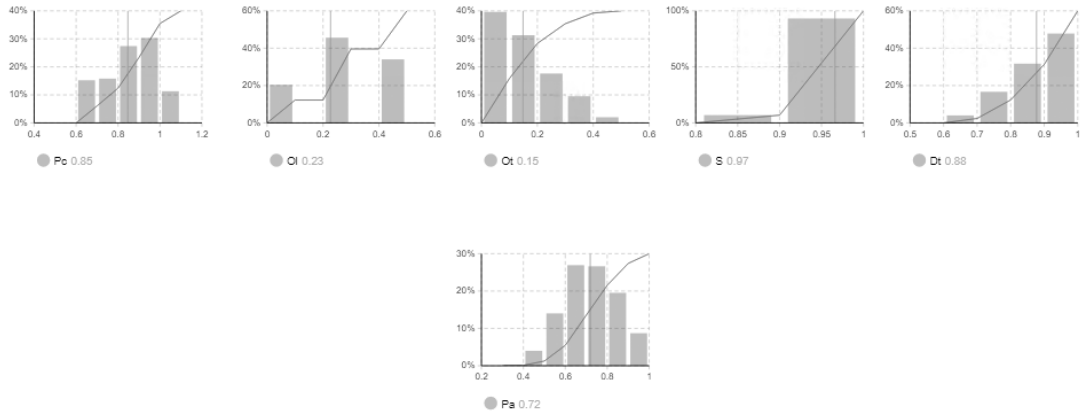

Рис. 2. Статистика измерений показателей эффективности аудита

Сформированный механизм оценки эффективности аудита информационной безопасности призван оценивать эффективность использования выделенных временных и человеческих ресурсов для достижения целей аудита. Показатель эффективности процесса аудита будет использоваться в целях проведения оценки доверия к процессу аудита информационной безопасности как мера работоспособности аудита в рамках реализации мероприятий по обеспечению информационной безопасности.

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. Information security audit for a manufacturing company / S.V. Shirokova [et al.] // Information and control systems. – 2023. – Vol. 122. – № 1. – P. 41-50.

2. Каширская Л.В. Объекты аудита информационной безопасности и направления их проверки / Л.В. Каширская, Ю.А. Зурнаджьянц // Аудитор. – 2022. – Vol. 8. – № 1. – P. 21-31.

3. Senkiv D.A. Audit as a Means of Ensuring Information Security of Web Applications and Used Computer Systems / D.A. Senkiv // American Scientific Journal. – 2020. – Vol. 40. – № 2. – P. 54-57.

4. Santi R. Information system security audit using ISO/IEC 27002:2013 at university of XXX / R. Santi, A.I. Alfresi, B. Octariana // Jurnal Teknik Informatika (Jutif). – 2023. – Vol. 4. – № 4. – P. 733-750.

5. Огнев И.А. Вопросы математической интерпретации процесса аудита информационной безопасности с применением сетей Петри / И.А. Огнев // Доклады Томского Государственного Университета Систем Управления И Радиоэлектроники. – 2024. – Vol. 27. – № 2. – P. 15-20.

6. Effectiveness of cybersecurity audit / S. Slapničar [et al.] // International Journal of Accounting Information Systems. – 2022. – Vol. 44. – P. 100548.

7. Макаренко С.И. Аудит безопасности критической информационной инфраструктуры / С.И. Макаренко. – СПб: Издательство «Наукоемкие технологии», 2023. – 122 p.

8. Денисенко В.В. Аудит Информационной Безопасности Организаций: Методы И Преимущества / В.В. Денисенко, А.М. Гончаров, И.П. Маслов // Наукосфера. – 2023. – № 11-2. – P. 135-140.

9. Ситская А.В. Вопросы аудита информационной безопасности / А.В. Ситская, В.В. Селифанов, П.А. Звягинцева // Безопасность цифровых технологий. – 2023. – Vol. 110. – № 3. – P. 67-82.

10. Чекулаева Е.Н. Методика аудита информационной безопасности предприятия с использованием причинно-следственной диаграммы / Е.Н. Чекулаева, Е.С. Кубашева // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и Инфокоммуникационные системы. – 2020. – Vol. 45. – № 1. – P. 58-68.

11. Héroux S. The internal audit function in information technology governance: A holistic perspective / S. Héroux, A. Fortin // Journal of Information Systems. – 2013. – Vol. 27. – № 1. – P. 189-217.

12. IT governance and IT controls: Analysis from an internal auditing perspective / T.-H. Wu [et al.] // International Journal of Accounting Information Systems. – 2024. – Vol. 52. – P. 100663.

13. Воеводин В.А. Концептуальная модель объекта аудита информационной безопасности / В.А. Воеводин // Computational nanotechnology. – 2019. – № 3. – P. 92-95.

14. Kotb A. Mapping of Internal Audit Research: A Post-Enron Structured Literature Review / A. Kotb, H. Elbardan, H. Halabi // Accounting Auditing & Accountability Journal. – 2020. – Vol. 33. – № 8. – P. 1969-1996.

15. Turetken O. Internal audit effectiveness: operationalization and influencing factors / O. Turetken, S. Jethefer, B. Ozkan // Managerial Auditing Journal. – 2020. – Vol. 35. – № 2. – P. 238-271.

16. Constructing internal audit quality evaluation index: evidence from listed companies in Jiangsu province, China / R. Kai [et al.] // Heliyon. – 2022. – Vol. 8. – № 9. – P. e10598.

17. Examining the critical factors of internal audit effectiveness from internal auditors' perspective: Moderating role of extrinsic rewards / H. Alqudah [et al.] // Heliyon. – 2023. – Vol. 9. – № 10. – P. e20497.

18. Ефремов А.В. Анализ существующих методик оценки средств аудита информационной безопасности / Ефремов А.В., Панамарев Г.Е. // ВЕСТНИК ВОЕННОГО ИННОВАЦИОННОГО ТЕХНОПОЛИСА "ЭРА." – 2021. – Vol. 2. – № 4. – P. 38-45.

19. Gaosong Q. Measurement of Internal Audit Effectiveness: Construction of Index System and Empirical Analysis / Q. Gaosong, Y. Leping // Microprocessors and Microsystems. – 2021. – P. 104046.

20. Roussy M. Internal audit: from effectiveness to organizational significance / M. Roussy, O. Barbe, S. Raimbault // Managerial Auditing Journal. – 2020. – Vol. 35. – № 2. – P. 322-342.

21. Сафохина Е.А. Эффективность внутреннего аудита как элемент обеспечения экономической безопасности хозяйствующего субъекта / Е.А. Сафохина // Вестник экономической безопасности. – 2022. – № 1. – P. 301-306.

22. Hutchinson B. Audit masquerade: How audits provide comfort rather than treatment for serious safety problems / B. Hutchinson, S. Dekker, A. Rae // Safety Science. – 2024. – Vol. 169. – P. 106348.

23. Макаренко С.И. Критерии и показатели оценки качества тестирования на проникновение / С.И. Макаренко // Вопросы кибербезопасности. – 2021. – Vol. 43. – № 3. – P. 43-57.

24. ISO 19011:2018 - Guidelines for auditing management systems.

25. Бусуёк Н.А. Аудит эффективности в системе внешнего государственного финансового контроля (аудита) / Н.А. Бусуёк, Л.М. Макарова // Вестник Московского финансово-юридического университета. – 2022. – № 3. – P. 140-145.

26. Calabrese K. The effects of time pressure on audit fees / K. Calabrese // Advances in Accounting. – 2023. – Vol. 63. – P. 100663.

27. Воеводин В.А. Определение весомости аудиторских свидетельств методом бальных оценок при аудите информационной безопасности / В.А. Воеводин, М.С. Маркина, П.В. Маркин // Computational nanotechnology. – 2020. – № 1. – P. 57-62.

28. Opening the black box of human resource allocations in audit firms: The assignment of audit partners to audit engagements / B. Wu [et al.] // The British Accounting Review. – 2024. – Vol. 56. – № 2. – P. 101231.

References

1. Shirokova S.V., Rostova O.V., Bolsunovskaya M.V., Dmitrieva L.A., Almataev T.O. Information security audit for a manufacturing company. Information and control systems, 2023, vol. 122, no. 1, pp. 41-50.

2. Kashirskaya L.V., Zurnadzh'yants Yu.A. Ob"ekty audita informatsionnoi bezopasnosti i napravleniya ikh proverki [Objects of information security audit and directions of their verification]. Auditor, 2022, vol. 8, no. 1, pp. 21-31. (In Russ.)

3. Senkiv D.A. Audit as a Means of Ensuring Information Security of Web Applications and Used Computer Systems. American Scientific Journal, 2020, vol. 40, no. 2, pp. 54-57.

4. Santi R., Alfresi A.I., Octariana B. Information system security audit using ISO/IEC 27002:2013 at university of XXX. Jurnal Teknik Informatika (Jutif), 2023, vol. 4, no. 4, pp. 733-750.

5. Ognev I.A. Voprosy matematicheskoi interpretatsii protsessa audita informatsionnoi bezopasnosti s primeneniem setei Petri [Issues of mathematical interpretation of the information security audit process using Petri nets]. Reports of Tomsk State University of Control Systems and Radioelectronics, 2024, vol. 27, no. 2, pp. 15-20. (In Russ.)

6. Slapničar S., Vuko T., Čular M., Drašček M. Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 2022, vol. 44, pp. 100548.

7. Makarenko S.I. Audit bezopasnosti kriticheskoi informatsionnoi infrastruktury [Security audit of critical information infrastructure]. SPb: Izdatel'stvo «Naukoemkie tekhnologii», 2023. — 122 p. (In Russ.)

8. Denisenko V.V., Goncharov A.M., Maslov I.P. Audit Informatsionnoi Bezopasnosti Organizatsii: Metody I Preimushchestva [Information Security Audit of Organizations: Methods and Advantages]. Naukosphere, 2023, no. 11-2, pp. 135-140. (In Russ.)

9. Sitskaya A.V., Selifanov V.V., Zvyagintseva P.A. Voprosy audita informatsionnoi bezopasnosti [Information security audit issues]. Digital Technology Security, 2023, vol. 110, no. 3, pp. 67-82. (In Russ.)

10. Chekulaeva E.N., Kubasheva E.S. Metodika audita informatsionnoi bezopasnosti predpriyatiya s ispol'zovaniem prichinno-sledstvennoi diagrammy [Methodology of enterprise information security audit using a cause-and-effect diagram]. Bulletin of the Volga State Technological University. Series: Radio Engineering and Infocommunication Systems, 2020, vol. 45, no. 1, pp. 58-68. (In Russ.)

11. Héroux S., Fortin A. The internal audit function in information technology governance: A holistic perspective. Journal of Information Systems, 2013, vol. 27, no. 1, pp. 189-217.

12. Wu T.-H., Huang S.Y., Chiu A.-A., Yen D.C. IT governance and IT controls: Analysis from an internal auditing perspective. International Journal of Accounting Information Systems, 2024, vol. 52, pp. 100663.

13. Voevodin V.A. Kontseptual'naya model' ob"ekta audita informatsionnoi bezopasnosti [Conceptual model of the object of information security audit]. Computational nanotechnology, 2019, no. 3, pp. 92-95. (In Russ.)

14. Kotb A., Elbardan H., Halabi H. Mapping of Internal Audit Research: A Post-Enron Structured Literature Review. Accounting Auditing & Accountability Journal, 2020, vol. 33, no. 8, pp. 1969-1996.

15. Turetken O., Jethefer S., Ozkan B. Internal audit effectiveness: operationalization and influencing factors. Managerial Auditing Journal, 2020, vol. 35, no. 2, pp. 238-271.

16. Kai R., Yusheng K., Ntarmah A.H., Ti C. Constructing internal audit quality evaluation index: evidence from listed companies in Jiangsu province, China. Heliyon, 2022, vol. 8, no. 9, pp. e10598.

17. Alqudah H., Amran N.A., Hassan H., Lutfi A., Alessa N., alrawad M., Almaiah M.A. Examining the critical factors of internal audit effectiveness from internal auditors' perspective: Moderating role of extrinsic rewards. Heliyon, 2023, vol. 9, no. 10, pp. e20497.

18. Efremov A.V., Panamarev G.E. Analiz sushchestvuyushchikh metodik otsenki sredstv audita informatsionnoi bezopasnosti [Analysis of existing methods for assessing information security audit tools]. BULLETIN OF THE MILITARY INNOVATIVE TECHNOPOLIS "ERA.", 2021, vol. 2, no. 4, pp. 38-45. (In Russ.)

19. Gaosong Q., Leping Y. Measurement of Internal Audit Effectiveness: Construction of Index System and Empirical Analysis. Microprocessors and Microsystems, 2021, pp. 104046.

20. Roussy M., Barbe O., Raimbault S. Internal audit: from effectiveness to organizational significance. Managerial Auditing Journal, 2020, vol. 35, no. 2, pp. 322-342.

21. Safokhina E.A. Effektivnost' vnutrennego audita kak element obespecheniya ekonomicheskoi bezopasnosti khozyaistvuyushchego sub"ekta [Effectiveness of internal audit as an element of ensuring economic security of an economic entity]. Bulletin of Economic Security, 2022, no. 1, pp. 301-306. (In Russ.)

22. Hutchinson B., Dekker S., Rae A. Audit masquerade: How audits provide comfort rather than treatment for serious safety problems. Safety Science, 2024, vol. 169, pp. 106348.

23. Makarenko S.I. Kriterii i pokazateli otsenki kachestva testirovaniya na proniknovenie [Criteria and indicators for assessing the quality of penetration testing]. Cybersecurity Issues, 2021, vol. 43, no. 3, pp. 43-57. (In Russ.)

24. ISO 19011:2018 - Guidelines for auditing management systems.

25. Busuek N.A., Makarova L.M. Audit effektivnosti v sisteme vneshnego gosudarstvennogo finansovogo kontrolya (audita) [Performance audit in the system of external state financial control (audit)]. Bulletin of the Moscow Financial and Law University, 2022, no. 3, pp. 140-145. (In Russ.)

26. Calabrese K. The effects of time pressure on audit fees. Advances in Accounting, 2023, vol. 63, pp. 100663.

27. Voevodin V.A., Markina M.S., Markin P.V. Opredelenie vesomosti auditorskikh svidetel'stv metodom bal'nykh otsenok pri audite informatsionnoi bezopasnosti [Determining the weight of audit evidence using the scoring method in information security audit]. Computational nanotechnology, 2020, no. 1, pp. 57-62. (In Russ.)

28. Wu B., Wu Y., Zhang M., Li J. Opening the black box of human resource allocations in audit firms: The assignment of audit partners to audit engagements. The British Accounting Review, 2024, vol. 56, no. 2, pp. 101231.

Иванов Андрей Валерьевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации, Новосибирский государственный технический университет. Область научных интересов: доверенное взаимодействие, защита информации. 630073, г. Новосибирск, проспект К. Маркса, 20. E-mail: andrej.ivanov@corp.nstu.ru.

Огнев Игорь Александрович, старший преподаватель кафедры защиты информации, Новосибирский государственный технический университет. Область научных интересов: оценка доверия, аудит информационной безопасности. 630073, г. Новосибирск, проспект К. Маркса, 20. E-mail: i.ognev@corp.nstu.ru.

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации, Новосибирский государственный технический университет. Область научных интересов: оценка доверия, управление информационной безопасностью. 630073, г. Новосибирск, проспект К. Маркса, 20. E-mail: selifanov@corp.nstu.ru.

Ivanov Andrey Valerievich, Candidate of Technical Sciences, Associate Professor, Head of the Information Security Department, Novosibirsk State Technical University. Research interests: trusted interaction, information security. 630073, Novosibirsk, avenue K. Marksa, 20. E-mail: andrej.ivanov@corp.nstu.ru.

Ognev Igor Aleksandrovich, Senior Lecturer, Information Security Department, Novosibirsk State Technical University. Research interests: trust assessment, information security audit. 630073, Novosibirsk, avenue K. Marksa, 20. E-mail: i.ognev@corp.nstu.ru.

Selifanov Valentin Valerievich, Senior Lecturer, Information Security Department, Novosibirsk State Technical University. Research interests: trust assessment, information security management. 630073, Novosibirsk, avenue K. Marksa, 20. E-mail: selifanov@corp.nstu.ru.