Алексей А. Сиротский¹, Сергей А. Резниченко²

¹Московский государственный технологический университет «СТАНКИН»,
Вадковский пер., 1, Москва, 127055, Россия

²Финансовый университет при правительстве РФ,
Ленинградский пр-кт, 49, Москва, 125993, Россия

¹e-mail: hotwater2009@yandex.ru, <https://orcid.org/0000-0002-9343-7185>

²e-mail: rsa_5@bk.ru, <https://orcid.org/0000-0002-1539-0457>

ФОРМАЛИЗОВАННАЯ МОДЕЛЬ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ НА ПРЕДМЕТ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ СТАНДАРТОВ

DOI: <http://dx.doi.org/10.26583/bit.2021.3.09>

Аннотация. Задача аудита информационной безопасности заключается в проверке соответствия системы защиты объекта совокупности критериев, определяющих требования к уровню защищенности. В этой связи необходимо определить и формализовать совокупность критериев, отражающих уровень защищенности объекта и выявление показателей, по которым можно провести объективные процедуры проверки. Аудит информационной безопасности проводится на предмет соответствия требованиям любых стандартов в области информационной безопасности. В связи с отсутствием практико-ориентированных инструктивно-методических материалов аудиторской деятельности по оценке соответствия информационной безопасности организаций требованиям ключевых документов и стандартов, были проведены исследования содержательности и формализуемости требований на примере стандарта ГОСТ Р ИСО/МЭК 17799-2005 в части разработки метода проведения аудита ИБ на предмет соответствия данному стандарту и инструкции по его реализации. Целью работы является формирование формализованной методики при проведении аудита информационной безопасности на предмет соответствия стандартам и нормативным требованиям по информационной безопасности. В статье представлена формализованная модель аудита информационной безопасности организации, которая базируется на принципах независимости и объективности аудиторской деятельности. Предложен подход, на основе системы объективных показателей, сопоставимых с функциями защиты, и заключающийся в формировании чек-листов с соответствующими критериями соотнесения показателей. В основу предлагаемого метода, и в целях повышения объективности результатов аудиторской работы, положен принцип подтверждения фактов, выявляемых в результате аудиторской проверки. В рамках метода предложена инструкция по разработке чек-листов, пригодная и адаптируемая для любого описательного стандарта, на предмет соответствия, которому может проводиться процедура аудиторской проверки.

Ключевые слова: аудит, информационная безопасность, стандарт, модель, контроль, показатели, методика, формализация.

Для цитирования: СИРОТСКИЙ, Алексей А.; РЕЗНИЧЕНКО, Сергей А. ФОРМАЛИЗОВАННАЯ МОДЕЛЬ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ НА ПРЕДМЕТ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ СТАНДАРТОВ. *Безопасность информационных технологий*, [S.l.], т. 28, № 3, с. 103–117, 2021. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1368>. DOI: <http://dx.doi.org/10.26583/bit.2021.3.09>.

Alexei A. Sirotskiy¹, Sergei A. Reznichenko²

¹Moscow State University of Technology «STANKIN»,
Vadkovskiy pereulok, 1, Moscow, 127055, Russia

²Financial University under the Government of the Russian Federation,
Leningradsky Prospekt, 49, Moscow, 125993, Russia

¹e-mail: hotwater2009@yandex.ru, <https://orcid.org/0000-0002-9343-7185>

²e-mail: rsa_5@bk.ru, <https://orcid.org/0000-0002-1539-0457>

A formalized model of an organization information security audit for compliance with the requirements of standards

DOI: <http://dx.doi.org/10.26583/bit.2021.3.09>

Abstract. In general the overall task of an information security audit is to verify that the security system of an object meets the set of criteria that determine the requirements for the security level. In this regard, it is necessary to define and to establish a set of criteria reflecting the security level of the facility and to identify indicators for which objective verification procedures can be carried out. Information security audits can be conducted to ensure compliance with all information security standards. Due to the lack of instructional methodologies for auditing activities to assess the compliance of organization information security with the requirements of systemically important generally applicable documents and standards, studies were carried out on the content and formalizability of requirements using the example of the GOST R ISO/IEC 17799-2005 standard in terms of the building an instructional methodology for auditing IS possibility for compliance with this standard. The purpose of the study is to form a formalized audit methodology when conducting an audit of information security for compliance with standards and regulatory requirements for information security in the absence of developed and generally accepted methods. In the following a formalized model for auditing the organization's information security for compliance with the requirements of standards is developed. The model is based on the principles of maximum independence and objectivity of audit activities. The authors of the paper suggest an approach, which is based on a system of objective indicators comparable to protection functions, and consists in the formation of check lists with appropriate criteria for the correlation of indicators and methods of proving the facts revealed as a result of an audit. On the basis of the proposed model and methodology, it is possible to develop the check lists for any descriptive standard for which an audit is required.

Keywords: audit, information security, standard, model, control, indicators, methodology, formalization.

For citation: SIROTSKIY, Alexei A.; REZNICHENKO, Sergei A. A formalized model of an organization information security audit for compliance with the requirements of standards. *IT Security (Russia)*, [S.l.], v. 28, n. 3, p. 103–117, 2021. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1368>. DOI: <http://dx.doi.org/10.26583/bit.2021.3.09>.

1. Введение

Аудит информационной безопасности (ИБ), как системное действие, направлено на контроль и проверку состояния ИБ объекта защиты (в частности, организации), а также оценку адекватности применяемых средств и методов защиты информации в соответствии с существующими угрозами.

Общая задача аудита ИБ заключается в проверке соответствия системы защиты объекта совокупности критериев, определяющих требования к уровню защищенности.

В этой связи возникает необходимость определения и формализации совокупности критериев, отражающих уровень защищенности объекта и выявление показателей, по которым возможно провести объективные процедуры проверки. Критерии должны быть четко определяемыми и по возможности измеряемыми [1, 2].

Объектами аудита ИБ могут быть любые объекты и процессы, например:

- деятельность компании в целом;
- автоматизированная или информационная система, либо их отдельные компоненты;
- организационно-управленческие процессы;
- технические средства;
- бизнес-процедуры [3, 4].

По форме проведения, аудит ИБ может быть организационно-нормативным [5] (когда предметом анализа являются мероприятия и нормативные документы по

обеспечению ИБ) и техническим (когда предметом анализа являются технические средства обработки информации).

Совокупность методов анализа рисков ИБ базируется на двух моделях:

- первая модель определяет риск на основе сопоставления соответствия объекта защиты набору требований по ИБ, которые исходят из стандартов, нормативно-правовых актов и условий эксплуатации систем;
- вторая модель определяет риск на основе оценки вероятностей реализации угроз и атак, а также величин потенциально возможного материального ущерба.

В рамках концептуальной модели аудита ИБ [5], можно выделить три практических и три теоретических подхода к проведению аудита ИБ.

Практическими подходами являются:

- аудит на основе анализа рисков;
- аудит на основе анализа стандартов ИБ;
- аудит на основе экспериментальных исследований объекта.

Теоретическими подходами являются:

- аудит на основе моделирования процессов;
- аудит на основе модели оценки;
- аудит на основе модели зрелости.

Исходя из этого, невозможно дать универсальные формализованные показатели и критерии проведения аудита, применимые во всех задачах и видах аудита.

Одним из наиболее распространённых методов является подход на основе анализа стандартов ИБ, хотя бы потому, что стандарты формируют совокупность требований и рекомендаций по обеспечению ИБ на основе накопленного профессионального опыта, а также являются регламентирующими документами, применяемыми в профессиональном сообществе. Кроме того, по ряду отраслей существуют обязательные к применению отраслевые стандарты. Примером обязательных к применению стандартов являются стандарты Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» и СТО БР ИББС-1.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности». Отраслевые стандарты определяют специфические задачи управления и обеспечения ИБ в своей сфере. Типичной является финансово-кредитная сфера, характеризующаяся ярко выраженными индивидуальными особенностями [6, 7].

Примерами общеприменимых основополагающих стандартов являются национальный стандарт российской Федерации ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» и международный стандарт ISO / IEC 27002-2013 «Информационные технологии – Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью».

Аудит ИБ может проводиться на предмет соответствия требованиям стандартов необходимых организации в соответствии с заданием на аудит. И если применительно к требованиям стандартов СТО БР ИББС-1.0 и СТО БР ИББС-1.1 Банком России разработана методика аудиторской проверки, изложенная в стандарте Банка России СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014», то применительно к общеприменимым стандартам ГОСТ Р ИСО/МЭК и ISO/IEC таких методик как правило нет. Можно отметить модель, реализованную в стандартах

ISO/IEC 15504-3 «Информационная технология. Оценка процесса», ISO/IEC 21827 «Инжиниринг безопасности систем – модель зрелости возможностей», COBIT (Control Objectives for Information and related Technology), но она не может быть прямо перенесена на другие стандарты и нормативные документы, в частности на стандарт ГОСТ Р ИСО/МЭК 17799-2005. В то же время стандарты ГОСТ Р ИСО/МЭК 17799-2005 и ISO / IEC 27002-2013 являются базовыми документами, определяющими основные направления обеспечения информационной безопасности организаций, и во множестве случаев могут быть основой для проводимой аудиторской проверки.

Целью работы является формирование формализованной аудиторской методики и практико-ориентированной инструкции, при проведении аудита ИБ на предмет соответствия стандартам и нормативным требованиям по ИБ. В рамках предлагаемой методики возможна разработка аналогичных инструкций применительно к любому стандарту.

2. Формализация проведения аудита информационной безопасности

Следует заметить, что подавляющее большинство базовых стандартов в области обеспечения ИБ объектов защиты и управлению ИБ на предприятиях, имеет явно выраженный описательный характер с указаниями по совокупности руководящих действий, и не содержат:

- критериев полноты руководящих действий;
- дискретных, однозначно трактуемых показателей выполнимости и результативности действий;
- методов достижения результатов;
- инструкций по реализации проверок на соответствие.

Основная трудность в проведении аудита ИБ на предмет соответствия требованиям стандартов заключается в отсутствии чёткой и последовательной методики аудита. В свою очередь при аудите ИБ следует исключить субъективности, исходя из понимания, что результаты аудита будут тем достовернее, чем в большей степени они будут формализованы. Исключить субъективности полностью, к сожалению, неосуществимо.

Формализация аудиторских процессов является актуальным и пока ещё мало изученным направлением исследований. Предпринимались различные попытки формализации, в основном применительно к отдельным аспектам аудита и с применением так называемого «аудиторского подхода на основе эталонной модели» [8, 9].

Задача формализации аудиторского процесса преследует цель повторяемости и независимости процедур и результатов аудита.

Одной из наилучших практик можно назвать создание так называемых «чек-листов» (контрольных карт), отражающих последовательность проведения аудиторской процедуры, проверяемые процессы и их дискретизированные показатели.

Рассмотрим аудиторские задачи и действия в рамках оценки соответствия ИБ организации требованиям стандарта ГОСТ Р ИСО/МЭК 17799-2005, которые по аналогии коррелируют и со стандартом ISO / IEC 27002-2013. Данный стандарт определяет требования к безопасности с учётом следующих факторов:

- оценка рисков ИБ;
- нормативные требования;
- специфические принципы, характерные для среды организации.

Стандарт ГОСТ Р ИСО/МЭК 17799-2005 выделяет три ключевые категории информации, защита которых должна обеспечиваться первоначально:

- персональные данные;

- учётные данные организации;
- интеллектуальная собственность.

Совокупность мероприятий определена следующим образом:

- наличие политик ИБ;
- распределение обязанностей по обеспечению ИБ;
- обучение по вопросам ИБ;
- информирование об инцидентах ИБ;
- управление непрерывностью бизнеса.

Защита персональных данных и персональной информации происходит из неприкосновенности личности и частной жизни, что имеет высокую актуальность в современном общественном устройстве [10–13]. Выделение данной категории в стандарте актуально ввиду наличия отдельного Федерального Закона¹ и подкрепляет практические аспекты реализации его требований.

В отношении каждой из категорий информации необходимы защитные мероприятия. Также и наоборот: защитные мероприятия должны быть направлены на обеспечение защиты всех категорий информации. Составим обобщённую матрицу защиты (табл. 1), в которой определим 15 функций защиты $F_{11} \dots F_{53}$, каждую из которых можно оценить по совокупности соответствия требованиям.

Таблица 1. Обобщённая матрица защиты

Мероприятия	Категории информации		
	Персональные данные	Учётные данные организации	Интеллектуальная собственность
Политики ИБ	F_{11}	F_{12}	F_{13}
Распределение обязанностей	F_{21}	F_{22}	F_{23}
Обучение персонала	F_{31}	F_{32}	F_{33}
Информирование об инцидентах	F_{41}	F_{42}	F_{43}
Управление непрерывностью бизнеса	F_{51}	F_{52}	F_{53}

Процессы управления ИБ в стандарте ГОСТ Р ИСО/МЭК 17799-2005 разделены на 10 направлений:

- политика безопасности;
- организация информационной безопасности;
- управление активами;
- безопасность человеческих ресурсов;
- физическая безопасность и безопасность окружения;
- управление передачей данных и операционной деятельностью;
- контроль доступа;
- разработка и обслуживание систем;
- управление непрерывностью бизнеса;
- соответствие требованиям.

Сопоставляя совокупность рекомендованных мероприятий и управленческих процессов, можно отметить, что частично они совпадают.

Непосредственные действия аудитора направлены на выявление соответствия защищённости объекта по указанным 10 направлениям. При этом проверки необходимо

¹Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ.

выполнять максимально объективными и повторяемыми методами. Разработанная модель аудиторского контроля, в рамках выделенных направлений, приведена на рис. 1.

Рис. 1. Модель аудиторского контроля
Fig. 1. Audit control model

Согласно предлагаемой модели, аудитор:

- определяет факты, относящиеся к проверяемым процедурам и методам защиты информации;
- собирает доказательства (подтверждения) определяемых фактов;
- использует исключительно объективные дискретные критерии;
- фиксирует результаты проверки в виде однозначно трактуемых или исчислимых показателей.

Принципиальным является вопрос о системе объективных показателей и критериев аудиторского контроля. В этих целях аудиторы, в частности, могут руководствоваться стандартом ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности», который существует в редакциях 2006 г. и 2013 г., которые имеют существенные отличия в части подходов к организации управления информационной безопасностью на предприятиях. Процедуры аудита по совокупности требований системы стандартов ISO 2700x и в рамках цикла PDCA имеют самостоятельную концепцию [14] и в данном случае не рассматриваются.

Стандарт ГОСТ Р ИСО/МЭК 27001-2006 в рекомендуемом приложении «А» приводит цели и меры управления, соответствующие направлениям, сформулированным в стандарте ГОСТ Р ИСО/МЭК 17799-2005, а стандарт ISO/IEC 27001-2013 в рекомендуемом приложении «А» приводит аналогичные цели и меры управления, соответствующие направлениям, сформулированным в стандарте ISO/IEC 27002-2013. Они имеют частичные совпадения и соответствия, поскольку перечень направлений, определяемых в ГОСТ Р ИСО/МЭК 17799-2005 и ISO/IEC 27002-2013 имеет различия.

В табл. 2 приведён в качестве примера перечень целей и мер управления из стандарта ГОСТ Р ИСО/МЭК 27001-2006 для направления «Политика информационной безопасности» стандарта ГОСТ Р ИСО/МЭК 17799-2005. Такие перечни целей и мер определены для всех направлений стандарта.

Таблица 2. Цели и меры управления политикой информационной безопасностью

А.5.1.1	Документирование политики информационной безопасности	Политика информационной безопасности должна быть руководством утверждена, издана и доведена до сведения всех сотрудников организации, а также сторонних организаций
А.5.1.2	Анализ политики информационной безопасности	Политика информационной безопасности организации должна быть подвергнута анализу и пересмотру через заданные промежутки времени или при появлении существенных изменений характеристик целей безопасности

Приведённая информация, безусловно, является определяющей для аудиторской оценки соответствия, поскольку указывает на необходимые факты, которые аудитором должны быть или подтверждены, или опровергнуты, но не содержит критериев проверки.

Таким образом, имеется потребность в создании формализованной схемы и/или алгоритма аудиторских действий, базирующейся на дискретных критериях и однозначно определяемых объективных исчисляемых показателях. Подобная модель может быть представлена в виде «чек-листов» однозначно поставленных вопросов, на которые могут быть даны только предельно чёткие ответы, исключающие субъективность.

Для создания чек-листов соответствующих ответов воспользуемся как сформулированными в стандарте ГОСТ Р ИСО/МЭК 27001-2006 целями и мерами, так и совокупностью требований, изложенных в стандарте ГОСТ Р ИСО/МЭК 17799-2005. Рассмотрим предлагаемое решение на примере направления «Политика информационной безопасности». Согласно указанным стандартам, цель политики ИБ – обеспечить участие высшего руководства организации в решении вопросов, связанных с обеспечением ИБ в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами.

В действующем законодательстве нет прямых требований по форме и содержанию политик ИБ, в связи, с чем можно наблюдать довольно разнообразные подходы организаций к формированию политик ИБ. В тоже время именно ГОСТ Р ИСО/МЭК 17799-2005 содержит указания на минимальные требования к содержательности политики ИБ, которая должна включать следующее:

а. определение информационной безопасности, ее общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

б. изложение целей и принципов информационной безопасности, сформулированных руководством;

в. краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например:

- 1) соответствие законодательным требованиям и договорным обязательствам;
- 2) требования в отношении обучения вопросам безопасности;
- 3) предотвращение появления и обнаружение вирусов и другого вредоносного ПО;
- 4) управление непрерывностью бизнеса;
- 5) ответственность за нарушения политики безопасности;

б) определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

7) ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для конкретных

информационных систем, а также правила безопасности, которым должны следовать пользователи.

Требования по управлению политикой ИБ следующие:

1. Необходимо, чтобы в организации назначалось ответственное за политику безопасности должностное лицо, которое отвечало бы за ее реализацию и пересмотр в соответствии с установленной процедурой.

2. Указанная процедура должна обеспечивать осуществление пересмотра политики информационной безопасности в соответствии с изменениями, влияющими на основу первоначальной оценки риска, например, путем выявления существенных инцидентов нарушения информационной безопасности, появление новых уязвимостей или изменения организационной или технологической инфраструктуры.

3. Периодические пересмотры должны осуществляться в соответствии с установленным графиком и включать:

- проверку эффективности политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушения информационной безопасности;
- определение стоимости мероприятий по управлению информационной безопасностью и их влияние на эффективность бизнеса;
- оценку влияния изменений в технологиях.

На основе совокупности перечисленных требований и указаний, аудитором составляется перечень вопросов, которые составят чек-лист, и на которые он будет искать ответы в виде доказательств и подтверждающих фактов в процессе проведения аудита.

Поскольку в рамках предлагаемой модели необходимы объективные, дискретные, исчисляемые, однозначно трактуемые критерии, то к перечню вопросов, входящих в чек-лист, предъявляются те же требования: ответом на вопрос может быть только неоспоримое и проверяемое утверждение, но ни в коем случае не рассуждение.

В табл. 3 приведено примерное содержание чек-листа для аудиторской проверки по направлению «Политика информационной безопасности». Предлагаемый чек-лист может быть расширен аудитором под конкретные задачи [15]. Поясним принципы составления чек-листа. Все вопросы сгруппированы по трём уровням (количество уровней может быть и больше). Идея уровней в том, что при отрицательном ответе на вопрос более высокого (например, первого) уровня, нет смысла искать ответы на вопросы более низкого (в данном случае – второго) уровня. Существуют также и альтернативные модели уровневой представления оценок безопасности объектов в процессе проведения аудита [16, 17].

Как видно из табл. 3, все собираемые подтверждающие сведения представляются либо в виде дискретных значений (да/нет, присутствует/отсутствует, соответствует/не соответствует, и т.п.), либо в исчисляемых (средний балл по тестированию [18], процент ознакомленных или обученных сотрудников, и т.п.). Не следует путать проверку (методом тестирования) знаний содержания конкретной политики ИБ организации как внутреннего локального нормативного документа и знаний сотрудниками теории и методологии защиты информации в целом.

Таблица 3. Чек-лист работы аудитора

№ п/п	Уровень	Вопрос для определения контрольного показателя	Ответ		Способ подтверждения факта
			Дискретный	Исчисляемый	
1	1	Есть ли политика безопасности как документ?	Да/нет	-	Наличие документа
2	2	Утверждена ли политика безопасности руководством (надлежащим образом)	Да/нет	-	Наличие реквизитов, подписей, печати
3	2	Размещена ли политика безопасности в свободном доступе, в том числе для сторонних контрагентов	Да/нет	-	а) место размещения; б) способ доступа
4	2	Доведена ли политика безопасности до всех сотрудников организации?	-	% ознакомленных сотрудников	а) лист ознакомления с подписями б) интервью с сотрудниками
5	2	Соответствуют ли изложенные в политике меры и процедуры обеспечения безопасности реально применяемым мерам в совокупности с видами защищаемой информации?	-	Полностью/ В большей мере/ Наполовину/ В меньшей мере/ Не соответствуют	Сопоставление указанных в политике ИБ видов защищаемой информации, должностей сотрудников, процедур взаимодействия, используемых средств обработки и защиты информации реальным бизнес-процессам организации
6	2	Соответствует ли политика ИБ требованиям стандарта	Да/нет (/частично)	-	Наличие отражённых вопросов согласно перечню стандарта
7	3	Понимают ли сотрудники содержание и требования политики безопасности?	-	% компетентных сотрудников	Тестирование сотрудников
8	3	Есть ли процедура пересмотра политики ИБ?	Да/нет	-	Наличие соответствующей записи в политике ИБ или отдельном локальном документе
9	1	Есть ли ответственное лицо за реализацию политики ИБ?	Да/нет	-	1. Наличие: а) должностной инструкции; б) приказа о назначении; в) трудового договора; 2. Проведение интервью с ответственным лицом
10	2	Распределены ли обязанности по обеспечению ИБ между сотрудниками?	-	% сотрудников, имеющих должностные функции по контролю за безопасностью	Наличие должностных инструкций для сотрудников (по категориям) с записями в них о действиях по обеспечению ИБ

Таблица 3. Чек-лист работы аудитора (продолжение)

№ п/п	Уровень	Вопрос для определения контрольного показателя	Ответ		Способ подтверждения факта
11	1	Есть ли методика оценки рисков ИБ в организации?	Да/нет	-	Наличие внутреннего локального документа
12	2	Регулярно ли проводится оценка рисков ИБ?	а) Да/нет; б) соответствует периодичности / не соответствует периодичности	-	а) наличие внутреннего нормативного документа организации с определенным порядком и периодичностью оценки рисков б) наличие отчетов о предыдущих оценках рисков
13	2	Принимались ли решения по результатам переоценки рисков?	Да/нет	-	а) наличие датированных документов по коррекции защитных мер; б) наличие датированных документов о закупке дополнительных средств защиты; в) наличие договоров об оказании услуг в области ИБ
14	3	Изменение количества инцидентов информационной безопасности за отчетный период	-	%	Исследование журналов регистрации инцидентов информационной безопасности.
15	3	Изменение количества предотвращенных событий нарушения информационной безопасности за отчетный период	-	%	Исследование записей о зарегистрированных попытках нарушения информационной безопасности, в том числе создаваемых автоматически в программных средах.
16	1	Обучались ли сотрудники по тематике ИБ?	-	% обучившихся сотрудников	Наличие документов о повышении квалификации и профессиональной переподготовке
17	2	Каков уровень знаний сотрудников в области ИБ?	-	Средний балл	Тестирование сотрудников с оценкой в виде набранных баллов
18	1	Есть ли регламент реагирования на инциденты ИБ?	Да/нет		Наличие внутреннего локального документа

Можно сформулировать следующие принципы составления чек-листов:

– выполнение каждого требования нормативного документа определяется контрольным показателем;

- каждый контрольный показатель выражается в виде предельно чёткого, однозначно трактуемого вопроса, предполагающего однозначный объективный ответ;
- ответ на вопрос может быть либо дискретным, либо в измеримых исчисляемых значениях;
- все вопросы, формирующие контрольные показатели, делятся на уровни;
- вопросы первого (высшего) уровня определяют глобально факты исполнения требований;
- вопросы второго и последующих (низших) уровней детализируют степень исполнения требований и характеризуют уровень защищённости;
- аудитор собирает ответы на вопросы с целью подтверждения фактов;
- при отрицательных ответах на вопросы верхних уровней, проверять утверждения по вопросам нижних уровней не имеет смысла;
- качество формулировок контрольных вопросов определяется их объективностью, выражающейся в неоспоримости ответов даже с позиций сторонней заинтересованности.

В общем случае, исходя из изложенного принципа формирования чек-листов, каждый вопрос (показатель) S_i описывается в виде следующей функции:

$$S_i(j) = \{X_i | Z_i\},$$

где i – номер вопроса, j – уровень вопроса, X – дискретное значение ответа (1 – «да», «выполняется», «есть»; 0 – «нет», «не выполняется», «отсутствует»); Z – исчисляемое значение ответа (в долях, процентах или иных единицах, а также в градациях, например: 1 – «полностью соответствует», 0,75 – «в большей мере», 0,5 – «наполовину», 0,25 – «в меньшей мере», 0 – «не соответствует»).

Для контроля первого уровня целесообразно применять вопросы только с дискретными ответами. Требованиями по прохождению аудита будет являться 100% результаты по критериям первого уровня: $S_i(1) = 1$ и набор минимальной (заранее установленной до начала аудита) результативности по второму и последующему уровням.

Для второго и последующих уровней задаются минимальные пороги результативности, которые могут быть сформулированы следующим образом:

- для второго уровня: не менее чем на 80% вопросов должны быть получены положительные ответы;
- для третьего уровня: не менее чем на 60% вопросов должны быть получены положительные ответы.

При подготовке к аудиту должны быть составлены чек-листы по всем имеющимся в стандарте 10 направлениям, причём, каждый из вопросов $S_i(n)$ ставится в соответствие с решаемой функцией (функциями) $F_{11} \dots F_{53}$, в виде матрицы соответствия (табл. 4). Следует достигать максимальной связности показателей и функций, для чего вычисляется общее количество соответствий по горизонталям t и вертикалям k .

Таблица 4. Матрица соответствия функций защиты по чек-листам

	F_{11}				F_{53}	Итого
$S_j(1)$	+					$t_1(1)$
$S_i(1)$		+	+			
.....						
$S_j(2)$			+			
$S_i(2)$		+		+		
.....						
$S_j(3)$					+	
$S_i(3)$	+					$t_i(3)$
Итого	k_1				k_{15}	-

Вычисляются суммы всех ответов для каждого уровня:

$$C_N = \sum t(j)_i,$$

где j – текущий уровень.

Вычисляются количество соответствий ответов и функций:

$$D_i = \sum S(j)_i,$$

Релевантность составленной модели оценивается по принципу однородности, т.е. полученные значения C_N и D_i не должны существенно отличаться друг от друга (для случая с 15-ю функциями $F_{11} \dots F_{53}$, C_N ориентировочно лежит в диапазоне 3 ... 5).

В процессе проверки аудитор для выявления адекватности и действенности мер по защите информации, может также включать в чек-листы проверочные мероприятия (либо организовать их в виде отдельной программы исследования безопасности). К таким мероприятиям могут относиться тесты на стойкость организационной структуры к информационно-психологическим или информационно-техническим воздействиям.

И если оценка стойкости к информационно-техническим воздействиям проводится в рамках технического и инструментального аудита, то оценка стойкости к информационно-психологическим воздействиям может оказаться полезным дополнением к документарному аудиту для выявления практического уровня стойкости коллектива организации в отношении угроз информационной безопасности. Такие тестовые мероприятия могут быть разработаны аудитором на основе структурных моделей социально-психологических угроз безопасности информации.

Предложенный метод проведения аудита заключается в формализации матрицы защиты и разработке объективных чек-листов. При этом сформированы принципы составления таких чек-листов и оценки их релевантности.

Таким образом, аудит информационной безопасности на основе сформированной и описанной модели, при его практическом применении даст не только объективный повторяемый и однозначный результат оценки уровня информационной безопасности организации, но и позволит выявить слабые стороны в системе защиты и сформировать рекомендации по повышению уровня защищённости объекта. Поэтому применение данной модели целесообразно при проведении аудита информационной безопасности в государственных структурах.

Заключение

В данной работе сформирована формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов, которая базируется на принципах независимости и объективности аудиторской деятельности.

Предложен подход, опирающийся на систему объективных показателей, сопоставимых с функциями защиты, и заключающийся в формировании чек-листов с соответствующими критериями соотнесения показателей и методами подтверждения фактов, выявляемых в результате аудиторской проверки.

На основе предложенной модели возможна разработка чек-листов применительно для любого стандарта и нормативного документа, на предмет соответствия, которому может быть востребовано проведение аудиторской проверки.

СПИСОК ЛИТЕРАТУРЫ:

1. Сиротский А.А. Метрический подход к оценке информационной безопасности в организациях банковской сферы. Системы безопасности, 2016. №25. С. 126–129. URL: <https://www.elibrary.ru/item.asp?id=28884138> (дата обращения: 01.04.2021).
2. Курило А.П. и др. Построение структуры показателей эффективности противодействия угрозам информационной безопасности в интересах оценки защищенности информационных. Безопасность информационных технологий, [S.I.], Т. 17. № 2. С. 16–18. 2010. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/720> (дата обращения: 01.04.2021).
3. Сиротский А.А. Технологии конкурентоспособного управления предприятиями машиностроения. Ученые записки РГСУ, 2013. №5. Т. 2. С. 177–181. URL: <https://www.elibrary.ru/item.asp?id=21408309> (дата обращения: 01.04.2021).
4. Hajo A. Reijers. Business Process Management: The evolution of a discipline, Computers in Industry, Vol. 126, 2021, 103404, ISSN 0166-3615. DOI: <https://doi.org/10.1016/j.compind.2021.103404>.
5. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности, 2018. №1. С. 1–29. URL: <http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf> (дата обращения: 01.04.2021). DOI: <http://dx.doi.org/10.24411/2410-9916-2018-10101>.
6. Stefan Bauer, Edward W.N. Bernroider, Katharina Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, Computers & Security. Vol. 68, 2017. P. 145–159, ISSN 0167-4048. DOI: <https://doi.org/10.1016/j.cose.2017.04.009>.
7. Nelli V. Syreyschikova, Danil Yu. Pimenov, Tadeusz Mikolajczyk, Liviu Moldovan, Information Safety Process Development According to ISO 27001 for an Industrial Enterprise, Procedia Manufacturing. Vol. 32, 2019. P. 278–285. ISSN 2351-9789. DOI: <https://doi.org/10.1016/j.promfg.2019.02.215>.
8. Oladko V.S The Model of Information Security Audit in the Information Systems of E-Commerce Type of B2E // Sochi Journal of Economy, 2016. Vol. 4, Issue 2. P. 117–126. URL: <https://www.elibrary.ru/item.asp?id=26747087> (дата обращения: 01.04.2021).
9. Воеводин В.А. Эталонная модель аудита информационной безопасности // Информатика, вычислительная техника и управление, серия «Естественные и технические науки», 2019. №9. С. 56–61. URL: <http://www.nauteh-journal.ru/files/718b40fd-8a0d-4d9b-ace4-c9f2c25cbb98> (дата обращения: 12.08.2021).
10. Liudmila Liutsko, Josep Maria Tous, Aleksander Veraksa, Sergey Leonov, Proprioceptive Indicators (Precision, Speed and Personality) of Age-depended Differences for Traffic Security, Procedia - Social and Behavioral Sciences, Volume 187, 2015. P. 491–496. ISSN 1877-0428. DOI: <https://doi.org/10.1016/j.sbspro.2015.03.092>.
11. Dontsov A.I., Drozdova A.V., Gritskov Y.V. Visual Culture and Personality Psychological Security, Procedia - Social and Behavioral Sciences. Vol. 86, 2013. P. 70–75. ISSN 1877-0428. DOI: <https://doi.org/10.1016/j.sbspro.2013.08.527>.
12. Дураковский А.П., Петров В.Р. О защите персональных данных в СКУД. Безопасность информационных технологий, [S.I.], Т. 19, № 1. С. 95–97, 2013. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/547>.
13. Сиротский А.А. Исследование угроз и организация менеджмента информационной безопасности в финансово-кредитных организациях // Информационные технологии. Радиоэлектроника.

- Телекоммуникации (ITRT-2016): сб. статей VI международной заочной научно-технической конференции. Ч.2. / Поволжский гос. ун-т сервиса. – Тольятти: Изд-во: ПВГУС, 2016. С. 213–221. URL: <https://ies.unitech-mo.ru/files/upload/publications/15844/a0d8c6cae8ae62dea212e274d18ba2ef.pdf> (дата обращения: 01.04.2021).
14. Бабуркина А.С., Широкова С.В., Ильяшенко О.Ю. Разработка процедуры проведения аудита безопасности информационной системы для ООО «Клиника современной косметологии» / Фундаментальные и прикладные исследования в области управления, экономики и торговли. Сборник трудов научной и учебно-практической конференции. СПб., 2017. С. 15–22. URL: <https://elibrary.ru/item.asp?id=29373585> pdf (дата обращения: 01.04.2021).
 15. Зефилов С.Л., Щербакова А.Ю. Оценка информационной безопасности объекта при проведении аудита информационной безопасности / Информационные системы и технологии ИСТ-2020. Сборник материалов XXVI Международной научно-технической конференции. Нижегородский государственный технический университет им. Р.Е. Алексеева. Н. Новгород, 2020. С. 517–522.
 16. Лившиц И.И. Методика определения активов при внедрении и сертификации СМИБ в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001-2006 и СТО Газпром серии 4.2 // Вопросы защиты информации, 2015. № 4(111). С. 43–51. URL: <https://elibrary.ru/item.asp?id=25484325> pdf (дата обращения: 01.04.2021).
 17. A.J. Burns, Clay Posey, Tom L. Roberts, Paul Benjamin Lowry, Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals, *Computers in Human Behavior*. Vol. 68, 2017. P. 190–209. ISSN 0747-5632. DOI: <https://doi.org/10.1016/j.chb.2016.11.018>.
 18. Ткачева А.Ю., Вигдорчик И.Э., Дубовик А.И. Аудит информационной безопасности и материально-техническое обеспечение ОВД как меры обеспечения информационной безопасности в ОВД // Успехи современной науки, 2016. №10. Т. 2. С. 102–104. URL: <https://elibrary.ru/item.asp?id=27433173> pdf (дата обращения: 01.04.2021).

REFERENCES:

- [1] Sirotskiy A.A. Metric approach to assessing information security in banking organizations. *Sistemy bezopasnosti*, 2016. No. 25. P. 126–129. URL: <https://www.elibrary.ru/item.asp?id=28884138> (accessed: 01.04.2021) (in Russian).
- [2] Kurilo A.P. et al. Construction of Structure of Indicators of Efficiency of Counteraction to Threats of Information Safety in Interests of the Estimation of Security of Information Processes in Computer Systems. *IT Security (Russia)*, [S.l.]. Vol. 17, no. 2. P. 16–18, 2010. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/720> (accessed: 01.04.2021) (in Russian).
- [3] Sirotskiy A.A. Technologies of competitive management of engineering enterprises. *Uchenye zapiski RSSU*, 2013. No. 5. Vol. 2. P. 177–181. URL: <https://www.elibrary.ru/item.asp?id=21408309> (accessed: 01.04.2021) (in Russian).
- [4] Hajo A. Reijers, Business Process Management: The evolution of a discipline, *Computers in Industry*, Vol. 126, 2021, 103404, ISSN 0166-3615. DOI: <https://doi.org/10.1016/j.compind.2021.103404>.
- [5] Makarenko S.I. Information security audit: milestones, conceptual framework, classification of activities. *Sistemy upravleniya, svyazi i bezopasnosti*, 2018. No. 1. P. 1–29. URL: <http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf> (accessed: 01.04.2021). DOI: <http://dx.doi.org/10.24411/2410-9916-2018-10101> (in Russian).
- [6] Stefan Bauer, Edward W.N. Bernroider, Katharina Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, *Computers & Security*. Vol. 68, 2017. P. 145–159, ISSN 0167-4048. DOI: <https://doi.org/10.1016/j.cose.2017.04.009>.
- [7] Nelli V. Syreishchikova, Danil Yu. Pimenov, Tadeusz Mikolajczyk, Liviu Moldovan, Information Safety Process Development According to ISO 27001 for an Industrial Enterprise, *Procedia Manufacturing*. Vol. 32, 2019. P. 278–285. ISSN 2351-9789. DOI: <https://doi.org/10.1016/j.promfg.2019.02.215>.
- [8] Oladko V.S. The Model of Information Security Audit in the Information Systems of E-Commerce Type of B2E. *Sochi Journal of Economy*, 2016. Vol. 4, Issue 2. P. 117–126. URL: <https://www.elibrary.ru/item.asp?id=26747087> (accessed: 01.04.2021).
- [9] Voevodin V.A. Reference model of information security audit. *Computer Science, computer engineering and management, series "Natural and Technical Sciences"*, 2019. No. 9. P. 56–61. URL: <http://www.nauteh-journal.ru/files/718b40fd-8a0d-4d9b-ace4-c9f2c25cbb98> (accessed: 12.08.2021) (in Russian).
- [10] Liudmila Liutsko, Josep Maria Tous, Aleksander Veraksa, Sergey Leonov, Proprioceptive Indicators (Precision, Speed and Personality) of Age-depended Differences for Traffic Security, *Procedia - Social and Behavioral Sciences*. Vol. 187, 2015. P. 491–496, ISSN 1877-0428. DOI: <https://doi.org/10.1016/j.sbspro.2015.03.092>.

- [11] Dontsov A.I., Drozdova A.V., Gritskov Y.V. Visual Culture and Personality Psychological Security, *Procedia - Social and Behavioral Sciences*. Vol. 86, 2013. P. 70–75. ISSN 1877-0428. DOI: <https://doi.org/10.1016/j.sbspro.2013.08.527>.
- [12] Durakovskiy A.P., Petrov V.R. On the Protection of Personal Data in the Access Control System. *IT Security (Russia)*, [S.l.]. Vol. 19, no. 1. P. 95–97, 2013. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/547> (in Russian).
- [13] Sirotskiy A.A. Threat Research and Organization of Information Security Management in Financial and Credit Organizations. *Informacionnye tehnologii. Radioelektronika. Telekommunikacii (ITRT-2016): Articles of the VI International Correspondence Scientific and Technical Conference*. Vol. 2. Povolzhskiy gos. Un-t servisa. – Toliatti: PVGUS, 2016. P. 213–221. URL: <https://ies.unitech-mo.ru/files/upload/publications/15844/a0d8c6cae8ae62dea212e274d18ba2ef.pdf> (accessed: 01.04.2021) (in Russian).
- [14] Baburkina A.S., Shirokova S.V., Ilyashenko O.Yu. Development of procedure of information system security audit for ООО "Clinic of modern cosmetology". *Fundamentalnye i prikladnye issledovaniya v oblasti upravleniya, ekonomiki i trgovli*. Collection of works of scientific and educational-practical conference. SPb., 2017. P. 15–22. URL: <https://elibrary.ru/item.asp?id=29373585> (accessed: 01.04.2021) (in Russian).
- [15] Zefirov S.L., Scherbakova A.Yu. Assessment of information security of an object during an information security audit / *Informacionnye sistemy i tehnologii IST-2020*. Collection of materials of the XXVI International Scientific and Technical Conference. Nizhny Novgorod State Technical University named after R.E. Alekseev. N. Novgorod, 2020. P. 517–522 (in Russian).
- [16] Livshits I. I. Methods of assets determination for ISMS implementation and certification in accordance with the requirements GOST R ISO/IEC 27001-2006 and STO Gazprom series 4.2. *Voprosy zaschity informacii*, 2015. № 4(111). P. 43–51. URL: <https://elibrary.ru/item.asp?id=25484325> (accessed: 01.04.2021) (in Russian).
- [17] A.J. Burns, Clay Posey, Tom L. Roberts, Paul Benjamin Lowry, Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals, *Computers in Human Behavior*. Vol. 68, 2017. P. 190–209, ISSN 0747-5632. DOI: <https://doi.org/10.1016/j.chb.2016.11.018>.
- [18] Tkacheva A.Yu., Vigdorchik I.E., Dubovik A.I. Information security audit and OVD logistics as information security measures in OVD. *Uspehi sovremennoi nauki*, 2016. No. 10. Vol.2. P. 102–104. URL: <https://elibrary.ru/item.asp?id=27433173> (accessed: 01.04.2021) (in Russian).

Поступила в редакцию – 08 апреля 2021 г. Окончательный вариант – 25 Августа 2021.
Received – April 08, 2021. The final version – August 25, 2021.