Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

8. ГОСТ Р ИСО/МЭК 17021:2011. Оценка соответствия. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента;

9. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems // Measurement, International Organization for Standardization. 2009. 55p.

МЕТОДИКА МГНОВЕННЫХ АУДИТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.И. ЛИВШИЦ, А.В. НЕКЛЮДОВ

Университет ИТМО, г. Санкт-Петербург

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). Эти постулаты могут быть эффективно применены при решении актуальных проблем в области информационной безопасности (ИБ). 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.

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. В этой ситуации предлагается применять не только технический подход (СрЗИ) для противодействия угрозам, 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 [5, 6]. В частности, рекомендуется применять дополнительно количественные метрики обеспечения ИБ из стандартов ISO серии 20000 (для управления ИТ-услугами, например – SLA) [7] и ISO серии 22301 (для управления непрерывностью бизнеса, например – RTO, RPO) [8]. Необходимо отметить, что сам процесс аудитов (в том числе ИБ) хорошо известен и является обязательным требованием всех упомянутых стандартов ISO, при этом на усмотрение организации отдаются вопросы планирования (частоты) выполнения аудитов и области охвата (“scope”) [9 – 11]. Именно на процесс аудитов, управляемый по частоте, возлагается задача оперативного выявления уязвимостей в информационных системах (ИС). Для формирования концепции мгновенных аудитов ИБ, как средства противодействия ATP, представляется полезным применить известное математическое понятие предела функции, точнее, предела слева, которое позволит формировать количественные оценки защищенности в процессе выполнения аудитов ИБ.

В настоящее не приходится ожидать, что процесс постоянного совершенствования только технических СрЗИ приведет к видимому успеху, т.к. охватывает только не-

которую часть (технических уязвимостей) инфраструктуры безопасности. 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”). Более того, расширение перечня применяемых стандартов ISO позволит реализовать интегрированную систему безопасности для выбранных критичных объектов, когда СМИБ дополняется требованиями указанных выше стандартов ISO [5, 7, 8].

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.

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. При этом отмечается, что 85% реально произошедших вторжений были обнаружены спустя месяцы (среднее время обнаружения – 5 месяцев). Рассмотрим дополнительно обоснование адекватности результатов оценки уровня защищенности для ИС, получаемых в случае применения концепции мгновенных аудитов.

Процесс аудитов, 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 управление «частотностью аудита» позволяет более оперативно контролировать динамику процесса изменения уровня защищенности против любых изменений (соответственно – «динамической перестройки» критериев аудита). 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 принятия «разумных решений» ЛПР [2].

Концепция мгновенных аудитов предполагает реализацию принципа выполнения аудитов ИБ с частотой, определяемой высшим менеджментом (ЛПР) и зависящей от предыдущего состояния «слева» уровня защищенности объекта [12]. 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.

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 ($t_k - t_i$) → 0.

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 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). Отметим снова, что полная «скорость реакции» СМИБ определяется частотой аудитов ИБ, что значительно превышает скорость полного цикла обновлений даже наилучших отраслевых решений CheckPoint. При этом объективно повышается способность системы (СМИБ или ИСМ) эффективно противодействовать угрозам в режиме, близком к режиму реального времени. В примере для одной переменной x_1 продемон-

стрировано увеличение скорости роста уровня защищенности СМИБ $\frac{\Delta R_k}{\Delta t_k}$ при известных переменных процесса аудитов ИБ (см. рисунок 1).

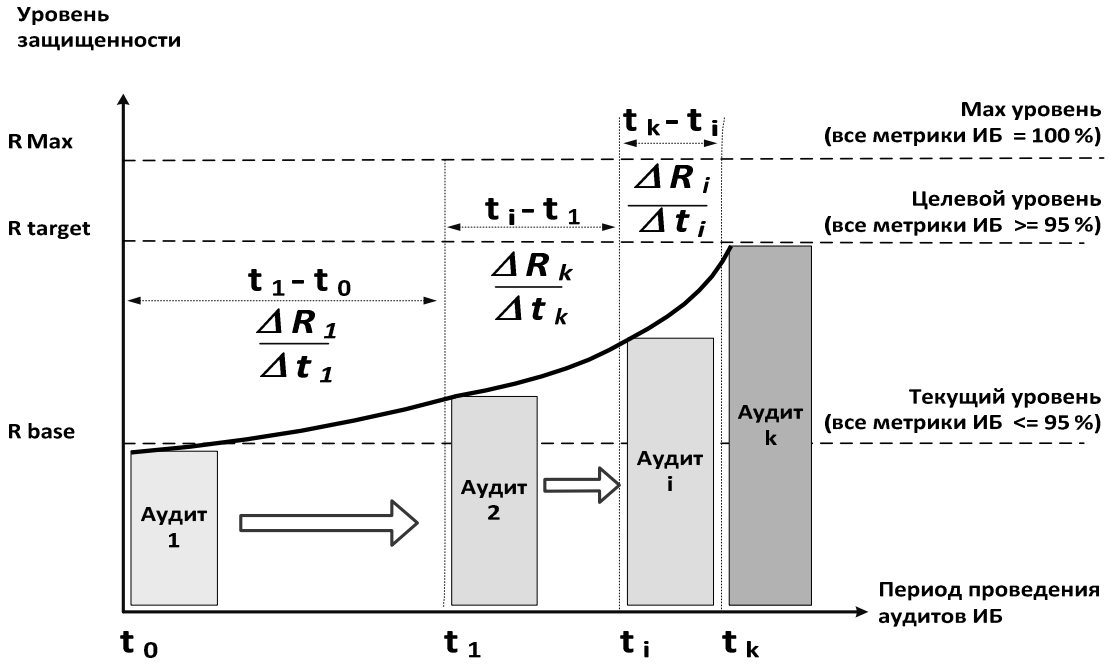

Рис. 1 – Пример увеличения скорости роста уровня защищенности

Список литературы

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. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems // Requirements, International Organization for Standardization. 2013. 23 p.

6. ISO 19011:2011. Guidelines for auditing management systems // International Organization for Standardization, 2011. 44 p.

7. ISO/IEC 20000-1:2011. Information technology. Service management. Part 1: Service management system requirements // International Organization for Standardization. 2011. 26p.

8. ISO 22301:2012. Societal security. Business continuity management systems // Requirements, International Organization for Standardization. 2012. 24 p.

9. 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.

10. Лившиц И.И. Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества. 2013. Вып. 1. С. 22–34.

11. 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.

12. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров // М.: Наука. 1978. 832 с.