ПОСТРОЕНИЕ МОДЕЛИ УЩЕРБА АКТИВАМ ОРГАНИЗАЦИИ ПРИ ВОЗНИКНОВЕНИИ ИНЦЕНДЕНТОВ, ПРИВОДЯЩИХ К НАРУШЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. Ю. Ермакова[1], А. Б. Лось[2]

[1]Российский технологический университет МИРЭА, Москва, Россия
[2]Национальный исследовательский университет «Высшая школа экономики», Москва, Россия
E-mail: a.alla1105@yandex.ru, alexloss2011@mail.ru

В статье рассматриваются вопросы оценки возможного ущерба информационным активам организации при возникновении различных инцидентов, приводящих к нарушению информационной безопасности, в частности, при успешных реализациях компьютерных атак. Развивается подход к оценке рисков информационной безопасности, основанный на исследовании динамики изменения функции ущерба во времени. В целях исследования информационных рисков и разработки методов оценки защищенности компьютерных систем построены прогнозные временные модели финансовых потерь от несанкционированных транзакций, реализуемых злоумышленниками, а также временные функции потерь атакованных злоумышленникам компьютеров с целью перехвата управления для последующего майнинга криптовалют.

BUILDING A MODEL OF DAMAGE TO AN ORGANIZATION'S ASSETS IN THE EVENT OF INCIDENTS THAT LEAD TO VIOLATION OF INFORMATION SECURITY

A. Y. Ermakova, A. B. Los

The article deals with the assessment of possible damage to the organization's information assets in the event of various incidents that lead to a violation of information security, in particular, during successful implementations of computer attacks. An approach to assessing information security risks based on the study of the dynamics of changes in the damage function over time is being developed. In order to study information risks and develop methods for assessing the security of computer systems, predictive time models of financial losses from unauthorized transactions implemented by hackers, as well as time functions of losses of computers attacked by hackers in order to intercept control for subsequent crypto currency mining, are constructed.

Введение.

В работе рассматриваются вопросы оценки стоимости информационных активов организации и методов оценки возможного ущерба при возникновении различного рода инцидентов, приводящих к нарушениям информационной безопасности. Общие вопросы оценки стоимости активов, методов оценки ущерба и информационных рисков изложены в руководящих документах ФСТЭК [1-3]. В работах [4-6] предложен подход к оценке возможного ущерба с позиции теории надежности в случае реализации DDoS-атак и потерь при отказах в обслуживании.

Исследование возможных потерь от инцидентов информационной безопасности необходимо, в частности, для разработки методики оценки рисков при

нарушении информационной безопасности и методов оценки защищенности информационных систем (ИС).

В традиционном подходе к проблеме оценки уровня защищенности ИС предполагается вычисление риска R нарушения информационной безопасности (ИБ), величина которого находится из соотношения:

$$R = \sum_{i=1}^{n} p(y_i) \cdot u_i, \tag{1}$$

где $p(y_i)$ – вероятность реализации злоумышленником угрозы y_i нарушения ИБ, u_i – величина ущерба от успешного осуществления данной угрозы.

Далее определяется граница допустимых потерь R_0 и, в случае выполнения условия

$$R \le R_0 \tag{2}$$

информационная система считается защищенной.

В работе [7] предложен, так называемый, временной подход к оценке защищенности ИС, суть которого состоит в определении вида зависимости величин $p(y_i)$ и u_i от времени t:

$$p(y_i) = p_{y_i}(t), u_i = u_i(t). \tag{3}$$

В этом случае риск R также становится функцией времени t:

$$R(t) = \sum_{i=1}^{n} p_{y_i}(t) \cdot u_i(t). \tag{4}$$

Поскольку, как правило, величины $p_{y_i}(t)$ и $u_i(t)$ являются неубывающими функциями времени t, то уравнение

$$R(t) = \sum_{i=1}^{n} p_{y_i}(t) \cdot u_i(t) = R_0 \tag{5}$$

имеет положительный корень T_0, который можно рассматривать как время безопасной работы ИС, поскольку, через данное время прогнозный риск достигнет максимально допустимого значения и работа системы теоретически перестанет быть безопасной.

Подходы к построению функций $p_{y_i}(t)$, учитывающих вероятность возникновения ущерба, предпринимались ранее в работах [8-14]. В настоящей работе рассматриваются подходы к построению непосредственно самих функций ущерба $u_i(t)$ и вычислению на этой основе величины T_0.

В целях развития подходов к оценке ущерба и возможных рисков при возникновении инцидентов, приводящих к нарушению информационной безопасности, в работе построены прогнозные модели финансовых потерь при несанкционированном доступе к соответствующим ресурсам и даны рекомендации по вычислению времени безопасной работы информационной системы.

Построение прогнозных моделей возможного ущерба при инцидентах, приводящих к нарушению информационной безопасности.

Ранее в работах [8-13] рассматривался подход к построению прогнозных моделей интенсивности компьютерных атак и инцидентов, приводящих к нарушению информационной безопасности. Суть данного подхода состоит в по-

строении по известным значениям исследуемых параметров за определенный предшествующий период (узловым точкам) непрерывной «аппроксимирующей» функции $F(x)$, наиболее близко отстоящей от узловых точек. Поиск указанной функции осуществляется в виде линейной комбинации элементарных (базовых) функций с применением метода наименьших квадратов, для ее построения разработано специальное программное обеспечение.

Прогнозная модель динамики ущерба от хищений со счетов юридических лиц с использованием платежных карт.

В данном эксперименте прогнозная модель строилась для изучения динамики ущерба от проведенных мошенниками несанкционированных операций (хищений) со счетов юридических лиц с использованием платежных карт. В табл. 1 приведена статистика объема несанкционированных операций со счетов юридических лиц за период с 1 квартала 2016 года по 4 квартал 2017 года. Данные взяты из официального сайта Банка России [15].

Таблица 1

Объем несанкционированных операций (хищений)

Период	Объем несанкционированных операций (хищений, млн. руб.)	Период	Объем несанкционированных операций (хищений, млн. руб.)
1 кв. 2016 г.	352,6	1 кв. 2017 г.	405,6
2 кв. 2016 г.	342,5	2 кв. 2017 г.	440,3
3 кв. 2016 г.	428,7	3 кв. 2017 г.	343,7
4 кв. 2016 г.	770,6	4 кв. 2017 г.	380,0

В рассматриваемом эксперименте для построения прогнозной функции $F(x)=F_1(x)$ использовались данные за период с 1 квартала 2016 года по 4 квартал 2017 года, за нулевое значение по оси OX принята дата: 4 квартал 2015 года.

Для данного эксперимента аппроксимирующая функция $F_1(x)$ имела вид:

$$F_1(x)=510,34+26,72\sqrt{x}+167,25\cdot\sin[2\cdot x]-6,05\cdot\cos[2\cdot x]+75,92\cdot\cos[4\cdot x]+$$
$$+100,62\cdot\cos[3\cdot x]-125,08\cdot\sin[x]-58,22\cdot\cos[x]$$

.

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

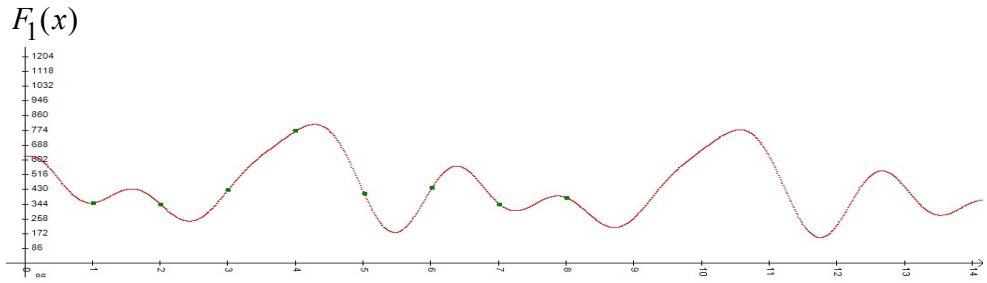

Рис.1. График функции $y=F_1(x)$.

В табл. 2 приведены результаты эксперимента по построению прогнозных значений ущерба от несанкционированных операций (хищений) со счетов юридических с использованием платежных карт на период с 1 квартала 2018 года по 2 квартал 2019 года.

Таблица 2

Прогноз объема несанкционированных операций

Период	Объем несанкционированных операций (млн. руб.)	Период	Объем несанкционированных операций (млн. руб.)
1 кв. 2018 г.	383	1 кв. 2018 г.	383
2 кв. 2018 г.	262	2 кв. 2018 г.	262
3 кв. 2018 г.	657	3 кв. 2018 г.	657
4 кв. 2018 г.	625	4 кв. 2018 г.	625
1 кв. 2019 г.	220	1 кв. 2019 г.	220
2 кв. 2019 г.	446	2 кв. 2019 г.	446

Прогнозная модель количества несанкционированных операций (хищений) со счетов юридических лиц с использованием платежных карт.

В данном эксперименте прогнозная модель строилась для изучения динамики инцидентов, связанных с общим количеством несанкционированных операций (хищений) со счетами юридических лиц. В табл. 3 приведена статистика количества несанкционированных операций (хищений) со счетами юридических лиц за период с 1 квартала 2016 года по 4 квартал 2017 года, представленная на официальном сайте Банка России [15].

Таблица 3

Количество несанкционированных операций (хищений)

Период	Количество несанкционированных операций	Период	Количество несанкционированных операций
1 кв. 2016 г.	196	1 кв. 2017 г.	182
2 кв. 2016 г.	161	2 кв. 2017 г.	256
3 кв. 2016 г.	164	3 кв. 2017 г.	217
4 кв. 2016 г.	196	4 кв. 2017 г.	186

В данном эксперименте для построения прогнозной аппроксимирующей функции $F(x)=F_2(x)$ использовались данные за период с 1 квартала 2016 года по 4 квартал 2017 года, за нулевое значение по оси OX принята дата: 4 квартал 2015 года.

Для данного эксперимента аппроксимирующая функция $F_2(x)$ имела вид:

$$F_2(x)=164{,}19+15{,}63\cdot\sqrt{x}-3{,}41\cdot\sin[x]-0{,}31\cdot\sin[2\cdot x]-23{,}48\cdot\sin[4\cdot x]+8{,}3\cdot\sin[3\cdot x]+$$
$$+15{,}13\cdot\cos[3\cdot x]+28{,}21\cdot\cos[x].$$

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

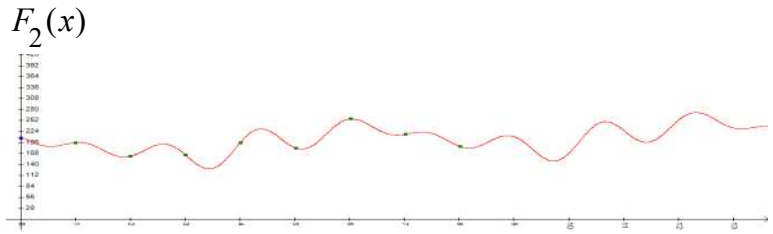

Рис. 2. График функции $y = F_2(x)$.

В табл. 4 приведены результаты эксперимента по построению прогнозных значений количества несанкционированных операций с использованием платежных карт на период с 1 квартала 2018 года по 2 квартал 2019 года.

Таблица 4

Прогноз количества несанкционированных операций

Период	Прогноз количества несанкционированных операций	Период	Прогноз количества несанкционированных операций
1 кв. 2018 г.	211	1 кв. 2019 г.	233
2 кв. 2018 г.	168	2 кв. 2019 г.	221
3 кв. 2018 г.	227	3 кв. 2019 г.	223
4 кв. 2018 г.	252	4 кв. 2019 г.	162

Построение прогнозной модели интенсивности компьютерных атак для майнинга криптовалют.

С появлением цифровых валют, требующих для выработки (майнинга) новых знаков (денежных единиц) значительных вычислительных ресурсов, у мошенников появилась новая цель несанкционированного доступа к компьютерам пользователей – перехват управления и использования вычислительных мощностей атакованных компьютеров для майнинга валют.

В данном эксперименте прогнозная модель строилась с целью изучения динамики интенсивности атак вредоносными программами для майнинга криптовалют. В табл. 5 приведена статистика указанных атак за период с августа 2017 года по апрель 2018 года, представленная в статье «Ландшафт угроз для систем промышленной автоматизации, Первое полугодие 2018, Kaspersky Lab ICS CERT» [16].

Таблица 5

Процент атакованных компьютеров

Период	Процент атакованных компьютеров	Период	Процент атакованных компьютеров
Август 2017	0,9	Декабрь 2017	1,6
Сентябрь 2017	1,3	Январь 2018	1,7
Октябрь 2017	2,1	Февраль 2018	1,1
Ноябрь 2017	1,1	Март 2018	1,6
Декабрь 2017	1,6	Апрель 2018	3,5

В эксперименте для построения прогнозной функции $F(x)=F_3(x)$ использовались данные за период с августа 2017 года по апрель 2018 года, за нулевое значение по оси OX принята дата июль 2017 года.

Для данного эксперимента аппроксимирующая функция $F_3(x)$ имела вид:

$$F_3(x)=-0,02\cdot\sin[x]+1,22\cdot\sqrt{x}-0,74\cdot Ln[x]-0,36\cdot\cos[x]-0,58\cdot\sin[2\cdot x]-$$
$$-0,01\cdot\cos[4\cdot x]-0,45\cdot\sin[4\cdot x]-0,05\cdot\cos[2\cdot x]+0,34\cdot\sin[3\cdot x].$$

График, прогнозной функции $F_3(x)$ представлен на рис. 3.

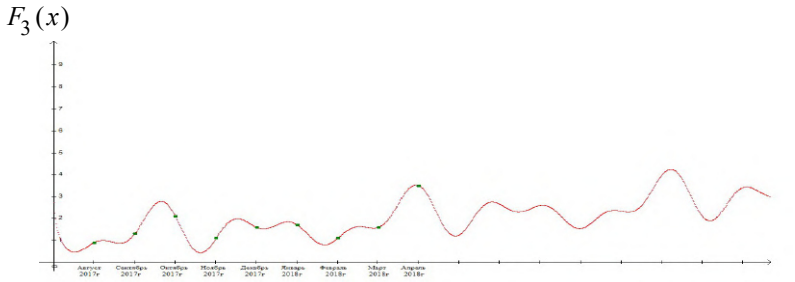

Рис. 3. График функции $y=F_3(x)$

В табл. 6 приведены результаты эксперимента по построению прогнозных значений интенсивности атак вредоносными программами для майнинга криптовалют на период с июня 2018 года по январь 2019 года.

Таблица 6

Прогноз интенсивности атак на период с июня 2018 г. по январь 2019 г.

Период	Процент атакованных компьютеров	Период	Процент атакованных компьютеров
Июнь 2018	2,7	Октябрь 2018	3,9
Июль 2018	2,6	Ноябрь 2018	2,1
Август 2018	1,6	Декабрь 2018	3,4
Сентябрь 2018	2,3	Январь 2019	3,1

Оценки времени безопасной эксплуатации информационной системы

В первом примере, в соответствии с описанным выше методом построения прогнозной модели ущерба от несанкционированных операций со счетов юридических лиц с использованием платежных карт, функция их числа $f(t)$ в зависимости от времени t имеет вид

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

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

При $t\geq 0$ для функции $f(t)$ имеет место очевидное неравенство:

$$f(t)\leq \alpha_9+\alpha_2\sqrt{t}, \qquad (6)$$

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

Обозначим через N - число юридических лиц (ИС), понесших ущерб от

действий злоумышленников.

Тогда прогнозная модель среднего ущерба юридического лица имеет вид:

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

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 оценку для величины T_0:

$$T_0 \ge \left(\frac{N \cdot R_0 - \alpha_9}{\alpha_2}\right)^2, \qquad (7)$$

где R_0 - максимально допустимый ущерб ИС.

Во втором примере, в соответствии с примененным выше методом построения прогнозной модели динамики инцидентов, связанных с количеством несанкционированных операций со счетов юридических лиц с использованием платежных карт, функция их числа $f(t)$ в зависимости от времени t имеет вид:

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

$$+ \alpha_8 \cdot \cos[t],$$

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

Аналогично (6) при $t \ge 0$ для функции $f(t)$ имеет место неравенство:

$$f(t) \le \alpha_9 + \alpha_2\sqrt{t},$$

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

Обозначим через u – средний ущерб от несанкционированной операции и, как и ранее, через N - число юридических лиц (ИС), понесших ущерб от действий злоумышленников.

Тогда прогнозная модель среднего ущерба юридического лица имеет вид:

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

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

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

откуда получаем:

$$T_0 \ge \left(\frac{N \cdot R_0 / u - \alpha_9}{\alpha_2}\right)^2, \qquad (8)$$

В третьем примере, в соответствии с прииненным выше методом построения прогнозной модели осуществления атак вредоносными программами для майнинга криптовалют, функция их интенсивности (процент атакованных компьютеров) $f(t)$ в зависимости от времени t имеет вид:

$$f(t) = -\alpha_1 \cdot \sin[t] + \alpha_2 \cdot \sqrt{t} - \alpha_3 \cdot Ln[t] - \alpha_4 \cos[t] - \alpha_5 \sin[2 \cdot t] - \alpha_6 \cdot \cos[4 \cdot t] -$$
$$-\alpha_7 \cdot \sin[4 \cdot t] - \alpha_8 \cdot \cos[2 \cdot t] + \alpha_9 \cdot \sin[3 \cdot t],$$

где α_i, $i = 1,2,...,9$ - соответствующие константы.

Аналогично (6) при $t \geq 1$ для функции $f(t)$ имеет место неравенство:

$$f(t) \leq \alpha_{10} + \alpha_2 \sqrt{t},$$

где $\alpha_{10} = \alpha_1 + \alpha_3 + ... + \alpha_9$.

Обозначим через u – средний ущерб, наносимый одному компьютеру (ИС).

Тогда прогнозная модель среднего ущерба ИС имеет

$$u \cdot f(t) \leq u \cdot \left(\alpha_{10} + \alpha_2 \sqrt{t}\right),$$

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

$$u \cdot \left(\alpha_{10} + \alpha_2 \sqrt{t}\right) = R_0,$$

откуда получаем:

$$T_0 \geq \left(\frac{R_0/u - \alpha_{10}}{\alpha_2}\right)^2, \qquad (9)$$

При наличии реальных данных об имевших место инцидентах, приводящих к нарушению информационной безопасности организации, соотношения (7) - (9) могут быть использованы для оценки уровня защищенности ее информационной системы.

Заключение.

В статье исследуются вопросы оценки ущерба информационным системам организации в результате появления инцидентов, приводящих к нарушению информационной безопасности. На основе реальных данных построены прогнозные модели ущерба от несанкционированных операций со счетами юридических лиц и ущерба от компьютерных атак, имеющих цель несанкционированного использования вычислительных мощностей для майнинга криптовалют. На основе построенных прогнозных моделей получены оценки для времени безопасной эксплуатации информационной системы организации. При наличии обоснованных данных об инцидентах, имевших место в конкретной организации, предложенный в настоящей работе подход может быть использован для оценки уровня защищенности данной организации.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 13335-1:2006. Информационные технологии. Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

2. ГОСТ Р ИСО/МЭК 13335-3:2007. Информационные технологии. Методы и средства обеспечения безопасности. Методы менеджмента безопасности информационных технологий.

3. ГОСТ Р ИСО/МЭК 13335-5:2007. Информационные технологии. Методы и средства

обеспечения безопасности. Руководство по менеджменту безопасности сети.

4. *Остапенко А. Г.* К вопросу об оценке выживаемости информационных систем инновационного характера // Информация и безопасность: Регион. науч.-техн. Журнал. Воронеж. 2012. № 3. С. 413-417.

5. *Остапенко А. Г.* К вопросу об оценке ущерба в жизнестойкости атакуемых распределенных информационных систем: Развитие методического обеспечения // Информация и безопасность. 2012. № 4. С. 583- 584.

6. *Остапенко А. Г.* Жизнестойкость атакуемых распределенных систем: оценка рисков фатальных отказов компонентов / А.Г. Остапенко, Д.Г. Плотников О.Ю. Макаров, Н.М. Тихомиров, В. Г. Юрасов; под ред. чл.-корр. РАН Д.А. Новикова / Монография. Воронеж: Научная книга. 2013. 160 с.

7. *Лось А. Б.* Временная модель оценки риска нарушения информационной безопасности //Доклады ТУСУР. Томск. 2012. № 1. Ч. 2. С. 87-91.

8. *Ермакова А. Ю.* Оценка качества прогнозирования динамики изменения валютных курсов на основе построения аппроксимирующих функций // Качество. Инновации. Образование. 2013. № 2 (93). С. 71-79.

9. *Ермакова А. Ю.* Исследование качества прогнозирования биржевых курсов драгоценных металлов // Качество. Инновации. Образование. 2014. № 1 (104). С. 49-56.

10. *Ермакова А. Ю.* Построение прогнозной модели динамики изменения цен на древесину // Лесной Вестник. 2016. № 6. С.88−97.

11. *Ермакова А. Ю.* Разработка методов прогнозирования на примере анализа средств вычислительной техники // Промышленные АСУ и контроллеры. 2017. № 1. С. 28−34.

12. *Ермакова А. Ю.* Об оценке точности прогнозирования состояния динамической системы методом построения аппроксимирующих функций // Промышленные АСУ и контроллеры. 2018. № 5. С. 36−42.

13. *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 науч.-практич. Конференции. Саратов. 2018. С. 144−149.

14. *Ермакова А. Ю.* Об одном подходе к оценке защищенности информационной системы на основе анализа инцидентов // Системы высокой доступности. 2018. № 4. С. 32−35.

15. *Калашников А. И.* Обзор несанкционированных переводов денежных средств за 2017 год. [Электронный ресурс]. URL: https://ural.ib-bank.ru/files/files/materials2018/45%20Kalashnikov.pdf (дата обращения 17.03.2019).

16. «Ландшафт угроз для систем промышленной автоматизации, Первое полугодие 2018, Kaspersky Lab ICS CERT», [Электронный ресурс]. URL: https:// securelist.ru/ (дата обращения 19.03.2019).