УДК 004.94

И.И. Лившиц

ФОРМИРОВАНИЕ КОНЦЕПЦИИ МГНОВЕННЫХ АУДИТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лившиц И.И. **Формирование концепции мгновенных аудитов информационной безопасности.**

Аннотация. В данной публикации рассмотрена проблема формирования концепции мгновенных аудитов информационной безопасности (ИБ), направленной, в т.ч. на обеспечение защиты от угроз «нулевого дня» (“zero-day”). Отмечается, что эффективное противодействие угрозам «нулевого дня» основывается на реализации комплекса упреждающих мер, а не только на внедрении новых технических средств защиты. Ключевой особенностью концепции мгновенных аудитов ИБ является формирование оценки как предела слева уровня защищенности в процессе выполнения аудитов ИБ. Методической базой концепции мгновенных аудитов является семейство стандартов ISO серии 27001 и 19011, дополненное множеством (расширяемым) метрик ИБ для формирования количественной оценки уровня защищенности объекта. Полученные результаты могут найти применение при создании моделей и методов обеспечения аудитов ИБ и непрерывного повышения уровня защищенности объектов, находящихся под воздействием угроз нарушения ИБ.

Ключевые слова: информационная безопасность; система менеджмента информационной безопасности; аудит; менеджмент рисков; угрозы; уязвимости; стандарты.

Livshits I.I. **Formation of the instantaneous Information Security Audit Concept.**

Abstract. This publication discusses the problem concerning the concept of the instantaneous information security (IT-Security) audits directed, including providing protection against “zero-day” threats. It is noted that effective "zero-day" counteraction based on implementation a set of preventive IT-Security controls, but not limited new technical facilities installation only. A key feature of this concept of instantaneous IT-Security audits is to assess how the left limit of the protection level in the process of IT-Security audits performing. Methodological basis of the concept of instantaneous IT-Security audits is ISO 27001 and 19011 standards series, supplemented by many (expandable) IT-Security metrics to quantify the object protection level. The obtained results can find application in create of models and methods of IT-Security audits performing and continuous improvement for object protection under the influence of IT-Security violation threats.

Keywords: Information security; Information Security Management System; audit; risk management; threats; vulnerabilities; Standards.

1. Введение. Проблема выполнения аудитов (как процесс оценки) для больших и/или сложных систем рассматривалась в классических трудах Н. Винера, Р. Кини, Х. Райфа, И. Пригожина [1–4]. В работе Н. Винера отмечено требование невмешательства человека в процесс, начиная с момента ввода исходных данных и до получения результата ([1], стр. 47). В работе Р. Кини и Х. Райфа важное внимание уделено потоку данных, поступающему уже непосредственно в самом процессе. Отмечается, что выработка и

анализ возможных альтернатив действий становится явно зависимым от информации, которая станет известна уже в процессе ([2], стр. 24). В работе И. Пригожина отмечается подход Карла Рубино (*Rubino C.)*, который обращает внимание на философский принцип выполнения любой деятельности, в том числе оценки – при рассмотрении любого предмета не следует стремиться к большей точности, чем допускает природа предмета [3]. Эти постулаты могут быть эффективно применены при решении актуальных проблем в области информационной безопасности (ИБ). В настоящее время представлены различные материалы по актуальной проблеме противодействия угрозам «нулевого дня» (“zero-day”). В частности отмечается, что «любые процессы, управляемые людьми, ненадёжны», поэтому крупнейшие поставщики средств ИБ предлагают «единственный» вариант – только постоянное совершенствование технических средств защиты информации (СрЗИ), в частности, Check Point Threat Emulation и Qualys Continuous Monitoring [5–7]. Подобная оценка представляется коммерчески выгодной, но весьма далекой от решения хорошо известной технической проблемы – противостояния СрЗИ как «брони» и угроз – как «снаряда».

Очевидно, что «гонка вооружения» между целевыми (таргетированными) атаками (“advanced persistent threats”, APT) не приведет в ближайшем времени к повышению уровня защищенности объектов, и это отмечается многими экспертами [8–10]. В этой ситуации предлагается применять не только технический подход (СрЗИ) для противодействия угрозам «нулевого дня», но предложить комбинированный метод, основанный на концепции мгновенных аудитов ИБ. Методической базой концепции мгновенных аудитов является семейство стандартов ISO серии 27001 и 19011, дополненное множеством (расширяемым) метрик ИБ для формирования количественной оценки уровня защищенности объекта [11 – 15]. В частности, рекомендуется применять дополнительно количественные метрики обеспечения ИБ из стандартов ISO серии 20000 (для управления ИТ-услугами, например – SLA) [16] и ISO серии 22301 (для управления непрерывностью бизнеса, например – RTO, RPO) [17]. Для успешного решения отраслевых задач ИБ необходимо принять во внимание дополнительно специфические отраслевые стандарты, в частности для аэродромных комплексов – IATA [18].

Необходимо отметить, что сам процесс аудитов (в том числе ИБ) хорошо известен и является обязательным требованием всех упомянутых стандартов ISO (в Российской Федерации они приняты

как ГОСТ Р ИСО), при этом на усмотрение организации отдаются вопросы планирования (частоты) выполнения аудитов и области охвата (“scope”) [19 – 21]. Именно на процесс аудитов, управляемый по частоте, возлагается задача оперативного (в режиме близком к режиму реального времени) выявления уязвимостей в информационных системах (ИС), которые могут быть использованы при реализации угроз «нулевого дня». В стандарте ISO 19011 установлены требования по формированию объема программы аудита, фокусирования на вопросах, наиболее важных для организации, принятие во внимание событий ИБ, произошедших утечек и иных инцидентов [15]. Для формирования концепции мгновенных аудитов ИБ, как средства противодействия АТР, представляется полезным применить известное математическое понятие предела функции, точнее, предела слева, которое позволит формировать количественные оценки защищенности в процессе выполнения аудитов ИБ.

2. Постановка задачи. Как отмечалось выше, в настоящее время для решения проблемы противодействия угрозам «нулевого дня» предлагается «единственный» вариант – только постоянное совершенствование технических СрЗИ, оснащенных новыми («виртуальными», «сканирующими», «аналитическими» и пр.) модулями, способными противостоять АРТ [8 – 10]. В тоже время не приходится ожидать, что процесс постоянного совершенствования только технических СрЗИ приведет к видимому успеху, т.к. охватывает только некоторую часть (технических уязвимостей) инфраструктуры безопасности. В частности, методология систем менеджмента информационной безопасности (СМИБ) рассматривает значительно больше уровней иерархии защиты и типов объектов (в терминологии ISO – “asset”), соответственно, предлагается и значительно больше мер (средств) обеспечения ИБ (в терминологии ISO – “control”) [12]. Более того, расширение перечня применяемых стандартов ISO позволит реализовать интегрированную систему безопасности для выбранных критичных объектов, когда СМИБ дополняется требованиями указанных выше стандартов ISO [16, 17]. В равной мере в указанных стандартах ISO отражено и требование выполнения аудитов и требование обеспечения безопасности, которые могут быть реализованы как в рамках отдельной СМИБ, так и интегрированной системы безопасности [11, 16, 17].

Реализация данных требований в предлагаемой концепции дополняется еще одним важным параметром – требуемой частотой выполнения аудитов с целью максимального повышения

осведомленности и скорости принятия адекватных решений об уязвимостях, которые могут быть использованы злоумышленниками для реализации АТР, об объективной оценке текущего уровня обеспечения ИБ. В этих условиях постановка задачи формулируется следующим образом – разработка концепции мгновенных аудитов ИБ на методической базе риск-ориентированных стандартов ISO, с целью обеспечения комплексного подхода для оценивания защищенности ценных для бизнеса объектов с любой требуемой частотой.

3. Обоснование практической ценности мгновенных аудитов. Практическая ценность предлагаемой концепции мгновенных аудитов основана на известных фактах, что порядка 96% успешных взломов можно было бы избежать, если бы был внедрен ряд простых мер ИБ, а более 75% атак использовали уже известные уязвимости, которые могли бы быть «закрыты» регулярными патчами безопасности [7, 8]. При этом отмечается, что 85% реально произошедших вторжений были обнаружены спустя месяцы (среднее время обнаружения – 5 месяцев) [7, 9].

Дополнительно представляется целесообразным отметить отчет ЦБ РФ за 2014 г. с актуальными данными по оценке обеспечения ИБ на уровне пользователей [22]. В целом банковская система РФ продемонстрировала способность останавливать от 46% до 38% несанкционированных операций (НСО), а средняя сумма одной НСО составляет 335 тыс. руб. В большинстве случаев НСО, связанные с попытками списания денежных средств посредством систем дистанционного банковского обслуживания, произошли вследствие воздействия вредоносного кода на используемое устройство. Также распространенной причиной НСО являлось применение социальной инженерии с использованием сети «интернет», электронной почты и услуг, предоставляемых операторами связи (распространение информации, побуждающей клиента сообщать информацию, необходимую для осуществления переводов денежных средств, в т.ч. информацию аутентификации).

В качестве мер противодействия угрозам «нулевого дня» в настоящее время применяются различные подходы, направленные, в основном, на пресечение последствий потенциально возможных угроз, но не на выявление и устранение уязвимостей, например:

1. «Песочницы», имитирующие рабочие станции организации, в которых анализируются запускаемые файлы на предмет возможных деструктивных воздействий;

2. Анализ аномальной сетевой активности, который осуществляется путем сравнения текущей сетевой активности с построенной эталонной моделью сетевого поведения;

3. Поведенческий анализ рабочих станций, основанный на сравнении активности рабочих станций с эталонной моделью (на уровне самой рабочей станции).

Соответственно, для атак «нулевого дня» (реакция на которые крайне критична по времени) указанные выше примеры дают известный эффект только при постоянном наращивании вычислительных ресурсов для сокращения времени «аналитических» проверок СрЗИ в режиме, близком к режиму реального времени. При этом не инициируется объективный анализ всей совокупности потенциальных уязвимостей и не затрагивается уровень технологических, программных и иных уязвимостей [11, 14].

Рассмотрим дополнительно обоснование адекватности результатов оценки уровня защищенности для ИС, получаемых в случае применения концепции мгновенных аудитов. В работе Ф. Перегудова и Ф. Тарасенко отмечается, что адекватность подразумевает выполнение определенных требований «не вообще», а в той мере, которая достаточна для достижения цели. Можно дать оценку адекватности, если ввести количественную меру, или, цитируя точно: “количественно выражаемую меру адекватности” ([4], стр. 51). Также можно применить рекомендации Р. Кини и Х. Райфа по введению групповых решений, которые, цитируя точно: “систематизируют решение конкретных проблем” ([2], стр. 22). На практике эти рекомендации применяются для формирования количественных метрик, пригодных, в том числе, для групповых оценок деятельности в области ИБ, например – динамика количества выявленных уязвимостей в ИС по результатам аудитов ИБ.

Процесс аудитов [15], как любой процесс оценки, предполагает получение объективных оценок на основании свидетельств аудита, которые затем могут быть воспроизведены, и дополнительно проверены независимыми экспертами (в соответствии с критериями аудита). При этом сам процесс оценки также предполагает определенные временные рамки (как было показано выше [2]), при этом управление «частотностью аудита» позволяет более оперативно контролировать динамику процесса изменения уровня защищенности против любых изменений (соответственно – «динамической перестройки» критериев аудита) [19, 20]. Важным преимуществом предложенной концепции является акцентирование именно на

получении численных оценок, а не простого «соответствия» или «несоответствия». Именно периодическое систематическое получение измеримых численных оценок ИБ, представляется практически полезным для лиц, принимающих решение (ЛПР). Соответственно, адекватность результатов оценки уровня защищенности ИС допустимо трактовать, во-первых, как соответствие установленным критериям аудита, во-вторых, соответствие процессным требованиям аудита ИБ, в-третьих – получение «текущих» значений уровня реализации мер (средств) обеспечения ИБ, необходимых для поддержки принятия «разумных решений» ЛПР [2].

4. Требования ISO к проведению аудитов СМИБ. Требования выполнения аудитов СМИБ на постоянной циклической основе определены в стандарте ISO/IEC 17021:2006. В частности, отмечается, что «программа аудита должна включать в себя проведение двухэтапного первичного аудита, надзорных аудитов в течение первого и второго года и ресертификационного аудита – в течение третьего года до истечения срока действия сертификата. Трехлетний цикл сертификации начинается с принятия решения о сертификации или ресертификации» (п. 9.1.1). Также отмечается частота выполнения надзорных аудитов – «надзорные аудиты (инспекционный контроль) должны проводиться, по крайней мере, один раз в год. Проведение первого надзорного аудита (инспекционного контроля) с момента первоначальной сертификации должно быть не позже, чем через 12 мес. после последнего дня второго этапа аудита» (п. 9.3.2.2). Аналогичные требования предъявляются к проведению аудитов по требованию PCI DSS, в частности все три вида аудитов (QSA – внешний, ISA – внутренний и SAQ – самооценка) проводятся с периодичность 1 раз в год.

Последовательность выполнения аудитов СМИБ с учетом требований ISO/IEC 17021:2006 состоит из: CA – сертификационных аудитов (1-й и 2-й этапы соответственно), SA – надзорных аудитов (1-го и 2-го года соответственно) и RA – ресертификационного аудита (см. рисунок 1). Для данной публикации важно, что интервалы ($t_1 - t_0$), ($t_2 - t_1$) и ($t_3 - t_2$) в общем случае (без экстраординарных ситуаций) равны. Дополнительно необходимо отметить, что аналогичного подхода придерживаются и иные международные системы аудитов, в частности – IATA [18, 23, 24]. В стандарте ISO 19011 (п. 5.2, e), h), j) непосредственно указано, что цели аудита должны формироваться с учетом: правовых и иных других требований, которые организация принимает на себя;

показателей деятельности организации (случаи возникновения нарушений, инцидентов или жалоб потребителей) и результатов предыдущих аудитов [15].

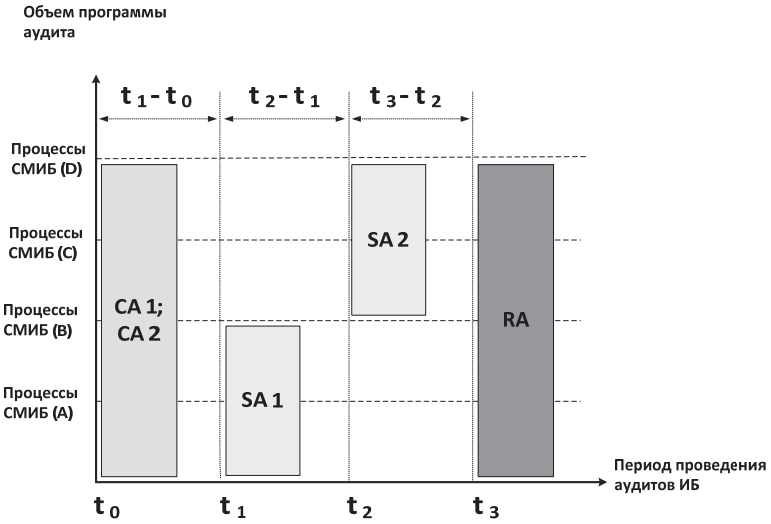

Рис. 1. Схема выполнения аудитов СМИБ

Также ISO 19011 (п. 5.3.3) при формировании объема программы аудита рекомендует принять во внимание факторы: законодательные, контрактные и другие требования, которые организация обязана выполнять; результаты предыдущих внутренних или внешних аудитов; существенные изменения в организации (ее деятельности); возникновение событий внутреннего и внешнего характеров, таких как утечки секретной информации, действия преступного характера [15]. Соответственно, представляется нелогичным и экономически нецелесообразным постоянно осуществлять значительные затраты на применение только дорогостоящих СрЗИ – если, например, на уровне рабочих станций не выполняются требования доменных политик ИБ, на уровне пользователей – не выполняется информирование о правилах работы в сети интернет, на уровне руководителей – не выполняются аудиты ИБ, анализ отчетов и принятия безотлагательных мер в области ИБ.

5. Концепция мгновенных аудитов СМИБ. Концепция мгновенных аудитов предполагает реализацию принципа выполнения аудитов ИБ с частотой, определяемой высшим менеджментом (ЛПР) и

зависящей от предыдущего состояния «слева» уровня защищенности объекта [15, 18, 24 – 26]. Иными словами, если предыдущий Аудит_1 ИБ, проведенный, предположим, месяц назад (отметка t_0) выявил ряд несоответствий (в терминах [15, 18]) и показал, что 40% компьютеров по-прежнему работают под Windows XP с SP2, на 60% рабочих станций пользователи обладают правами администратора, на 70% ноутбуков обновление антивируса не выполняются и/или отключены, то оценка (отметка t_1) текущего уровня защищенности $R_{base} \mid t_1 <= R_{base} \mid t_0$, т.е. не выше предыдущей (см. рисунок 2).

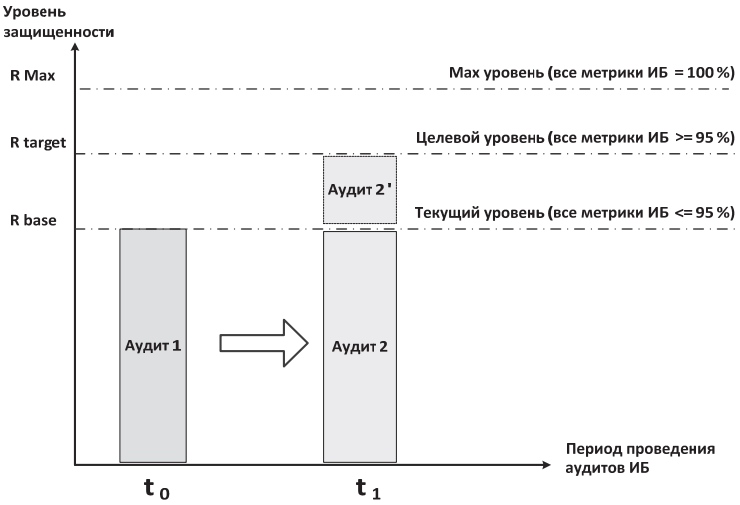

Рис. 2. Оценка достижения уровней защищенности

Также маловероятно и экономически нецелесообразно проводить Аудит_2′ в надежде достигнуть на отметке t_1 целевой уровень защищенности R_{target}, например, 95% (смотри рисунок 2). Соответственно, текущая защищенность объекта (отметка t_1) $R_{target} \mid t_1$ соответствует оценке слева (отметка t_0) $R_{base} \mid t_0$ при отсутствии изменений в состоянии защищенности объекта, выявленных предыдущем Аудит_1. При изменении на интервале ($t_0 – t_1$) состава мер (средств) ИБ, закрытия выявленных на Аудит_1 несоответствий (например, проведения дополнительного обучения), выполнение последующего аудита (Аудит_2′) может иметь смысл для достижения R_{target}. Важно, что частота выполнения аудитов ИБ определяется, в

том числе и допустимым уменьшением интервала ($t_0 - t_1$), например, с ежегодного (как это принято в СМИБ, PCI DSS, IATA) до ежемесячного (еженедельного) и чаще – по требованию ЛПР.

Проблема определения оптимальной частоты аудитов ИБ определяется решением ЛПР на основании полученных наборов оценок защищенности и проведенного анализа в рамках стандартной процедуры «Анализ со стороны руководства» ("Management review") [11, 15, 17, 18]. Очевидно, что бессмысленно выполнять подряд аудиты ИБ друг за другом, не успевая исправить выявленные несоответствия, не успевая полностью реализовать комплекс корректирующих мер. В частности, метрикой для «старта» следующего аудита ИБ, может являться скорость «замыкания» мини-цикла PDCA, которая, объективно, формирует предел lim ($t_k - t_i$). Соответственно, для достижения R_{target} период аудитов ИБ может уменьшаться как lim ($t_k - t_i$) $\rightarrow 0$ (см. рисунок 3).

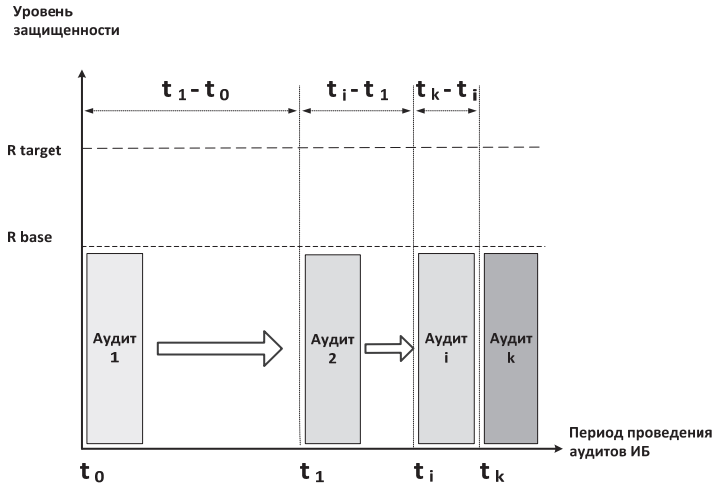

Рис. 3. Снижение периода оперативного противодействия угрозам

Кроме того, для эффективного противодействия APT необходимо уменьшить период выявления, анализа и «закрытия» несоответствий, так как успешная реализация этого процесса представляется значительно быстрее, чем выбор, закупка, доставка, установка и настройка новых и новых СрЗИ. При этом, во-первых, выполняются все требования ISO, во-вторых, дополнительно выполняются требования ЛПР (не желающих ждать целый год для приведения ИБ к требуемому бизнесом уровню защищенности), а в-

третьих, решаются вопросы оперативного противодействия современным угрозам (в пределе «время реакции» СМИБ ($t_k - t_i$) стремится к нулю).

6. Система метрик процесса мгновенных аудитов. Любая концепция обеспечения ИБ требует обоснования у ЛПР (владельцев ценных для бизнеса активов) численных оценок достигнутого (реального) уровня защищенности. Предлагаемая концепция мгновенных аудитов применяет систему количественных (численных) метрик ИБ на базе:

1. Рекомендации SANS;
2. Рекомендации PCI DSS (например, версии 3.0);
3. Стандарты ISO (например, ISO 27004);
4. Стандарты Центрального банк РФ (например, СТО БР ИББС);
5. Документы ФСТЭК (например, приказ ФСТЭК № 31).

Рассмотрим на примере систему мер (средств) обеспечения ИБ, сформированную на базе рекомендаций SANS [6, 9], документов ФСТЭК и стандарта ISO 27001 [11]. Примем во внимание, что предлагаемый состав метрик ИБ не является фиксированным (возможно расширение по требованию ЛПР, регуляторов, контрагентов и пр.), и рекомендуемые метрики содержат не только СрЗИ, но и комплекс организационных мер (см. таблица 1).

Таблица 1. Соответствие мер (средств) обеспечения ИБ

№ п.п.	Контроль SANS	Мера ИБ (ISO 27001)	Мера защиты информации (ФСТЭК)
1.	Учет авторизованных (неавторизованных) устройств	A.8.1.1 – A.8.1.4, A.11.2.8	ИАФ.2
2.	Учет авторизованного (неавторизованного) ПО	A.8.1.1 – A.8.1.4	ИАФ.7 ОПС.0 - ОПС.4
3.	Безопасная конфигурация рабочих станций, серверов, ноутбуков	A.12.1, A.18.2.3	ЗСВ.7, ЗИС.29 УКФ.0 – УКФ.5
4.	Постоянное обнаружение и оценка уязвимостей	A.12.6, A.17.1.2	АНЗ.1 ОБР.1
5.	Защита почтовых приложений	A.12.5.1, A. 13.2.3	АВЗ.0 – АВЗ.3
6.	Прикладное ПО для обеспечения ИБ	A.9.4.4	ИАФ.7 ЗИС.25
7.	Контроль беспроводных соединений	A.9.1.2	УПД.14 ЗИС.3, ЗИС.20
8.	Резервирование (архивирование) данных	A.12.3.1	ОДТ.2 ЗСВ.8, ДНС.4
9.	Обучение и тренинги в области ИБ	A.7.2.2	ДНС.2 ИПО.0 – ИПО.3
10.	Безопасная конфигурация сетевых устройств	A.13.1.1	УПД.3

7. Обоснование математической базы концепции мгновенных аудитов. Для формирования оценки защищенности по результатам аудитов ИБ необходимо применять достоверные математические понятия, дающие обоснование предложенной концепции, в частности одностороннего предела (точнее, предела функции слева). Число $A \in R$ называется левым пределом (или пределом слева) функции *f(x)* в точке a, если для всякого положительного числа ε отыщется отвечающее ему положительное число δ, такое, что для всех точек x из интервала (a – δ, a) справедливо неравенство [27]:

$$| f(x) - A | < \varepsilon.$$

или

$$\lim_{x \to a-0} f(x) = A \Leftrightarrow \forall \varepsilon > 0 \; \exists \delta = \\ = \delta(\varepsilon) > 0 \; \forall x \in (a - \delta, a): | f(x) - A | < \varepsilon.$$

Производная функции *f (x)*:

$$\lim_{\Delta x \to 0} = \frac{f(x+\Delta x) - f(x)}{\Delta x} = \lim \frac{d}{dx} f(x) = f'(x).$$

Соответствующий односторонний предел называют левой производной, обозначают $f'_{-}(x)$ [27, 28].

8. Пример определения частных производных для мгновенных аудитов ИБ. Левая производная позволяет оценить требуемый интервал, на котором допустимо (по времени) могут быть выполнены необходимые изменения в СМИБ и обосновано проведение нового аудита ИБ. Для цели противодействиям угрозам «нулевого дня» рассмотрим действительную функцию переменных:

$$y = f(x_1, x_2, x_3, \ldots, x_n),$$

где, например, первые 4 переменные описывают атрибуты аудитов ИБ:

x_1 – частота проведения аудитов, определяемая как отношение кол-ва аудитов в СМИБ к наблюдаемому периоду;

x_2 – объем программы аудитов, определяемый как отношение кол-ва охваченных процессов к общему кол-ву процессов в заявленной области сертификации СМИБ;

x_3 – метрика достижения уровня защищенности, определяемая как мера результативности СМИБ R_{base} / R_{Max};

x_4 – метрика выполнения корректирующих действий, запланированных на интервал проведения аудитов ИБ.

Тогда частная производная первого порядка по первой переменной x_1 имеет вид:

$$\lim_{\Delta x_1 \to 0} = \frac{f(x_1 + \Delta x_1, x_2, x_3, \ldots, x_k) - f(x_1, x_2, x_3, \ldots, x_k)}{\Delta x_1} = \frac{\partial}{\partial x_1} f(x).$$

Для одной изменяемой переменной x_1 (например, частоты проведения аудитов ИБ) оценим практическое значение частной производной (при неизменности иных переменных), получаем оценку скорости роста уровня защищенности СМИБ:

$$\frac{\partial}{\partial x_1} = f'x_1(x_1, x_2, x_3, \ldots, x_n) = \frac{\Delta R_k}{\Delta t k}.$$

Реализация концепции мгновенных аудитов для оценки защищенности ценных для бизнеса активов с любой требуемой частотой, может быть продемонстрирована как сокращение периода (увеличение частоты) проведения аудитов ИБ при использовании предела слева функции переменных. Заметим, что предложенная концепция позволяет дополнительно исправлять возможные ошибки, присущие сложному процессу аудита, методом локализации обратным процессом, как показано в работе Н. Винера ([1], стр. 222). «Второй контур контроля», реализующий локализацию ошибки стартует с точки, где она замечена, но крайне важно обеспечить, чтобы проверка и отработка выявленной ошибки шла с такой же скоростью, как и сам процесс аудита ИБ, иначе «эффективная скорость» процесса обеспечения ИБ (в составе СМИБ или ИСМ) может снижаться из-за более медленного процесса аудита ИБ.

Отметим снова, что полная «скорость реакции» СМИБ определяется частотой аудитов ИБ, что значительно превышает скорость полного цикла обновлений даже наилучших отраслевых решений CheckPoint [6, 7, 10]. При этом объективно повышается способность системы (СМИБ или ИСМ) эффективно противодействовать угрозам «нулевого дня» в режиме, близком к режиму реального времени. В примере для одной переменной x_1 продемонстрировано увеличение скорости роста уровня защищенности СМИБ $\frac{\Delta R_k}{\Delta t k}$ при известных переменных процесса аудитов ИБ (см. рисунок 4).

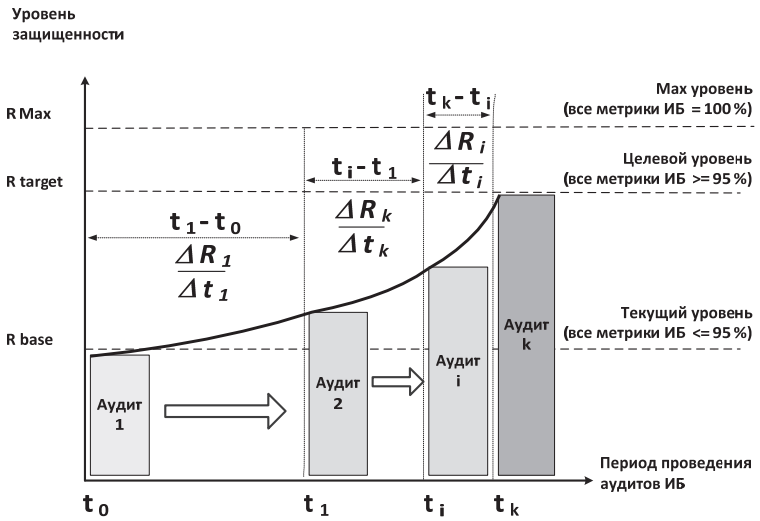

Рис. 4. Пример увеличения скорости роста уровня защищенности

9. Заключение. Предлагаемая концепция мгновенных аудитов ИБ базируется на формировании оценки «предела слева» функции переменных, характеризующих процесс выполнения аудитов ИБ, и направлена на создание непрерывной системы комплексного обеспечения ИБ, в том числе для защиты от угроз «нулевого дня» (“zero-day”).

Литература

1. *Винер Н.* Кибернетика, или управление и связь в животном и машине. 2-е издание // М.: Наука; Главная редакция изданий для зарубежных стран. 1983. 344 с.
2. *Р.Л. Кини, Х. Райфа.* Принятие решений при многих критериях: Предпочтения и замещения: Пер. с англ./ Под ред. И.Ф. Шехнова // М.: Радио и Связь. 1981. 560 с.
3. *Пригожин И., Стенгерс И.* Время. Хаос. Квант. К решению парадокса времени // М.: Едиториал УРСС, 2003. 240 с.
4. *Перегудов Ф.И., Тарасенко Ф.П.* Введение в системный анализ // М.: Высшая школа. 1989. 360 с.
5. Официальный сайт Center for strategic and International Studies. URL: www.csis.org (дата обращения 07.07.2015).
6. Официальный сайт Infosecurity Russia. URL: www.infosecurityrussia.ru (дата обращения 07.07.2015).
7. Официальный сайт Trustwave. URL: www.trustwave.com (дата обращения 07.07.2015).
8. An Osterman Research White Paper «Dealing with Data Breaches and Data Loss Prevention» // Osterman Research, Inc. 2015.

9. Официальный сайт Reuters. URL: www.reuters.com (дата обращения 07.07.2015).
10. *Morvay Z., Gvozdenac D.* Applied Industrial Energy and Environmental Management // John Wiley & Sons, Chichester, UK, 2008.
11. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems // Requirements, International Organization for Standardization. 2013. 23 p.
12. ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems // Overview and vocabulary, International Organization for Standardization. 2014. 31 p.
13. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems // Measurement, International Organization for Standardization. 2009. 55p.
14. ISO/IEC 27005-2011 Information technology. Security techniques. Information security management systems // International Organization for Standardization. 2011. 68 p.
15. ISO 19011:2011. Guidelines for auditing management systems // International Organization for Standardization, 2011. 44 p.
16. ISO/IEC 20000-1:2011. Information technology. Service management. Part 1: Service management system requirements // International Organization for Standardization. 2011. 26p.
17. ISO 22301:2012. Societal security. Business continuity management systems // Requirements, International Organization for Standardization. 2012. 24 p.
18. IATA Reference Manual for Audit Programs // Effective, 5-rd Edition. 2014.
19. *Лившиц И.И.* Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов BSI и ISO // Информатизация и Связь. 2013, Вып. 6. С. 62–67.
20. *Лившиц И.И.* Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества. 2013. Вып. 1. С. 22–34.
21. *Лившиц И.И.* Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. 2014. Вып. 6. С. 72–94.
22. Официальный сайт Центрального Банка РФ URL: www.cbr.ru (дата обращения 07.07.2015).
23. *Шмельова Т.Ф., Сікірда Ю.В., Ассаул О.Ю.* Вплив факторів середовища менеджменту авіапіприемства на безпеку авіаційної діяльності // Технологический аудит и резервы производства. 2015. Т. 2. № 3 (22). С. 17-24.
24. *Нехорошкин Н.И.* Проблемы и возможности информационно-аналитического обеспечения аудита проектов и программ // Вестник АКСОР. 2010. Т. 1. № 12. С. 41-45.
25. *Голощапов А.Н., Рыжов И.В.* Общая характеристика и алгоритм проведения внутреннего аудита системы менеджмента качества организации // Экономика и предпринимательство. 2012. № 5 (28). С. 244-248.
26. *Васильков Ю.В., Гущина Л.С.* Система менеджмента рисков как инструмент управления экономикой предприятия // Методы менеджмента качества. 2012. № 2. С. 10-15.
27. *Ильин В. А., Садовничий В. А., Сендов Бл. Х.* Глава 3. Теория пределов. Математический анализ / Под ред. А. Н. Тихонова. — 3-е изд., перераб. и доп. // М.: Проспект, 2006. Т. 1. 672 с.
28. *Корн Г., Корн Т.* Справочник по математике для научных работников и инженеров // М.: Наука. 1978. 832 с.

References

1. Viner N. *Kibernetica ili upravlenie i svyaz v zhivotnom i mashine*. [Cybernetics or Control and Communication in the Animal and the Machine]. M.: Nauka, 1983. 344 p. (in Russ).
2. Kini R., Raifa X. *Prinyatie resheni pri mnogih kriteriyah: predpochteniya i zamesheniya*. [Decisions with multiple objectives: Preferences and substitution]. M.: Radio i Svyaz,1981. 240 p. (in Russ).
3. Prigozhin I., Stengers I. Vremya. Haos, Kvant. *K resheniu paradoksa vremeni.* [Time. Chaos. Quantum. To the solution of the paradox of time]. M.: Editorial URSS, 2003. 240 p. (in Russ).
4. Peregudov F., Tarasenko F. Vvedenie v sistemnyi analis. [Introduction to system analysis]. M.: Higher school, 1989. 360 p. (in Russ).
5. Oficial'nyi sait "Center for strategic and International Studies" [Official web site of "Center for strategic and International Studies"]. Available at: www.csis.org (accessed 07.07.2015).
6. Oficial'nyi sait "Infosecurity Russia" [Official web site of "Infosecurity Russia"]. Available at: www.infosecurityrussia.ru (accessed 07.07.2015). (in Russ).
7. Oficial'nyi sait Trustwave [Official web site of Trustwave]. Available at: www.trustwave.com (accessed 07.07.2015).
8. An Osterman Research White Paper «Dealing with Data Breaches and Data Loss Prevention». Osterman Research, Inc. 2015.
9. Oficial'nyi sait Reuters [Official web site of Reuters]. Available at: www.reuters.com (accessed 07.07.2015).
10. Morvay Z., Gvozdenac D. Applied Industrial Energy and Environmental Management. John Wiley & Sons, Chichester, UK. 2008.
11. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization. 2013. 23 p.
12. ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems. Overview and vocabulary, International Organization for Standardization. 2014. 31 p.
13. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems. Measurement, International Organization for Standardization. 2009. 55p.
14. ISO/IEC 27005-2011 Information technology. Security techniques. Information security management systems. International Organization for Standardization. 2011. 68 p.
15. ISO 19011:2011. Guidelines for auditing management systems. International Organization for Standardization, 2011. 44 p.
16. ISO/IEC 20000-1:2011. Information technology. Service management. Part 1: Service management system requirements. International Organization for Standardization. 2011. 26p.
17. ISO 22301:2012. Societal security. Business continuity management systems. Requirements, International Organization for Standardization. 2012. 24 p.
18. IATA Reference Manual for Audit Programs. Effective, 5-rd Edition. 2014.
19. Livshitz I. [Joint problem solving information security audit and ensure the availability of information systems based on the requirements of international standards BSI / ISO]. *Informatisatia i Svyaz' – Informatization and Communication*. 2013. vol. 6. pp. 62–67. (In Russ).

20. Livshitz I. [Practical purpose methods for ISMS evaluation]. *Menedzhment kachestva – Quality Management*. 2013. vol. 1. pp. 22–34 (In Russ).
21. Livshitz I. [Approaches to the application of the integrated management system model for carrying out audits for complex industrial facilities – airport complexes]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2014. vol. 6, pp. 72–94. (In Russ).
22. Oficial'nyi sait Cenral'nogo Banka RF [Official web site of Central Bank of RF]. Available at: www.cbr.ru. (accessed 07.07.2015). (In Russ).
23. Shmeleva T., Sikirda Y., Assaul O. [The influence of environmental factors management of the airline safety aviation activity]. *Tehnologicheskij audit i rezervy proizvodstva – Technological audit of production and reserves*. 2015. vol. 2 part 3. pp. 17–24 (in Ukrainian).
24. Nechorochkin N. [Challenges and opportunities of information and analytical support for the projects and programmes audit]. *Vestnik AKCOR – Bulletin AKSOR*. 2010. vol. 1, part 12, pp. 41–45. (In Russ).
25. Goloshapov A., Ryzhov I. [General characteristics of the algorithm and the internal audit of the quality management system of the organization]. *Ekonomika i predprinimatel'stvo – Economics and Business*. 2012. vol. 5. pp. 244–248. (in Russ).
26. Vasil'kov Y., Gushina L. [The risk management system as a tool of enterprise economic management]. Metody menegementa kachestva – Methods of Quality Management. 2012. vol. 2. pp. 10–15. (In Russ).
27. Il'in V., Sadovnichi V., Sendov B. *Glava 3. Teoria predelov. Matematicheskiy analis* [Chapter 3. Theory of limit. Mathematical Analysis]. M.: Prospect. 2006. vol. 1. 672 p. (in Russ).
28. Korn G., Korn T. *Spravochnik po matematike dlya nauchnich rabotnikov I inzhenerov* [Mathematics handbook for scientist and engineers]. M.: Nauka, 1978. 832 p. (in Russ).

Лившиц Илья Иосифович — к-т техн. наук, ведущий аналитик, ООО "Газинформсервис". Область научных интересов: системный анализ, защита информации, риск-менеджмент. Число научных публикаций — 50. Livshitz.il@yandex.ru; 197082, Санкт-Петербург, Богатырский пр.; р.т.: +7(921) 934-48-46.

Livshitz Ilya Iosifovich — Ph.D., lead analyst, LLC "Gasinformservice". Research interests: system analyses, IT-security, risk-management. The number of publications — 50. Livshitz.il@yandex.ru; 197082, Saint-Petersburg, Bogatirskyi str.; office phone: +7(921) 934-48-46.

РЕФЕРАТ

Лившиц И.И. **Формирование концепции мгновенных аудитов информационной безопасности.**

В данной публикации кратко рассмотрена проблема формирования концепции мгновенных аудитов информационной безопасности (ИБ), направленной, в т.ч. на обеспечение защиты от угроз «нулевого дня» (“zero-day”). В настоящее время представлены различные материалы по актуальной проблеме противодействия угрозам «нулевого дня», в частности отмечается, что «любые процессы, управляемые людьми, ненадёжны».

В этой ситуации предлагается применять не только технические методы, но предложить комбинированный метод, основанный на концепции мгновенных аудитов ИБ. Методической базой концепции мгновенных аудитов является семейство стандартов ISO серии 27001 и 19011, дополненное множеством (расширяемым) метрик ИБ для формирования количественной оценки уровня защищенности объекта.

Для формирования оценки защищенности по результатам аудитов ИБ необходимо применять достоверные математические понятия, дающие обоснование предложенной концепции. Решение поставленной задачи – обеспечение комплексного подхода для оценки защищенности ценных для бизнеса активов с любой требуемой частотой, может быть продемонстрировано как сокращение периода (увеличение частоты) проведения аудитов ИБ при использовании предела слева функции переменных. В примере для одной переменной продемонстрировано увеличение скорости роста уровня защищенности СМИБ при известных переменных процесса аудитов ИБ, что позволяет успешно противодействовать угрозам «нулевого дня».

Данные результаты могут найти применение при создании моделей и методов обеспечения аудитов СМИБ и мониторинга состояния объектов, находящихся под воздействием угроз нарушения ИБ, а также при создании моделей и методов оценки защищенности информации объектов СМИБ.

SUMMARY

Livshits I.I. **Formation of the instantaneous Information Security Audit Concept.**

This publication discusses the problem of formation the concept of the instantaneous information security (IT-Security) audits directed, including providing protection against “zero-day” threats. Various recent materials are presented to the actual problem of counter zero-day threats notes that "*any process-driven people, unreliable*". In this situation it is proposed to use not only a technical methods to counter “zero-day” threats, but to offer a combined method based on the concept of instantaneous IT-Security audits. Methodological basis of the concept of instantaneous audits both the ISO 27001 and ISO 19011 standards, which extended with the set of (extensible) metrics for IT-Security formation to quantify the object protection level.

For the formation of IT-Security assessment on the results of IT-Security audits it is necessary to use accurate mathematical concepts, giving the rationale for the proposed concept. The solution of this problem – providing an integrated approach to IT-Security evaluate of valuable business objects with any desired frequency can be shown as a reduction of the period (increase the frequency of IT-Security audits when using the left limit of the function variables. In the example for one variable was demonstrated an increase in the rate of growth of the ISMS level variables with known IT-Security audits process. These results can be used to create models and methods to ensure the ISMS audits and monitoring of objects under the influence of threats to IT-Security violations, as well as the creation of models and methods of estimation of IT-Security facilities ISMS.