УДК 004.56

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО ВРЕМЕНИ РЕАКЦИИ СИСТЕМЫ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ф.Н. Шаго[a]

[a] Университет ИТМО, Санкт-Петербург, Россия, dreamcast73@yandex.ru

Аннотация. Оценивание эффективности системы менеджмента информационной безопасности является важным этапом в циклической взаимосвязи видов деятельности системы менеджмента информационной безопасности, в ходе которого определяется соответствие системы заданным требованиям информационной безопасности организации. Исходя из анализа текущей практики оценивания эффективности систем менеджмента информационной безопасности, можно сделать вывод о том, что в большинстве случаев проводится независимое оценивание отдельных атрибутов информационной безопасности без учета их взаимодействия, в ходе измерений атрибутов не учитывается наличие неопределенности стохастического характера. Существует перечень взаимосвязанных мер и средств контроля и управления, однако конструктивные элементы измерений для оценки данных взаимодействий отсутствуют. Таким образом, возникает важная и актуальная задача совершенствования методологии оценки эффективности системы менеджмента информационной безопасности, решение которой возможно путем введения нового интегрального показателя эффективности системы, который бы позволил учесть вышеуказанные недостатки.

В работе предлагается использовать новый интегральный показатель эффективности – время реакции системы на инциденты информационной безопасности. Использование этого показателя позволит перейти от бинарной оценки эффективности системы «удовлетворяет – не удовлетворяет» к количественной. Предложенный показатель эффективности позволяет учесть неопределенности стохастического характера атрибутов мер и средств управления и контроля, дает количественную оценку состояния информационной безопасности, имеет ясную физическую трактовку для руководства организации и службы информационной безопасности. Динамика изменения показателя от проверки к проверке позволяет судить о состоянии системы менеджмента информационной безопасности в целом и о результативности принимаемых мер и средств управления и контроля. Методика расчета нового показателя эффективности системы менеджмента информационной безопасности основана на применении методологического аппарата теории планирования экспериментов. Достоинство методики – в том, что персоналу службы информационной безопасности предоставляется возможность управления измерениями атрибутов, обеспечивается одинаковая точность оценок параметров атрибутов в процессе измерений, с помощью коэффициентов регрессии выявляется степень взаимодействия атрибутов и их значимость в расчете показателя эффективности системы менеджмента информационной безопасности, а также формируется аналитическая модель показателя эффективности.

Ключевые слова: информационная безопасность, эффективность систем менеджмента информационной безопасности, показатель качества, оценка эффективности.

EFFECTIVENESS ASSESSMENT METHODOLOGY OF INFORMATION SECURITY MANAGEMENT SYSTEM THROUGH THE SYSTEM RESPONSE TIME TO INFORMATION SECURITY INCIDENTS

F.N. Shago[a]

[a] ITMO University, Saint Petersburg, Russia, dreamcast73@yandex.ru

Abstract. Quality assessment of information security management system is an important step for obtaining baseline data for analysis of the security system control effectiveness, and evaluating implementation of the specified information security requirements of the organization. Proceeding from current analysis practice of information security management systems effectiveness assessment, it can be concluded that, in most cases, independent measurement of security control is carried out without regard to their interaction. The uncertainty of the stochastic nature of the measured security controls is not taken into account. There is a list of related measures for control and management; however, structural elements for measuring of these interactions are absent. Thus, there is an important and urgent task of improving the effectiveness assessing methodology for information security management system that can be solved by introducing a new integral effectiveness indicator of the system, which would give the possibility to take into account the above-mentioned shortcomings.

The author proposes the usage of a new integral efficiency indicator - system response time to information security incidents. This efficiency indicator will make it possible to pass from the binary effectiveness assessment of the system "approve or disapprove" to a quantitative one. New performance indicator gives the possibility to take into account the uncertainty of the stochastic nature of the attributes and measures of management and control, provides a quantitative assessment of the information security state and has a clear physical interpretation for the organization management and information security officers. Dynamics of the indicator change from test to test will assess the information security management system state in general and effectiveness of taken control and management measures. The method for calculating of the new information security management system performance indicator is based on the experimental design theory. Its advantages are: information security service staff has an opportunity to control the attributes measurement, the same accuracy of estimates for attribute parameters during the measurement is provided, interaction degree between attributes and their importance in the computation of the effectiveness of information security management is revealed by means of the regression coefficients, and also an analytical model of performance indicator can be obtained.

Keywords: information security, effectiveness of information security management system, ISMS quality index, ISMS efficiency assessment.

Введение

Выполнение мероприятий по оценке эффективности системы менеджмента информационной безопасности (СМИБ) связано с проведением большого объема работ для получения показателей качества СМИБ. Сбор информации о состоянии информационной безопасности (ИБ) организации в циклической взаимосвязи видов деятельности СМИБ осуществляется посредством проведения измерений. В ходе измерения атрибутов объектов измерений изучается документация, проводится интервьюирование сотрудников и технические тесты [1, 2]. Работа с документацией и интервьюирование являются, несомненно, важной частью проверок, однако обладают некоторыми недостатками – ручной сбор информации, низкая степень автоматизации, субъективность оценок, зависимость от уровня компетентности аудитора [2]. Технические тесты позволяют получить количественные оценки показателей качества СМИБ. Проводя тестирование, аудитор выступает в роли легального злоумышленника, внося искусственные нарушения в функционирование СМИБ. Технические методы тестирования могут проводиться с помощью широко известных автоматизированных средств (программный инструментарий оценки состояния ИБ – CSET (Cyber Security Evaluation Tool – инструмент оценки кибербезопасности), сетевой сканер XSpider, т.п.). В итоге на основании полученных показателей качества руководством производится анализ эффективности деятельности СМИБ и определяются направления дальнейшего развития системы. В процессе анализа эффективности СМИБ, в соответствии с требованиями руководящих документов [3–5], необходимо оценивать полученные показатели качества мер и средств контроля и управления. В действующей практике показатели оцениваются независимо друг от друга. Методики расчета показателей качества СМИБ не учитывают наличие неопределенности измеряемых атрибутов стохастического характера – например, при оценке рисков во время планирования СМИБ, при оценке недостатков процессов функционирования действующей СМИБ, при использовании мер и средств контроля и управления ИБ, а также ошибки измерений. В конечном итоге оценка эффективности СМИБ сводится к принятию бинарного решения «удовлетворяет – не удовлетворяет» [6]. Таким образом, возникает важная и актуальная задача совершенствования методологии оценки эффективности СМИБ, решение которой возможно путем разработки интегрального показателя эффективности СМИБ, который бы позволил учесть вышеуказанные недостатки и в то же время имел ясную физическую трактовку для руководства организации и службы ИБ. В настоящей работе вводится понятие нового критерия эффективности СМИБ – времени реакции системы на инциденты ИБ, а также предлагается методологический аппарат его вычисления. Выбор в качестве критерия эффективности СМИБ времени реакции системы на инциденты ИБ доказывает руководителю организации рентабельность затрат на построение и развитие СМИБ и способствует повышению качества оценивания текущего состояния СМИБ и улучшению ИБ.

Обоснование интегрального показателя эффективности СМИБ

Для оценивания эффективности СМИБ необходимо проводить измерение показателей качества СМИБ [7]. Цель проводимых измерений заключается в получении оценки эффективности реализованных мер и средств контроля и управления и получении оценки эффективности реализованной СМИБ. Измерения проводятся повсеместно в циклической взаимосвязи видов деятельности СМИБ (их «входов–выходов»), на базе цикла «Планирование–Внедрение–Проверка–Действие» (PDCA, Plan–Do–Check–Act).

В соответствии с циклом деятельности СМИБ PDCA для проверки эффективности реализованной СМИБ необходимо управлять программой измерений для достижения установленных целей измерений на всех этапах деятельности [7, 8]. Особенно это важно для этапа «Внедрение». Измерения на этапе «Внедрение» оказывают существенное влияние на показатели качества СМИБ. Далее, на этапе «Проверка», полученные показатели качества сравниваются с пороговыми критериями, и по результатам проверки принимается решение о соответствии или несоответствии меры и средства контроля и управления СМИБ требованиям.

Регулярные измерения показателей качества СМИБ дают временной срез состояния системы, который будет оцениваться относительно предыдущих результатов измерений. Однако эта информация жестко привязана к времени измерения, и по совокупности полученных показателей невозможно определить, насколько изменилась эффективность СМИБ между периодами проверок. Проблема существующих механизмов получения показателей заключается в том, что при измерении атрибутов объектов измерения все атрибуты, кроме одного, остаются неизменными, их как бы «замораживают», измеряя последовательно в рассматриваемых пределах лишь один атрибут. Не учитывается наличие неопределенностей стохастического характера, например, при оценке рисков во время планирования СМИБ, при использовании мер и средств контроля и управления ИБ, а также недостатки процессов функционирования действующей СМИБ и ошибки измерений.

Как уже говорилось, в конечном итоге оценка показателя качества СМИБ сводится к принятию бинарного решения «удовлетворяет–не удовлетворяет». Таким образом, возникает важная и актуальная задача по разработке интегрального критерия эффективности СМИБ, который бы позволил учесть вышеуказанные недостатки и в то же время имел ясную физическую трактовку для руководства организации и

персонала службы ИБ. Решение этой задачи видится в разработке такого показателя эффективности СМИБ, который будет связан с организацией объективных и повторяемых процессов измерения. Данный показатель будет объективно отражать состояние СМИБ, и на его основании соответствующие заинтересованные стороны смогут определить потребности в усовершенствовании реализованной СМИБ, включая область ее применения, политики, цели, меры и средства контроля и управления, а также процессы и процедуры. В роли такого показателя эффективности СМИБ необходимо принять *время реакции системы на инциденты ИБ*.

Анализ методов оценки эффективности мер и средств управления и контроля СМИБ [5, 8–12] показал, что около 80% от общего перечня мер и средств управления и контроля оценивается по временным показателям – например, по времени обнаружения инцидента ИБ, времени внесения информации об инциденте ИБ в базу данных, времени блокирования несанкционированного действия нарушения ИБ, времени оповещения персонала службы ИБ организации об инциденте ИБ. В зависимости от того, какой компонент системы реагирует на инцидент (СОВ – защита периметра сети от вторжений, изменение политик безопасности, управление системой физического и логического доступа и множество других компонентов), меняется не только время реакции, но и оценка скорости реакции. Для некоторых ситуаций хорошим результатом является практически мгновенная реакция, изменение политик безопасности может потребовать несколько недель или даже месяцев.

Время реакции СМИБ на инциденты ИБ может выступать интегральным показателем эффективности СМИБ:

$$T_{\text{рсИБ}} = \sum_{i=1}^{k} (T_{\text{обнИБ}_i} + T_{\text{блокИБ}_i} + T_{\text{регИБ}_i} + T_{\text{оповИБ}_i}),$$

где k – количество атрибутов, подлежащих измерению; $T_{\text{рсИБ}}$ – время реакции СМИБ на инцидент ИБ; $T_{\text{обнИБ}_i}$ – время обнаружения инцидента ИБ; $T_{\text{блокИБ}_i}$ – время блокирования несанкционированных действий по нарушению ИБ; $T_{\text{регИБ}_i}$ – время регистрации события, связанного с инцидентом ИБ; $T_{\text{оповИБ}_i}$ – время оповещения персонала службы ИБ о выявленном инциденте ИБ.

Для расчета показателя необходимо разделение мер и средств управления и контроля для выполнения проверок на группы по времени реагирования на инцидент ИБ. Например, можно установить такой вид группирования:

– немедленный контроль (время реакции – несколько минут ($T_{\text{рсИБ}} \leq 10$ мин));
– суточный контроль (время реакции – в течение суток ($T_{\text{рсИБ}} \leq 24$ ч));
– контроль изменения политик ИБ (время реакции – в течение нескольких суток ($T_{\text{рсИБ}} \leq 10$ сут)).

Динамика изменения интегрального показателя $T_{\text{рсИБ}}$ от проверки к проверке позволит судить о состоянии системы в целом, о результативности принимаемых мер и средств управления и контроля. В формировании данного показателя будет учитываться уникальность СМИБ организации. Дополнительно получение показателя $T_{\text{рсИБ}}$ может быть встроено в обычные процессы функционирования СМИБ и выполняться через постоянные интервалы времени, определяемые руководством СМИБ.

Изменения, вносимые методикой получения интегрального показателя в модель измерений СМИБ, связывающую информационную потребность с соответствующими объектами измерений и их атрибутами, позволит получать воспроизводимые, объективные и пригодные результаты измерений (рисунок).

Методика получения показателя эффективности СМИБ позволит исследовать взаимное влияние показателей качества объектов измерений. В руководящих документах [5, 9] определен перечень взаимосвязанных конструктивных элементов измерений. Однако существующий перечень представляет только базовые взаимодействия и не учитывает особенности СМИБ организации. В рамках работы по совершенствованию оценки эффективности СМИБ и получения достоверных результатов измерения показателей качества СМИБ предлагается использование стохастических аналитических моделей, в частности, статистических. Данные модели предпочтительны потому, что учитывают вероятностную составляющую атрибутов (факторов), которые подлежат измерению; кроме того, случайное воздействие может подаваться на вход модели измерений как в процессе проведения измерений, так и от датчиков случайных чисел, применяемых в самой модели. Еще одним достоинством применения статистической модели является то, что в ней самой уже заложен алгоритм статистической обработки результатов измерений. Наиболее выгодным, с точки зрения достижения результативности измерений, является широкое использование в качестве аналитических моделей для показателя эффективности СМИБ модели регрессионного анализа. Преимущество данной модели относительно других статистических моделей (дисперсионного, корреляционного, параметрического анализа и др.) состоит в том, что, помимо получения вывода о причинно-следственном механизме исследуемых зависимостей, получают конкретные сведения о форме и виде зависимости. Помимо этого, аппарат регрессионного анализа широко представлен во всех современных программных средствах математической автоматизации (таких как семейство Mathcad, Scilab, GNU Oc-

tave, Mathematica, MATLAB и др.), и в автоматизированных средствах обработки статистических данных (STATISTICA, SYSTAT, JMP и т.д).

Рисунок. Изменение модели измерений СМИБ, связанные с получением обобщающего показателя эффективности СМИБ

Выбор аппроксимирующего полинома для показателя эффективности СМИБ

Для исследуемых мер и средств управления и контроля СМИБ функция отклика (аналитической модели), описывающей показатель эффективности СМИБ, трудно поддается простому аналитическому описанию [13, 14]. Целесообразно произвести аппроксимацию зависимой переменной в виде алгебраического полинома. Допустим, что необходимо изучить влияние k количественных атрибутов $x_1, x_2, \cdots, x_k$ на некоторый отклик η в определенной для измерений локальной области пространства атрибутов (факторов). Функцию отклика $\Psi(x_1, x_2, \cdots, x_k)$ можно с достаточной точностью представить в виде полинома степени $m \geq 2$ от k переменных [14]:

$$\eta = b_0 + \sum_{i=1}^{k} b_i x_i + \sum_{i=1}^{k}\sum_{j=1}^{k} b_{ij} x_i x_j + \cdots + \sum_{i_1=1}^{k}\cdots\sum_{i_m=1}^{k} b_{i_1, i_2, \cdots i_m} \cdot x_{i_1} \cdot x_{i_2} \cdots \cdot x_{i_m}. \quad (1)$$

Коэффициенты b_0 и b_i описывающего полинома (1) характеризуют степень влияния рассматриваемых атрибутов измерений на функцию отклика. Например, аппроксимация полиномом второго порядка функциональной зависимости показателя эффективности от одного независимого атрибута (переменной) (однофакторная модель) может быть представлена в виде следующего уравнения регрессии:

$$y = b_0 + b_1 x_1 + b_{11} x_1^2.$$

Аппроксимирующий полином второго порядка с учетом зависимости от двух атрибутов может быть представлен в виде

$$y = b_0 + b_1 x_1 + b_2 x_2 + b_{12} x_1 x_2.$$

Более сложные СМИБ требуют применения полиномов с большим числом учитываемых атрибутов и большим порядком. Сформулировать однозначные рекомендации о выборе необходимой степени аппроксимирующего полинома трудно, поэтому одна и та же СМИБ вполне может быть описана различными аппроксимирующими полиномами. При выборе вида полинома или типа регрессионной модели необходимо руководствоваться характером исследуемого физического процесса, связанного с мерой и средством контроля и управления ИБ. Отметим, что выбор общего вида функции регрессии (параметризация модели) является ключевым и окажет существенное влияние на точность восстановления неизвестной функции отклика $\Psi(X)$ в дальнейшем. В настоящее время не существует системы стандартных методов и рекомендаций, образующих строгую теоретическую базу для эффективного выбора аппроксимирующего полинома. Выбор общего вида уравнения регрессии [14] должен быть связан с тремя основными моментами:

1. максимальное использование априорной информации о содержательной (физической, экономической и т.п.) сущности анализируемой зависимости;
2. предварительный анализ геометрической сущности анализируемой зависимости;

3. использование различных статистических приемов обработки исходных данных, предоставляющих выбор из нескольких сравниваемых вариантов.

На практике для аппроксимации неизвестной функции регрессии чаще применяются линейные уравнения регрессии. Зачастую использование линейной или полиномиальной регрессии не позволяет получить желаемую точность приближения. В этом случае приходится использовать другие виды зависимостей: гиперболическую, степенную, показательную и др. В ряде ситуаций применение этих зависимостей более удобно, так как путем преобразования удается привести их к линейному виду [14, 15].

При классическом (традиционном) методе измерений все атрибуты, кроме одного, остаются неизменными, их как бы «замораживают», изменяя последовательно в рассматриваемых пределах лишь один атрибут. Подобный метод обладает рядом недостатков, наиболее существенный из которых состоит в том, что при этом методе не удается в полной мере выявить влияние взаимодействия атрибутов [16].

Проводя измерения в условиях, соответствующих некоторому значению вектора **x**, можно получить результаты измерений, в общем случае представляющие собой случайные величины, поэтому обычно говорят о функциональной зависимости среднего значения искомой характеристики от контролируемых атрибутов. Эта зависимость в общем виде может быть представлена так:

$$E\,(y/\mathbf{x}) = \eta\,(\mathbf{x};\,\mathbf{B}),$$

где $E\,(y/\mathbf{x})$ – среднее значение искомой величины y; **x** – вектор-столбец, координаты которого – управляемые переменные, принадлежащие данному пространству атрибутов; $\eta\,(\mathbf{x};\,\mathbf{B})$ – функция отклика, зависящая от неизвестных параметров $b_i \in \mathbf{B}$ ($i = 1, 2,.., m$).

Чтобы определить параметры b_i, необходимо выбрать в данном пространстве атрибутов некоторую совокупность точек, пригодных для выполнения измерений в процессе проверки. Если при выборе точек осуществлять одновременное варьирование несколькими переменными ($x_1\ x_2,\ ...,\ x_k$), то результаты проверок будут получены с учетом эффекта взаимодействия атрибутов.

Таким образом, задача, связанная с получением наилучшего представления о влиянии выбранных переменных на функцию отклика показателя эффективности СМИБ, сводится к выбору оптимального в некотором смысле расположения точек в пространстве атрибутов. Очевидно, что при различном подходе к выбору расположения точек значения оценок b_i могут отличаться друг от друга. Выбор наилучшего варианта модели измерений, приводящей к лучшим оценкам в смысле их близости к истинным значениям b_i, можно основывать в классе линейных оценок на сравнении дисперсионных матриц $\mathbf{D}(b)$ или некоторых комбинаций из их элементов.

Применение факторного планирования для расчета показателя эффективности СМИБ

Для построения функции отклика, описывающей показатель эффективности СМИБ, предлагается воспользоваться научно-методическим аппаратом теории планирования эксперимента. В литературе, посвященной теории планирования эксперимента [16, 17], можно встретить описание A-, E-, G- и D-оптимальных планов, удовлетворяющих различным критериям. При достаточно большом числе учитываемых факторов (атрибутов) с целью уменьшения числа измерений прибегают к построению планов второго порядка, близких к D-оптимальным планам.

D-оптимальный план обеспечивает одинаковую точность оценок параметров на равных удалениях во всех направлениях от центральной точки измерения. Если ковариационная матрица оценок параметров имеет вид $c\mathbf{I}$, где c – постоянная, а **I** – единичная матрица, то утверждается, что критерии оптимальности в смысле D, E, A совпадают. План, удовлетворяющий этим критериям, является ортогональным и ротатабельным [16, 17].

В ортогональных факторных планах каждый фактор варьирует симметрично относительно начала координат на двух уровнях. В выбранной области проведения измерений устанавливается основной уровень x_i^0 и определяется интервал варьирования. Основной уровень может либо соответствовать номинальным значениям параметров, либо выбираться в центре области их изменения, подлежащей проверке. Интервал варьирования J_{x_i} устанавливается симметрично относительно основного уровня по формуле

$$J_{x_i} = \frac{x_i^{\mathrm{B}} - x_i^{\mathrm{H}}}{2}, \qquad (2)$$

где $x_i^{\mathrm{B}}, x_i^{\mathrm{H}}$ – верхнее и нижние натуральные значения фактора.

Переход к безразмерной системе координат (нормировка) осуществляется по формулам

$$\frac{x_{i\,\max} - x_i^0}{J_{x_i}} = +1,\ \frac{x_{i\,\min} - x_i^0}{J_{x_i}} = -1. \qquad (3)$$

Из-за особенностей проверяемой СМИБ возможность варьирования некоторых атрибутов может быть существенно ограничена по отношению к возможности варьирования других атрибутов. Это может сказываться на адекватности математической модели. Для учета данного обстоятельства предлагается осуществлять расчет интервала варьирования в соответствии с формулой

$$J_{x_i} = q_{\min} \cdot \Delta x_i^a,$$

где

$$q_{\min} = \min_i \left\{ q_i = \frac{\Delta x_i^a}{\Delta x_i^S} \right\},$$

Δx_i^a – предельно возможный интервал изменения атрибута в условиях проверяемой СМИБ; Δx_i^S – предельно возможный интервал изменения атрибута.

Свойство ортогональности обеспечивает значительные упрощения последующих вычислений.

Подобные ортогональные факторные планы обладают рядом отличительных свойств. При выполнении условий и свойств составления плана коэффициенты уравнения регрессии b получаются с минимальными и равными ошибками.

Допустим, что в ходе измерений необходимо получить показатель эффективности СМИБ, учитывая взаимодействие двух ($k = 2$) мер и средств управления и контроля – «Контроль доступа в запрещенную зону» (п.А.9.1.2 приложения А ГОСТ [4]) и «Управление съемными носителями информации» (п.А.10.7.1 приложения А ГОСТ [4]). Для исследования выбрано уравнение регрессии

$$y = b_0 + b_1 x_1 + b_2 x_2 + b_{12} x_1 x_2. \quad (4)$$

Количество различных экспериментов N определяется числом всех неповторяющихся комбинаций, которые можно составить из k рассматриваемых независимых переменных, имеющих по два уровня, и будет равно 2^k. Осуществление всех 2^k возможных и неповторяющихся комбинаций реализуется в *полном факторном плане*. Структура плана, соответствующая выбранному уравнению регрессии (4) и требованиям D-оптимального плана, представлена в табл. 1.

Опыт	x_0	x_1	x_2	$x_1 x_2$	y
1	+1	–1	–1	+1	y_1
2	+1	+1	–1	–1	y_2
3	+1	–1	+1	–1	y_3
4	+1	+1	+1	+1	y_4

Таблица 1. Матрица проведения измерений, отвечающая требованиям D-оптимального плана, в соответствии с выбранным для исследования уравнением регрессии (4)

Добавим к исследуемым атрибутам еще одну независимую переменную ($k = 3$) меру управления и контроля «Управление изменениями» (п.А.10.1.2 приложения А ГОСТ [4]), и изменим вид регрессионного уравнения:

$$y = b_0 + b_1 x_1 + b_2 x_2 + b_3 x_3 + b_{12} x_1 x_2 + b_{13} x_1 x_3 + b_{23} x_2 x_3 + b_{123} x_1 x_2 x_3. \quad (5)$$

План проведения исследований для сочетаний различных уровней независимых переменных при $k = 3$ будет уже иметь вид (табл. 2).

Опыт	x_0	x_1	x_2	x_3	$x_1 x_2$	$x_1 x_3$	$x_2 x_3$	$x_1 x_2 x_3$	y	$\hat{y}$
1	+1	–1	–1	–1	+1	+1	+1	–1	y_1	9
2	+1	+1	–1	–1	–1	–1	+1	+1	y_2	5
3	+1	–1	+1	–1	–1	+1	–1	+1	y_3	6
4	+1	+1	+1	–1	+1	–1	–1	–1	y_4	11
5	+1	–1	–1	+1	+1	–1	–1	+1	y_5	7
6	+1	+1	–1	+1	–1	+1	–1	–1	y_6	9
7	+1	–1	+1	+1	–1	–1	+1	–1	y_7	8
8	+1	+1	+1	+1	+1	+1	+1	+1	y_8	13
b_j	$b_0 = 8{,}5$	1	1	0,75	1,5	0,75	0,25	–0,75		

Таблица 2. Матрица проведения измерений, отвечающая требованиям D-оптимального плана, в соответствии с выбранным для исследования уравнением регрессии (5)

Несложно заметить, что в табл. 2 дважды повторена матрица для $k = 2$ (табл. 1), первый раз для значений x_3 на нижнем уровне (–1) и повторно для значений x_3 на верхнем уровне (+1).

Вычисление коэффициентов регрессии b производится с помощью простой формулы:

$$b_j = \frac{1}{N} \sum_{i=1}^{N} x_{ij} y_i \,. (j = 1,2, \dots, m), \quad (6)$$

где N – число экспериментов, проведенных в соответствии с выбранным планом; x_{ij} – нормированное значение (3) атрибута j в зависимости от опыта i; y_i – значение функции отклика, полученное в опыте i; m – количество факторов и их сочетаний, представленных в матрице планирования. Для примера покажем расчет некоторых коэффициентов регрессии:

$$b_0 = \frac{9 \cdot (+1) + 5 \cdot (+1) + 6 \cdot (+1) + 11 \cdot (+1) + 7 \cdot (+1) + 9 \cdot (+1) + 8 \cdot (+1) + 13 \cdot (+1)}{8} = 8{,}5,$$

$$b_1 = \frac{9 \cdot (-1) + 5 \cdot (+1) + 6 \cdot (-1) + 11 \cdot (+1) + 7 \cdot (-1) + 9 \cdot (+1) + 8 \cdot (-1) + 13 \cdot (+1)}{8} = 1,$$

….

$$b_8 = \frac{9\cdot(-1)+5\cdot(+1)+6\cdot(+1)+11\cdot(-1)+7\cdot(+1)+9\cdot(-1)+8\cdot(-1)+13\cdot(+1)}{8} = 0{,}75.$$

Коэффициенты b_i определяются независимо, что имеет существенное значение при переходе к более сложной форме уравнения связи (нет необходимости пересчитывать полученные ранее значения коэффициентов).

Допустим, что в ходе измерений в соответствии с матрицей эксперимента (табл. 2), в столбце «$\hat{y}$» были записаны значения времени реакции СМИБ (в минутах) на инциденты ИБ, при условиях совместного влияния трех факторов (атрибутов). После вычисления коэффициентов регрессии b_i уравнение регрессии (5) примет следующий вид:

$$\hat{y} = 8{,}5 + x_1 + x_2 + 0{,}75x_3 + 1{,}5x_1x_2 + 0{,}75x_1x_3 + 0{,}25x_2x_3 - 0{,}75x_1x_2x_3.$$

Далее проверяем значимость коэффициентов регрессии, а также адекватность полученной зависимости исследуемому процессу [16, 17].

К сожалению, существенным недостатком полных факторных планов является быстрый рост числа измерений с ростом числа факторов (в 2^k раз). В случае, когда взаимодействия второго и выше порядка отсутствуют или малы, целесообразно реализовать матрицу планирования, содержащую лишь часть полного факторного плана, в противном случае перейти к дробному факторному плану. Сущность применения такого планирования сводится к сокращению числа членов полинома за счет смешивания основных факторов с теми факторами, которые на основании априорных или экспертных оценок слабо влияют на изучаемый процесс [16–18]. Для рассмотренного выше уравнения регрессии, допустив, что взаимные смешения основных факторов ничтожны, можно ввести в план дополнительно до четырех факторов (атрибутов) (табл. 3).

№ опыта	x_0	x_1	x_2	x_3	$x_1\,x_2$	$x_1\,x_3$	$x_2\,x_3$	$x_1\,x_2\,x_3$	y
					x_4	x_5	x_6	x_7	

Таблица 3. Ввод новых атрибутов, для исследования влияния на функцию отклика показателя качества СМИБ, вместо сочетаний атрибутов, оказывающих слабое влияние на исследуемый процесс

Дробный факторный план (ДФП) имеет вид 2^{k-p}, где p – количество факторов, введенных посредством замещения исключаемых из рассмотрения взаимодействий, и существенно сокращает число измерений при проверке. В рассмотренном выше примере при построении полного факторного эксперимента для $k = 3$ необходимо проведение 8 измерений, если же ввести еще один фактор x_4 и приравнять x_4 двойному взаимодействию x_1x_2, то количество опытов останется неизменным, а вместо полного факторного плана 2^4 получим полуреплику 2^{4-1}, что соответствует линейному уравнению регрессии

$$y = b_0 + b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4.$$

Коэффициенты регрессии таком случае будут представлены в виде смешанных оценок генеральных коэффициентов: $b_1 = \beta_1 + \beta_{234}$, $b_2 = \beta_2 + \beta_{134}$, $b_3 = \beta_3 + \beta_{124}$, $b_4 = \beta_4 + \beta_{123}$, т.е. коэффициенты β_i, не удастся оценить отдельно [14].

Генерирующие соотношения можно составлять таким образом, чтобы в зависимости от наличия предварительных сведений получать полуреплики, сокращающие вдвое число опытов по сравнению с полным факторным экспериментом, или четвертьреплики, уменьшающие количество опытов в четыре раза, и т.д. Для определения того, какие оценки являются смешанными, используют определяющий контраст [16–18].

В соответствии с вышесказанным методика расчета показателя эффективности СМИБ включает в себя следующие процедуры.

1. Осуществить выбор требуемого количества атрибутов k и требуемого числа измерений N.
2. Исходя из априорных данных и экспертных оценок, выбрать аппроксимирующую модель, описывающую функциональную зависимость времени реакции СМИБ на инциденты ИБ, с учетом выбранных атрибутов.
3. Определить интервалы варьирования для атрибутов с учетом особенности СМИБ организации (2) по формуле (3).
4. Выбрать факторный план проведения измерений, полный (для $k \le 3$) или дробный (для $k > 3$).
5. Составить матрицу плана, удовлетворяющую требованиям D-оптимального плана, определить правила получения коэффициентов регрессии b_i в соответствии с выбранным планом.
6. Провести измерения, варьируя параметры атрибутов, в соответствии с матрицей плана.
7. Рассчитать коэффициенты регрессии b_i по результатам измерений (6).
8. Проверить полученную модель показателя на значимость коэффициентов регрессии, а также на адекватность исследуемому процессу.

Таким образом, предложенный показатель эффективности позволяет учесть неопределенности стохастического характера атрибутов объектов измерения, получить количественную оценку состояния ИБ, имеет ясную физическую трактовку для руководства организации и службы ИБ. Динамика его изменения от проверки к проверке позволит судить о состоянии СМИБ в целом, о результативности прини-

маемых мер и средств управления и контроля. Предложенная методика оценки эффективности СМИБ заключается в применении методологического аппарата теории планирования экспериментов для расчета времени реакции СМИБ на инциденты ИБ. Достоинством методики является то, что она дает возможность управления измерениями атрибутов, обеспечивает одинаковую точность оценок параметров атрибутов в процессе измерений, с помощью коэффициентов регрессии позволяет выявить влияние взаимодействия атрибутов и их значимость в расчете показателя эффективности СМИБ, а также позволяет получить аналитическую модель показателя эффективности СМИБ.

Заключение

Оценивание эффективности СМИБ является важным этапом в циклической взаимосвязи видов системы. На этом этапе оценивается степень реализации заданных требований информационной безопасности организации. Организация данного процесса оказывает существенное влияние на точность и достоверность оценок показателей качества СМИБ.

В ходе решения задачи совершенствования методологии оценки эффективности СМИБ автором предлагается использование нового интегрального показателя эффективности – времени реакции системы на инциденты ИБ. Использование данного показателя эффективности позволит перейти от бинарной оценки эффективности системы «удовлетворяет – не удовлетворяет» к количественной.

Показаны роль и место нового показателя эффективности СМИБ в цикле деятельности системы, а также изменения, вносимые в модель измерений в связи с расчетом показателя. Предложен выбор статистической модели, описывающей функцию отклика нового показателя эффективности системы. Для расчета нового показателя эффективности СМИБ предложена методика, основанная на использовании аппарата теории планирования эксперимента, в частности, выбор уравнения регрессии, построение факторных планов и получение коэффициентов регрессии. Приведен пример построения матрицы измерений с участием трех атрибутов, рассчитаны коэффициенты регрессии для функции отклика, описывающей показатель эффективности СМИБ. Выбор в качестве показателя эффективности времени реакции системы на инциденты ИБ может служить обоснованием для руководителей организации, рентабельности затрат на построение и развитие СМИБ и способствует повышению качества оценивания эффективности системы.

Литература

1. ISO/IEC 19011:2011. Guidelines for auditing management systems. 11.11.2011. Geneva, International Organization for Standardization. 44 p.
2. Аксенов В.В. Аудит системы менеджмента информационной безопасности. Руководство [Электронный ресурс]. Режим доступа: itsec.by/wp-content/uploads/2012/10/Auditors-Guide-ISO-27001-on-Russian.pdf, свободный. Яз. рус. (дата обращения 20.04.2014).
3. ISO/IEC 27000:2013. Information security management systems – Overview and vocabulary. 14.01.2013. Geneva, International Organization for Standardization. 25 p.
4. ISO/IEC 27001:2013, Information security management systems – Requirements. 25.09.2013. Geneva, International Organization for Standardization. 23 p.
5. Приказ ФСТЭК России №17. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Введ. 11.02.2013. М.: ФСТЭК РФ. 37 с.
6. Зикратов И.А., Одегов С.В., Смирных А.В. Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 1 (83). С. 141–144.
7. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. Введ. 01.01.2012. М.: Стандартинформ, 2012. 62 с.
8. Шаго Ф.Н., Зикратов И.А. Методика оптимизации планирования аудита системы менеджмента информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2 (90). С. 111–117.
9. Critical Security Controls for Effective Cyber Defense [Электронный ресурс]. Режим доступа: http://www.sans.org/critical-security-controls/, свободный. Яз. англ. (дата обращения 20.04.2014).
10. Зикратов И.А., Одегов С.В. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 4 (80). С. 121–126.
11. Catteddu D., Hogben G. Cloud computing: benefits, risks and recommendations for information security. Heraklion: ENISA, 2009. 125 p.
12. Macaulay T. Upstream intelligence: anatomy, architecture, case studies and use-cases // Information Assurance Newsletter. 2011. V. 14. P. 18–22.

13. Мартыщенко Л.А., Ивченко В.П., Монастырский М.Л. Теоретические основы информационно-статистического анализа сложных систем. СПб: Лань, 1997. 320 с.
14. Айвазян С.А., Енюков И.С., Мешалкин Л.Д. Прикладная статистика. Исследование зависимостей. М.: Финансы и статистика, 1985. 487 с.
15. Лебедев А.Н., Куприянов М.С., Недосекин Д.Д., Чернявский Е.А. Вероятностные методы в инженерных задачах: Справочник. СПб: Энергоатомиздат, 2000. 333 с.
16. Зедгенидзе И.Г. Планирование эксперимента для исследования многокомпонентных систем. М.: Наука, 1976. 390 с.
17. Бендат Дж., Пирсол А. Прикладной анализ случайных данных: Пер. с англ. М.: Мир, 1989. 540 с.
18. Спиридонов А.А. Планирование эксперимента при исследовании технологических процессов. М.: Машиностроение, 1981. 184 с.

Шаго Федор Николаевич – аспирант, Университет ИТМО, Санкт-Петербург, Россия, dreamcast73@yandex.ru

Fedor N. Shago – postgraduate, ITMO University, Saint Petersburg, Russia, dreamcast73@yandex.ru

Принято к печати 24.04.14
Accepted 24.04.14