Максим О. Таныгин[1], Юлия А. Будникова[2], Андрей С. Булгаков[3], Михаил А. Марченко[4]
[1,2]Юго-Западный государственный университет,
ул. 50 лет октября, 94, Курск, 305040, Россия
[3,4]Национальный исследовательский университет «Московский институт электронной техники»,
площадь Шокина, 1, Зеленоград, Москва, 124498, Россия,
[1]e-mail: tanygin@yandex.com, https://orcid.org/0000-0002-4099-1414
[2]e-mail: juli-budni19ok@mail.ru, https://orcid.org/0000-0002-1010-5709
[3]e-mail: bulgakov1703@yandex.ru, https://orcid.org/0000-0003-4374-8409
[4]e-mail: marchenko14120@gmail.com, https://orcid.org/0000-0001-6885-8415

МОДЕЛЬ ОЦЕНКИ УЩЕРБА ОТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2021.2.09

Аннотация. Любая информационная система в процессе эксплуатации требует резервирования определённого объёма средств на ликвидацию последствий инцидентов информационной безопасности в случае их возникновения. Для оценки величины ущерба использовались многомодальные законы распределения плотностей вероятностей ущерба в единичном инциденте информационной безопасности, а инциденты информационной безопасности рассматриваются как события пуассоновского потока. В работе определены зависимости между интенсивностью возникновения событий информационной безопасности, характеристиками распределения плотностей вероятностей ущерба и необходимой величиной резервируемых средств. Представленная модель оценки ущерба от инцидентов информационной безопасности позволяет более точно подходить к оценке требуемого объем резервируемых средств. Показано, что экономия средств достигает 40-50% в сравнении с подходом, основанным на оценке ущерба исходя только из среднего числа инцидентов и среднего ущерба от единичного инцидента информационной безопасности.

Ключевые слова: инциденты информационной безопасности, угрозы информационной безопасности, плотность вероятности распределения ущерба, оценка величины ущерба, ликвидация последствий инцидентов информационной безопасности.

Для цитирования: ТАНЫГИН, Максим О. и др. МОДЕЛЬ ОЦЕНКИ УЩЕРБА ОТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 98–106, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1347>. Дата доступа: 13 may 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.09.

Maxim O. Tanygin[1], Yulia A. Budnikova[2], Andrey S. Bulgakov[3], Mikhail A. Marchenko[4]
[1,2]South-West State University,
50 Let Oktyabrya str., 94, Kursk, 305040, Russia
[3,4]National Research University of Electronic Technology,
Shokin Square, 1, Zelenograd, Moscow, 124498, Russia
[1]e-mail: tanygin@yandex.com, https://orcid.org/0000-0002-4099-1414
[2]e-mail: juli-budni19ok@mail.ru, https://orcid.org/0000-0002-1010-5709
[3]e-mail: bulgakov1703@yandex.ru, https://orcid.org/0000-0003-4374-8409
[4]e-mail: marchenko14120@gmail.com, https://orcid.org/0000-0001-6885-8415

A model for assessing information security incidents damage

DOI: http://dx.doi.org/10.26583/bit.2021.2.09

Abstract. Any information system requires the funds reservation for the elimination of the consequences of information security incidents in the event of their occurrence. To estimate the amount of damage, we used multi-modal probability densities distribution laws for the damage in a single information security incident, while the information security incidents are considered as Poisson flow events. The paper defines the relationships between the intensity of information security events, the characteristics of the

distribution of probability densities of damage, and the required amount of reserved funds. The presented model of damage assessment from information security incidents allows a more accurate approach for estimation of the required amount of reserved funds. It is shown that the cost saving reaches 40-50% in comparison with the damage assessment approach using only on the average number of incidents and the average damage from a single incident of information security.
Keywords: information security incidents, information security threats, probability density of damage distribution, damage assessment, elimination of consequences of information security incidents.
For citation: TANYGIN, Maxim O. et al. A model for assessing information security incidents damage. IT Security (Russia), [S.l.], v. 28, n. 2, p. 98–106, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1347>. Date accessed: 13 may 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.09.

Введение

Инциденты информационной безопасности (ИИБ), происходящие в информационной системе, требуют от владельца информационной системы (ИС) затрат на ликвидацию их последствий. Это могут быть затраты на закупку вышедшего из строя оборудования, оплату труда специалистов, ликвидирующих последствия инцидентов, компенсация расходов, связанных с потерей системой работоспособности и прочее [1, 2]. Ущерб, понесенный владельцем, можно всегда оценить в денежном эквиваленте. Организация должна зарезервировать некоторый объём денежных средств, которые расходуются в случае реализации угрозы информационной безопасности [3, 4]. При этом способ резервирования этих средств должен позволять использовать их непосредственно после возникновения ИИБ [5, 6], что подразумевает снижение их стоимости в результате инфляции. Таким образом, перед владельцем ИС стоит задача, с одной стороны, обеспечения возможности компенсации затрат на ликвидацию последствий ИИБ, а с другой стороны – минимизировать объём средств, задепонированных с этой целью [7]. Величина ущерба, понесённого владельцем ИС в результате ИИБ, является случайной величиной, а наступление самого ИИБ – случайное событие. Для определения целесообразного объёма резервируемых средств необходимо выполнить оценку вероятности ущерба, исходя из истории ИИБ.

1. Модель оценки ущерба

При оценке величины ущерба от единичного ИИБ важной характеристикой является плотность распределения вероятности ущерба $p(U)$, где U – величина ущерба от инцидента информационной безопасности, выраженная в некоторых условных единицах (рублях, человеко-часах и пр.). Статистика ИИБ и аналитические материалы позволяет утверждать, что нормальный закон распределения ущерба не подходит для описания функции $p(U)$ из-за того, что частота возникновения инцидентов, ущерб от которых неформально можно классифицировать как «незначительный», «средний», «значительный» отличается несущественно [8]. Поэтому нельзя пренебречь вкладом ни одной из указанных категорий ИИБ в общий размер ущерба. И при этом величина ущерба, которая позволяет отнести ИИБ к категории «значительный», может на порядки превышать величину ущерба, классифицируемого как «незначительный» [9]. Таким образом, функция распределения $p(U)$ имеет так называемый «тяжелый конец» (англ. – heavy-tailed distribution) [10].

Использованное для моделирования ущерба логнормальное распределение [11] также является одномодальным, что не позволяет адекватно моделировать ущерб. Причиной этого является то, что объектами угроз являются конкретные компоненты информационных систем. Ущерб, нанесенный в результате таких угроз, обычно лежит в

узком диапазоне, число же таких компонент, подверженных атакам в реальных системах, невелико [12]. Такая особенность обуславливает применение многомодальных распределений плотностей вероятностей ущерба [13].

Модель оценки ущерба предполагает представление функции распределения ущерба в единичном ИИБ, рассматриваемом исходя из двух неравновероятных нормальных распределений $p_1(U)$ (условно, инциденты с малым ущербом) и $p_2(U)$ (инциденты с большим ущербом) с различными математическими ожиданиями ущерба μ_1 и μ_2 ($\mu_1 < \mu_2$) и дисперсиями σ_1 и σ_2 соответственно:

$$p^1(U) = k_1\, p_1(U) + k_2 \cdot p_2(U), \tag{1}$$

где k_1 и k_2 – веса двух распределений ($k_1 > k_2$). Они определялись исходя из параметра модели K – отношения весов двух распределений и условия нормировки:

$$K = k_1 / k_2,$$
$$\int_{-\infty}^{\infty} \left(k_1 p_1(U) + k_2 p_2(U)\right) dU = 1. \tag{2}$$

Соотношения между параметрами μ_1 и μ_2 рассматриваемой модели выбирались в диапазоне от 7 до 12, исходя из имеющихся данных по величине ущерба информационной безопасности от различных угроз [14, 15]. Значения среднеквадратических отклонений σ_i, i = 1,2 выбирались в диапазоне 0.3…0.7 μ_i. Следует отметить, что в рамках модели значения имели именно отношения между данными параметрами, а не их абсолютные значения, так как изначально единица измерения величины ущерба U выбирается, исходя из особенностей каждой моделируемой ИС.

Отдельно стоит рассмотреть интервал модельного времени. Для получения более точных результатов интервал должен быть таким, чтобы среднее число λ инцидентов в нем лежало в диапазоне от 0.5 до 4.0. В противном случае, при числе ИИБ большем 4, расчет ущерба, выполняемый, как будет показано в дельнейшем, путём многократного нахождения численными методами значений двойного интеграла на бесконечном интервале численных методов будет сопряжен с большим объемом вычислений. Помимо факториального роста времени расчёта, это даст значительную погрешность из-за накапливаемой в каждой итерации ошибки вычислений. Если число ИИБ в течение интервала времени, выбранного за единицу модельного времени, выходит из указанного диапазона, то для получения более точных оценок ущерба единицу модельного времени следует изменить. Например, если среднее число ИИБ в течение года будет слишком велико, то следует считать среднее число ИИБ в квартал и т.д. На практике это будет означать переход от годового планирования к поквартальному [16].

Так как число инцидентов информационной безопасности в интервале модельного времени является случайной величиной, необходимо определить функцию распределения $p^{(n)}(U)$ плотностей вероятностей ущерба от n инцидентов ИБ. Для нахождения $p^{(n)}(U)$ будем использовать рекуррентную формулу:

$$p^{(n)}(U) = \frac{\int_0^U p^{(n-1)}(U-u) \cdot p^1(u)\, du}{\int_0^\infty \int_0^\infty p^{n-1}(u_1) \cdot p^1(u_2)\, du_1 du_2}, \tag{3}$$

где знаменатель введен для выполнения условия: $\int_0^\infty p^{(n)}(U)dU = 1$, а в числителе подынтегральное выражение – это плотность распределения вероятности события, при котором величина от одного ИИБ равна u, а от оставшихся $(n-1)$ ИИБ – $(U-u)$.

2. Результаты моделирования

На рис. 1 в качестве примера приведены полученные для одного набора параметров $\{K, \mu_1, \mu_2, \sigma_1, \sigma_2\}$ зависимости плотностей вероятностей ущерба для одной, двух, трёх и четырех угроз ИИБ. Значения параметров выбраны таким образом, чтобы проиллюстрировать возникновение второго локального максимума, значительно отличающегося по высоте от первого, на графике плотности распределения вероятностей.

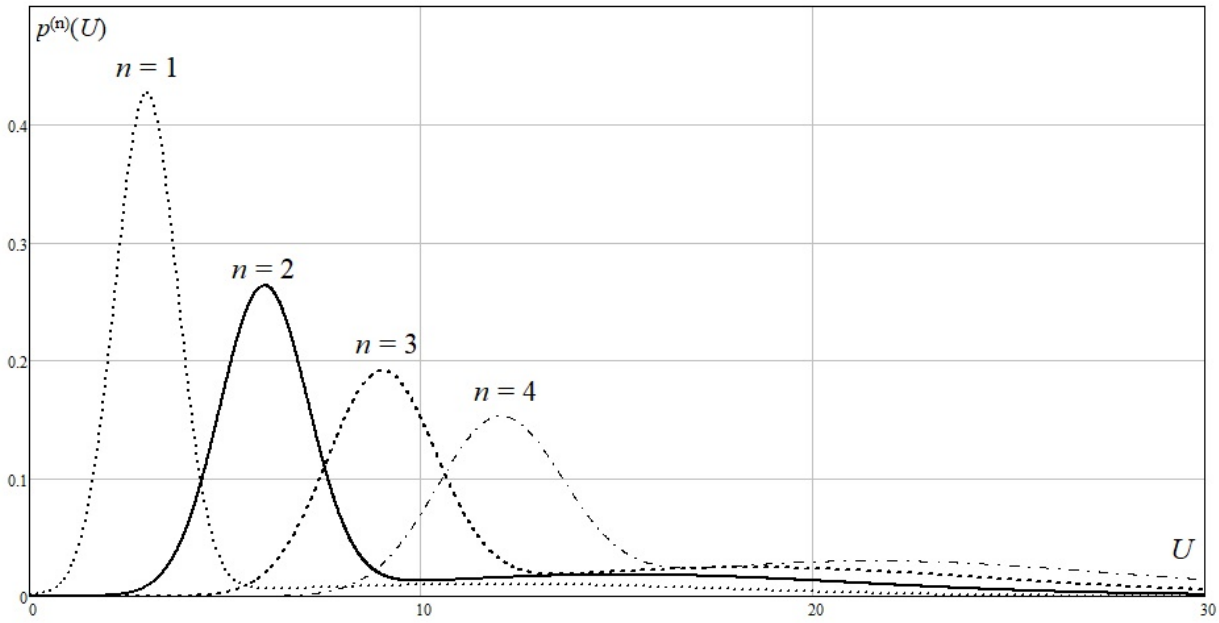

Рис. 1. Зависимость плотности вероятностей ущерба при K=6, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8 и числе инцидентов n

Fig. 1. The probability density distribution of damage at K=6, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8, and number of incidents n

Влияние каждого из параметров математической модели на характер зависимости различно. С увеличением соотношения между весами распределения второй локальный максимум в правой части графиков становится менее значительным, рост отношения μ_2/μ_1 сдвигает позицию второго локального максимума вправо, делая сам максимум более заметным на фоне значений, даваемых распределением $p_1(U)$. Увеличение дисперсии σ_1 делает второй максимум, наоборот, менее заметным в правой части графика. С ростом числа n инцидентов информационной безопасности (при n=5, 6 …) влияние так называемого «тяжелого конца» в функции распределения плотностей вероятности ущерба от единичного инцидента растет. Форма кривой $p^{(n)}(U)$ становится более пологой, первый локальный максимум в окрестности $U = n \cdot \mu_1$ становится менее значительным, значение плотности вероятностей в окрестности второго локального максимума ($U = n \cdot \mu_2$) растет, как и растёт значение плотности вероятностей между максимумами (при $n \to \infty$ график выродится в одномодальный график с математически ожиданием $k_1 \cdot \mu_1 + k_2 \cdot \mu_2$).

Результирующая плотность вероятности распределения ущерба определяется по формуле:

$$p(U) = \sum_{i=1}^{\infty} p_{sl}(i) \cdot p^{(i)}(U), \quad (4)$$

где $p_{sl}(i)$ – вероятность возникновения i инцидентов информационной безопасности в течение интервала модельного времени.

Если исходить из предположения, что инциденты информационной безопасности порождаются множеством независимых субъектов, активность которых не зависит друг от друга, то для нахождения вероятности числа инцидентов будем использовать распределение Пуассона с интенсивностью λ [15] равной среднему наблюдаемому числу инцидентов информационной безопасности в течение исследуемого интервала:

$$p_{sl}(i) = \frac{\lambda^i}{i!} e^{-\lambda}, \quad (5)$$

График плотности вероятности ущерба при разных значениях интенсивностей приведен на рис. 2.

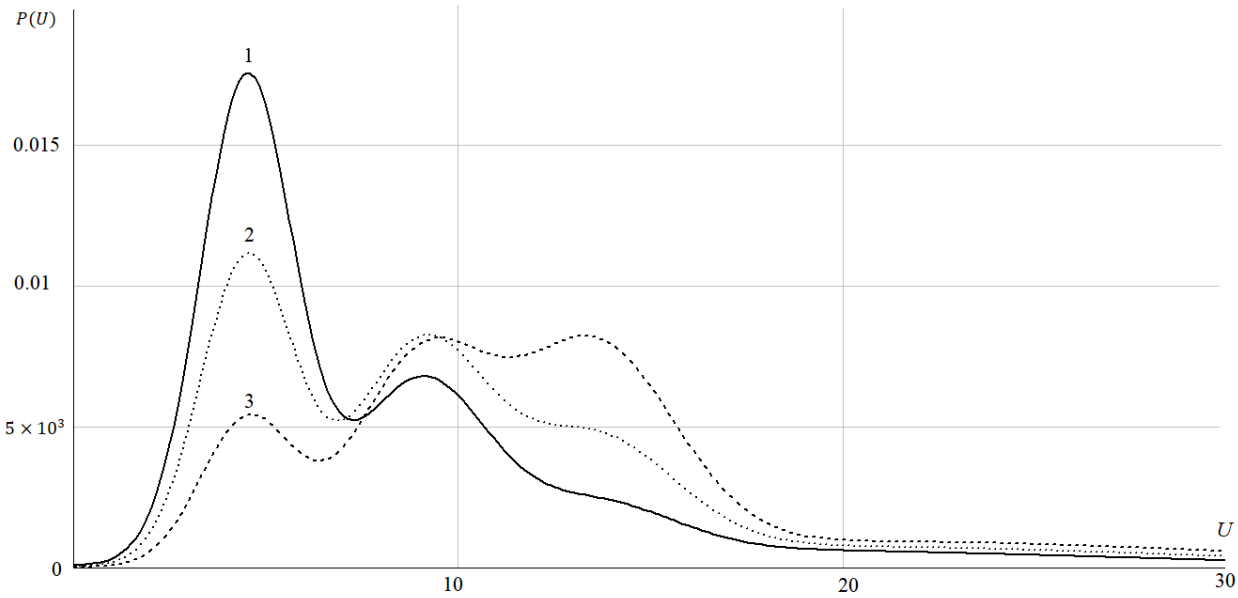

Рис. 2. Графики плотности распределения вероятностей ущерба при K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8: 1) λ = 1.0;2) λ = 2.0;3) λ = 4.0

Fig. 2. Graphs of the probability distribution density of damage at K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8: 1) λ = 1.0;2) λ = 2.0;3) λ = 4.0

Из формы графиков видно, что, увеличение интесивности возникновения инцидентов смещает вправо области наиболее вероятных значений, делая более заметным влияние «тяжелого конца» исходного распределения (1). При этом, в исследуемых диапазонах изменения параметра λ наблюдается незначительный рост функции распределения вероятностей при $U > 10 \cdot \mu_2$ (значения функции плотности ущерба близко к нулю). Последний факт создает предпосылки к игнорированию таких ситуаций с высоким суммарным ущербом от ИИБ как маловероятных [17, 18].

3. Прогнозирование величины затрат на устранение последствий инцидентов информационной безопасности

Так как начальная задача исследования формулировалась как определение величины необходимых депонируемых средств для нейтрализации угроз, а размер максимального ущерба неограничен, то необходимо ввести параметр D – доля угроз, на нейтрализацию которых задепонированных средств будет достаточно [19]. Эта доля определится как значение функции распределения вероятностей ущерба $p(U)$ (см. формулу (4)) при $U = U^{\max}$:

$$D = \int_0^{U^{\max}} \left[\sum_{i=1}^{\infty} p_{sl}(i) \cdot p^{(i)}(U) \right] dU, \qquad (6)$$

где $U^{\max}$ – величина ущерба, которую с вероятностью D не превысит суммарный ущерб от всех ИИБ в течение единицы модельного времени. На основании зависимости (6) определяется $U^{\max}$ как функция всех описанных выше параметров модели, а также параметра D.

График зависимости размера резервируемых средств от интенсивности возникновения ИИБ приведен на рис. 3, линии 1 и 2.

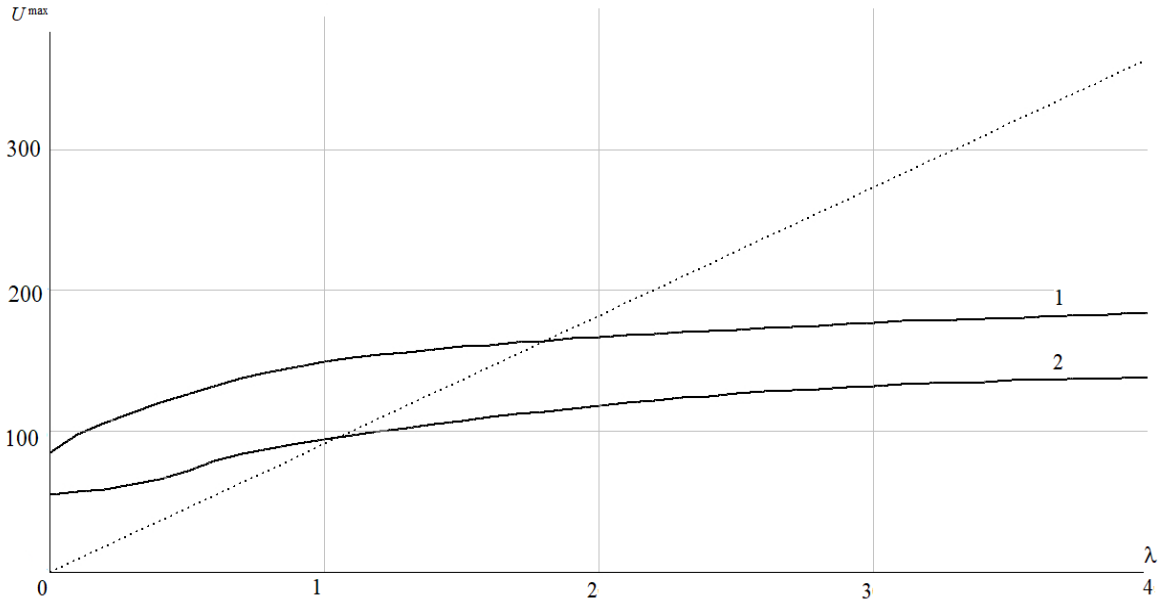

Рис. 3. График зависимости размера резервируемых средств U^{max} от интенсивности возникновения инцидентов λ
1) K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8, D=0.9;
2) K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8, D=0.7
Fig. 3. Graph of the reserved funds amount U^{max} dependence on the incidents occurrence intensity λ
1) K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8, D=0.9;
2) K=15, μ_1=1.5, μ_2=3.0, σ_1=0.2, σ_2=0.8, D=0.7

В качестве эталона была взята модель определения величины ущерба как произведение среднего ущерба от единичного ИИБ на среднее число таких же λ инцидентов с аналогичной долей D от полученного значения величины депонированных средств (зависимость показана пунктирной линией на рис. 3). Сравнение эталонных значений необходимого объёма депонированных средств $U^{\max}$ и значений, полученных на рассматриваемой в статье модели, показало, что последняя даёт более точную оценку

величины ущерба за счёт учёта вероятности возникновения ИИБ с высоким ущербом. Это позволяет резервировать на 40–50% меньше средств при больших ($\lambda>3$) значениях среднего числа ИИБ в выбранную единицу времени по сравнению с простым анализом средних значений ущерба (правая часть графиков). При небольшой же интенсивности инцидентов разработанная модель дает больший объем резервируемых средств, что позволяет ликвидировать последствия ИИБ в более полном объеме.

Заключение

Предложенная в настоящей статье математическая модель прогнозирования затрат на устранения последствий ИИБ основывается на представлении плотности распределения вероятностей ущерба от единичного инцидента в виде многомодального распределения. Исходя из рассчитанной величины ущерба от нескольких ИИБ, получены численные зависимости требуемого объема средств от среднего числа ИИБ в единицу модельного времени. В практическом плане это позволит, основываясь на истории понесенных затрат, более точно прогнозировать объём резервируемых на ликвидацию последствий ИИБ средств и оценивать максимальные затраты на внедрение и обслуживание дополнительных подсистем обеспечения ИБ.

Кроме того, получена зависимость требуемого объема средств от планируемой доли инцидентов, последствия которых удастся компенсировать или ликвидировать. Рассмотренная модель позволяет снизить размер депонируемых средств в некоторых случаях на 40–50% по сравнению с моделями, основанными исключительно на математических ожиданиях ущерба и числа инцидентов.

СПИСОК ЛИТЕРАТУРЫ:

1. Hui P. Construction of Information Security Risk Assessment Model in Smart City / 2020 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), Shenyang, China, 2020. P. 393–396. DOI: http://dx.doi.org/10.1109/TOCS50858.2020.9339614.
2. Белов В.М., Пестунов А.И., Пестунова Т.М. Методика оценки рисков информационной безопасности бизнес-процессов // ОмГТУ. 2016. №1. С. 158–161. URL: https://www.elibrary.ru/item.asp?id=27410988 (дата обращения: 01.03.2021).
3. Xiaoqian Wu, Yongjun Shen, Guidong Zhang, & Hua Zhi. Information security risk assessment based on D-S evidence theory and improved TOPSIS. 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2016. P. 153–156. DOI: http://dx.doi.org/10.1109/icsess.2016.7883037.
4. Станиславчик Е.Н. Риск-менеджмент на предприятии. Теория и практика. М.: «Ось-89». 2002. – 80 с.
5. Wangen, G. An initial insight into information security risk assessment practices / Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS. 2016. Vol. 8. P. 999–1008. DOI: http://dx.doi.org/10.15439/2016F158.
6. Luo H., Shen Y., Zhang G., & Huang L. Information security risk assessment based on two stages decision model with grey synthetic measure. 2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS). Beijing, China, 2015. P. 795–798. DOI: http://dx.doi.org/10.1109/icsess.2015.7339176.
7. Репин М.М., Сакулина А.В., Пшехотская Е.А. Построение модели оценки экономической эффективности системы информационной безопасности // Научно-методическое обеспечение оценки качества образования. 2017. №2 (3). С. 80–84. URL: https://cyberleninka.ru/article/n/postroenie-modeli-otsenki-ekonomicheskoy-effektivnosti-sistemy-informatsionnoy-bezopasnosti (дата обращения: 01.03.2021).
8. Голубинский А.Н., Алехин И.В. Анализ распределений ущербов при реализации угроз в информационно-технических системах // Вестник ВИ МВД России. 2016. №3. С. 24–32. URL: https://www.elibrary.ru/item.asp?id=26683939 (дата обращения: 01.03.2021).
9. Andress Jason, Leary Mark. Building a Practical Information Security Program // Syngress. 2017. – 192 p.
10. Klebanov L. Heavy Tailed Distributions. Matfyzpress, Prague, 2003. – 176 p. ISBN: 80-86732-02-9.

11. Казакова А.В. Модель угроз информационной безопасности промышленных предприятий // Проблемы совершенствования организации производства и управления промышленными предприятиями: Межвузовский сборник научных трудов. 2011. № 1. С. 88–96. URL: https://www.elibrary.ru/item.asp?id=20405652 (дата обращения: 01.03.2021).
12. Wangen G. (2019) Quantifying and Analyzing Information Security Risk from Incident Data. In: Albanese M., Horne R., Probst C. (eds) Graphical Models for Security. GraMSec 2019. Lecture Notes in Computer Science, Vol. 11720. Springer, Cham. P. 129–154. DOI: http://dx.doi.org/10.1007/978-3-030-36537-0_7.
13. Вадзинский Р.Н. Справочник по вероятностным распределениям. СПб.: Наука. 2001. – 295 с.
14. Peter H. Gregory Risk assessment in audit planning / Peter H. Gregory. 2018. – 46 p.
15. Peter H. Gregory CISM Certified Information Security Manager All-in-One Exam Guide» // Peter H. Gregory. 2018. – 1104 p.
16. Репин М.М. Пшехотская Е.А. Методика расчета показателя эффективности противодействия информационным угрозам в платёжной системе // Научно-методический журнал «Научно-методическое обеспечение оценки качества образования» – ГБУ ДПО РЦОКИО. 2018. №2(5). С. 141–148. URL: https://cyberleninka.ru/article/n/metodika-rascheta-pokazatelya-effektivnosti-protivodeystviya-informatsionnym-ugrozam-v-platezhnoy-sisteme (дата обращения: 01.03.2021).
17. Арсеньев В.Н., Силантьев С.Б., Ядренкин А.А. Использование априорной информации для коррекции модели потока событий в сложной системе // Изв. ВУЗов. Приборостроение. 2017. Т. 60. № 5. С. 391–397. DOI: http://dx.doi.org/10.17586/0021-3454-2017-60-5-391-397.
18. Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие. СПб: Университет ИТМО. 2015. – 93 с.
19. Пугин В.В. Губарева О.Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия // T-Comm – Телекоммуникации и Транспорт. 2012. Т. 6, № 6. С. 54–57. URL: https://www.elibrary.ru/item.asp?id=18848583 (дата обращения: 01.03.2021).

REFERENCES:

[1] Hui P. Construction of Information Security Risk Assessment Model in Smart City. 2020 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), Shenyang, China, 2020. P. 393–396. DOI: http://dx.doi.org/10.1109/TOCS50858.2020.9339614.
[2] Belov V.M., Pestunov A.I., Pestunova T.M. Metodika ocenki riskov informacionnoj bezopasnosti biznes-processov. OmGTU. 2016. №1. P. 158–161. URL: https://www.elibrary.ru/item.asp?id=27410988 (accessed: 01.03.2021) (in Russian).
[3] Xiaoqian Wu, Yongjun Shen, Guidong Zhang, & Hua Zhi. Information security risk assessment based on D-S evidence theory and improved TOPSIS. 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2016. P. 153–156. DOI: http://dx.doi.org/10.1109/icsess.2016.7883037.
[4] Stanislavchik E.N. Risk-menedzhment na predpriyatii. Teoriya i praktika. M.: «Os'-89». 2002. – 80 p. (in Russian).
[5] Wangen, G. An initial insight into information security risk assessment practices. Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS. 2016. Vol. 8. P. 999–1008. DOI: http://dx.doi.org/10.15439/2016F158.
[6] Luo H., Shen Y., Zhang G., & Huang, L. Information security risk assessment based on two stages decision model with grey synthetic measure. 2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS). Beijing, China, 2015. P. 795–798. DOI: http://dx.doi.org/10.1109/icsess.2015.7339176.
[7] Repin M.M., Sakulina A.V., Pshekhotskaya E.A. Postroenie modeli ocenki ekonomicheskoj effektivnosti sistemy informacionnoj bezopasnosti. Nauchno-metodicheskoe obespechenie ocenki kachestva obrazovaniya. 2017. №2 (3). S. 80–84. URL: https://cyberleninka.ru/article/n/postroenie-modeli-otsenki-ekonomicheskoy-effektivnosti-sistemy-informatsionnoy-bezopasnosti (accessed: 01.03.2021) (in Russian).
[8] Golubinskij A.N., Alekhin I.V. Analiz raspredelenij ushcherbov pri realizacii ugroz v informacionno-tekhnicheskih sistemah. Vestnik Voronezhskogo instituta MVD Rossii, 2016. no. 3. S. 24–32. URL: https://www.elibrary.ru/item.asp?id=26683939 (accessed: 01.03.2021) (in Russian).
[9] Andress Jason, Leary Mark. Building a Practical Information Security Program. 2017. – 192 p.
[10] Klebanov L. Heavy Tailed Distributions. Matfyzpress, Prague, 2003. – 176 p. ISBN: 80-86732-02-9.

[11] Kazakova A.V. Model' ugroz informacionnoj bezopasnosti promyshlennyh predpriyatij. Problemy sovershenstvovaniya organizacii proizvodstva i upravleniya promyshlennymi predpriyatiyami: Mezhvuzovskij sbornik nauchnyh trudov, 2011. no. 1. S. 88–96. URL: https://www.elibrary.ru/item.asp?id=20405652 (accessed: 01.03.2021) (in Russian).

[12] Wangen G. (2019) Quantifying and Analyzing Information Security Risk from Incident Data. In: Albanese M., Horne R., Probst C. (eds) Graphical Models for Security. GraMSec 2019. Lecture Notes in Computer Science, Vol. 11720. Springer, Cham. P. 129–154 DOI: http://dx.doi.org/10.1007/978-3-030-36537-0_7.

[13] Vadzinskij R.N. Spravochnik po veroyatnostnym raspredeleniyam. SPb.: Nauka. 2001. – 295 s. (in Russian).

[14] Peter H. Gregory Risk assessment in audit planning. Peter H. Gregory. 2018. – 46 p.

[15] Peter H. Gregory CISM Certified Information Security Manager All-in-One Exam Guide. 2018. – 1104 p.

[16] Repin M.M., Pshekhotskaya E.A. Metodika rascheta pokazatelya effektivnosti protivodejstviya informacionnym ugrozam v platyozhnoj sisteme. Nauchno-metodicheskij zhurnal «Nauchno-metodicheskoe obespechenie ocenki kachestva obrazovaniya» – GBU DPO RCOKIO. 2018, no. 2 (5) S. 141–148. URL: https://cyberleninka.ru/article/n/metodika-rascheta-pokazatelya-effektivnosti-protivodeystviya-informatsionnym-ugrozam-v-platezhnoy-sisteme (accessed: 01.03.2021) (in Russian).

[17] Arsenyev V.N., Silantyev S.B., Yadrenkin A.A. Using a priori information for correction of the events stream model in complex system. 2017. Vol. 60, no. 5. P. 391–397. DOI: http://dx.doi.org/10.17586/0021-3454-2017-60-5-391-397 (in Russian).

[18] Shcheglov A.Yu., Shcheglov K.A., Matematicheskie modeli i metody formal'nogo proektirovaniya sistem zashchity informacionnyh sistem. Uchebnoe posobie. SPb: Universitet ITMO, 2015. – 93 s. (in Russian).

[19] Pugin V. V. Gubareva O. YU. Obzor metodik analiza riskov informacionnoj bezopasnosti informacionnoj sistemy predpriyatiya. T-Comm – Telekommunikacii i Transport. 2012. T. 6, no. 6. S. 54–57. URL: https://www.elibrary.ru/item.asp?id=18848583 (accessed: 01.03.2021) (in Russian).

Поступила в редакцию – 09 апреля 2021 г. Окончательный вариант – 12 мая 2021 г.
Received – April 09, 2021. The final version – May 12, 2021.