Научная статья

УДК 004.056
DOI 10.25205/1818-7900-2023-21-1-19-31

Анализ рисков нарушения информационной безопасности от компьютерных атак при нарастающей величине потерь от их реализации

Алла Юрьевна Ермакова[1]
Алексей Борисович Лось[2]

[1]МИРЭА – Российский технологический университет
Москва, Россия

[2]Национальный исследовательский университет «Высшая школа экономики»
Москва, Россия

[1]ermakova_a@mirea.ru

[3]alos@hse.ru

Аннотация

В статье рассматриваются вопросы анализа рисков нарушения информационной безопасности в случае необходимости учета суммарного ущерба при возникновении компьютерных инцидентов.

В качестве математической модели возникновения инцидентов рассматривается дискретная временная модель, при которой инциденты в информационной системе возникают в случайные дискретные моменты времени. Под инцидентами при этом понимаются как непреднамеренные события, такие как сбои в работе, нарушения правил эксплуатации, так и преднамеренные – компьютерные атаки, попытки несанкционированного доступа и аналогичные ситуации. В случае применения риск-ориентированного подхода считаем, что наступление каждого инцидента сопровождается ущербом, величина которого фиксирована. Настройка реагирования на инциденты рассмотрена в двух основных сценариях с накоплением потерь и без таковой.

В работе в рамках рассматриваемых сценариев оцениваются риски нарушения информационной безопасности, в частности, найдено вероятностное распределение времени безопасной работы информационной системы. В качестве иллюстрации рассматриваемого подхода построены прогнозные модели количества несанкционированных операций со счетами юридических лиц и количества несанкционированных операций с использованием платежных карт. Рассматриваемые модели строятся по реальным данным об инцидентах, с применением разработанного ранее метода прогнозирования на основе непрерывной аппроксимирующей функции.

Ключевые слова

модель управления рисками, инциденты информационной безопасности, ущерб информационным активам, защищенность информационной системы, прогнозирование инцидентов.

Для цитирования

Ермакова А. Ю., Лось А. Б. Анализ рисков нарушения информационной безопасности от компьютерных атак при нарастающей величине потерь от их реализации// Вестник НГУ. Серия: Информационные технологии. 2023. Т. 21, № 1. С. 19–31. DOI 10.25205/1818-7900-2023-21-1-19-31

Analysis of the Risks of Information Security Violations from Computer Attacks with an Increasing amount of Damage from Their Implementation

Alla Yu. Ermakova[1], Alexey B. Los[2]

[1]Russian Technological University
Moscow, Russian Federation

[2]HSE University
Moscow, Russian Federation

[1]ermakova_a@mirea.ru
[3]alos@hse.ru

Abstract

The article discusses the issues of analyzing the risks of information security violations if it is necessary to take into account the total damage in the event of computer incidents.

A discrete time model is considered as a mathematical model of the occurrence of incidents, in which incidents in an information system occur at random discrete moments of time. Incidents are understood as unintended events, such as malfunctions, violations of operating rules, and intentional – computer attacks, unauthorized access attempts and similar situations. In the case of a risk-based approach, we believe that the occurrence of each incident is accompanied by damage, the magnitude of which is fixed.

The use of protective equipment reduces the likelihood of the risk of incidents. But setting up an incident response can be implemented in one of two main scenarios.

In one variant, when another incident occurs, the corresponding amount of damage is compared with its maximum allowable value. If the amount of damage received, regardless of the damage caused by other incidents, does not exceed the specified threshold, then the information system continues to operate normally. Otherwise, the security policy is reviewed, the necessary additional protective measures are introduced and other measures are taken to improve the security of the information system.

In another variant of the scenario, when incidents occur that lead to a violation of information security, the values of damages from successive incidents are summed up and the value of the sum is compared with the maximum allowable amount of damage. If, during the next incident, the total damage from all previous incidents does not exceed the maximum set value, the information system continues to operate normally. Otherwise, it is concluded that it is necessary to introduce additional protection measures.

In the work, within the framework of the models under consideration, the risks of information security violations are assessed, in particular, the probabilistic distribution of the time of safe operation of the information system is found. As an illustration of the considered approach, predictive models of the number of unauthorized transactions with accounts of legal entities and the number of unauthorized transactions using payment cards are constructed. The models under consideration are based on real data about incidents, using a previously developed forecasting method based on a continuous approximating function.

Keywords

risk management model, information security incidents, property damage to information assets, information system security, predicting incidents.

For citation

Ermakova A.Yu., Los A. B. Analysis of the Risks of Information Security Violations from Computer Attacks with an Increasing amount of Damage from Their Implementation. *Vestnik NSU. Series: Information Technologies*, 2023, vol. 21, no. 1, pp. 19–31. (in Russ.) DOI 10.25205/1818-7900-2023-21-1-19-31

Введение

В данной работе рассматривается актуальная задача разработки теоретико-вероятностных моделей, применяемых при оценке уровня защищенности информационных систем. Процедура защиты информационной системы (далее – ИС) направлена прежде всего на предотвращение возникновения ситуаций, нарушающих штатный режим работы, в частности, компьютерных атак злоумышленников, ошибок в действиях персонала, сбоев в работе оборудования и других аналогичных событий. Компьютерные атаки на информационные системы различных

организаций давно уже стали одной из главных проблем в их работе и причиняют значительный ущерб в различных вариантах, начиная с хищений денежных средств и заканчивая потерей репутации и различной клиентуры. В связи с возрастанием интенсивности компьютерных атак и расширением их спектра возникает вопрос оценки уровня защищенности конкретной информационной системы. Различным подходам к решению данной задачи посвящено много работ в научной литературе [1–3].

В большинстве публикуемых работ аналитическое прогнозирование рисков предлагается осуществлять на основе вероятностного моделирования исследуемых систем [4–6]. Модели процесса проведения компьютерных атак, модели их количественного оценивания и вопросы оценки защищенности информационных систем исследовались в работах [7–9].

В основных нормативных документах по защите информации подход к данной проблеме основан на оценке рисков, возникающих при появлении различных инцидентов в информационной системе, которые приводят к нарушению штатного режима ее работы. При этом функция риска вычисляется с учетом вероятности появления данных инцидентов и ущерба, возникающего от их реализации. Принятие решения о защищенности системы будет в случае, когда значение риска не превышает максимального уровня ущерба.

Однако, как было отмечено ранее в работах [10–15], такой подход позволяет сделать вывод о достаточности мер защиты системы только на момент исследования, и не дает возможности оценить временной промежуток, в течение которого будет обеспечиваться защищенность информационной системы.

Ранее авторами предлагался подход к оценке уровня защищенности информационной системы, основанный на построении временных моделей компьютерных атак и моделей возможных потерь от их реализации.

Смысл такого подхода состоит во введении зависимости от времени t величин, входящих в формулу риска: $p(y_i)$ – вероятности наступления инцидента (реализации угрозы) y_i и u_i – величины ущерба:

$$p(y_i) = p_{y_i}(t),\ u_i = u_i(t).$$

В этом случае функция рисков R также становится функцией от времени t:

$$R = R(t) = \sum_{i=1}^{n} p_{y_i}(t) \cdot u_i(t).$$

Поскольку функции $p_{y_i}(t)$ и $u_i(t)$, как правило, являются неубывающими функциями времени t, нетрудно видеть, что функция рисков $R(t)$ также будет неубывающей функцией времени t.

В этом случае для оценки времени безопасной работы информационной системы можно составить уравнение относительно неизвестного переменного t:

$$R(t) = \sum_{i=1}^{n} p_{y_i}(t) \cdot u_i(t) = R_0.$$

Обозначим через T_0 корень данного уравнения, при котором

$$R(t) - R_0 = 0. \quad (1)$$

Заметим, что в данной модели величина T_0 является временным промежутком, в течение которого ущерб ИС при реализации возникающих угроз достигнет предельно допустимого значения и эксплуатация ИС, согласно введенной модели, перестанет быть безопасной.

В таком случае целесообразно рассматривать величину T_0 как объективную характеристику защищенности ИС. В рамках такого подхода основной задачей становится разработка способов построения непрерывных функций $p_{y_i}(t)$ и $u_i(t)$.

При наличии объективных данных об имевших место инцидентах, которыми обычно располагают службы защиты информации в организациях, одним из возможных подходов к построению непрерывных функций $p_{y_i}(t)$ и $u_i(t)$ может быть разработанный ранее и подробно изложенный в работах [11–13], основанный на построении функций метод прогнозирования состояний динамических систем, наиболее близко расположенных от имеющихся значений параметров состояний указанных систем.

Далее представлены результаты экспериментов по построению функций прогнозирования потерь от хищений со счетов юридических лиц с использованием платежных карт и вычислению на их основе величины T_0 – времени безопасной работы (эксплуатации) ИС.

Также рассмотрен предлагаемый метод, основанный на оценке рисков информационной безопасности, предполагающий суммирование ущерба от происходящих инцидентов и позволяющий оценить время T_0, в течение которого обеспечивается защита ИС.

Модели компьютерных инцидентов и оценки рисков нарушения информационной безопасности

Для описания теоретико-вероятностной модели событий будем полагать, что в случайные моменты времени в системе происходят инциденты I_k, $k = 1, 2, ...$, сопровождаемые ущербом (потерями) и приводящие к нарушению ее штатного режима работы: сбои, компьютерные атаки и тому подобное.

Положим, $u = \{u_1, ..., u_m\}$, $u_i > 0$, $i = 1, 2, ... m$ – возможные варианты значений потерь при выявлении инцидентов. На инциденты реагируют средства защиты информационной системы, и дальнейшее развитие событий может осуществляться по следующим сценариям.

Первый вариант развития сценария состоит в следующем.

При возникновении очередного инцидента I_k величина потерь u_k последовательно сравнивается с максимально допустимой величиной ущерба R_0 . Если

$$u_k < R_0,$$

информационная система продолжает работу в штатном режиме. Иначе необходимо предпринять дополнительные меры защиты и произвести корректировку политики безопасности.

Рассмотрим второй из возможных вариантов сценария.

При выявлении инцидентов $I_{t_1}, I_{t_2}, ..., I_{t_n}, ...$ в моменты времени $t_1, t_2, ..., t_N, ...$ производится последовательное суммирование значений соответствующих ущербов $u_{t_1}, u_{t_2}, ..., u_{t_N}, ...$, вычисление статистики

$$S_N = \sum_{j=1}^{N} u_{t_j}$$

и сравнение ее значения с максимально допустимым значением ущерба R_0.

Если при выявлении инцидента I_{t_n} будет выполнено условие $S < R_0$, в соответствии со сценарием считается, что информационная система работает в штатном режиме. Иначе принимается решение о введении дополнительных мер информационной защиты и пересмотре политики безопасности.

В соответствии с первым сценарием рассмотрим математическую модель реагирования системы на появление инцидентов.

Пусть $\{\xi_t\}$, $t = 1, 2, ..., N$ – последовательность независимых, одинаково распределенных индикаторов,

$$p\{\xi_t = 1\} = p,\ p\{\xi_t = 0\} = 1 - p,$$

соответствующих моментам выявления инцидентов.

Без ограничения общности полагаем, что инциденты появляются независимо друг от друга, а вероятность появления каждого равна p.

Далее, как и ранее, положим, $u = \{u_1,...,u_m\}$ – множество возможных значений величин потерь при наступлении инцидентов и полагаем, что при наступлении инцидента u_k с номером k, вероятность возникновения соответствующего ущерба равна p_k, $\sum_{k=1}^{m} p_k = 1$.

Пусть также для значений $k_1, k_2, ..., k_s, k_j \in \{1, ..., m\}$ имеет место неравенство

$$u_{k_j} \geq R_0, j \in \{1, ..., s\},$$

а для значений $k_j \in \{1, ..., m\} \backslash \{k_1, k_2, ..., k_s\}$ имеет место неравенство

$$u_k < R_0.$$

Положим, далее $q = \sum_{j=1}^{s} p_{k_j}$.

С последовательностью $\{\xi_t\}$ свяжем последовательность индикаторов $\{\zeta_t\}$:

$$\zeta_t = \begin{cases} 1, \textit{если } \xi_t = 1 \textit{ и наступил инцидент } I_k, \textit{ где } k \in \{k_1, k_2, ..., k_s\} \\ 0, \textit{в противном случае} \end{cases}$$

и случайную величину τ:

$$\tau = \min\{t \mid \zeta_t = 1\},$$

момент наступления критического события, при котором информационная система нуждается в дополнительных средствах защиты.

В рамках рассматриваемой модели вероятностное распределение случайной величины τ имеет вид:

$$p\{\tau = k\} = p \cdot q \cdot (1 - p \cdot q)^{k-1}, \quad k = 1, 2, ...,$$

что является геометрическим распределением.

Таким образом, оценкой среднего времени безопасной работы ИС может служить математическое ожидание случайной величины τ равное.

Перейдем ко второму варианту сценария, в котором учитывается общая сумма потерь от инцидентов.

С последовательностью индикаторов выявления инцидентов $\{\xi_t\}$ свяжем последовательность $\{\eta_t\}$:

$$\eta_t = \begin{cases} 1, \textit{если } S_{t-1} < R_0, S_t \geq R_0 \\ 0, \textit{в противном случае} \end{cases}, t = 1, 2, ...,$$

последовательность моментов времени, при которых общая сумма потерь от инцидентов превышает установленную границу R_0. Очевидно, что $\{\eta_t\}$ – это последовательность моментов времени, при которых имеют место критические события. В этих случаях система не обеспечивает требуемый уровень защиты и, следовательно, нуждается в ее усилении.

Определим случайную величину χ:

$$\chi = \min\{t \mid \eta_t = 1\},$$

момент первого наступления критического события.

В рамках введенной теоретико-вероятностной модели для решения поставленной выше задачи найдем распределение случайной величины χ: $p\{\chi = N\}$, где N – натуральное число.

Обозначим $\overline{\alpha}_N = (\alpha_1, ..., \alpha_m)$ – первичную спецификацию исходов последовательности $\{\xi t\}_t^N$, где α_s – число инцидентов, при которых потери составили величину u_s, $s = 1, 2,..., m$, $\alpha_1 + ... + \alpha_m = N$ и положим:

$$\mathrm{M}_{N-1}\left(u_k\right) = \left\{\overline{\alpha}_{N-1} \mid \alpha_1 + ... + \alpha_m = N-1, R_0 - u_k \le \sum_{s=1}^{m} \alpha_s \cdot u_s < R_0\right\}.$$

Тогда для вероятности первого наступления критического события получаем выражение:

$$p\left\{\chi = N\right\} = \sum_{k=1}^{m} p_k \cdot \sum_{\overline{\alpha}_{N-1} \in M_{N-1}(u_k)} \left(1-p\right)^{\alpha_0} \cdot p^{N-\alpha_0} \cdot \prod_{k=1}^{m} p_k^{\alpha_k}\left(\alpha_{N-1}\right),$$

а также

$$p\left\{\chi = N\right\} = \sum_{k=1}^{m} p_k \sum_{\overline{\alpha}_{N-1} \in M_{N-1}(u_k)} C_{N-1}^{m} \cdot \prod_{s=1}^{m} p_s^{\alpha_s}$$

На основании последнего соотношения могут быть построены оценки времени безопасной эксплуатации информационной системы.

Далее в статье представлены результаты экспериментов по построению прогнозных моделей в задачах определения возможной величины потерь юридических лиц от реализации компьютерных инцидентов. Дано описание экспериментов по вычислению времени безопасной эксплуатации информационной системы.

Прогнозная модель потери от хищений со счетов юридических лиц с использованием платежных карт

В настоящее время финансово-кредитным организациям приходится принимать различные меры для противодействия попыткам хищений денежных средств со счетов как юридических, так и физических лиц. С этой целью каждая транзакция проверяется на легитимность путем применения ряда процедур. В случае выявления признаков мошенничества проведение транзакции останавливается для проведения дополнительных процедур подтверждения. Однако в ряде случаев мошенникам все же удается совершить несанкционированные операции, далее называемые неостановленными.

В данном эксперименте прогнозная модель строилась для изучения динамики потери от совершенных мошенниками несанкционированных операций (хищений) со счетов юридических лиц с использованием платежных карт. В табл. 1 приведена статистика объема несанкционированных операций со счетами юридических лиц за период с 1 квартала 2018 года по 4 квартал 2019 года, представленная на официальном сайте Банка России [16]. Данные за указанный период взяты в связи с тем, что в последующие периоды сведения о возникающих потерях организаций полностью перестали публиковаться.

В эксперименте для построения прогнозной аппроксимирующей функции $F(x)$ использовались данные за период с 1 квартала 2018 года по 4 квартал 2018 года, за нулевое значение по оси OX принята дата 4 квартал 2017 года.

Для данного эксперимента аппроксимирующая функция $F(x)$ имела вид:

$$F_1(x) = 510.34 + 26.72\sqrt{x} + 167.25 \cdot \sin\left[2 \cdot x\right] - 6.05 \cdot \cos\left[2 \cdot x\right] + 75.92 \cdot \cos\left[4 \cdot x\right] +$$

$$+ 100.62 \cdot \cos\left[3 \cdot x\right] - 125.08 \cdot \sin\left[x\right] - 58.22 \cdot \cos\left[x\right].$$

График, прогнозной функции $F_1(x)$ представлен на рис. 1.

Таблица 1

Объем несанкционированных операций (хищений) со счетами организаций

Table 1

Volume of unauthorized transactions (embezzlement) with accounts of organizations

Период	Объем несанкционированных операций (хищений, млн руб.)
1 квартал 2018 г.	352,6
2 квартал 2018 г.	342,5
3 квартал 2018 г.	428,7
4 квартал 2018 г.	770,6
1 квартал 2019 г.	405,6
2 квартал 2019 г.	440,3
3 квартал 2019 г.	343,7
4 квартал 2019 г.	380,0

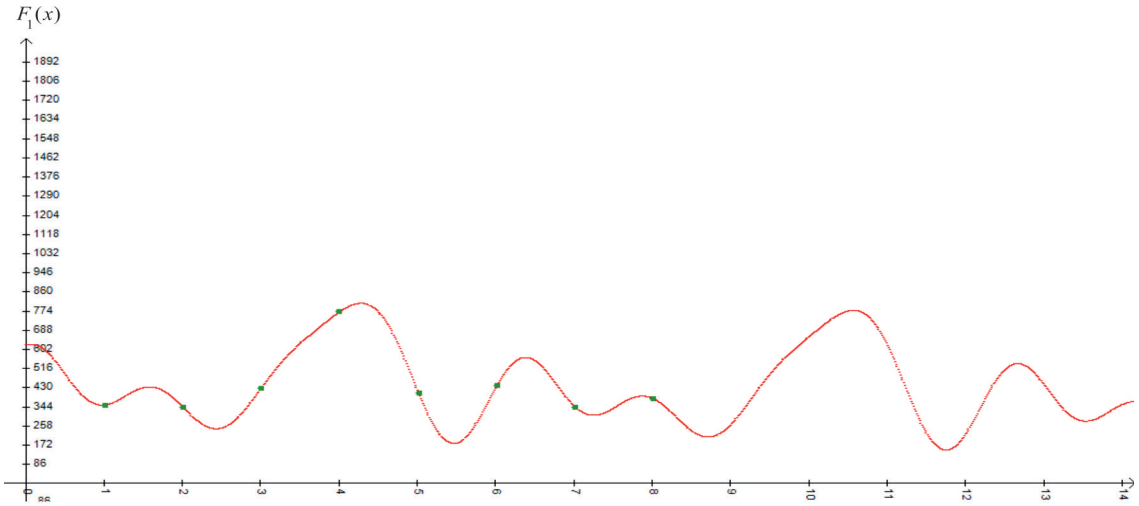

Рис. 1. График функции $y = F_1(x)$

Fig. 1. Graph of the function $y = F_1(x)$

В табл. 2 приведены результаты эксперимента по построению прогнозных значений ущерба от несанкционированных операций (хищений) со счетов юридических лиц с использованием платежных карт на период с 1 квартала 2020 года по 2 квартал 2021 года.

В данном примере, в соответствии с примененным выше методом построения прогнозной модели динамики инцидентов, связанных с объемом несанкционированных операций со счетами юридических лиц с использованием платежных карт, функция их числа $f_1(x)$ в зависимости от времени t имеет вид:

$$f_1(t) = \alpha_1 + \alpha_2\sqrt{t} + \alpha_3 \sin[2{\cdot}t] - \alpha_4 \cos[2{\cdot}t] + \alpha_5 \cos[4{\cdot}t] + \alpha_6 \cos[3{\cdot}t] - \alpha_7 \sin[{\cdot}t] - \alpha_8 \cos[t],$$

где α_i, $i = 1, 2, ..., 8$ – соответствующие константы.

Таблица 2

Прогноз объема несанкционированных операций (хищений)
со счетами организаций

Table 2

Forecast of the volume of unauthorized transactions (embezzlement)
with accounts of organizations

Период	Объем несанкционированных операций (млн руб.)
1 квартал 2020 г.	383
2 квартал 2020 г.	262
3 квартал 2020 г.	657
4 квартал 2020 г.	625
1 квартал 2021 г.	220
2 квартал 2021 г.	446

При $t \geq 0$ для функции $f_1(x)$ имеет место неравенство:

$$f_1(t) \leq \alpha_9 + \alpha_2\sqrt{t},$$

где $\alpha_9 = \alpha_1 + \alpha_3 + ... + \alpha_8$.

Обозначим через N число юридических лиц (организаций, информационных систем), понесших ущерб от действий злоумышленников.

Тогда на основании уравнение (1) прогнозная модель среднего ущерба юридического лица имеет вид:

$$\frac{1}{N} f(t) \leq \frac{1}{N}\left(\alpha_9 + \alpha_2\sqrt{t}\right),$$

при этом оценка для времени T_0 безопасной эксплуатации ИС может быть найдена из уравнения

$$\frac{1}{N}\left(\alpha_9 + \alpha_2\sqrt{t}\right) = R_0,$$

откуда получаем:

$$T_0 \geq \left(\frac{N \cdot R_0 - \alpha_9}{\alpha_2}\right)^2,$$

где R_0 – максимально допустимый ущерб для организации.

В табл. 3 представлен расчет параметра T_0 – времени (в годах) безопасной эксплуатации ИС, вычисления проведены для значений параметра N=10.

Таблица 3

Время (в годах) безопасной эксплуатации информационной системы

Table 3

Time (in years) of safe operation of the information system

R_0 (тыс. руб). / N	1100	1150	1200	1250	1300
10	1,1	4	8,6	15	23

Прогнозная модель неостановленных нелегитимных операций (хищений) со счетов юридических лиц

В рассматриваемом эксперименте прогнозная модель строилась для изучения динамики инцидентов, связанных с количеством неостановленных несанкционированных операций с использованием платежных карт. В табл. 4 приведена статистика в процентном соотношении количества неостановленных нелегитимных операций за период с 1 квартала 2018 года по 4 квартал 2019 года, представленная в [16].

Таблица 4

Процент неостановленных нелегитимных операций

Table 4

Percentage of unstoppable illegitimate operations

Период	Процент неостановленных несанкционированных операций (хищений)
1 квартал 2018 г.	0,27
2 квартал 2018 г.	0,55
3 квартал 2018 г.	0,28
4 квартал 2018 г.	0,61
1 квартал 2019 г.	0,51
2 квартал 2019 г.	0,54
3 квартал 2019 г.	0,51
4 квартал 2019 г.	0,39

В данном эксперименте для построения прогнозной функции $F(x)$ использовались данные за период с 1 квартала 2018 года по 4 квартал 2019 года, за нулевое значение по оси OX принята дата 4 квартал 2016 года.

Для данного эксперимента аппроксимирующая функция $F(x)$ имела вид:

$$F_2(x)=\frac{1.62}{\sqrt{x}}-0.053\cdot\sin x+0.075\cdot\cos x\frac{1.2}{x}+0.075\cdot\cos 3x+5\cdot10^{-4}\cdot x^2-0.039\cdot\sin 4x-0.07\cdot\cos 4x.$$

График прогнозной функции $F_2(x)$ представлен на рис. 2.

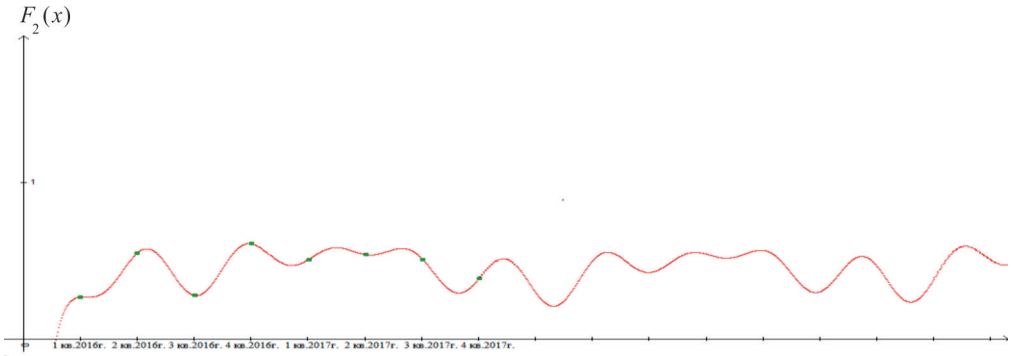

Рис. 2. График функции $y = F_2(x)$

Fig. 2. Graph of the function $y = F_2(x)$

В табл. 5 приведены результаты эксперимента по построению прогнозных значений количества неостановленных несанкционированных операций с использованием платежных карт на период с 1 квартала 2020 года по 2 квартал 2021 года.

Таблица 5

Прогноз количества неостановленных нелегитимных операций

Table 5

Forecast of the number of unidentified illegitimate operations

Период	Процент неостановленных нелегитимных операций
1 квартал 2020 г.	0,3
2 квартал 2020 г.	0,5
3 квартал 2020 г.	0,43
4 квартал 2020 г.	0,54
1 квартал 2021 г.	0,57
2 квартал 2021 г.	0,3
3 квартал 2021 г.	0,47
4 квартал 2021 г.	0,39

В соответствии с примененным выше методом построения прогнозной модели динамики инцидентов, связанных с относительным количеством неостановленных несанкционированных операций с использованием платежных карт, функция их числа имеет вид:

$$f_2(t) = \frac{\alpha_1}{\sqrt{t}} - \alpha_2 \cdot \sin t + \alpha_3 \cdot \cos t - \frac{\alpha_4}{t} + \alpha_5 \cdot \cos 3t + \alpha_6 \cdot t^2 - \alpha_7 \cdot \sin 4t - \alpha_8 \cdot \cos t,$$

где α_i, $i = 1, 2, ..., 8$ – соответствующие константы.

При $t \geq 1$ для функции $f_2(t)$ имеет место неравенство:

$$f_2(t) \leq \alpha_9 + \alpha_6 \cdot t^2,$$

где $\alpha_9 = \alpha_1 + \alpha_2 + \alpha_{3\,+}\alpha_4 + \alpha_5 + \alpha_7 + \alpha_8$.

Обозначим через N количество несанкционированных операций с использованием платежных карт, а через U – средний ущерб, наносимый одной транзакции.

Тогда прогнозная модель среднего ущерба, наносимого информационной системе организации за исследуемый промежуток времени имеет вид:

$$U \cdot N \cdot f(t) \leq U \cdot N \cdot (\alpha_9 + \alpha_6 \cdot t^2).$$

При этом оценка для времени T_0 безопасной эксплуатации ИС может быть найдена как корень уравнения относительно неизвестного аргумента t:

$$U \cdot N \cdot (\alpha_9 + \alpha_6 \cdot t^2) = R_0,$$

откуда получаем:

$$T_0 \geq \sqrt{\left(\frac{R_0/(U \cdot N) - \alpha_9}{\alpha_6}\right)},$$

где R_0 – максимально допустимый ущерб, наносимый организации.

В табл. 6 представлены примеры расчетов времени (в годах) безопасной эксплуатации информационной системы (параметр T_0). Расчеты проведены для значений $N=1000$ нелегитимных операций с целью использования платежных карт.

Таблица 6

Время (в годах) безопасной эксплуатации информационной системы

Table 6

Time (in years) of safe operation of the information system

R_0(млн руб) / U (тыс. руб).	20	30	40	50	60	70	80	90	100
1	0,5	0,62	0,73	0,82	0,91	1	1,06	1,33	1,2

Заключение

В статье исследованы подходы к оценке защищенности информационных систем. Рассмотрены проблемы построения и исследования модели управления рисками информационной безопасности, в которой учитывается накопление ущерба от реализации инцидентов, приводящих к нарушению информационной безопасности.

Построены алгоритмическая и теоретико-вероятностная модели инцидентов, приводящих к нарушению информационной безопасности и предусматривающих различные сценарии работы информационной системы в зависимости от имеющего место ущерба. На основании изложенных результатов построены прогнозные оценки параметра T_0 – времени безопасной работы информационной системы. В качестве примера построены экспериментальные прогнозные модели количества нелегитимных операций со счетами юридических лиц, в том числе с использованием платежных карт. Данные модели основаны на данных о реальных инцидентах и строятся с применением разработанных ранее методов прогнозирования состояния динамических систем путем нахождения непрерывных аппроксимирующих функций. Полученные результаты могут быть применены для дальнейшего развития методологии оценки защищенности информационных систем, в частности, для оценки времени их безопасной работы.

Список литературы

1. Экспертиза и аудит информационной безопасности. [Электронный ресурс]. Режим доступа: https://sudexpa.ru/expertises/ekspertiza-i-audit-informatcionnoi-bezopasnosti/ (дата обращения 17.02.2020)
2. Аудит информационных систем. Регола-мониторинг. [Электронный ресурс]. Режим доступа: https://spb.systematic.ru/about/news/regola-monitoring.htm (дата обращения 20.02.20)
3. Обзор рынка SIEM-систем. [Электронный ресурс]. Режим доступа: https://www.antimalware.ru/node/11 637 (дата обращения 15.03.2020).
4. **Artemyev V., Kostogryzov A., Rudenko J., Kurpatov O., Nistratov G., Nistratov A.** Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS- 2017), December 20–22, 2017, Milan, Italy, pp. 368–373
5. **Kostogryzov A, Nistratov A.** Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In “Safety and Reliability of Systems and Processes”, Gdynia Maritime University, 2020. pp. 153–174. DOI: 10.26408/srsp-2020

6. **Kostogryzov A., Nistratov A., Nistratov G.** (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp. 352–364.
7. **Егошин Н. С.** Модель типовых угроз безопасности информации, основанная на модели информационных потоков // Доклады Томского государственного университета систем управления и радиоэлектроники. 2021. Т. 24. № 3. С. 21–25.
8. **Кондаков С. Е., Рудь И. С.** Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий // Вопросы кибербезопасности. 2021. № 5(45). С. 12–20.
9. **Калашников А. О., Бугайский К. А., Аникина Е. В.** Модели компьютерных атак //Информация и безопасность. 2019. Т. 22. № 4. С. 517–538.
10. **Ермакова А. Ю.** Разработка методов прогнозирования на примере анализа средств вычислительной техники//Промышленные АСУ и контроллеры. 2017. № 1. С. 28−34.
11. **Ермакова А. Ю., Лось А. Б.** Исследование прогнозных моделей динамической системы на примере прогноза инцидентов информационной безопасности // Компьютерные науки и информационные технологии: сборник статей Международной научной конференции. Саратов: Издательский центр «Наука», 2018 С. 144–149.
12. **Ермакова А. Ю.** Об оценке точности прогнозирования состояний динамической системы методом построения аппроксимирующих функций //Промышленные АСУ и контроллеры. 2018. № 5. С. 36−42.
13. **Ермакова А. Ю.** Об одном подходе к оценке защищенности информационной системы на основе анализа инцидентов // Системы высокой доступности. 2018. № 4. С. 32−35.
14. **Ермакова А. Ю.** Модели DDoS-атак и исследование защищенности информационной системы от данного типа угроз // Промышленные АСУ и контроллеры. 2019. № 12. С. 54−59. DOI: 10.25791/asu.12.2019.1074
15. **Ермакова А. Ю.** Модель компьютерной атаки в условиях ограниченных возможностей защиты и построение прогнозных моделей компьютерных инцидентов // Промышленные АСУ и контроллеры. 2020. № 6. С. 50−57. DOI: 10.25791/asu.6.2020.1194
16. **Калашников А. И.** Обзор несанкционированных переводов денежных средств за 2019 год. Электронный ресурс (режим доступа – свободный): https://ural.ibbank.ru/files/files/aterials 2018/45%20Kalashnikov.pdf/ (дата обращения 11.04.2020).

References

1. Examination and audit of information security. [Electronic resource]. Access mode: https:// sudexpa.ru/expertises/ ekspertiza-i-audit-informatcionnoi-bezopasnosti/ (date of application 17.02.2020).
2. Audit of information systems. Regola-monitoring. [Electronic resource]. Access mode: https:// spb.systematic.ru/about/news/regola-monitoring.htm/ (date of application 20.02.2020).
3. Market overview of SIEM systems. [Eelectronic resource]. Access mode: https://www.antimal ware.ru/node/11 637 (date of application 15.03.2020).
4. **Artemyev V., Kostogryzov A., Rudenko J., Kurpatov O., Nistratov G., Nistratov A.** Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS- 2017), December 20-22, 2017, Milan, Italy, pp. 368-373
5. **Kostogryzov A, Nistratov A.** Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In “Safety and Reliability of Systems and Processes”, Gdynia Maritime University, 2020. pp. 153-174. DOI: 10.26408/srsp-2020

6. **Kostogryzov A., Nistratov A., Nistratov G.** (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352-364.
7. **Egoshin N. S.** Model' tipovy'x ugroz bezopasnosti informacii, osnovannaya na modeli informacionny'x potokov / N. S. Egoshin //Doklady' Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioe'lektroniki. – 2021. – T. 24. – № 3. – S. 21-25.
8. **Kondakov S. E.** Model' processa provedeniya komp'yuterny'x atak s ispol'zovaniem special'ny'x informacionny'x vozdejstvij / S. E.Kondakov, I. S. Rud' // Voprosy' kiberbezopasnosti. – 2021. № 5(45). S. 12-20.
9. **Kalashnikov A. O.** Modeli kolichestvennogo ocenivaniya komp'yuterny'x atak / A.O. Kalashnikov, K.A. Bugajskij, E.V. Anikina //Informaciya i bezopasnost'. – 2019. – T. 22. – № 4. – S. 517-538.
10. **Ermakova A. Y.** Razrabotka metodov prognozirovaniya na primere analiza sredstv vichisliterlnoy techniki//Promishlennie ASU i kontrolleri. –2017. – № 1. – С. 28−34.
11. **Ermakova A.Y., Los A.B.,** Issledovanie prognoznich modeley dinamicheskoj sistemi na primere prognoza insidentov informatinnoj bezopasnosti//Kompjuternie nauki i informationnie technologii: sbornik statei Mezdunarodnoj nauchnoj konferentcii. Saratov: Izdatelskij Center «Nauka», 2018 – С. 144-149.
12. **Ermakova A. Y.** Ob otcenke tochnosti prognozirovanija sostojanij dinamicheskoj sistemi metodom postroenija approksimirujushej funktcii// Promishlennie ASU i kontrolleri. –2018. – № 5. – С.36−42.
13. **Ermakova A.Y.** Ob odnom podchode k otcenke zashishennosti informatcionnoj sistemi na osnove analiza intcidentov//Systemi visokoj dostupnosti. –2018. – № 4. – С. 32−35.
14. **Ermakova A. Y.** Modeli DDoS atak i issledovanie zashishennosti informatcionnoj sistemi ot dannogo tipa ugroz // Promishlennie ASU i kontrolleri.– 2019. – №12. – С. 54−59. DOI: 10.25791/asu.12.2019.1074
15. **Ermakova A. Y.** Model kompjuternoj ataki v uslovijach ogranichennoj vozmojnosti zashiti i postroenie prognoznich modelej compjuternich incidentov // Promishlennie ASU i kontrolleri.–2020. – № 6. – С. 50−57. DOI: 10.25791/asu.6.2020.1194
16. **Kalashnikov A. I.** Review of unauthorized money transfers for 2017. Electronic resource (free access mode) :https://ural.ib-bank.ru/files/files/aterials2018/45%20Kalashnikov.pdf/ (date of application 11.04.2019)

Информация об авторах

А.Ю. Ермакова, доцент кафедры информационного противоборства МИРЭА – Российского технологического университета

А.Б. Лось, доцент кафедры компьютерной безопасности Национального исследовательского университета «Высшая школа экономики»

Information about the Authors

A.Yu. Ermakova, associate professor Department Russian Technological University, Moscow

A.B. Los, associate professor Department National Research University Higher School of Economics

Статья поступила в редакцию 27.02.2023;
одобрена после рецензирования 24.03.2023; принята к публикации 24.03.2023
The article was submitted 27.02.2023;
approved after reviewing 24.03.2023; accepted for publication 24.03.2023