Байесовский подход к оценке влияния факторов организации и управления систем финансового сектора на защищенность объектов критической информационной инфраструктуры

М.Г. Журавлева

Финансовый университет при Правительстве Российской Федерации

Аннотация: Предложено оценивать значения частных показателей, характеризующих степень защищенности объектов критической информационной инфраструктуры банковской системы с точки зрения выполнения требований к организационной структуре и управлению, на основе байесовского подхода. Представлена модель, включающая частные и обобщенные показатели, применение которой позволит усовершенствовать определенный стандартами подход к анализу уровня защищенности рассматриваемых объектов при проведении внутреннего аудита благодаря возможности оценивать значения частных показателей в непрерывной шкале и учитывать историю изменения характеристик требований к обеспечению информационной безопасности.
Ключевые слова: информационная безопасность, байесовский подход, объекты критической информационной инфраструктуры, показатели выполнения требований информационной безопасности, уровень защищенности объектов, модель с вероятностными компонентами.

Введение

Обеспечение информационной безопасности (ИБ) объектов критической информационной инфраструктуры (КИИ) финансового сектора предполагает реализацию комплекса мер, нацеленных на повышение уровня защищенности информации [1-3]. Уязвимость таких объектов для внешних и внутренних угроз часто усугубляется недостаточным уровнем управления процессами, связанными с их защитой, и организации службы ИБ. Задача обеспечения ИБ посредством учета влияния аспектов организационной структуры и управления на уровень защищенности объектов КИИ весьма актуальна и в первую очередь решается при реализации внутреннего аудита.

Для выявления множества требований к обеспечению ИБ в контексте исследования влияния определенных факторов на уровень защищенности можно строить онтологические модели [4], описывать актуальные угрозы с проблемами, которые они порождают, и возможностями их

предотвращения [5]. Для организаций банковской системы (БС), представляющих большую часть субъектов финансового сектора, в области обеспечения ИБ применяются, в частности, стандарты СТО БР ИББС-1.0-2014 с методикой оценки соответствия СТО БР ИББС-1.2-2014, принятые и введенные в действие Распоряжением Банка России от 17.05.2014 N Р-399, и Национальные стандарты РФ: ГОСТ Р 57580.1-2017 с методикой ГОСТ Р 57580.2-2018, утвержденные и введенные в действие приказами Федерального агентства по техническому регулированию и метрологии от 08.08.2017 N 822-ст. и от 28.03.2018 N 156-ст. соответственно. Они содержат описание множества требований в области обеспечения ИБ и порядок оценки их выполнения. Требования к обеспечению ИБ организаций банковской системы РФ задаются также с помощью Положения Банка России от 17.08.2023 № 821-П, которое является обязательным, но учитывает ИБ лишь в рамках переводов денежных средств. В организациях БС часто используется стандарт СТО БР ИББС-1.0-2014, который широко охватывает различные аспекты ИБ, соответствует международным стандартам в области защиты информации, описывает единый подход к построению системы обеспечения ИБ, опираясь на требования российского законодательства. При реализации внутреннего аудита применяется методика СТО БР ИББС-1.2-2014, которая включает способ оценки уровня соответствия ИБ требованиям данного стандарта на основе частных и групповых (агрегированных частных) показателей, характеризующих степень выполнения тех или иных требований по обеспечению ИБ, в том числе в контексте организационной структуры и управления. В ней предлагается задавать конкретные дискретные значения частных показателей с помощью экспертного оценивания: проверки наличия или отсутствия документации и/или выполнения требований, предъявляемых к обеспечению ИБ. Такой подход субъективен, в частности, задача проверки выполнения требований не всегда

может быть решена однозначно. В [6] также отмечено, что стандарты не объясняют, как можно эффективно извлекать уроки из инцидентов нарушения ИБ и на основе этого снижать вероятности их появления в будущем.

Более гибкий подход предполагает оценку значений каждого частного показателя в непрерывной шкале на основе совокупности характеристик требований по обеспечению ИБ, доступных на момент проведения аудита, а также позволяет учитывать влияние истории изменения характеристик на результирующий уровень защищенности объектов КИИ.

Оценка показателей выполнения требований по обеспечению ИБ с помощью байесовского подхода

Для оценки значений частных показателей, характеризующих степень выполнения требований по обеспечению ИБ, можно применить байесовский подход [7, 8]. Пусть P_{ij} – частный показатель, для которого наблюдается n элементов из общей совокупности характеристик, отражающих выполнение определенного требования по обеспечению ИБ. Например, для показателя М1.21 из методики СТО БР ИББС-1.2-2014: «Приравнивается ли невыполнение работниками организации БС РФ требований ИБ к невыполнению должностных обязанностей и приводит ли как минимум дисциплинарной ответственности?» множество элементов, отражающих выполнение данного требования к ИБ, составляют:

– документы, в которых описан порядок фиксации нарушений работниками требований ИБ, применения взысканий (дисциплинарной ответственности);

– документы, содержащие факты нарушений за некоторый период времени и информация о предпринятых действиях в отношении нарушителей;

– факты/действия по обеспечению требования к ИБ и т.п.

Общая совокупность таких элементов включает документы, факты, действия за весь период функционирования организации БС.

О каждом частном показателе имеется априорная информация, отражающая априорные ожидания к его значению, возможно, зафиксированная с помощью предыдущих проверок. Во время предстоящего внутреннего аудита, связанного с оцениванием уровня защищенности объектов КИИ, выбираются n элементов, на основании которых можно получить апостериорную оценку значения показателя.

Показатель P_{ij} представляет собой долю элементов из совокупности характеристик определенного требования по обеспечению ИБ, которые удовлетворяют данному требованию, и является одним из чисел отрезка от 0 до 1. Можно говорить о том, что показатель принимает значение p_{ij} из [0, 1], подчиняющееся некоторому вероятностному распределению. Подходящим априорным распределением P_{ij} является бета-распределение $B(\alpha_{ij}, \beta_{ij})$ с параметрами α_{ij}, β_{ij} и функцией плотности вероятностей [7]:

$$f_{P_{ij}}\left(p_{ij}\right)=\begin{cases} p_{ij}^{\alpha_{ij}-1}(1-p_{ij})^{\beta_{ij}-1}, 0\le p_{ij}\le 1, \\ 0, \textit{иначе}. \end{cases} \quad (1)$$

Известно, что среднее $\mathrm{E}_{p_{ij}}$ и дисперсия $\sigma^2_{p_{ij}}$ в этом случае вычисляются по формулам:

$$\mathrm{E}_{p_{ij}}=\frac{\alpha_{ij}}{\alpha_{ij}+\beta_{ij}},\ \sigma^2_{p_{ij}}=\frac{\alpha_{ij}\beta_{ij}}{(\alpha_{ij}+\beta_{ij})^2(\alpha_{ij}+\beta_{ij}+1)} \quad (2)$$

Апостериорное распределение показателя можно получить на основе фактической информации о выполнении соответствующего требования, т.е. указанных выше элементов – документов, фактов и т.д. Для этого воспользуемся теоремой Байеса в форме, представленной в [7], стр. 107:

$$g_{P_{ij}}\left(p_{ij}\mid x_{ij}\right)=g_{X_{ij}}\left(x_{ij}\mid p_{ij}\right)f_{P_{ij}}\left(p_{ij}\right), \quad (3)$$

где X_{ij} – переменная, отражающая факты соответствия или несоответствия характеристик требованию по обеспечению ИБ в виде наблюдений $x_{ij} = 1$ (характеристика соответствует) или $x_{ij} = 0$ (характеристика не соответствует); $g_{P_{ij}}\left(p_{ij} \mid x_{ij}\right)$ – апостериорная оценка значения показателя при условии, что получена информация x_{ij}, т.е. учтены документы или факты и т.д., связанные с выполнением или невыполнением рассматриваемого требования к обеспечению ИБ; $g_{X_{ij}}\left(x_{ij} \mid p_{ij}\right)$ – правдоподобие получения информации x_{ij} при данном значении p_{ij}; $f_{P_{ij}}\left(p_{ij}\right)$ – априорная функция плотности распределения P_{ij}, вычисляемая в соответствии с (1).

Определим правдоподобие получения информации о показателе. Пусть вначале выбирается всего один элемент из совокупности характеристик требования к обеспечению к ИБ. Если он удовлетворяет требованию, то $x_{ij} = 1$, а вероятность такого исхода равна p_{ij}, в противном случае $x_{ij} = 0$, а вероятность исхода, состоящего в том, элемент не удовлетворяет требованию, равна $1 - p_{ij}$. Правдоподобие $g_{X_{ij}}\left(x_{ij} \mid p_{ij}\right)$ можно записать (см. [7], стр. 128) в виде:

$$g_{X_{ij}}\left(x_{ij} \mid p_{ij}\right) = \begin{cases} p_{ij}^{x_{ij}}\left(1-p_{ij}\right)^{1-x_{ij}}, x_{ij} = 0 \text{ или } 1, \\ 0, x_{ij} \neq 0 \; и \; x_{ij} \neq 1. \end{cases} \tag{4}$$

Апостериорное распределение показателя P_{ij} может быть получено подстановкой (1) и (4) в (3):

$$g_{P_{ij}}\left(p_{ij} \mid x_{ij}\right) = \begin{cases} p_{ij}^{x_{ij}}\left(1-p_{ij}\right)^{1-x_{ij}} p_{ij}^{\alpha_{ij}-1}\left(1-p_{ij}\right)^{\beta_{ij}-1}, x_{ij} = 0 \text{ или } 1, \; p_{ij} \in [0,1] \\ 0, x_{ij} \neq 0 \; и \; x_{ij} \neq 1, p_{ij} < 0 \text{ или } p_{ij} > 1, \end{cases} =$$

$$= \begin{cases} p_{ij}^{\alpha_{ij}+x_{ij}-1}\left(1-p_{ij}\right)^{\beta_{ij}+(1-x_{ij})-1}, x_{ij} = 0 \text{ или } 1, \; p_{ij} \in [0,1], \\ 0, x_{ij} \neq 0 \; и \; x_{ij} \neq 1, p_{ij} < 0 \text{ или } p_{ij} > 1. \end{cases} \tag{5}$$

Из (5) следует, что апостериорное распределение P_{ij} есть бета-распределение с параметрами $\alpha_{ij} + x_{ij}$ и $\beta_{ij} + (1 - x_{ij})$. Т.е. если выбранный

элемент из совокупности характеристик требования, показатель P_{ij} которого оценивается, соответствует требованию и $x_{ij} = 1$, апостериорное распределение данного показателя будет бета-распределением $B(\alpha_{ij} + 1, \beta_{ij})$, а если не соответствует – апостериорное распределение будет $B(\alpha_{ij}, \beta_{ij} + 1)$.

В общем случае среди n элементов, характеризующих требование, которое оценивает показатель P_{ij}, имеется q_{ij} позитивных (например, документов и фактов персонификации ролей, настроек прав пользователей, должностных инструкций, журналов событий), и r_{ij} дефицитов (просрочек, выявленных несоответствий). Тогда, по аналогии с представленным выше описанием, можно получить функцию правдоподобия для переменной Q_{ij}, определяющей число позитивных элементов в выборке из n элементов, относительно p_{ij}:

$$g_{Q_{ij}}\left(q_{ij} \mid p_{ij}\right) = \begin{cases} p_{ij}^{q_{ij}} (1 - p_{ij})^{r_{ij}} \text{ при } q_{ij} = 0,1,\ldots,n, r_{ij} = n - q_{ij} \\ 0, \text{ иначе.} \end{cases} \quad (6)$$

Апостериорное распределение показателя при этом есть бета-распределение с параметрами $\alpha_{ij} + q_{ij}$ и $\beta_{ij} + r_{ij}$: $B(\alpha_{ij} + q_{ij}, \beta_{ij} + r_{ij})$.

Вероятностная модель оценки степени защищенности объектов КИИ

В соответствии с методикой СТО БР ИББС-1.2-2014 модель оценки уровня защищенности объектов КИИ организаций БС на основе внутреннего аудита имеет трехуровневую структуру:

– базовый уровень, включающий частные показатели;

– средний уровень, включающий групповые показатели, вычисляемые с помощью агрегирования частных показателей;

– верхний уровень, включающий коэффициенты, характеризующие текущий уровень, менеджмент и уровень осознания ИБ организации, а также итоговый коэффициент, отражающий степени защищенности объектов КИИ.

Если учитывать лишь факторы организационной структуры и управления, можно выделить следующие групповые показатели:

– структуру или иерархию управления;

– наличие, полномочия и процессы службы ИБ;

– распределение ролей и полномочий;

– уровень подготовки персонала;

– процессы реагирования на инциденты.

Каждому групповому показателю соответствует множество частных показателей, относящихся к рассматриваемым факторам. Будем оценивать их значения на основе представленного выше байесовского подхода. На первом этапе следует задать начальные оценки параметров α_{ij}^0 и β_{ij}^0 с помощью априорного значения каждого частного показателя. Так как рассматривается случайная величина, подчиняющаяся бета-распределению, можно учесть близость бета-распределения к нормальному и использовать широко распространенный доверительный интервал, равный шести стандартным отклонениям, в котором лежит большая часть значений нормально распределенной величины [9, 10]. Если, например, известно, что априорное значение показателя P_{ij} находится на отрезке от 0,2 до 0,8, тогда среднее значение равно 0,5, среднеквадратическое отклонение $\sigma = 0{,}1$, т.е. априорное значение показателя лежит в границах $0{,}5 \pm 3\sigma$. При этом из (2) можно получить начальные значения параметров: $\alpha_{ij}^0 = \beta_{ij}^0 = 12$. С другой стороны, априорные значения частных показателей могут быть известны в результате предшествующих аудитов. Если априорное значение частного показателя близко к единице, т.е. позитивных характеристик наблюдалось больше, чем дефицитов, то следует задать $\alpha_{ij}^0 > \beta_{ij}^0$, если априорное значение частного показателя около 0,5 – $\alpha_{ij}^0 = \beta_{ij}^0$, а если оно близко к нулю – $\alpha_{ij}^0 < \beta_{ij}^0$ [7].

Среднее значение частного показателя $\mathrm{E}_{p_{ij}}$, вычисляемое на основе его апостериорного распределения, в соответствии с (2) и с учетом (6) равно

$$\mathrm{E}_{p_{ij}} = \frac{\alpha_{ij}^{0} + q_{ij}}{\alpha_{ij}^{0} + \beta_{ij}^{0} + n}, \tag{7}$$

где q_{ij} – количество позитивных элементов, характеризующих требование, которое оценивает показатель P_{ij}. Таким образом, с помощью (7) можно получать оценки значений частных показателей, предварительно определяя количество позитивных элементов q_{ij} и дефицитов r_{ij}.

Групповые показатели P_i в простом случае могут быть вычислены с помощью усреднения соответствующих частных показателей:

$$P_i = \frac{1}{h_i} \sum_{j=1}^{h_i} \mathrm{E}_{p_{ij}},$$

где h_i – количество частных показателей, соответствующих групповому показателю P_i. На верхнем уровне на основе групповых показателей P_i вычисляется коэффициент P, отвечающий за уровень защищенности объектов КИИ, как минимальное значение среди групповых показателей организационной структуры и управления:

$$P = \min_{i \in \{1,2,\ldots,h\}} (P_i),$$

где h – количество групповых показателей.

Таким образом, детализацию процесса анализа требований к обеспечению ИБ в организации БС целесообразно проводить на базовом уровне, накапливая документы, факты, методики, настройки программного обеспечения и т.д., относящиеся к выполнению тех или иных требований. В таком случае каждый внутренний аудит позволит уточнять оценки значений частных показателей. Совокупности характеристик требований по обеспечению ИБ образуют выборки, на основе которых вычисляются оценки средних значений частных показателей выполнения требований как числа из

диапазона [0, 1]. Такой подход представляется гибким и объективным для оценки степени выполнения требований по обеспечению ИБ.

Заключение

В работе рассмотрено применение байесовского подхода для оценки значений частных показателей выполнения требований по обеспечению ИБ в организациях БС. Предложена модель оценки уровня обеспечения ИБ на основе внутреннего аудита, факторами которой являются требования к организационной структуре и управлению, использующая вероятностные компоненты в виде оценок частных показателей. В модель могут быть добавлены и другие факторы, влияющие на уровень ИБ, также возможна ее модификация посредством задания иерархии показателей. Такой подход позволяет усовершенствовать методики построения моделей для оценки уровня защищенности объектов КИИ в организациях БС с помощью всестороннего охвата характеристик требований по обеспечению ИБ, измерения значений частных показателей выполнения требований в непрерывной шкале и учета влияния истории изменений характеристик требований по обеспечению ИБ на результирующий уровень защищенности.

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

Литература

1. Токарев В.Л., Сычугов А.А. Интеллектуальная поддержка обнаружения инцидентов информационной безопасности. Моделирование, оптимизация и информационные технологии. 2023. №1. URL: moitvivt.ru/ru/journal/pdf?id=1271.
2. Palchevsky E.V., Antonov V.V., Filimonov N.B., Rodionova L.E., Kromina L.A., Abdulnagimov A.I., Oleynikov A., Breikin T. Development of a Method for Training a Pulse Neural Network and its Application in a New

Approach for Analyzing Network Traffic and Detecting DDos Attacks. Available at SSRN: ssrn.com/abstract=5009235 or dx.doi.org/10.2139/ssrn.5009235.

3. Ганжур М.А., Ганжур А.П., Борисенко И.М. Обеспечение компьютерной безопасности с использованием метода «безопасность через неясность» // Инженерный вестник Дона. 2019. №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5755/.
4. Колесникова Д.С., Верещагина Е.А., Гуляев В.Е. Построение онтологической модели для предметной области «Информационная безопасность» // Инженерный вестник Дона. 2023. №7. URL: ivdon.ru/ru/magazine/archive/n7y2023/8532/.
5. Нечаев С.В., Занин И.Ф., Беспалова Н.В., Ершов А.С., Хороводова Н.Ю. Безопасность Android-приложений // Инженерный вестник Дона. 2025. №7. URL: ivdon.ru/ru/magazine/archive/n7y2025/10238/.
6. Patterson C. M., Nurse J. R. C., Franqueira V. N. L. Learning from cyber security incidents: A systematic review and future research agenda. Computers & Security. 2023. V. 132. P. 103309.
7. Хей Дж. Введение в методы байесовского статистического вывода. Москва: Финансы и статистика. 1987. 336 с.
8. Heard N. An Introduction to Bayesian Inference, Methods and Computation. Cham, Switzerland: Springer. 2021. 169 p.
9. Шторм Р. Теория вероятностей. Математическая статистика. Статистический контроль качества. Москва: Мир. 1970. 368 с.
10. Brue G. Six Sigma for Managers, Second Edition. New York: McGraw-Hill. 2015. 272 p.

References

1. Tokarev V.L., Sychugov A.A. Modelirovanie, optimizatsiya i informatsionnye tekhnologii. 2023. №1. URL: moitvivt.ru/ru/journal/pdf?id=1271.
2. Palchevsky E.V., Antonov V.V., Filimonov N.B., Rodionova L.E., Kromina L.A., Abdulnagimov A.I., Oleynikov A., Breikin T. Development of a Method for Training a Pulse Neural Network and its Application in a New Approach for Analyzing Network Traffic and Detecting DDos Attacks. Available at SSRN: ssrn.com/abstract=5009235 or dx.doi.org/10.2139/ssrn.5009235.
3. Ganzhur M.A., Ganzhur A.P., Borisenko I. M. Inzhenernyj vestnik Dona. 2019. №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5755/.
4. Kolesnikova D. S., Vereshchagina E. A., Gulyaev V. E. Inzhenernyj vestnik Dona. 2023. №7. URL: ivdon.ru/ru/magazine/archive/n7y2023/8532/.
5. Nechaev S.V., Zanin I.F., Bespalova N.V., Ershov A.S., Khorovodova N. Yu. Inzhenernyj vestnik Dona. 2025. №7. URL: ivdon.ru/ru/magazine/archive/n7y2025/10238/.
6. Patterson C. M., Nurse J. R. C., Franqueira V. N. L. Learning from cyber security incidents: A systematic review and future research agenda. Computers & Security. 2023. V. 132. P. 103309.
7. Hey J. Vvedenie v metody bayesovskogo statisticheskogo vivoda [An introduction to Bayesian statistical inference for economists]. Moskva: Financy i statistika. 1987. 336 p.
8. Heard N. An Introduction to Bayesian Inference, Methods and Computation. Cham, Switzerland: Springer. 2021. 169 p.
9. Shtorm R. Teoriya veroyatnostey. Matematicheskaya statistika. Statisticheskiy control kachestva [Probability theory. Mathematical statistics. Statistical quality control]. Moskva: Mir. 1970. 368 p.

10. Brue G. Six Sigma for Managers, Second Edition. New York: McGraw-Hill. 2015. 272 p.

Дата поступления: 10.08.2025

Дата публикации: 25.09.2025