УДК 004.094 **DOI** 10.15622/sp.2020.19.2.6

И.И. Лившиц

МЕТОД ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ИТ-КОМПОНЕНТ ПО КРИТЕРИЯМ СУЩЕСТВУЮЩИХ СТАНДАРТОВ

Лившиц И.И. **Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов.**

Аннотация. Приводится анализ известных методов обеспечения информационной безопасности, рассматриваются методы оценивания безопасности как отдельных ИТ-компонент, так и облачных сервисов в целом.

Предпринята попытка проанализировать облачные сервисы не с позиции коммерчески успешного и популярного маркетингового продукта, а с позиции системного анализа. Введенный ранее порядок оценивания ИТ-компонент нестабилен, поскольку у конечного пользователя нет 100% гарантии доступа ко всем ИТ-компонентам, а тем более к компонентам удаленного и неподконтрольного облачного сервиса. В ряде обзоров отмечается рост усилий по созданию сетевой безопасной архитектуры и по обеспечению непрерывного контроля отклонений от установленных бизнес-целей. В отличие от моделей Zero Trust и Zero Trust eXtended, согласно которым на существующие ИТ-компоненты накладываются дополнительные функции безопасности, предлагается рассматривать совокупность ИТ-компонент как новую сущность – систему обработки информации. Это позволит перейти к формальным процессам оценивания степени соответствия по критериям стандартов как для существующих, так и для перспективных ИТ-компонент при обеспечении безопасности облачных сервисов.

Предложен новый метод оценивания на базе ранее разработанной гибридной методики с использованием формальных процедур, основанных на двух системах критериев – оценивании степени соответствия систем менеджмента (на базе ИСО/МЭК серии 27001) и оценивании требований функциональной безопасности (на базе МЭК серии 61508 и ИСО/МЭК серии 15408). Этот метод дает воспроизводимые и объективные оценки рисков безопасности облачных ИТ-компонент, которые могут быть предъявлены для проверки независимой группе оценщиков. Полученные результаты возможно применить для защиты объектов критической информационной инфраструктуры.

Ключевые слова: система менеджмента, риск, информационная технология, информационная безопасность, аудит, стандарт, экспертиза, оценивание.

1. Введение. В последние годы количество угроз информационной безопасности (ИБ) значительно возросло, и в этой связи малоизученная проблема оперативного оценивания безопасности информационных технологий (ИТ) для различных объектов критической информационной инфраструктуры (КИИ) становится особенно актуальной [1-3]. Очевидно, это обстоятельство справедливо и для ИТ-компонент, размещенных или планируемых для размещения в облаке [4-6]. Проблема оценивания для такого класса объектов КИИ должна решаться в соответствии с установленными требованиями (например, ФЗ-187, постановление Правительства

№ 127, приказы ФСТЭК России № 235 и № 239), а также с использованием соответствующих процессов, позволяющих выполнять аудит безопасности требуемых ИТ-компонент на соответствующих уровнях [7, 8], и в том числе на уровне программного обеспечения (ПО) [9].

В отличие от известных моделей Zero Trust и Zero Trust eXtended, в которых на существующие ИТ-компоненты накладываются дополнительные функции безопасности (ФБ), в предложенной модели рассматривается совокупность таких ИТ-компонент в составе КИИ, как новая сущность, – система обработки информации (СОИ) [10, 11]. В этом случае появляется возможность облачных сервисов оптимизировать затраты путем использования уже существующих и практически отработанных ФБ в составе СОИ. Для облачных компонент эффективным решением будет оценивание уже имеющегося уровня безопасности в ИТ-компонентах, обусловленного существующей архитектурой СОИ и полученного в результате сочетания ИТ-компонентов и ФБ. По итогам оценивания возможно принятие обоснованного и объективного решения о реализации новых и/или дополнительных ФБ (в том числе для КИИ) [10, 11]. Целью данной статьи является разработка нового метода оценивания на базе предложенной ранее гибридной методики с использованием формальных процедур, основанных на двух системах критериев – оценивании степени соответствия систем менеджмента (на базе ИСО/МЭК серии 27001) и оценивании требований функциональной безопасности (на базе МЭК серии 61508 и ИСО/МЭК серии 15408). Основным результатом является новый метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов.

2. Обзор существующих методов. Важным аспектом для бизнес-заказчиков являются гарантии обеспечения заданного уровня ИБ для различных типов ИТ-компонент [12, 13]. В частности, критичным может оказаться недостаточный контроль предоставления доступа к различным видам облачных хранилищ корпоративных данных [14, 15]. В существующих решениях по сетевой безопасности учтены требования бизнеса к внутренним зашифрованным коммуникациям, сетевой сегментации и детальному мониторингу [16-18]. В [19] отражены решения для интероперабельности и способности проводить измерения стандартными процедурами, обеспечивающими непрерывный контроль отклонений от установленных бизнес-целей. В [20] показан характерный пример недостаточного контроля имеющихся ФБ, заключающийся в ошибках конфигурации из-за низкой квалификации системных администраторов, что приводит к

неавторизованному доступу. Процесс оценивания можно рассмотреть с позиции значимости отечественного сегмента рынка ИТ-компонентов по сравнению с мировыми тенденциями и оценить объем новых технологий, которые могут быть успешно применены в России. Например, представлена оценка Gartner и IDC [21], что весь ИТ-рынок России составляет примерно 2% от мирового, а сегмент ИТ-услуг занимает только 0,5% от общего объема. Отчасти этот незначительный уровень является не только отражением способности оценить (в том числе и в аспекте ИБ) новые облачные сервисы, как было показано на примере нормативно-методических документов (НМД) ФСТЭК, но он также связан с проблемами квалификации обслуживающего персонала.

В аналитическом обзоре [22] отмечается, что атаки осуществляются через бреши в обороне, которые в основном появляются в связи с расширением Интернета вещей (IoT) и незащищенными технологиями при использовании облачных сервисов. Соответственно, совокупное применение небезопасных «модных» технологий IoT и активно рекламируемых как панацея, но недоверенных облачных сервисов, может привести к появлению еще большего количества комбинаций для компрометации ИТ-компонент, особенно на объектах КИИ. Следует учесть, что любые ИТ могут выступать как инструментом бизнеса, так и оружием против него в том случае, если они не прошли в установленном порядке процесс оценивания безопасности. Это предположение подтверждается фактами, что злоумышленникам удается для преодоления защитных функций применять в качестве инструмента облачные сервисы и другие ИТ-компоненты, используемые в легитимных целях [23]. В [23] показано, что вместо настройки серверов с шифрованием, злоумышленники используют SSL-сертификат легитимного сервиса, приобретение которого в настоящее время не является проблемой. В данном случае для противодействия данной атаке, использующей легитимные сервисы, применяют следующие факторы: частый обмен сертификатами с легитимными сервисами и выявление большого объема образцов, попадающих в «песочницу» в связи с подозрительными DNS-обращениями на легитимные сервисы. Но, к сожалению, в этой работе не предложены идеи и примеры практической реализации. В технической литературе достаточно негативных примеров слабой реализации защитных механизмов [24]. Отметим, что лидерство по утечкам из облачных хранилищ несколько лет подряд удерживает «Amazon» (рис. 1).

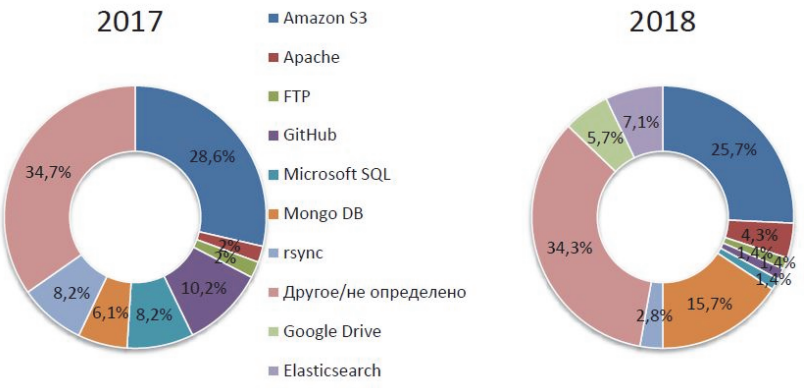

Рис. 1. Распределение скомпрометированных облачных хранилищ [24]

Вопросы измерения и мониторинга безопасности ИТ-компонент рассмотрены в отчете [25]. В частности, приведен ряд барьеров, препятствующих созданию эффективных центров оперативного реагирования на инциденты ИБ (Security Operation Centers, SOC). Отметим аспекты, которые позволяют определять вероятности преодоления защиты с позиции облачных сервисов:

– нехватка квалифицированного персонала;
– отсутствие интеграции между ИТ-компонентами;
– недостаточная поддержка руководства;
– недостаточное документирование процессов;
– отсутствие кооперации между службами;
– недостаточное выполнение требований регуляторов.

Таким образом, можно предположить, насколько сложно обеспечить измерение и мониторинг достижения установленных метрик ИБ для потенциально небезопасных облачных сервисов, если даже для собственных SOC, с учетом известной практики, эксперты признают ряд серьезных проблем [4, 18, 26]. В [27] отмечается важность и приоритетность автоматизации функций ИБ (более 57%), что значительно увеличивает риски при внедрении новых ИТ. В этом отчете отмечено, что новые ИТ-компоненты добавляются стихийно, а времени на обучение сотрудников и изучения функционала не хватает.

Следует полагать с высокой вероятностью, что в обеспечении безопасности предприятия постоянно появляются серьезные пробелы [28]. В отчете [23] приведено исследование базы, содержащей более 150 тыс. пользователей. Исследование выявило, что всего 0,5% пользователей совершают подозрительные действия. Показано, что эта

мизерная группа смогла скачать 3,9 млн. документов из корпоративных облачных систем (в среднем, более 5 тыс. документов на пользователя за 1,5 месяца), при этом примерно 60% скачиваний выполнено в рабочие часы, а 40% – в выходные. Далее, в том же отчете показано, что 27% специалистов по информационной безопасности используют внешние частные облака (этот показатель стабильно растет в течение 3-х лет), а 52% сообщили, что их сети размещены на локальном частном облаке. Из организаций, использующих облачные сервисы, 35% размещают в облаке от 50% до 74% своей инфраструктуры (рис. 2).

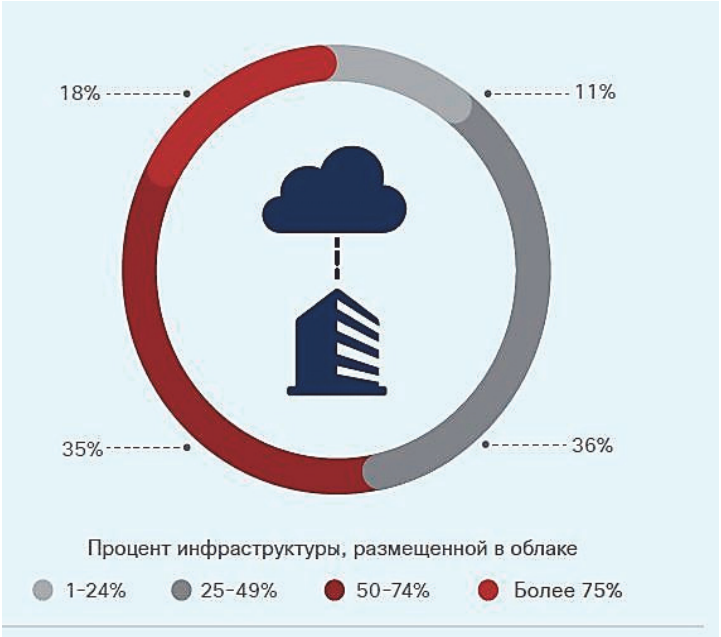

Рис. 2. Размещение инфраструктуры организаций в облаке [23]

Очевидно, следует задаться вопросом – а как же обеспечивается безопасность ИТ-компонент при таком широком распространении частных облаков для бизнес-заказчиков? Следующий вопрос – как именно обеспечивается в бизнесе соответствие заданного уровня ИБ для конкретных приложений, перенесенных в облако? Обратимся к факту, согласно которому бизнес-заказчики чаще всего называют ключевым преимуществом именно безопасность размещения своей ИТ-инфраструктуры в облаке. Например, по данным [23], около 57%

клиентов предпочитают размещать в облаке свои критичные ИТ-активы из-за более высокого уровня защиты данных; 48% – из-за масштабируемости, а 46% – из-за удобства использования. Тем не менее часть критической инфраструктуры может остаться в будущем под управлением собственных ИТ (ИБ) служб. Как показано в [29], полностью корпоративные центры обработки данных (ЦОД) не исчезнут, и часть компаний будет размещать критически важные бизнес-процессы (рис. 3) на своей контролируемой территории.

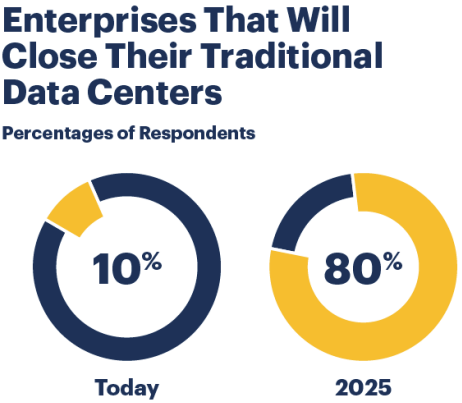

Рис. 3. Прогноз сокращения собственных дата-центров [29]

Следует отметить, что эта часть компаний (сегодня – 10 %, а в перспективе примерно 20%) весьма обеспокоена обеспечением необходимого для собственных бизнес-процессов уровня безопасности и не готова доверять облачным провайдерам ни при каких соглашениях (Service Level Agreement, SLA).

Известная модель Zero Trust, так же, как и расширенная модель – Zero Trust eXtended (ZTX) [30], является реализацией принципа «Доверяй, но проверяй». Модель предполагает, что к действиям пользователя, находящегося внутри периметра корпоративной сети, надо относиться так же подозрительно, как и к действиям того, кто запрашивает доступ к этой сети извне. Эта модель включает [31] валидацию устройств, оценивание контекста для пользователя, авторизацию доступа, верификацию сети, выявление угроз и восстановление устойчивости перед предоставлением доступа устройств или пользователей. Следует отметить, что хотя о концепции Zero Trust говорится в мире достаточно давно (более 5 лет), нигде документально не показано, как обеспечивается безопасность в облаке.

Бизнес должен получить доказательство невозможности какой-либо утечки информации изнутри облачных сервисов на базе формализации настроек сетевой безопасности [32-34]. Значительным преимуществом для бизнеса может оказаться система [35] из 15 критериев. По оценкам [36], бизнес готов реагировать на инициативу Zero-trust policies в двух основных аспектах: в области обнаружения и идентификации атак (более 80% опрошенных экспертов) и в области снижения поверхности атак (более 50% опрошенных экспертов). Процесс обеспечения ИБ облачных технологий является заботой экспертов почти всех крупных компаний, поскольку статистические данные, экспертные отчеты и публичные аналитические доклады не дают гарантий спокойствия [11, 12]. Даже в таком важном для любого эксперта ИБ вопросе, как обеспечение государственной тайны, к сожалению, есть серьезные проблемы. Как показано в отчете компании «InfoWatch» [24], в России в 2017 году в общем объеме утечек данных из облачных сервисов почти 7% составила информация, отнесенная к государственной тайне (рис. 4).

Рис. 4. Анализ утечек данных из облачных серверов [24]

Если на объекте нет «внятной» системы ИБ, то чувствительные данные, и, как показал пример выше, даже сведения, отнесенные к государственной тайне, могут беспрепятственно покинуть периметр облака, особенно если служба ИБ не знает или не может обеспечить требуемый уровень безопасности. К сожалению, ни ФСТЭК России, ни ФСБ России в данный момент не могут предоставить действенные процессы оценивания уровня ИБ в облаке, а существующие НМД по аттестации объектов информатизации не применимы. Приведем статистику (рис. 5), согласно которой примерно 20% компаний разрабатывают для оценки соответствия заданным критериям безопасности собственный фреймворк, еще примерно 20%

комбинируют компоненты иных способов экспертизы, а 23% используют стандарты (NIST, ITIL и пр.).

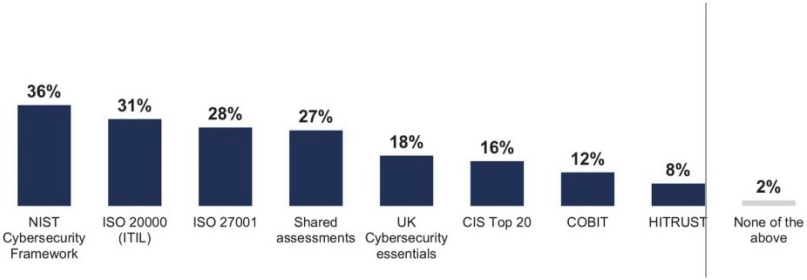

Рис. 5. Статистика использования способов экспертизы [29]

Перейдем теперь к практике в Российской Федерации. Например, в [37] указано требование к проверке (Приложение 2, подпункт 2.5.5.1), в котором определено, что оператору для переводов денежных средств необходимо использовать программное обеспечение (ПО), сертифицированное ФСТЭК, или ПО, в отношении которого проведен анализ уязвимостей по требованиям к оценочному уровню доверия (ОУД). При этом точно определено, что уровень доверия должен быть не ниже, чем ОУД 4 в соответствии с требованиями ISO/IEC 15408 [38-40]. В указанном стандарте установлены требования для ОУД 4, в частности обеспечение доверия на основе формирования задания по безопасности (ЗБ) и посредством анализа выполнения ФБ из данного ЗБ. Анализ выполнения ФБ предусматривает предоставление функциональной спецификации, полной спецификации интерфейсов, руководств, описания базового проекта для объекта оценки (ОО), а также подмножества реализации для понимания режима безопасности (таблица 1).

Таблица 1. Оценочный уровень доверия ОУД 4

Класс доверия	Компоненты доверия
ALC: Поддержка жизненного цикла	ALC_CMC.4 Поддержка производства, процедуры приемки и автоматизации
	ALC_CMS.4 Охват УК отслеживания проблем
	ALC_DEL.1 Процедуры поставки
	ALC_DVS.1 Идентификация мер безопасности
	ALC_LCD.1 Определенная разработчиком модель ЖЦ
	ALC_TAT.1 Полностью определенные инструментальные средства разработки

Известно, что ОУД 4 представляет значительное увеличение степени доверия по сравнению с ОУД 3, требуя более детальное

описание проекта, реализации для всех функций безопасности объекта (ФБО) и улучшенные механизмы и/или процедуры, что дает уверенность в том, что в ОО не будут внесены искажения во время разработки [40]. Следует отметить, что в класс доверия ACL включены компоненты ALC_DVS.1 и ALC_LCD.1, что устанавливает требования по идентификации мер безопасности и наличие определенной разработчиком модели жизненного цикла (ЖЦ). Эти два компонента применены в оценивании безопасности ИТ-компонент в облаке.

3. Постановка задачи. В качестве исходных данных рассматриваются существующие виды экспертиз, которые могут быть применены в процессе оценивания безопасности ИТ-компонент. Как показано в [11], проблема получения *оценки соответствия* (в формулировке стандартов ISO/IEC [38-40] – оценка соответствия установленным критериям безопасности) в определенной предметной области может быть решена при наличии определенного количества экспертиз (таблица 2).

Таблица 2. Типы экспертиз для получения результатов процесса оценивания соответствия установленным критериям

Наименование типа экспертизы	Достоинства	Недостатки
Индивидуальная экспертиза (ИЭ)	Оперативно, конфиденциально, просто	Низкая объективность и достоверность
Шаблонная экспертиза (ШЭ)	Требования доступны и стандартизированы	Значительная погрешность в силу слишком большого обобщения требований
Расчетная экспертиза (РЭ)	Точность, обусловленная квалифицированным выбором методик измерения и современным уровнем инженерных и научных задач	Требуется высокая квалификация для выбора методики измерения и интерпретации результатов

Графически пространство исходных комбинаций экспертиз можно представить в виде треугольника (рис. 6).

Как показывает практика [41, 42], значительное количество проблемных вопросов может быть успешно решено как при использовании одной экспертизы, так и произвольной их комбинации. Например, для многих заказчиков вполне достаточно только ШЭ (на соответствие, например, НМД ФСТЭК России) или только ИЭ (например, для создания различных программных компонент, к которым изначально не предъявляются требования оценивания

соответствия [9]). Проблема заключается в поиске сочетания экспертиз, обеспечивающего взаимную компенсацию недостатков и максимальное усиление достоинств. Вершины треугольника символизируют полюса экспертиз (см. рис. 6). Точка «Б» внутри треугольника либо точка «А» на его стороне символизируют некоторое частное предпочтительное сочетание экспертиз.

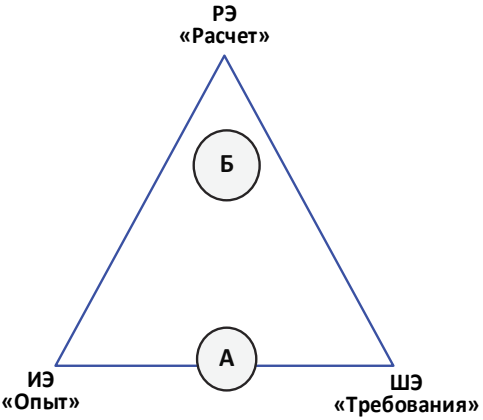

Рис. 6. Схема экспертиз оценки соответствия

Легко заметить, что подавляющее большинство проект ов (работ) в области создания защищенных ИТ проходят экспертизу ИЭ, и лишь некоторые демонстрируют результаты прохождения ШЭ. Этот вывод, высказанный ранее [10, 11], можно подтвердить доступными актуальными данными: в частности, в отчете [2] показано, что организации, внедряющие изначально безопасность в ЖЦ ПО, демонстрируют лучшие результаты в обеспечении ИБ. Такие же данные приводятся в отчете [43] о формальном соответствии требованиям известных стандартов ISO/IEC. В простейшем случае ШЭ выполняется по требованиям ФСТЭК России и/или ФСБ России, для более серьезных проектов ШЭ выполняется по требованиям функциональной безопасности (Safety Integrity Level, SIL) дополнительно [44-46]. Точку сочетания экспертиз технически необходимо сдвинуть со стороны ИЭ-ШЭ внутрь треугольника в направлении вершины РЭ (точка «Б»), добавив точный расчет и формируя область оптимума для конкретных применений (рис. 7).

В качестве критериев предлагается рассматривать существующие международные стандарты ISO и/или ISO/IEC и их национальные аналоги в системе ГОСТ Р. С учетом исходных данных,

эти критерии можно сопоставить по рассмотренным выше полюсам. Состояние российских ИЭ и ШЭ, к сожалению, далеко от необходимого уровня, диктуемого современными вызовами противоборствующих сторон, в том числе для рассматриваемых облачных сервисов. Именно поэтому для России очень важна «подвижка» точки сочетания экспертиз от стороны треугольника ИЭ-ШЭ в направлении вершины РЭ. Для этой цели в России могут применяться национальные ГОСТ Р ИСО/МЭК, для наполнения полюса ШЭ:

– ISO/IEC серии 15408 [38-40];
– ISO/IEC серии 27001 [47];
– ISO/IEC серии 27005 [48].

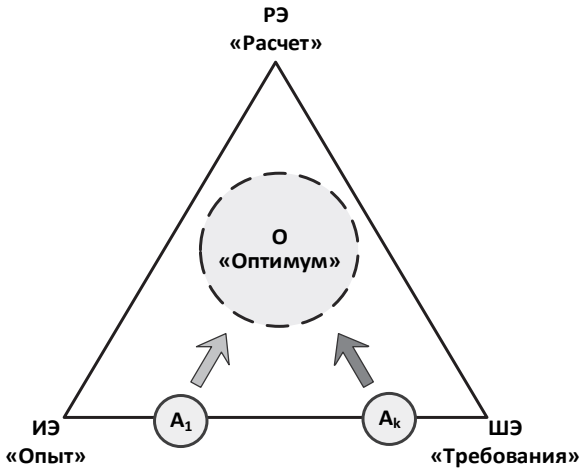

Рис. 7. Поиск оптимума видов экспертиз

Необходимо отметить, что ISO/IEC серии 15408 может быть использован не только для полюса ШЭ, но и для полюса РЭ, что обусловлено достаточно мелкой ценой деления и заложенной возможностью практически любой адаптации различных множеств требований ФБ и требований доверия к безопасности под текущие потребности для конкретных решений (рис. 8).

Отметим сопоставление нотаций ИСО/МЭК 27001 и ИСО/МЭК 15408 – почти по всем основным сущностям (объект, состав, риски, меры защиты) наблюдаются аналогии, что может быть эффективно применено на практике при выполнении оценки соответствия установленным критериям.

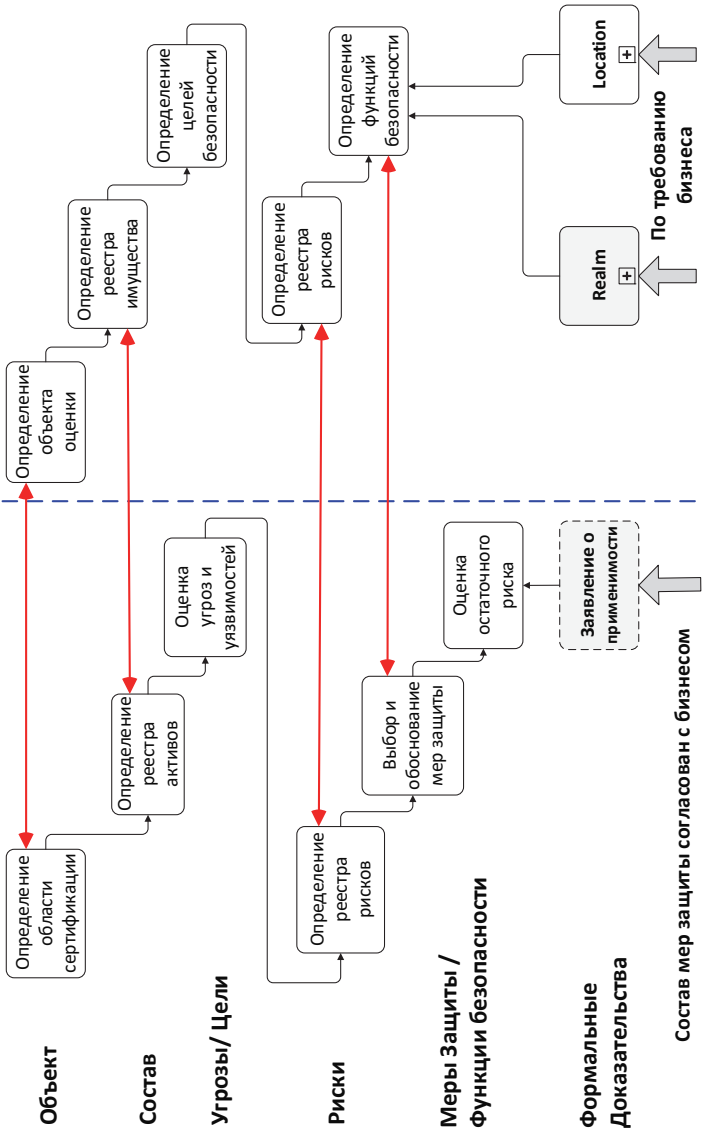

Рис. 8. Сопоставление компонент ИСО/МЭК 27001 и ИСО/МЭК 15408

В качестве ограничений, прежде всего, рассматриваются ограничения множества ФБ, которые могут быть выбраны из существующих стандартов и применены для обеспечения безопасности ИТ-компонент, ограничения компетенций привлекаемых экспертов для получения достоверных результатов процесса оценивания соответствия установленным критериям и ограничения времени, установленные в ряде НМД для оценки значимых объектов КИИ. В качестве двух важнейших допущений рассматриваются возможность метода формировать воспроизводимые и объективные оценки рисков безопасности для облачных ИТ-компонент, которые могут быть предъявлены для проверки независимой группе оценщиков, и возможность надежной и независимой верификации данных статистики по ряду проектов для оценки априорных вероятностей угроз ИБ.

4. Описание метода. В предлагаемом методе оценивания безопасности облачных ИТ-компонент вероятности реализации угроз ИБ исчисляются на основании статистических данных, в отличие от установленных в НМД России. Соответственно, в существующих НМД России не обеспечивается логическая цепочка зависимости от сформированного исходного множества угроз ИБ, полученных далее оценок актуальности этих угроз ИБ, результативности применения рекомендованных средств защиты информации (в том числе сертифицированных), до принятия финального решения об общем уровне обеспечения безопасности ИТ. В новом методе оценивания безопасности облачных ИТ-компонент предполагается рассмотрение ОО как функционирующего в установленных границах (Trusted boundaries, ТВ), определяемых на модели СОИ. Именно ТВ ставятся в соответствие, с одной стороны, требования ФБ, требования доверия к безопасности [38-40] и требования к менеджменту ИБ [37, 47] (таблица 3), а с другой стороны, СОИ, в которых реализуются ТВ.

В новом методе оценивания безопасности облачных ИТ-компонент дополнительно могут быть включены требования ФБ (таблица 4). Отметим, что дополнение мер обеспечения ИБ из ISO/IEC серии 27001 [47] требованиями ФБ из IEC серии 61508 ([44-46]) позволяет оценить аспекты безопасности применяемых ИТ-компонент по всей вертикали стека ISO/OSI.

Таблица 3. Меры обеспечения ИБ для облачных сервисов

ISO/IEC 27001 (Приложение А)	Наименование меры обеспечения ИБ
A.6.1.1	Роли и ответственность в рамках ИБ
A.7.1.1	Проверка благонадежности
A.7.2.2	Осведомленность по ИБ, обучение и инструктажи
A.8.1.1	Инвентаризация активов
A.8.2.3	Приемлемое использование активов
A.9.2.2	Инициализация доступа пользователя
A.9.4.1	Ограничение доступа к информации
A.10.1.1	Политика использования средств криптографии
A.11.2.4	Техническое обслуживание оборудования
A.12.1.2	Управление изменениями
A.12.1.3	Управление мощностями
A.12.3.1	Резервируемая информация
A.13.2.4	Соглашение о неразглашении информации
A.16.1.2	Оповещение о событиях ИБ
A.16.1.5	Реагирование на инциденты ИБ
A.17.1.2	Внедрение непрерывности ИБ
A.18.2.1	Независимый пересмотр (аудит) ИБ
A.18.2.2	Соответствие политикам безопасности и стандартам
A.18.2.3	Проверка соответствия техническим требованиям

Таблица 4. Требования функциональной безопасности для облачных сервисов

№	Стандарт	Требование
1.	п. 1.2 g) 61508-1	Спецификации требований безопасности систем, связанных с безопасностью, могли быть определены на основе систематического анализа рисков
2.	п. 6.2.1 61508-1	Организация, ответственная за систему, связанную с безопасностью, или за одну или несколько стадий ЖЦ всей системы безопасности, должна выделить … сотрудников, несущих полную ответственность за: – координацию действий, связанных с безопасностью, которые выполняются на этих стадиях; – взаимодействие между этими стадиями и другими стадиями, выполняемыми другими организациями; – удостоверение того, что функциональная безопасность достигнута и продемонстрировано соответствие целям и требованиям настоящего стандарта

Продолжение таблицы 4.

3.	п. 6.2.14 61508-1	Соответствие компетентности должно рассматриваться для конкретной области применения с учетом всех факторов, включая: – возможные последствия в случае отказа систем, связанных с безопасностью; – уровни полноты безопасности систем, связанных с безопасностью; – инженерные знания в области безопасности, соответствующие применяемой технологии; – знание законодательной базы и нормативно-правовой базы в области безопасности
4.	п. 7.3.2.2 61508-2	При планировании подтверждения соответствия системы, связанной с безопасностью, должны быть использованы: – требования, определенные в спецификации требований к системе безопасности и в спецификации требований к проектированию системы; – процедуры, применяемые для подтверждения соответствия полноте безопасности каждой функции безопасности по критериям «прошла испытания/не прошла испытания»; – процедуры оценочных испытаний (с обоснованиями)
5.	п. 7.4.8.2 61508-3	Проверки интеграции системы ПО должны определять: – контрольные примеры и контрольные данные; – типы проверок, которые должны быть проведены; – условия тестирования, конфигурацию и программы; – условия, при которых проверка считается выполненной; – процедуры, которые необходимо выполнить, если проверка дала отрицательный результат

Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов предусматривает последовательность следующих этапов:

– структурирование ИТ, при этом выполняется структурирование всей совокупности ИТ-компонент, обеспечивающих автоматизацию бизнес-процессов, на несколько областей (R);

– структурирование физического пространства, при этом выполняется структурирование пространства, занимаемого ИТ-компонентами, на несколько локаций (L);

– формирование модели СОИ, при этом определяется необходимое количество моделей;

– определение проблемы безопасности, при этом последовательно определяются угрозы ИБ, политики безопасности и предположения безопасности для заданной среды функционирования;

– определение целей безопасности, при этом предоставляется краткое изложение предполагаемого решения проблемы, определенной ранее. Обосновывается заключение, что если все цели безопасности достигнуты, то ранее определенная проблема безопасности решена, всем выявленным угрозам обеспечено эффективное противостояние, а предположения безопасности реализованы.

Угрозы, которым должна противостоять СОИ, определяются по реестру рисков (например, по возрастанию значимости [48]). Реестр рисков либо формируется по модели СОИ, либо используется уже существующий в организации [42, 49]. Однако следует принять во внимание, что объемные каталоги и таксономии сотен угроз, применение которых определено в действующих НМД регуляторов, уже не имеют практического применения, как 20-30 лет назад. В частности, это определяется незначительной долей известных уязвимостей, через которые реально можно реализовать угрозы: по данным [50], только 2-5% от всех критических уязвимостей действительно эксплуатируются в реальных атаках. Схожие данные показаны в [51]: только 5,5% уязвимостей используются в реальных атаках (из 76 тыс. багов, выявленных в период с 2009 по 2018 гг., эксплуатировались лишь около 4 тыс., и только для половины из этих 4 тыс. уязвимостей были свободно доступны эксплойты). По данным [52], доля уязвимостей, для которых реально есть эксплойты, всего лишь 1,4%. Здесь необходимо сделать отступление и акцентировать внимание на том, что угрозы определяются именно через риски вне зависимости от отраслевой принадлежности (финансы, транспорт, промышленность, здравоохранение, ИТ) [44-46]. Практикуемое в России формирование фиксированных моделей угроз ИБ свидетельствует об игнорировании международного опыта (ISO, NIST, FIPS, IATA и пр.) [53]. В результате оценивания безопасности облачных ИТ-компонент по новому методу бизнес получает документальные свидетельства достаточности и корректности контрмер [47]. Достаточность контрмер определяется в измеряемых единицах – ФБ, сопоставленных с ТВ [38-40]. Корректность контрмер определяется в измеряемых единицах – требованиях доверия к безопасности и требованиях к менеджменту ИБ, в точном соответствии с критериями существующих стандартов. Достаточные и корректные контрмеры обеспечивают минимизацию риска (остаточного риска) для активов. Таким образом, достигается «доверие через оценку». Этот процесс дает воспроизводимые и объективные свидетельства

оценивания СОИ, которые могут быть предъявлены для проверки независимой группе оценщиков, имеющих должную квалификацию. Отчет об оценивании, выраженный в измеряемых величинах, является веским аргументом в пользу безопасности ИТ-компонент, а также облачных ИТ-компонент. При этом метод оценивания безопасности облачных ИТ-компонент опирается на национальные стандарты ГОСТ Р [44-46] в России, которые соответствуют международным стандартам ISO и/или ISO/IEC. Дополнительным преимуществом использования критериев существующих стандартов является возможность оперировать отчетом оценки в интересах бизнеса в пределах и российской, и зарубежных юрисдикций.

5. Практические результаты исследования. Рассмотрим пример применения метода оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов. Известно, что заложенная в стандартах [38-40] гибкость допускает применение множества методов оценки по отношению к множеству свойств безопасности ИТ-продуктов, а также указанные стандарты позволяют существенно упростить процесс оценивания безопасности для ОО, например, при описании границ доверия (ТВ), процессов (Р), целей и предположений безопасности. На рисунке 9 представлен пример описания облачного сервиса в новой нотации, в котором указаны процессы, выполняющие обработку информации в составе СОИ и взаимодействующие либо с процессами, либо с конечными сущностями (*External Entity*, ЕЕ). Соответственно, для оценивания рисков (и остаточных рисков [47, 48]) новый метод позволяет проследить не сам отдельный факт инцидента ИБ (в действительности, только с его дискретной вероятностью и последствиями), а факт наличия в нужном месте последовательности реализованных (встроенных) ТВ для СОИ как достаточной оцениваемой преграды для инцидентов ИБ.

В данном примере показано, что в локации L4 в единой области R4.1 размещены несколько критичных процессов (Р5 – Р7) СОИ, доступ к которым предоставляется только по защищенным каналам (пара ТВ1.1 и ТВ 4.1, соответственно, в областях R1.1 и R 4.1). Обратим внимание, что указанная пара на практике может быть реализована как VPN (например, на базе российских или зарубежных решений). При этом конкретные VPN-решения для указанной пары могут иметь сертификацию (например, в системе ФСБ России или FIPS 140-2), допускать резервирование (например, основной канал – проводной и резервный – спутниковый), но описание СОИ и суть выполнения оценки через доверие от этого не меняются.

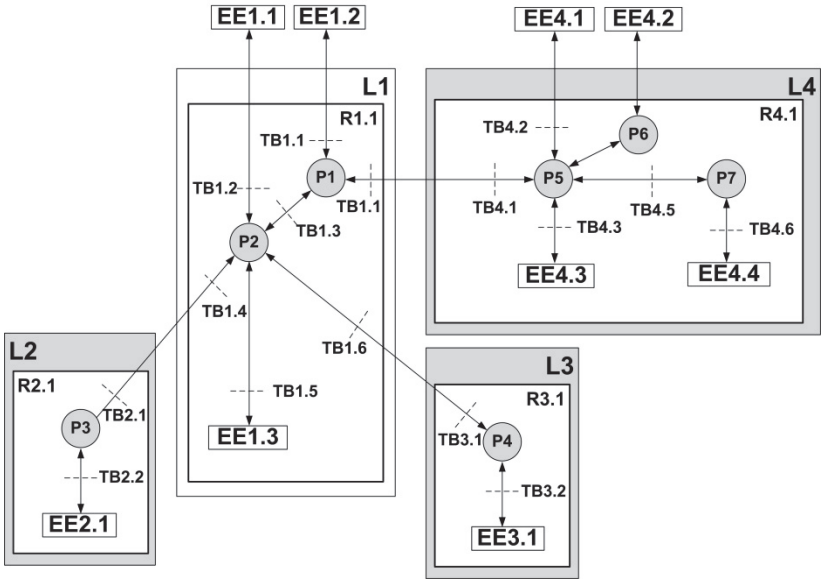

Рис. 9. Пример описания облачного сервиса

Также обратим внимание, что бизнес-заказчик может принять во внимание свои резоны при проектировании особо защищенного доступа к облачным сервисам, например обеспечивая единый доступ к провайдеру только одним внешним каналом (рассмотренная выше пара ТВ1.1 и ТВ 4.1) и реализуя собственными силами и по своим регламентам внутренние защищенные коммуникации – например, пары ТВ1.6 и ТВ 3.1 и пары ТВ1.4 и ТВ 2.1. Практически это означает применение различных программных (программно-аппаратных) решений для построения множества каналов VPN, соответствующих как национальным требованиям (сертифицированные в ФСБ России средства криптографической защиты информации), так иным криптографическим стандартам (например RSA и 3DES) для защищенных коммуникаций с зарубежными партнерами. С другой стороны, бизнес-заказчик надежно контролирует через «свои» ТВ (ТВ1.2, ТВ 1.1, ТВ 1.5, ТВ 2.2 и ТВ3.2) только «свои» ЕЕ (в частности, ЕЕ1.1, ЕЕ1.2, ЕЕ1.3, ЕЕ2.1 и ЕЕ3.1), но вынужден доверять провайдерам облачных сервисов в локации L4 в части обеспечения безопасного доступа к потенциально недоверенным ЕЕ4.1, ЕЕ4.2, ЕЕ4.3 и ЕЕ4.4. Следует предположить, что и «чужие» ЕЕ могут, в свою очередь, контролироваться далее в цепочке провайдерами других облачных сервисов в следующих потенциально недоверенных

локациях и, следовательно, необходимо учесть «эффект домино». Однако на практике такие риски хорошо идентифицируются и парируются на базе известных мер безопасности из [47, 48] и известных требований к поставщикам [44-46], что позволяет бизнесу применять SLA и формировать процедуры оценки соответствия указанным критериям. Можно отметить предположения безопасности, что все указанные EE4.* в локации L4 оснащены достаточным количеством эффективных ТВ, находящихся под определенным и разумным контролем провайдера, и это может быть объективно подтверждено в установленном порядке аудита [47].

Можно отметить, что метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов отличается важным преимуществом – возможностью вычислять априорные риски с учетом множества угроз ИБ, характерных для каждой конкретной ИТ-компоненты и в целом для СОИ. Это преимущество может быть весьма ценным и в российской юрисдикции (ФСБ России или ФСТЭК России), и в международной (ISO/IEC серии 15408 или IEC серии 61508 и/или 61511). Например, при исследовании оценок рисков безопасности для современного морского порта такими ИТ-компонентами могут быть промышленные контроллеры Honeywell котельной и очистных сооружений, станции промышленной сети Wi-Fi Huawei и прочие. Для оценивания рисков ИБ применялись компоненты «ущерб» (*size of impact*) и «вероятность» (*probability*), точно так же, как и при определении риска (остаточного риска) [47, 48]. Владелец СОИ определяет необходимый уровень детализации, в частности фиксируются ТВ, контекст, меры (средства) обеспечения ИБ и прочее. Соответственно, все оценки для СОИ формируются в расчетных (проверяемых) оценках вероятности надежной и бесперебойной работы. Например, для терминалов промышленной сети Wi-Fi могут быть определены статистические данные отказов, основанные как на данных владельца, собирающего информацию об инцидентах ИБ (FW, SIEM, IPS/IDS, SOC и пр.), так и поставщиков в данном конкретном регионе с учетом температурно-влажностного режима.

Количественная оценка рисков СОИ для одной *j*-угрозы области R_i вычисляется следующим образом:

$$R_{ij} = \frac{V_{ij}^{k} \cdot S_{ij}^{n}}{V^{max} \cdot S^{max}}, \quad (1)$$

где $V^{(k)}_{ij}$ – априорная вероятность реализации *j*-угрозы в области R_i; $S^{(n)}_{ij}$ – априорное значение ущерба *j*-угрозы в области R_i; V^{max} – максимальная

величина вероятности реализации угрозы; S^{max} – максимальная априорная величина ущерба реализации угрозы; k –максимальное значение вероятности (количественная оценка вероятности); n – максимальное значение ущерба (количественная оценка ущерба).

Установлены ограничения при расчете по формуле (1):

$$0 \le R_{ij} \le 1; V^{(k)}{}_{ij} \le k; S^{(n)}{}_{ij} \le n.$$

Значения аргументов $V^{(k)}{}_{ij}$ и $S^{(n)}{}_{ij}$, как и значения максимальных величин V^{max} и S^{max} в (1), определяются в общем случае владельцем соответствующих ИТ-компонент или в простейшем случае – владельцем СОИ. Как показано ранее, одной из отличительных особенностей нового метода оценивания безопасности облачных ИТ-компонент является возможность вычислять априорные риски с учетом множества угроз ИБ, характерных для каждой конкретной ИТ-компоненты и в целом для СОИ. Например, для примера морского порта принимались оценки на базе априорных значений по каждому ИТ-компоненту за пятилетний период наблюдений, а диапазон значений вероятности V^{max} и ущерба S^{max} при реализации угроз ИБ определены для V^{max} от 0 до 1 и для S^{max} от 0 до 3 соответственно. Эти же данные впоследствии применялись и в процессе категорирования данного объекта по требованиям КИИ (ФЗ-187), в частности, в соответствии с постановлением Правительства № 127 (п. 10 е) в качестве исходных данных учитывались статистические данные о компьютерных инцидентах, произошедших ранее. В таблице 5 представлен пример расчета рисков от 5 угроз ИБ для ИТ-компонент, размещенных в области R_4 локации L4 (см. рис. 9).

В таблице 5 представлены наиболее значимые угрозы (на основании Приложения С [48]), которые можно ожидать для каждой из четырех областей (R_i) в полной совокупности рассматриваемых локаций (L). Именно по этой причине индексы процессов P определены от 1 до 7, но в данной конкретной в области R4.1 (локации L4) рассматриваются только 3 процесса: P_5, P_6 и P_7. Значение вероятности (V) находится в диапазоне (0;1), значение ущерба (S) находится в диапазоне (0;3), значения R_j (для одной угрозы) и $R_{apr\,i}$ (общий) находятся в диапазоне (0;1). Критерий принятия риска для данного конкретного примера (R_{cr}) определен как 10%.

Таблица 5. Пример расчета рисков реализации угроз

Угроза	Уязвимость	P (1;7)	V_{4j} (0;1)	S_{4j} (0;3)	R_{4j} (0,1)	R_{cr} (10%)	ТВ
Подслушивание	Плохой менеджмент паролей	P_5	0,50	2	0,33		A.10.1.1. A.12.1.2
Злоупотребление правами	Незащищенное хранение	P_7	0,25	2	0,17		A.9.2.2 A.16.1.2
Отказ телекоммуникационного оборудования	Единственная точка отказа	P_5	0,25	1	0,08	ОК	A.10.1.1 A.17.1.2
Преступное использование ПО	Недостатки найма персонала	P_6	0,05	3	0,05	ОК	A.8.1.2 A.16.1.2
Незаконная обработка данных	Малое число ревизий	P_7	0,05	2	0,03	ОК	A.9.4.1 A.18.2.3

Необходимо дать некоторые пояснения по расчету отдельных рисков для конкретных угроз R_{4j}: для угрозы «преступное использование ПО» (например, при обеспечении процесса бухгалтерского учета) вероятность реализации угрозы определена $V^{(1)}{}_4 = 0{,}05$, уровень величины ущерба составляет $S^{(3)}{}_4 = 3$ (максимальный), что по формуле (1) при $V^{max} = 1$ и $S^{max} = 3$ позволяет определить значение риска $R_{41} = 0{,}05$. Следует отметить, что вероятность $V^{(1)}{}_4 = 5\%$ получена ранее на основе статистики в ряде проектов, и такие же данные представлены в [23], то есть все эти исходные данные могут быть верифицированы надежно и независимо. После оценки всех R_{4j} (для каждой j-угрозы) по таблице 5 следует, что значимых рисков только 2 (соответственно, R_{41} и R_{42}).

Далее выполняется определение количественной оценки риска $R_{apr\,i}$ для СОИ по формуле:

$$R_{apr\,i} = \frac{1}{j}\sum_{j=1}^{m} R_{ij} \cdot K_j, \qquad (2)$$

где $R_{apr\,i}$ – оценка априорного риска в области R_i; R_{ij} – оценка риска для j-угрозы в области R_i; K_j – весовой коэффициент критичности (значимости) риска в области R_i; m – количество рисков в области R_i, превышающих R_{cr}.

Установлены ограничения при расчете по формуле (2):

$$0 \le R_{apr\ i} \le 1; \sum K_j = 1.$$

Для данного примера СОИ априорный риск в области R4.1 (локации L4) R_{apr} составит 12,5% (при допущении $K_1 = K_2 = 0{,}5$):

$$R_{apr\,4} = \frac{1}{2}\left(R_{41} \cdot K_1 + R_{42} \cdot K_2\right) = \frac{1}{2}\left(0{,}33 \cdot 0{,}5 + 0{,}17 \cdot 0{,}5\right) = 0{,}125.$$

Очевидно, может возникнуть вопрос, как отличались бы риски, рассчитанные по формулам (1) и (2), при тех же угрозах ИБ для ИТ-компонентов распределенной СОИ, например, находящейся под полным контролем бизнеса, без использования облачных сервисов. Ответ может быть следующий: для точного результата и сопоставления результатов по предложенному методу оценивания безопасности облачных ИТ-компонент необходимы данные реализованных мер защиты (в частности, ТВ), отражающие текущий уровень безопасности. Например, для рассмотренной распределенной СОИ при допущении более строгих мер контроля, в том числе встроенных ФБ (см. табл. 4) в применяемое ПО и дополнительных процедур, реализованных по требованиям бизнеса, можно ожидать более низкий уровень величин ущерба $S^{(1)}{}_4$ и $S^{(2)}{}_4$. Но в любом случае это предположение должно быть проверено в рамках выполняемого периодического оценивания (аудита) до принятия решения о переходе к облачным сервисам.

6. Заключение. Проблема обеспечения безопасности ИТ-компонент, в том числе обеспечения информационной безопасности объектов, использующих облачную инфраструктуру, в настоящий момент является весьма важной. Представлены результаты анализа известных методов обеспечения безопасности и оценивания степени обеспечения информационной безопасности отдельных ИТ-компонент. В статье предложен новый метод оценивания безопасности облачных ИТ-компонент на базе ранее разработанной гибридной методики с использованием формальных процедур, основанных на двух системах критериев – оценивании степени соответствия систем менеджмента (на базе ИСО/МЭК серии 27001) и оценивании требований функциональной безопасности (на базе МЭК серии 61508 и ИСО/МЭК серии 15408). Данный метод позволяет получить воспроизводимые и объективные оценки рисков безопасности

облачных ИТ-компонент, которые могут быть представлены для проверки независимой группе оценщиков. Полученные результаты могут быть применимы при формировании независимой оценки объектов критической информационной инфраструктуры.

Литература

1. *Лившиц И.И., Неклюдов А.В.* Применение гибридной методики при оценке безопасности информационных технологий для сложных промышленных объектов // Менеджмент качества. 2018. № 1. С. 48–61.
2. Six Pillars of DevSecOps. URL: https://cloudsecurityalliance.org/artifacts/cloud-security-complexity (дата обращения: 10.03.2020).
3. The 2019 Study on the Cyber Resilient Organization // Ponemon Institute. 2019. URL: https://www.techrepublic.com/resource-library/whitepapers/2019-ponemon-institute-study-on-the-cyber-resilient-organization/ (дата обращения: 10.03.2020).
4. *Malladi A., Potluri S.* A study on technologies in Cloud-based design and manufacturing // International Journal of Mechanical and Production Engineering Research and Development. 2018. vol. 8. no. 6. pp. 187–192.
5. *Souri A., Navimipour N.J., Rahmani A.M.* Formal verification approaches and standards in the Cloud computing: A comprehensive and systematic review // Computer Standards & Interfaces. 2018. vol. 58. pp. 1–22.
6. *Bologa R., Lupu A.R., Boja C., Georgescu T.M.* Sustaining employability: A process for introducing Cloud computing, big data, social networks, mobile programming and cybersecurity into academic curricula // Sustainability. 2017. vol. 9. no. 12. pp. 2235.
7. *Barrett M.P.* Framework for Improving Critical Infrastructure Cybersecurity // National Institute of Standards and Technology Gaithersburg. 2018.
8. *Moore T., Dynes S., Chang F.R.* Identifying How Firms Manage Cybersecurity Investment // Workshop on the Economics of Information Security (WEIS). 2016. pp. 1–27.
9. *McIntosh S., Kamei Y., Adams B., Hassan A.E.* The Impact of Code Review Coverage and Code Review Participation on Software Quality: A Case Study of the Qt, VTK, and ITK Projects // Proceedings of International Working Conference on Mining Software Repositories (MSR 2014). 2014. pp. 192–201.
10. *Лившиц И.И., Неклюдов А.В.* Гибридная методика оценки безопасности информационных технологий // Автоматизация в промышленности. 2017. № 7. С. 36–41.
11. *Лившиц И.И., Неклюдов А.В.* Гибридная методика безопасности информационных технологий для критически важных объектов энергетики // Энергобезопасность и энергосбережение. 2017. № 4. С. 5–11.
12. *Jeong C.Y., Lee S.Y.T., Lim J.H.* Information Security Breaches and IT Security Investments: Impacts on Competitors // Information & Management. 2019. vol. 56. no. 5. pp. 681–695.
13. *Oltsik J.* Cybersecurity Snippets. URL: https://www.csoonline.com/article/3406475/must-have-features-in-a-modern-network-security-architecture.html (дата обращения: 10.03.2020).
14. *Tan D.P. et al.* An Embedded Cloud Database service Method for distributed industry monitoring // IEEE Transactions on Industrial Informatics. 2018. vol. 14. no. 7. pp. 2881–2893.
15. *Akbaripour H., Houshmand M., van Woensel T., Mutlu N.* Cloud manufacturing service selection optimization and scheduling with transportation consideration: mixed-integer programming model // The International Journal of Advanced Manufacturing Technology. 2018. vol. 95. no. 1-4. pp. 43–70.
16. *Kobayashi N., Kume S., Lenz K., Masuya H.* Riken metadatabase: A database platform for health care and life sciences as a microcosm of linked open data cloud //

International Journal on Semantic Web and Information Systems. 2018. vol. 14. no. 1. pp. 140–164.
17. *Kumar M.M., Nandakumar A.N.* Exploring multilateral Cloud computing security architectural design debt in terms of technical debt // Smart Innovation, Systems and Technologies. 2018. vol. 78. pp. 567–579.
18. *Jun Z.* A security architecture for Cloud computing alliance // Recent Advances in Electrical and Electronic Engineering. 2017. vol. 10. no. 3. pp. 195–201.
19. Using standards to mitigate risks. URL: https://www.dhs.gov/sites/default/files/publications/2018_AEP_Artificial_Intelligence.pdf (дата обращения: 10.03.2020).
20. *Жукова К.* Хакеры открыли базы. URL: https://www.kommersant.ru/doc/3939724?from=four_tech (дата обращения: 10.03.2020).
21. Обзор: Рынок ИТ-услуг. URL: http://www.cnews.ru/reviews/rynok ituslug 2018/articles/vse_kak_servis_rynok_itsl ug rastet ne tolko v dengah (дата обращения 10.03.2020).
22. Rise of Legitimate Services for Backdoor Command and Control. URL: https://www.anomali.com/resources/anomali-labs-reports/rise-of-legitimate-services-for-backdoor-command-and-control (дата обращения: 10.03.2020).
23. Threats are rising. URL: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html (дата обращения: 10.03.2020).
24. Исследование утечек конфиденциальной информации через незащищенные облачные хранилища. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Report_open servers 2016 2018.pdf?rel=1 (дата обращения: 10.03.2020).
25. *Crowley C.* Common and Best Practices for Security Operations Centers Survey. URL: https://www.sans.org/media/vendor/Common-and-Best-Practices-for-Security-Operations-Centers.pdf (дата обращения: 10.03.2020).
26. *Bangui H. et al.* Multi-criteria decision analysis methods in the mobile Cloud offloading paradigm // Journal of Sensor and Actuator Networks. 2017. vol. 6. no. 4. pp. 25.
27. The State of Threat Detection Report 2019. URL: https://www.fidelissecurity.com/resource/report/threat-detection-2019 (дата обращения: 10.03.2020).
28. Отсутствие автоматизации остается главной проблемой для безопасников. URL: https://www.securitylab.ru/news/500340.php (дата обращения: 10.03.2020).
29. Strategic planning guides for leaders across the enterprise. URL: https://www.gartner.com/en/insights/strategic-planning, (дата обращения: 03.03.2020).
30. Forrester оценила поставщиков решений для реализации стратегии ZTX. URL: https://www.securitylab.ru/news/496550.php (дата обращения: 03.03.2020).
31. Zero Trust redefines security in a perimeter-less world. URL: https://www.mobileiron.com/en/solutions/zero-trust (дата обращения: 03.03.2020).
32. *Hudic A., Smith P., Weippl E.R.* Security assurance assessment methodology for hybrid Cloud // Computers & Security. 2017. vol. 70. pp. 723–743.
33. *Yin C. et al.* Code: An Erasure Code algorithm for big data storage system // Journal of University of Science and Technology of China. 2016. vol. 46. no. 3. pp. 188–199.
34. *Goyal T. et al.* Big data handling over Cloud for internet of things // International Journal of Information Technology and Web Engineering. 2018. vol. 13. no. 2. pp. 37–47.
35. The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018. URL: https://reprints.forrester.com/?fbclid=IwAR3iPICwQnteW1BF7VgoISlz0P2d5nVB11aoQsrEqYbHu4R2USf6wrFUG7w#/assets/2/219/RES141666/reports (дата обращения: 03.03.2020).
36. 5 Key Findings from Forbes Insights' 2019 Cybersecurity Survey. URL: https://www.vmware.com/radius/forbes-insights-cybersecurity-strategy-report (дата обращения: 03.03.2020).

37. ГОСТ Р ИСО/МЭК 15408-1 – 2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель // М.: ФАТРиМ. 2012.
38. ГОСТ Р ИСО/МЭК 15408-2 – 2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности // М.: ФАТРиМ. 2013.
39. ГОСТ Р ИСО/МЭК 15408-3 – 2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности // М.: ФАТРиМ. 2013.
40. *Лившиц И.И.* Проектирование, создание и внедрение комплексных систем обеспечения информационной безопасности на базе ISO/IEC 27001:2005 // Электросвязь. 2010. № 4. С. 49–51.
41. *Лившиц И.И., Лившиц Н.В.* Подходы к синтезу моделей систем менеджмента информационной безопасности при оценке утечек конфиденциальных данных // Лизинг. 2013. № 3. С. 70–80.
42. State of Application Security: Balancing Speed and Risk. URL: https://www.sans.org/reading-room/whitepapers/analyst/2017-state-application-security-balancing-speed-risk-38100 (дата обращения: 10.03.2020).
43. ГОСТ Р МЭК 61508-1—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования». 2012.
44. ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам». 2012.
45. ГОСТ Р МЭК 61508-3—2018 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению». 2018.
46. *Schweizerische S.N.V.* Information technology-Security techniques-Information security management systems-Requirements //ISO/IEC International Standards Organization. 2013.
47. ISO/IEC 27005-2018 Information technology — Security techniques — Information security risk management, International Organization for Standardization. 2011. 68 p.
48. *Лившиц И.* Система менеджмента информационной безопасности по международным стандартам // Управление качеством. 2011. № 9. С. 6–11.
49. Представлена система оценки вероятности использования уязвимостей в реальных атаках. URL: https://www.securitylab.ru/news/500398.php (дата обращения: 10.03.2020).
50. Только 5,5% уязвимостей используются в реальных атаках. URL: https://www.securitylab.ru/news/499359.php (дата обращения: 10.03.2020).
51. Improving Vulnerability Remediation Through Better Exploit Prediction. URL: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_53.pdf (дата обращения: 10.03.2020).
52. Artificial Intelligence: Potential Benefits and Ethical Considerations. URL: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI(2016)571380_EN.pdf (дата обращения: 10.03.2020).

Лившиц Илья Иосифович — д-р техн. наук, доцент, факультет безопасности информационных технологий, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (НИУ ИТМО). Область научных интересов: системный анализ, защита информации, риск-менеджмент. Число научных публикаций — 90. Livshitz.il@yandex.ru; ул. Ломоносова, 9, 191002, Санкт-Петербург, Россия; р.т.: +7 812 934-48-46.

DOI 10.15622/sp.2020.19.2.6

I. LIVSHITZ

METHOD FOR EVALUATING SECURITY OF CLOUD IT-COMPONENTS BASED ON EXISTING STANDARDS CRITERIA

Livshits I. **Method for Evaluating Security of Cloud IT-Components based on Existing Criteria.**

Abstract. The analysis of well-known methods for ensuring IT-security is presented, methods for evaluating security of IT-components and Cloud services in general are considered.

An attempt to analyze cloud services not from a commercial position of a popular marketing product, but from a position of system analysis is made. The previously introduced procedure for IT-components evaluation is not stable, since the end user has not a 100% guarantee of access to all IT-components, and even more so to the remote and uncontrolled Cloud service. A number of reviews point at increased efforts to create a secure network architecture and ability to continuously monitor deviations from established business goals. In contrast to the Zero Trust and Zero Trust eXtended models, according to which additional security functions are superimposed on existing IT-components, it is proposed to consider the set of IT-components as a new entity – an Information Processing System. This allows moving to formal processes for assessing the degree of compliance with the criteria of standards for both existing and prospective IT-components while ensuring security of Cloud services.

A new evaluation method based on the previously developed hybrid methodology using formal procedures based on two systems of criteria - assessment of the degree of compliance of Management systems (based on ISO/IEC 27001 series) and assessment of functional safety requirements (based on IEC 61508 series and ISO/IEC 15408 series) is proposed. This method provides reproducible and objective assessments of security risks of Cloud-based IT-components that can be presented to an independent group of evaluators for verification. The results obtained can be applied in the independent assessment, including critical information infrastructure objects.

Keywords: Management System, Risk, Information Technology, IT-security, Audit, Standard, Expertise, Assessment.

Livshitz Ilya — Ph.D., Dr.Sci., Associate Professor, Faculty of Secure Information Technologies, ITMO University (Saint Petersburg National Research University of Information Technologies, Mechanics and Optics). Research interests: system analyses, IT-security, risk-management. The number of publications — 90. Livshitz.il@yandex.ru; 9, Lomonosova str., 191002, St. Petersburg, Russia; office phone: +7 812 934-48-46.

References

1. Livshits I.I., Neklyudov A.V. [Application of hybrid methodology in the assessment of information technology security for complex industrial facilities]. *Menedzhment kachestva – Quality Management*. 2018. vol. 1. pp. 48–61. (In Russ).
2. Six Pillars of DevSecOps. Available at: https://cloudsecurityalliance.org/artifacts/cloud-security-complexity (accessed: 10.03.2020).
3. The 2019 Study on the Cyber Resilient Organization. Ponemon Institute. 2019. Available at: https://www.techrepublic.com/resource-library/whitepapers/2019-ponemon-institute-study-on-the-cyber-resilient-organization/ (accessed: 10.03.2020).
4. Malladi A., Potluri S. A study on technologies in Cloud-based design and manufacturing. *International Journal of Mechanical and Production Engineering Research and Development.* 2018. vol. 8. no. 6. pp. 187–192.

5. Souri A., Navimipour N.J., Rahmani A.M. Formal verification approaches and standards in the Cloud computing: A comprehensive and systematic review. *Computer Standards & Interfaces*. 2018. vol. 58. pp. 1–22.
6. Bologa R., Lupu A.R., Boja C., Georgescu T.M. Sustaining employability: A process for introducing Cloud computing, big data, social networks, mobile programming and cybersecurity into academic curricula. *Sustainability*. 2017. vol. 9. no. 12. pp. 2235.
7. Barrett M.P. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology Gaithersburg. 2018.
8. Moore T., Dynes S., Chang F.R. Identifying How Firms Manage Cybersecurity Investment. Workshop on the Economics of Information Security (WEIS). 2016. pp. 1–27.
9. McIntosh S., Kamei Y., Adams B., Hassan A.E. The Impact of Code Review Coverage and Code Review Participation on Software Quality: A Case Study of the Qt, VTK, and ITK Projects. Proceedings of International Working Conference on Mining Software Repositories (MSR 2014). 2014. pp. 192–201.
10. Livshits I.I., Neklyudov A.V. [Hybrid method of information technology security assessment]. *Avtomatizatia v promushlennosti – Automation in industry*. 2017. vol. 7. pp. 36–41. (In Russ).
11. Livshits I.I., Neklyudov A.V. [Hybrid method of information technology security for critical energy facilities]. *Energobezopastnost' i Energosberezhenie – Energy Security and energy saving.* 2017. vol. 4. pp. 5–11. (In Russ).
12. Jeong C.Y., Lee S.Y.T., Lim J.H. Information Security Breaches and IT Security Investments: Impacts on Competitors. *Information & Management.* 2019. vol. 56. no. 5. pp. 681–695.
13. Oltsik J. Cybersecurity Snippets. Available at: https://www.csoonline.com/article/3406475/must-have-features-in-a-modern-network-security-architecture.html (accessed: 10.03.2020).
14. Tan D.P. et al. An Embedded Cloud Database service Method for distributed industry monitoring. *IEEE Transactions on Industrial Informatics.* 2018. vol. 14. no. 7. pp. 2881–2893.
15. Akbaripour H., Houshmand M., van Woensel T., Mutlu N. Cloud manufacturing service selection optimization and scheduling with transportation consideration: mixed-integer programming model. *The International Journal of Advanced Manufacturing Technology.* 2018. vol. 95. no. 1-4. pp. 43–70.
16. Kobayashi N., Kume S., Lenz K., Masuya H. Riken metadatabase: A database platform for health care and life sciences as a microcosm of linked open data cloud. *International Journal on Semantic Web and Information Systems.* 2018. vol. 14. no. 1. pp. 140–164.
17. Kumar M.M., Nandakumar A.N. Exploring multilateral Cloud computing security architectural design debt in terms of technical debt. Smart Innovation, Systems and Technologies. 2018. vol. 78. pp. 567–579.
18. Jun Z. A security architecture for Cloud computing alliance. *Recent Advances in Electrical and Electronic Engineering*. 2017. vol. 10. no. 3. pp. 195–201.
19. Using standards to mitigate risks. Available at: https://www.dhs.gov/sites/default/files/publications/2018_AEP_Artificial_Intelligence.pdf (accessed: 10.03.2020).
20. Zhukova K. Hakery otkryli bazy [Hackers have opened the base]. Available at: https://www.kommersant.ru/doc/3939724?from=four_tech (accessed: 10.03.2020). (In Russ.).
21. Obzor: Rynok IT-uslug [Overview: IT Services Market]. Available at: http://www.cnews.ru/reviews/rynok_ituslug_2018/articles/vse_kak_servis_rynok_itsl ug_rastet_ne_tolko_v_dengah (accessed: 10.03.2020). (In Russ.).

22. Rise of Legitimate Services for Backdoor Command and Control. Available at: https://www.anomali.com/resources/anomali-labs-reports/rise-of-legitimate-services-for-backdoor-command-and-control (accessed: 10.03.2020).
23. Threats are rising. Available at: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html (accessed:10.03.2020).
24. Issledovanie utechek konfidencial'noj informacii cherez nezashchishchennye oblachnye hranilishcha [Research of personal data leakage from unprotected cloud storage]. Available at: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Report_open_servers_2016_2018.pdf?rel=1 (accessed: 10.03.2020). (In Russ.).
25. Crowley C. Common and Best Practices for Security Operations Centers Survey. Available at: https://www.sans.org/media/vendor/Common-and-Best-Practices-for-Security-Operations-Centers.pdf (accessed: 10.03.2020).
26. Bangui H. et al. Multi-criteria decision analysis methods in the mobile Cloud offloading paradigm. *Journal of Sensor and Actuator Networks.* 2017. vol. 6. no. 4. pp. 25.
27. The State of Threat Detection Report 2019. Available at: https://www.fidelissecurity.com/resource/report/threat-detection-2019 (accessed: 10.03.2020).
28. Otsutstvie avtomatizacii ostaetsya glavnoj problemoj dlya bezopasnikov [The main problem still automation outstanding for IT-security personnel]. Available at: https://www.securitylab.ru/news/500340.php (accessed: 10.03.2020). (In Russ.).
29. Strategic planning guides for leaders across the enterprise. Available at: https://www.gartner.com/en/insights/strategic-planning (accessed 10.03.2020).
30. Forrester ocenila postavshchikov reshenij dlya realizacii strategii ZTX [Forrester was assessed the suppliers of ZTX]. Available at: https://www.securitylab.ru/news/496550.php (accessed: 10.03.2020). (In Russ.).
31. Zero Trust redefines security in a perimeter-less world. Available at: https://www.mobileiron.com/en/solutions/zero-trust (accessed: 03.03.2020).
32. Hudic A., Smith P., Weippl E.R. Security assurance assessment methodology for hybrid Cloud. *Computers & Security*. 2017. vol. 70. pp. 723–743.
33. Yin C. et al. Code: An Erasure Code algorithm for big data storage system. *Journal of University of Science and Technology of China*. 2016. vol. 46. no. 3. pp. 188–199.
34. Goyal T. et al. Big data handling over Cloud for internet of things. International Journal of Information Technology and Web Engineering. 2018. vol. 13. no. 2. pp. 37–47.
35. The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018. Available at: https://reprints.forrester.com/?fbclid=IwAR3iPICwQnteW1BF7VgoISlz0P2d5nVB11aoQsrEqYbHu4R2USf6wrFUG7w#/assets/2/219/RES141666/reports (accessed: 03.03.2020).
36. 5 Key Findings from Forbes Insights' 2019 Cybersecurity Survey. Available at: https://www.vmware.com/radius/forbes-insights-cybersecurity-strategy-report (accessed: 03.03.2020).
37. GOST R ISO / IEC 15408-1 – 2012 [Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model]. M.: FATRiM. 2012. (In Russ).
38. GOST R ISO / IEC 15408-2 – 2013 [Information technology. Security techniques. Evaluation criteria for IT security. Part 2. Security functional components]. M.: FATRiM. 2012. (In Russ).
39. GOST R ISO/IEC 15408-3 – 2013 [Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance requirements]. M.: FATRiM. 2012. (In Russ).

40. Livshits I.I. [Design, creation and implementation of complex Information security systems based on ISO/IEC 27001:2005]. *Elektrosv'yaz – Telecommunication*. 2010. vol. 4. pp. 49–51. (In Russ).
41. Livshits I.I,, Livshits N.V. [Approaches to the synthesis of models of Information Security Management Systems in the assessment of confidential data leaks]. *Lising – Leasing*. 2013. vol. 3. pp. 70–80. (In Russ).
42. State of Application Security: Balancing Speed and Risk. Available at: https://www.sans.org/reading-room/whitepapers/analyst/2017-state-application-security-balancing-speed-risk-38100 (accessed: 10.03.2020).
43. GOST R ISO/IEC 61508-1-2012 [Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 1. General requirements]. 2012. (In Russ.).
44. GOST R ISO/IEC 61508-2-2012 [Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 2. Requirements for systems]. 2012. (In Russ.).
45. GOST R ISO/IEC 61508-3-2018 [Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 3. Software requirements]. 2018. (In Russ.).
46. Schweizerische S.N.V. Information technology-Security techniques-Information security management systems-Requirements. ISO/IEC International Standards Organization. 2013.
47. ISO/IEC 27005-2018 Information technology — Security techniques — Information security risk management, International Organization for Standardization. 2011. 68 p.
48. Livshits I. [Information Security Management System according to International Standards]. *Menedzhment kachestva – Quality Management*. 2011. vol. 9. pp. 6–11. (In Russ).
49. Predstavlena sistema ocenki veroyatnosti ispol'zovaniya uyazvimostej v real'nyh atakah [System of likelihood assessment for vulnerabilities usage in real attach has been presented]. Available at: https://www.securitylab.ru/news/500398.php (accessed: 10.03.2020). (In Russ.).
50. Tol'ko 5,5% uyazvimostej ispol'zuyutsya v real'nyh atakah [Only 5,5 % vulnerabilities was implement in real attack]. Available at: https://www.securitylab.ru/news/499359.php (accessed: 10.03.2020). (In Russ.).
51. Improving Vulnerability Remediation Through Better Exploit Prediction. Available at: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_53.pdf (accessed: 10.03.2020).
52. Artificial Intelligence: Potential Benefits and Ethical Considerations. Available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI(2016)571380_EN.pdf (accessed: 10.03.2020).