Проблемы обеспечения безопасности облачной компоненты информационных технологий

И.И. Лившиц (Университет ИТМО),
А.А. Зайцева (СПИИРАН)

— А где же наша гвардия? Гвардия где?
— Очевидно, обходит с флангов.
— Кого?
— Всех!
«Тот самый Мюнхгаузен»

Предпринята попытка исследования и оценки возможности обеспечения заданного уровня безопасности для современных «облачных» сервисов. Приводятся различные экспертные мнения российских и иностранных экспертов по широкому диапазону вопросов обеспечения информационной безопасности как отдельных компонент, так и «облачных» сервисов в целом. Предлагается перейти к формальным методам оценки степени соответствия существующих и перспективных компонентов при обеспечении безопасности «облачных» сервисов. В статье предложен подход, основанный на ранее разработанной «гибридной» методике с использованием ряда формальных процедур на базе двух систем критериев: оценки степени соответствия систем менеджмента по ИСО/МЭК серии 27001 и оценки требований функциональной безопасности по МЭК серии 61508 и ИСО/МЭК серии 15408.

Ключевые слова: информационная технология, информационная безопасность, аудит, оценка соответствия, меры (средства) защиты.

Введение

Замысел данной статьи появился в результате анализа процессов, происходящих в последние несколько лет в области разработки информационных систем различной степени критичности, и оценки различных аспектов безопасности используемых компонентов информационных технологий, в том числе находящихся в «облаке».

Заметим, что подходов к анализу данной ситуации может быть несколько, и, очевидно, нет необходимости определять единственную верную систему предоставления доказательств. Отчасти это может определяться различными занимаемыми позициями дискутирующих — например, разработчики предполагают возможным тиражировать многократно примененные на практике облачные системы, оперируя человеко-годам на разработку и числом реализованных проектов. С другой стороны, веское слово могут сказать аудиторы, применяющие различные инструменты, позволяющие с завидной частотой и гарантированным результатом выявлять серьезные уязвимости практически во всех реально применяемых компонентах. Весьма ценным представляется и анализ позиции регуляторов, призванных определять «руководящую и направляющую» линию для каждого применения информационных технологий.

Аналитический обзор

Краткий аналитический обзор начнем с цитирования ряда экспертов, чья острота публикаций неизменно показывает широчайший спектр оценок текущей ситуации для всех начинаний (технических, юридических) наших регуляторов в области информационной безопасности (ИБ). Приведем цитату А. Лукацкого[1]: *«ФСТЭК становится оторванной от жизни, как и депутаты. И тому есть две причины. Первая заключается в том, что ФСТЭК сама не сталкивается со многими процессами, для которых она пишет требования по ИБ. У нее нет облаков, она блокирует использование мобильных устройств, она не использует средства аналитики ИБ и Threat Intelligence[2] (вы когда-нибудь слышали про SOC ФСТЭК?). Да и средства защиты, которые она использует, только сертифицированные и преимущественно отечественные. То есть сама ФСТЭК не понимает проблем регулируемых ею потребителей».* В данном утверждении содержится серьезный упрек одному из главных регуляторов в РФ в области ИБ, поскольку все современные технологии должны проходить необходимую оценку ИБ по установленным требованиям. В равной мере это должно затрагивать и новые «облачные» технологии, активно рекламируемые и применяемые в государственном секторе РФ, но пока ФСТЭК не разработала никаких адекватных решений.

[1] https://www.securitylab.ru/blog/personal/Business_without_danger/346065.php?R=1
[2] Технология Threat Intelligence описывает методы регулярного сбора информации об угрозах, их анализ и распространение.

В продолжение темы интересным представляется суждение эксперта В. Комарова[3] в части внесения изменений в приказ 239, а именно: *«При этом в объектах 1 категории значимости применяются сертифицированные средства защиты информации, соответствующие 4 или более высокому уровню доверия. В объектах 2 категории значимости применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В объектах 3 категории значимости применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия. Учитывая, что по ГОСТ Р ИСО/МЭК 15408 (и по действующим руководящим документам ФСТЭК России) оценочный уровень доверия (ОУД) 1 — это минимальный уровень доверия, а ОУД7 — максимальный уровень доверия, получается, что для объектов критической информационной инфраструктуры (КИИ) третьей (минимальной) категории требования к доверию выше, чем объектов КИИ второй и первой категории, что не логично и, с одной стороны, влечет дополнительные затраты на создание системы защиты объектов КИИ с минимальными требованиями по безопасности, а с другой — появляется возможность использования средств защиты с меньшим уровнем доверия для объектов, требующих повышенной защиты»*.

Как следует из данного текста, надежды на то, что ФСТЭК приведет новую систему своих приказов для обеспечения объектов КИИ в соответствии с лучшими международными практиками, не оправданы. В данное время нет уверенности в реализации новаций в области оценки соответствия на базе хорошо известной в мире серии стандартов IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security. Таким образом, при оценке соответствия объектов КИИ в ближайшее время не будет предложено удобного, эффективного и достоверного методического аппарата, предоставляющего бизнесу объективные и проверяемые оценки ИБ для компонент ИТ.

Определенное внимание можно обратить на иные современные нормативные новые документы в области оценки соответствия ИБ, кроме ставших уже «классическими» требований ISO/IEC серии 27001 Information technology — Security techniques — Information security management systems. В качестве дополнительных требований, на которые уже обратил внимание эксперт С. Борисов[4], можно отметить документ CIS (Center for Internet Security) «20 CIS Controls». Не вдаваясь в детали и оставляя все нюансы для более вдумчивого исследования другим экспертам, отметим три уровня реализации мер защиты (Basic, Foundation, Organization), в каждом из которых обязательно присутствует «наследование» хороших общеизвестных практик. К таким практикам ИБ, например, можно отнести инвентаризацию технических средства (отметим, что корректнее говорить об «активах»), контролируемый доступ на основе ролей и применение независимых проверок и пентестов (тестирование на проникновение).

Важный аспект для бизнес-заказчиков — предоставление гарантий обеспечения заданного уровня ИБ для различных типов компонентов ИТ. В частности, кричным аспектом может оказаться контроль предоставления доступа (в равной степени — отзыв прав доступа) к различным видам «облачных» хранилищ чувствительных корпоративных данных. Рассмотрим пример, опубликованный в издании «Коммерсант»[5]: *«Главной причиной неавторизованного доступа к облачным базам данных становятся ошибки конфигурации из-за низкой квалификации администраторов этих баз данных, — полагает основатель и технический директор DeviceLock Ашот Оганесян. — Кроме того, по содержимому открытой базы данных не всегда можно идентифицировать ее владельца, а хостеры не выдают такую информацию, потому непонятно, кому сообщить о том, что доступ к ней нужно закрыть»*.

В определенной мере вопросы оценки соответствия можно рассмотреть с точки зрения значимости нашего отечественного сегмента рынка ИТ компонентов по сравнению с мировыми тенденциями и оценить объем новых технологий, способных «проникать» в РФ. Например, в обзоре РБК[6] показано, что *«несмотря на популярность облачных и прочих сервисов, российский рынок ИТ-услуг еще далек от того, чтобы называться развитым: весь ИТ-рынок России составляет примерно 2% от мирового, а сегмент ИТ-услуг занимает только 0,5% от общего «пирога», по данным Gartner и IDC»*. Отчасти этот мизерный уровень является не только отражением способности оценить (в том числе и в аспекте ИБ) новые предлагаемые «облачные» технологии, как было показано выше на примере нормативных документов ФСТЭК, но также связан с проблемами квалификации обслуживающего персонала. Этот тезис можно подкрепить мнением ИТ-директора АО «Северсталь» С. Дунаева[7]: *«Главная проблема — мало умных людей. В том смысле, что мало специалистов, глубоко разбирающихся в том, что они делают. Сплошь и рядом возникают ситуации, когда не удается найти человека, чтобы толком обсудить возникшую задачу. Мы это видим и в мире в целом, и в России»*.

[3] https://www.securitylab.ru/blog/personal/valerykomarov/345991.php
[4] https://www.securitylab.ru/blog/personal/sborisov/346070.php
[5] https://www.kommersant.ru/doc/3939724?from=four_tech
[6] http://www.cnews.ru/reviews/rynok_ituslug_2018/articles/vse_kak_servis_rynok_ituslug_rastet_ne_tolko_v_dengah
[7] http://www.cnews.ru/articles/2019-04-11_kadrovyj_golod_porodil_padenie_kachestva_ituslugmnenie_zakazchikov

Вопросы обеспечения безопасного применения «облачных» компонентов

Начиная с этого момента, можно суммировать все острые и принципиальные моменты, о которых справедливо говорили выше различные эксперты — как представители бизнеса, так и независимые. Очевидно, что необходимо подойти к вопросу обеспечения безопасного применения «облачных» компонентов с позиции анализа истории развития ИТ и путем постепенной миграции от раздельного применения компонентов ИТ и ИБ к созданию компонентов, безопасных изначально.

Отчасти это сделать достаточно сложно, и этот путь может быть пройден не сразу и не быстро, но зато позволит предоставить высшему менеджменту (справедливо пекущемуся о «разрухе в головах»), другой метод. В XX веке произошла последовательная смена нескольких подходов к созданию ИТ и ИБ, и в некоторых странах с определенного момента не разделяются ИТ и ИБ [1, 2]. К сожалению, в РФ такое разделение по-прежнему осталось неизжитым пережитком, и этот «перегиб на местах» привел к широчайшему спектру «токсичных активов» в виде «наложенных» средств защиты информации (СЗИ). С точки зрения маркетинга и государственной поддержки все было стройно и красиво — на любой иностранный (и потенциальный вредоносный компьютер) ставилось сертифицированное СЗИ с печатью ФСТЭК и/или ФСБ. Потом, правда, появились вопросы к оснащению СЗИ «потенциально» опасных промышленных контроллеров, сетевого оборудования, телефонных станций, и поводов для оптимизма стало уже существенно меньше.

В настоящее время введенный 25 лет назад порядок уже не является стабильным, поскольку у конечного пользователя уже нет 100% гарантии доступа ко всем компонентам ИТ, а тем более с учетом удаленного и абсолютного неподконтрольного «облачного» сервиса. В настоящее время регуляторы не готовы предложить методы оценки соответствия требованиям ИБ для этих ИТ компонентов, не говоря уже о перспективных. Проблема усугубляется еще тем, что в РФ никто не занимался созданием полного стека национальных суверенных ИТ компонентов с 1 по 7 уровень классической модели OSI/ISO. Никто не желал трогать «базу», оперируя только «надстройкой» в виде ограниченного перечня СЗИ с ограниченной же функциональностью. Прекрасным примером данной ситуации может служить анализ безопасности одного иностранного ИТ компонента (платы) экспертом белорусского НИИ ТЗИ Д. И. Вержбаловичем[8] на международной конференции «Комплексная защита информации» в Минске в 2015 г. В докладе было показано, какие потенциальные опасности недокументированных возможностей содержатся в современных вычислительных средствах и как можно их выявить.

Таблица 1. Анализ утечек данных из облачных серверов

Виды данных	2017 г.	2018 г.
Персональные данные	77,7 %	81,6 %
Коммерческие секреты	8,9%	9,2%
Платежная информация	6,7%	9,2%
Государственная тайна	6,7%	-

• Windows 7	60,2%
• Windows 10	28,9%
• Windows 8.1	5,3%
• Windows XP	4,4%
• Windows XP 64 bit	0,5%
• Windows 8	0,4%
• Windows Vista	0,2%
• Windows 2000	0,1 %

Рис. 1. Распространения ОС MS Windows

В защиту предыдущего подхода, применявшегося более 25 лет (с даты принятия системы нормативно-методических документов Гостехкомиссии с 1992–1994 гг.), отметим, что жесткие требования по изоляции внутренних ведомственных сетей могли быть в определенной степени результативны. Действительно, в замкнутой изолированной сети это не представляло серьезной угрозы, если исключить сценарии подмены и/или использования съемных неучтенных носителей, элементарных методик социальной инженерии и пр. Но вот пришел неизбежный прогресс и в РФ, в частности, началось активное строительство различных центров обработки данных (ЦОД), и бизнес ринулся в новый неизведанный мир «облаков», больших данных и стандартов TIER... Однако не все так прекрасно, как хотелось бы. По прогнозам компании «451 Research»[9] от 2015 г. в 2016 г. мировой рынок коммерческих дата-центров вырастет как минимум на 11% по сравнению с 2015 г., и такие темпы роста сохранятся до 2018 г. Но уже в 2018 г. поступили иные данные. Исследовательская компания IDC[10] сообщила, что на протяжении последних трех лет число ЦОДов в мире, в том числе в США, постепенно сокращается — на 2...3% ежегодно с 2016 г. В России[11] в это же время число ЦОДов, напротив, продолжает достаточно бурно расти.

И вопрос обеспечения информационной безопасности «облачных технологий» уже является заботой экспертов почти всех крупных компаний, поскольку статистические данные, экспертные отчеты и публичные аналитические доклады не дают ни одного шанса на спокойствие. Даже в вопросах наивысшей важности для любого «безопасника» — обеспечение государственной тайны, есть серьезные проблемы. Как показано в отчете компании InfoWatch[12], в 2017 г. в общем объеме утечек данных из облачных серверов более 6% данных как раз составила информация, отнесенная к государственной тайне (табл. 1).

Этому примеру удивляться не приходится, поскольку байт информации с коммерческой тайной выглядит ровно также, как и байт информации с го-

[8] https://2015.kzi.su/program_kzi
[9] https://asp24.com.ua/blog/tsod-v-mire-chto-novogo/
[10] http://www.cnews.ru/news/top/2018-08-20_zakupki_serverov_v_rossijskih_tsodah_vyrastut
[11] http://dcdeforum.ru/news/rynok-tsodov-v-rossii-i-ssha-trendy-ne-sovpadayut
[12] https://www.infowatch.ru/analytics/reports/15553

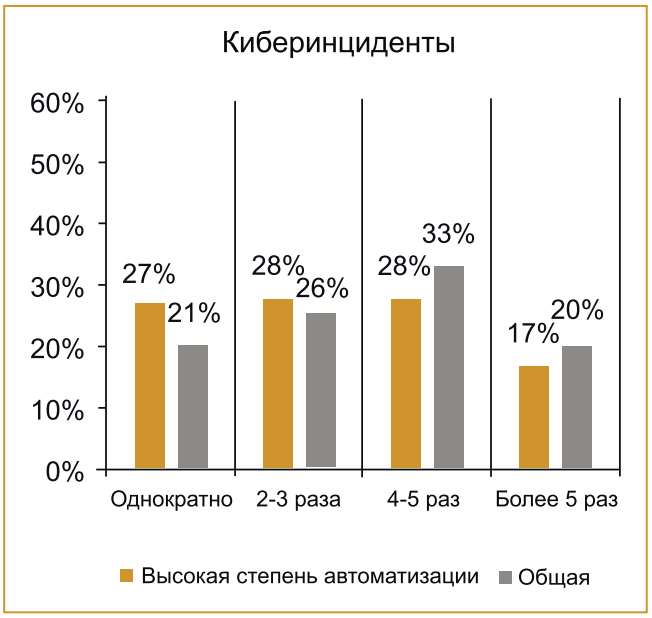

Рис. 2. Распределение частоты киберинцидентов

Таблица. 2. Функциональность приложений, применяемых для защиты от кибератак

Функциональность	2016	2017	2018
Способность сохранить работоспособности системы даже после успешной кибератаки	32%	48%	54%
Способность предупредить кибератаки	40%	55%	53%
Быстрое обнаружение кибератаки	49%	52%	53%
Идентификация типа киберприложения (вирус, шифровальщик, DDOS и др.)	53%	50%	49%
Определение источника кибератаки	-	54%	53%

сударственной тайной. И если на объекте нет внятной системы ИБ, оба эти байта могут беспрепятственно покинуть периметр «облака», особенно если «безопасник» не знает, не умеет или не может обеспечить эту самую безопасность. И, к сожалению, ни ФСТЭК, ни ФСБ не могут быть полезны на острие технического прогресса, и существующие нормативно-методические документации по аттестации объектов информатизации тоже мало применимы.

Рис. 3. Метрики, применяемые при оценке систем безопасности

Следующий вопрос по иерархии изложения — от «облачных» серверов — к конкретным ИТ компонентам, например, операционным системам. На рис. 1 представлен анализ распространения ОС семейства MS Windows из отчета «Security in the Era of Industry 4.0: Dealing With Threats to Smart Manufacturing Environments» [3].

Рисунок дает достаточно много материала для разнопланового анализа, например, по следующим вопросам:

– Сколько ОС сейчас уже сняты с поддержки компании разработчика?

– Сколько ОС планируется снять в ближайшее время?

– Сколько ОС прошли сертификацию в РФ и внесены в реестр СЗИ (ФСТЭК и ФСБ)?

– Сколько ОС прошли независимую международную оценку соответствия?

В качестве комментария к заданным выше вопросам отметим, что в реестре ФСТЭК РФ на июль 2019 г. было представлено две ОС MS Windows, но в нем нет ни одного «лидера» рейтинга — Windows 7 и Windows 10, занимающих более 90% всех указанных ОС.

В отчете «The 2019 Study on the Cyber Resilient Organization», представленном Ponemon Institute в апреле 2019 г. [4], представлена статистика по частоте проявления киберинцидентов (рис. 2).

Отметим, что ЦОД может быть отнесен к категории ИТ компонентов с высоким уровнем автоматизации. В этом случае, как следует из статистики, обнаружение пяти и более инцидентов выявлено в 20% случаях. Очевидно, следует задаться вопросом о полноте тестирования, о качестве реализации проекта, о выполненных аудитах ИБ, если такие проводились и пр. Для конечного пользователя и мнительного «безопасника» значимыми являются вопросы: кто обеспечивает реагирования на эти инциденты? Кому он подчиняется: какова его квалификация? Где он расположен и как с ним связаться в экстренном случае? Дополнительно для нагнетания некоторой истерии можно аккуратно упомянуть еще и популярные атаки на «цепочку поставок», чтобы уважаемые «безопасники» почувствовали себя как в реальном бою. Под атаками на «цепочку поставок» понимается практика внедрения вредоносного кода в многоэтапный процесс разработки ИТ компонентов, как правило, с помощью стороннего недоверенного программного обеспечения. Известно несколько печальных примеров таких успешных атак, например: атака на British Airways[13] и атака ShadowHammer на ноутбуки Asus[14].

Для ответа на эти и иные вопросы можно обратиться к анализу функциональности приложений ИБ, применяемых для защиты от кибератак (табл. 2). С одной стороны, не все так ужасно, на-

[13] https://www.securitylab.ru/blog/company/PandaSecurityRus/345497.php
[14] https://www.securitylab.ru/blog/company/kaspersky/346406.php

пример, динамика роста устойчивости к кибератакам повышается год от года на 10%, незначительно растет и способность быстрого обнаружения кибератак, но, с другой стороны, к сожалению, способность анализа содержимого кибератак снижается.

Далее предлагается рассмотреть крайне важный аспект любой системы ИБ, построенной «под бизнес» и подчиняющейся общим требованиям бизнеса, а именно: обеспечение измерений и выполнение мониторинга по определенным ключевым показателям (метрикам). В отчете [4] представлена статистика по некоторым метриками (рис. 3).

Обратим внимание, какое место в общем рейтинге из 10 позиций занимают две метрики: «время доступности ЦОД» и «снижение операционных издержек» — 27% и 15% соответственно.

С учетом рассмотренных выше известных угроз и проблем соответствия текущей нормативно-методической базы регуляторов в области ИБ в РФ, представляется весьма сложным обеспечить надлежащее решение задачи безопасности «облачных» сервисов. Как следствие, бизнес может задать ряд вопросов, как именно «безопасники» планируют обеспечить заданный уровень всех ИТ компонентов корпоративного ландшафта при поставленной бизнес-цели снижения издержек, повышения скорости обработки данных без ограничения регионального присутствия и пр. Соответственно встает вопрос о предоставлении определенных гарантий для бизнеса — со стороны разработчиков (кто проводит оценку соответствия, например, по критериям ISO/IEC серии 15408 или 27001), со стороны аудиторов (кто проводит аудит соответствия ИБ, например, по критериям ISO серии 17021) и пр. Вопрос о предоставлении гарантий со стороны государства в данной статье не рассматривается по понятным причинам.

Таблица 3. Опросник на базе ИСО 27001 и 27005 для «облачных» решений (фрагмент)

№	Пункт 27001 (Приложение А)	Наименование контроля	Примечание
1.	A.6.1.1	Роли и ответственность в рамках ИБ	Все ответственности в поле ИБ должны быть определены и закреплены.
2.	A.6.1.2	Разделение обязанностей	Обязанности и зоны ответственности должны быть разделены.
3.	A.7.1.1	Проверка благонадежности	Должна проводиться проверка информации по всем кандидатам на должности.
4.	A.7.2.2	Осведомленность в поле ИБ, обучение и инструктажи	Все сотрудники организации должны обучаться повышению осведомленности.
5.	A.7.2.3	Дисциплинарный процесс	Должен существовать формализованный дисциплинарный процесс за нарушения ИБ
6.	A.8.1.1	Инвентаризация активов	Активы, связанные с информацией и средствами для обработки информации, должны быть определены, и реестр этих активов должен быть составлен и поддерживаться.
7.	A.8.1.2	Владельцы активов	Активам, приведенным в реестре активов, должны быть определены владельцы.
8.	A.8.2.3	Приемлемое использование активов	Процедуры по приемлемому использованию активов должны быть разработаны и внедрены.
9.	A.9.2.2	Инициализация доступа пользователя	Формализованный процесс инициализации доступа должен быть внедрен для назначения или отмены прав доступа для всех типов пользователей во всех системах и услугах.
10.	A.9.2.3	Управление правами привилегированного доступа	Распределение и использование прав привилегированного доступа должно быть ограничено и контролироваться.
11.	A.9.4.1	Ограничение доступа к информации	Доступ к информации и функциям прикладных систем должен быть ограничен в соответствии с политикой управления доступом.
12.	A.9.4.1	Ограничение доступа к информации	Доступ к информации и функциям прикладных систем должен быть ограничен.
13.	A.10.1.1	Политика использования средств криптографии	Политика использования средств криптографии должна быть разработана и внедрена.
14.	A.11.2.4	Техническое обслуживание оборудования	Оборудование должно поддерживаться в надлежащем состоянии для обеспечения его доступности и целостности.
15.	A.12.1.2	Управление изменениями	Изменения в организации, бизнес-процессах, средствах и системах обработки информации, влияющих на ИБ, должны контролироваться.
16.	A.12.1.3	Управление мощностями	Использование ресурсов должно быть контролируемым, приведенным к соответствию с текущими требованиями.
17.	A.12.3.1	Резервируемая информация	Должно выполняться резервное копирование информации, а резервные копии должны регулярно тестироваться в соответствии с утвержденной политикой.
18.	A.13.2.4	Соглашение о неразглашении информации	Должны быть определены требования к соглашениям о неразглашении.
19.	A.16.1.2	Оповещение о событиях ИБ	События ИБ должны быть сообщены по соответствующим управляемым каналам как можно быстрее.
20.	A.16.1.5	Реагирование на инциденты ИБ	Реагирование на инциденты ИБ должно быть установлено в соответствии с документированными процедурами.
21.	A.17.1.2	Внедрение непрерывности ИБ	Организация должна установить, документировать, внедрить и поддерживать процессы, процедуры и средства контроля для обеспечения требуемого уровня непрерывности ИБ во время неблагоприятной ситуации
22.	A.18.2.1	Независимый пересмотр (аудит) ИБ	Подход организации к управлению ИБ должен независимо пересматриваться через запланированные интервалы или когда происходят значительные изменения
23.	A.18.2.2	Соответствие политикам безопасности и стандартам	Менеджеры должны регулярно проводить пересмотр соответствия обработки информации и процедур в пределах своей ответственности
24.	A.18.2.3	Проверка соответствия техническим требованиям	Информационные системы должны регулярно пересматриваться на предмет соответствия политики ИБ организации.

Предложения

С учетом представленных выше тезисов, представляется возможным рассмотреть «облачные» технологии как новый «токсичный» актив, который недостаточно компетентными «эффективными» менеджерами снова предлагается как «серебряная пуля», способная «волшебным образом» решить все проблемы бизнеса разом. В частности, предлагается перемещение всех значимых ИТ-активов в «облака». Именно так, в кавычках, не принимая во внимание ни один технический, технологический, функциональный и пр. резон на базе математических формальных и/или полуформальных моделей. В некоторых проектах были озвучены предложения: давайте, просто перенесем бухгалтерию, логистику и корпоративную почту в «облако» — куда-то далеко, и сразу волшебным образом решатся все вопросы... Предлагались решения по консолидации всех (!) критичных активов в едином «облаке», без обеспечения нужных сервисных контрактов (в том числе ИБ). В ряде случаев представителям ИБ удавалось представить свои аргументы и внести определенный порядок в безопасное «облачное» будущее компании, и один из таких примеров будет представлен далее. В качестве примера представлены два фрагмента вопросников (чек-листов), которые представители подразделений ИБ сначала разработали сами, а затем потребовали заполнить до начала миграции (табл. 3 и 4 соответственно). Первый опросник сформирован на базе пары стандартов ИСО/МЭК серии 27001 и 27005 (компонент «гибридной» методики [5], а второй опросник — на базе стандартов МЭК серии 61508 и стандартов МЭК серии 62443.

Обратим внимание, что ответы на вопросы (A.7.1.1, A.8.2.3, A.9.2.3, A.9.4.1 A.10.1.1, A.11.2.4 и A.18.2.2) являются исключительно важными и критичными для принятия решения о возможности применения «облачных» технологий, так как утрата доверия по одному пункту или нескольким сводит все усилия по за-

Таблица 4. Опросник на базе МЭК 61508 для «облачных» решений (фрагмент)

№	Пункт стандарта	Требование
1.	п. 1.2 g) 61508-1:2010	Рассматривают системы, связанные с безопасностью, и другие меры снижения риска для того, чтобы спецификации требований безопасности систем, связанных с безопасностью, могли быть определены на основе систематического анализа рисков
2.	п. 6.2.1 61508-1:2010	Организация, ответственная за систему, связанную с безопасностью, или за одну или несколько стадий жизненных циклов всей системы безопасности, системы безопасности и ПО системы безопасности, должна выделить … сотрудников, несущих полную ответственность за: • координацию действий, связанных с безопасностью, выполняемых на этих стадиях; • взаимодействие между этими стадиями и другими стадиями, выполняемыми другими организациями; • координацию оценки функциональной безопасности (…), особенно на тех стадиях, где выполнение оценки функциональной безопасности различается, включая взаимодействие, планирование, а также обобщение документации, обоснований и рекомендаций; • удостоверение того, что функциональная безопасность достигнута и продемонстрировано соответствие с целями и требованиями настоящего стандарта.
3.	п. 6.2.14 61508-1:2010	Соответствие компетентности должно рассматриваться для конкретной области применения с учетом всех факторов, включая: c) возможные последствия в случае отказа систем, связанных с безопасностью, - чем серьезнее последствия, тем более строгой должна быть спецификация компетентности; d) уровни полноты безопасности систем, связанных с безопасностью, - чем выше уровень полноты безопасности, тем более строгой должна быть спецификация компетентности; h) инженерные знания, соответствующие области применения и технологии; i) инженерные знания в области безопасности, соответствующие применяемой технологии; j) знание законодательной базы и нормативно-правовой базы в области безопасности
4.	п. 7.6.2.9 61508-1:2010	При завершении проработки распределения требования к полноте безопасности для каждой функции безопасности, распределенные по системе(ам), связанной(ым) с безопасностью, должны быть выражены в терминах полноты безопасности в соответствии
5.	п. 7.3.2.2 61508-2:2012	При планировании подтверждения соответствия системы, связанной с безопасностью, должны быть использованы: a) требования, определенные в спецификации требований к системе безопасности и в спецификации требований к проектированию системы; b) процедуры, применяемые для подтверждения соответствия тому, что каждая функция безопасности правильно выполняется по критериям «прошла испытания/не прошла испытания»; c) процедуры, применяемые для подтверждения соответствия полноте безопасности каждой функции безопасности по критериям «прошла испытания/не прошла испытания»; d) требуемые условия окружающей среды, при которых проводят испытания, включая необходимые инструменты и оборудование (в том числе план, в соответствии с которым эти инструменты и оборудование должны быть калиброваны); e) процедуры оценочных испытаний (с обоснованиями).
6.	п. 7.4.1.5 61508-3:2012	Пятой целью является проверка выполнения требований к ПО, связанному с безопасностью (в отношении необходимых функций безопасности и стойкости к систематическим отказам ПО)
7.	п. 7.4.8.2 61508-3:2012	Проверки интеграции системы ПО должны определять: a) разделение ПО на контролируемые интегрируемые подмножества; b) контрольные примеры и контрольные данные; c) типы проверок, которые должны быть проведены; d) условия тестирования, используемые инструменты, конфигурацию и программы; e) условия, при которых проверка считается выполненной, и f) процедуры, которые необходимо выполнить, если проверка дала отрицательный результат.
8.	п. 8 61508-3:2012	Оценка функциональной безопасности. Свойства стойкости к систематическим отказам ПО • Моделирование • Диаграммы потоков данных • Метод конечных автоматов • Формальные методы • Моделирование во времени сетями Петри • Моделирование реализации • Макетирование/анимация • Структурные диаграммы

щите ИТ к нулю. Были выбраны намеренно примеры участия человека, так как очевидно, что именно этот тип источника угроз является основным и наиболее сложным для оценки, анализа и построения эффективной системы противодействия для «областных» сервисов. Эта проблема не является в чем-либо уникальной, и хотя блестящих успехов не так много, в целом можно полагать, что подходы к обеспечению защиты от «человеческого фактора» имеются.

Более интересным представляется попытка анализа проблемы противодействия техническим угрозам, задуманным и реализованным также не без участия человека, скрытым от беглого взгляда «эффективных» менеджеров, но так и не ставших от этого менее опасными. Речь снова пойдет о функциональной безопасности. В представленной «гибридной» методике ([5]) за этот блок «отвечает» стандарт оценки МЭК серии 15408, но представляется полезным заглянуть в начало базового жизненного цикла электронных компонентов ИТ. Как было многократно замечено: «Разруха не в клозетах, разруха — в головах!» — если для критичных ИТ компонентов далекого «облака» не могут быть получены объективные и проверяемые оценки функциональной безопасности, далее говорить не о чем. Определенно, контроллер в системе охлаждения насоса компрессорной станции или блока бесперебойного питания в ЦОДе могут принести разный вред, но от этого проверка их злонамеренной программной и/или программно-аппаратной архитектурной уязвимости не станет менее актуальной. Дело даже не в том, понесет ли бизнес ущерб, а в том, сможет ли бизнес затребовать от поставщика «облачных» услуг гарантию, исчисленную в количественных оценках надежности, живучести, времени наработки на отказ и пр., как было показано выше ([3, 4]). С учетом «контролей» ([5]) предпримем попытку изучения проблемы безопасности инженерных систем с помощью стандартов МЭК серии 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems и стандартов МЭК серии 62443 Industrial communication networks — Network and system security.

Знание может быть двух видов. Мы знаем сами об объекте, или мы знаем, где можно найти информацию о нем.
С.Джонсон

Заключение

С учетом представленных опросников при решении задачи обеспечения безопасности «облачных» сервисов баланс сил представителей службы ИБ и «эффективных» менеджеров может значительно измениться. В пользу предложенного подхода можно отметить, что появляются формальные требования: «систематический анализ рисков», «примеры», «проверки», «инженерные знания» и пр., которые достаточно сложно имитировать как успешные. Кроме того, подход «гибридной» методики основан на балансе проверяемых требований, и, в частности, если по одному из критериев (например, безопасности инженерных систем) наблюдается двойное несоответствие — и по ИСО/МЭК 27001 (табл. 1) и по ИСО/МЭК 61508 (табл. 2), вся система безопасности предлагаемого «облачного» сервиса «схлопывается» в малопривлекательный нуль.

Список литературы

1. *Лившиц И.И.* Анализ существующих ИТ активов для обеспечения информационной безопасности / И.И. Лившиц, А.В. Неклюдов // Вопросы защиты информации. – 2017. – № 1 (116). – С. 46-57.
2. *Livshitz I., Neklyudov A., Lontsikh P.* Evaluation of IT security — genesis and its state-of-art. IOP Conf. Series: Journal of Physics: Conf. Series 1015 (2018) 042029 DOI: 10.1088/1742–6596/1015/4/042029.
3. *Matsukawa Bakuei, Ryan Flores, Vladimir Kropotov, and Fyodor Yarochkin. S*ecuring Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.0.
4. The 2019 Study on the Cyber Resilient Organization. Ponemon Institute, April 2019.
5. *Livshitz I.I., Neklyudov A.V., Lontsikh P.A.* Security Evaluation – “Hybrid” Approach and Risk of its Implementation. В сборнике: Journal of Physics: Conference Series Сер. "International Conference Information Technologies in Business and Industry 2018 - Enterprise Information Systems" 2018. С. 042030.

Лившиц Илья Иосифович *– канд. техн. наук, доцент факультета безопасности информационных технологий НИУ ИТМО (Университет ИТМО),*

Зайцева Александра Алексеевна *– канд. техн. наук, старший научный сотрудник лаборатории автоматизации научных исследований ФГБУН Санкт-Петербургского института информатики и автоматизации РАН.*
E-mail: cher@iias.spb.su

Компания Zecurion разработала защиту от фотографирования экранов компьютеров

Компания Zecurion, разработчик решений по кибербезопасности, анонсировала выпуск уникального модуля защиты от фотографирования экранов компьютеров и ноутбуков — Zecurion Camera Detector. Таким образом, Zecurion DLP становится на сегодняшний день первым DLP-решением, контролирующим такой канал утечки информации.

Zecurion Camera Detector выявляет фотографирование экранов корпоративных компьютеров на смартфон за счет использования технологий машинного обучения на базе нейронных сетей. При обнаружении подозрительных действий пользователя Zecurion DLP позволяет своевременно оповестить службу информационной безопасности о потенциальной угрозе и снизить риски утечек данных, а сам факт фиксируется в архиве DLP.

Модуль определяет смартфоны, независимо от цвета корпуса и модели, а также подавляет шумы и игнорирует лишние объекты на фоне для более точного определения устройств и уменьшения числа ложных срабатываний. Важно, что модуль работает вне зависимости от того, используется ли камера другими приложениями или нет. То есть DLP-система может контролировать съемку экрана, даже если сотрудник в это время общается по Skype или участвует в видеоконференции.

В будущем компания планирует расширить возможности модуля и типы распознаваемых объектов. Также будет возможность настраивать различные реакции системы при выявлении инцидента — гашение экрана или блокировка учётной записи нарушителя до выяснения ситуации.

Http://www.zecurion.ru