Ольга С. Макарова[1], Сергей В. Поршнев[1,2]
[1]Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, ул. Мира, 19, Екатеринбург, 620002, Россия
[2]Институт математики и механики Уральского отделения Российской академии наук, ул. Софьи Ковалевской, 16, Екатеринбург, 620108, Россия
[1]e-mail: o.s.makarova@urfu.ru, https://orcid.org/0000-0003-4585-6702
[2]e-mail: s.v.porshnev@urfu.ru, https://orcid.org/0000-0001-8620-0350

ОЦЕНИВАНИЕ ВЕРОЯТНОСТЕЙ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ ФУНКЦИЙ

DOI: http://dx.doi.org/10.26583/bit.2020.2.07

Аннотация. Объективная оценка уровня защиты информационной системы (ИС) организации, обеспечиваемой соответствующей системой информационной безопасности (ИБ), как на этапе ее проектирования, так и на этапе эксплуатации, возможна на основе использования оценок текущих и прогнозируемых вероятностей компьютерных атак нарушителей на данную ИС, использующих уязвимости системы ИБ. В статье для оценивания вероятности компьютерной атаки нарушителя предложено использовать функцию ожидаемой полезности, учитывающую ключевые факторы возможности проведения компьютерной атаки (критерии выбора объекта компьютерной атаки нарушителем, этапы и методы реализации атаки, методы получения информации об объекте, навыки нарушителя) и ожидаемую полезность атаки (мотивы нарушителя, состояние нарушителя до компьютерной атаки, в частности, его доход, принципы принятия решения о проведении/продолжении/прекращении компьютерной атаки нарушителем), модернизированную с учетом особенностей данного типа и преступлений в компьютерной сфере. Предложенное решение базируется на теории положений по криминологии, утверждающей, что атака реализуется нарушителем в тех случаях, когда имеется возможность реализации атаки и, одновременно, ожидаемая полезность атаки с точки зрения нарушителя оказывается достаточной. Продемонстрировано, что выбранная функция полезности адекватно описывает связь между вероятностью компьютерной атаки и ключевыми факторами компьютерной атаки. Проведен анализ модернизированной функции полезности, результаты которого показали, что: 1) значение ожидаемой полезности, при прочих равных условиях, для нарушителя, склонного к риску, определяется вероятностью его разоблачения, равной единице минус вероятность проведения незаметной компьютерной атаки, для нарушителя, не склонного к риску, – тяжестью наказания, поэтому необходимо выстраивать дифференцированную систему защиты в зависимости от типа нарушителя; 2) существует возможность значительного сокращения числа потенциальных нарушителей за счет увеличении доходов от легальной деятельности специалистов в области ИБ; 3) существует зависимость количества компьютерных атак за определенный период времени от вероятности проведения незаметной компьютерной атаки, тяжести наказания, наличия и величины альтернативных доходов (выгод).

Ключевые слова: информационная система, информационная безопасность, компьютерная атака, нарушитель, вероятность компьютерной атаки, функция ожидаемой полезности, ключевые факторы компьютерной атаки, теория положений по криминологии.
Для цитирования: МАКАРОВА, Ольга С.; ПОРШНЕВ, Сергей В. ОЦЕНИВАНИЕ ВЕРОЯТНОСТЕЙ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ ФУНКЦИЙ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 86-96, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1273>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.07.

Olga S. Makarova[1], Sergey V. Porshnev[1,2]
[1]Federal State Autonomous Educational Institution of Higher Education "Ural Federal University named after the first President of Russia B.N. Yeltsin", 19 Mira Str., Ekaterinburg, 620002, Russia
[2]Institute of mathematics and mechanics of the Ural branch of the Russian Academy of Sciences, Sophia Kovalevskaya Str., 16, Ekaterinburg, 620108, Russia

[1]*e-mail: o.s.makarova@urfu.ru, https://orcid.org/0000-0003-4585-6702*
[2]*e-mail: s.v.porshnev@urfu.ru, https://orcid.org/0000-0001-8620-0350*

Assessment of probabilities of computer attacks based on function

DOI: http://dx.doi.org /10.26583/bit.2020.2.07

Abstract. An objective assessment of the level of protection of an organization's information system provided by an appropriate information security system (ISS), both at the stage of its design and at the operation stage, is possible based on the use of estimates of current and predicted probabilities of computer attacks of intruder of this IS using vulnerabilities ISS. To assess the probability of a computer attack by an intruder, this study proposes to use the expected utility function that takes into account key attack criteria of the possibility of a computer attack (criteria for choosing an object of a computer attack by an intruder, stages and methods of implementing an attack, methods of obtaining information about an object, skills of an intruder) and the expected usefulness of the attack (motives the offender, the state of the offender before a computer attack, in particular, his income, the principles for deciding on the conduct / continuation / termination of a computer attack intruder), modernized taking into account the characteristics of this type and crimes in the computer sphere. The proposed solution is based on the theory of provisions in criminology, which states that an attack is implemented by an intruder in cases where it is possible to implement an attack and, at the same time, the expected utility of the attack from the point of view of the offender is sufficient. It is demonstrated that the selected utility function adequately describes the relationship between the probability of a computer attack and the key attack criteria of a computer attack. The analysis of the modernized utility function, the results of which showed that: 1) the value of the expected utility, ceteris paribus, for the offender prone to risk, is determined by the probability of exposing it (which is equivalent to the likelihood of an inconspicuous computer attack), for the offender not prone to risk, – the severity of the punishment, therefore it is necessary to build a differentiated protection system depending on the type of intruder; 2) there is the possibility of a significant reduction in the number of potential violators by increasing revenues from the legal activities of security experts; 3) there is a dependence of the number of computer attacks for a certain period of time on the probability of an inconspicuous computer attack, the severity of the punishment, the presence and magnitude of alternative income (benefits).

Keywords: information system, information security, computer attack, intruder, probability of threats, expected utility, computer attack, expected utility function, key attack criteria of computer attack, criminology theory.

For citation: MAKAROVA, Olga S.; PORSHNEV, Sergey V. Assessment of probabilities of computer attacks based on function. IT Security (Russia), [S.l.], v. 27, n. 2, p. 86-96, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1273>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.07.

Введение

Анализ современных методов построения систем информационной безопасности (ИБ) и научных исследований в данной области, в том числе по расчету вероятности угроз [1], выявлению новых и/или существующих уязвимостей, используемых злоумышленниками [2, 3] по оценке прогнозирования уязвимостей ИБ [4], вероятностей угроз и векторов атак [5] позволяют сделать обоснованный вывод об отсутствии единого метода прогнозирования наиболее вероятных векторов атак [4]. Данный вывод, в том числе, подтверждается результатами соревнований по кибербезопасности между командами атакующих, защитников и специалистов в области мониторинга ИБ,

свидетельствующими об отсутствии сегодня системных подходов, обеспечивающих существенное сокращение числа результативных атак на организации[1,2].

Анализ ограничений классических подходов к построению системы ИБ, подробно описан в [5, 6], где также предложена методика динамического оценивания вероятности угроз ИБ с позиции нарушителя, основанная на использовании метода анализа иерархий (МАИ) с динамическими приоритетами и предпочтениями [8]. Выбор данного метода обоснован тем, что он позволяет:

– отказаться от учета ограниченного набора требований к системам ИБ, используемого в классических подходах построения систем ИБ;

– рассматривать вероятность реализации угрозы с точки зрения нарушителя;

– проводить динамическую оценку вероятностей реализации угроз ИБ.

В свою очередь, подходу, предложенному в [8], присущ известный ряд недостатков, обусловленных тем, что выбранный подход базируется на методе экспертных оценок, а также оказывается сложно реализуемым при большом перечне атак, устранить которые, потенциально, возможно за счет использования соответствующей функции, описывающей зависимость вероятности атаки от ключевых факторов, учитываемых при прогнозировании вектора возможных атак на систему ИБ организации.

В статье изложены научные обоснования выбора данной функции и описана методика оценки ее параметров.

1. Обоснование выбора функции, описывающей зависимость вероятности атаки на систему информационной безопасности организации от ключевых факторов атаки

Ключевые факторы, которые должны учитываться при прогнозировании вектора возможных атак на систему ИБ организации, определены в [6, 7]. К ним отнесены факторы, характеризующие нарушителя, в том числе:

– мотивы нарушителя;

– критерии выбора объекта атаки нарушителем;

– этапы и методы реализации атаки;

– методы получения информации об объекте;

– принципы принятие решения о проведении/продолжении/прекращении атаки нарушителем;

– тип, характер и навыки нарушителя;

– а также факторы, характеризующие защищаемую информационную систему;

– перечень компонентов, архитектуру и используемые настройки системы ИБ защищаемой информационной системы;

– компетенции, как рядовых, так и привилегированных сотрудников организации.

Решение задачи выбора функции, описывающей зависимость вероятности атаки от ключевых факторов атаки на систему ИБ организации, существенно осложняет необходимость одновременного учета большого числа разнородных факторов, от которых оцениваемая вероятность зависит. Здесь представляется целесообразным использовать системный подход, рекомендующий в подобных ситуациях проводить анализ структуры факторов и их группировку. Для формализации функциональных зависимостей между

[1]Кибербитва на PHDays, или Как за 30 часов взломать городскую инфраструктуру. phdays.com URL:https://www.phdays.com/ru/press/news/kiberbitva-na-phdays-ili-kak-za-30-chasov-vzlomat-gorodskuyu-infrastrukturu/ (дата обращения: 27.04.2020).

[2]PHDays: точно в девятку. phdays.com URL:https://www.phdays.com/ru/press/news/phdays-tochno-v-devyatku/ (дата обращения: 27.04.2020).

вероятностью атаки на систему ИБ организации и учитываемыми ключевыми факторами мы обратились к опыту, накопленному в экономической и финансовой сферах [9, 10], а также при предупреждении преступлений общей практики [11].

Экономические подходы к анализу мотивов преступников обоснованы Ч. Беккариа и И. Бентама в теории положений по криминологии [11–13] (ТПК). Ее суть состоит в том, что любой человек, потенциально, может стать нарушителем при выполнении следующих условий:

1) наличия возможности совершения преступления;

2) получения в случае совершения преступления достаточной (с точки зрения нарушителя) полезности.

В ТПК условие совершения преступления сформулирована в виде следующего условия: «если ожидаемая полезность от преступления превышает полезность от иной деятельности, на которое были бы затрачены те же силы и время, то нарушитель совершит преступление». Следовательно, в соответствие с ТПК атака реализуется нарушителем в тех случаях, когда, одновременно, имеется возможность реализации атаки и ожидаемая полезность атаки с точки зрения нарушителя оказывается достаточной. Поэтому вероятность реализации атаки, реализуемой нарушителем, является ни чем иным, как условной вероятностью достаточности ожидаемой полезности атаки при наличии возможности атаки как таковой:

$$\rho\left(\frac{EU}{A}\right) = \frac{\rho(EUA)}{\rho(A)}, \quad (1)$$

где $\rho(A)$ – вероятность наличия возможности реализовать атаку А нарушителем,

$\rho\left(\frac{EU}{A}\right)$ – условная вероятность достаточности ожидаемой полезности атаки для нарушителя, при оценивании которой учитывается возможность провести атаку незаметно.

Таким образом, в соответствие с ТПК, выделенные выше ключевые факторы следует сгруппировать в два фактора атаки:

– возможность атаки, включающая в себя критерии выбора объекта атаки нарушителем, этапы и методы реализации атаки, методы получения информации об объекте, навыки нарушителя;

– ожидаемую полезность атаки, включающую в себя мотивы нарушителя, принципы принятие решения о проведении/продолжении/прекращении атаки нарушителем.

Далее в статье подробно рассматривается второй фактор атаки – ожидаемая полезность. Формирование, обоснование и примеры вычисления количественных значений вероятностей возможности реализации атаки нарушителем являются предметом дальнейших исследований.

2. Способ оценки ожидаемой полезности атаки на систему информационной безопасности организации

Ожидаемая полезность – это ценность выгоды от атаки, зависящая не от конкретной выгоды, а от дополнительной единицы выгоды. Дополнительная единица выгоды – это выгода нарушителя в единицу времени, полученная им в дополнение к ранее

приобретенной выгоде. В соответствии с законом Госсена[3] [14] полезность от каждой дополнительной единицы выгоды сокращается, так как человек приходит к состоянию насыщения. Далее будем использовать это утверждение, учитывая при этом, что нарушитель является среднестатистическим человеком не склонным к риску.

Отметим, что компьютерные преступления, в отличие от правонарушений, являющихся предметом, изучаемым криминологией, требуют от нарушителя наличия специальных знаний, умений и навыков, а также возможности совершить компьютерную атаку. Для связывания факторов, характеризующих нарушителя, друг с другом можно использовать метод анализа иерархий с динамическими приоритетами и предпочтениями [6, 7].

Таким образом, функция ожидаемой полезности, определенная в ТПК [11–13], модернизированная с учетом описанных выше особенностей компьютерных атак и преступлений в информационной сфере, может быть записана в следующем виде:

$$EU = (1-\rho_n)U(W_m + W_i) + \rho_n U(W_m + W_i - F), \quad (2)$$

где $U(\xi)$ – функция полезности,

ρ_n – вероятность разоблачения нарушителя (соответственно, вероятность проведения незаметной атаки $\rho_m = 1-\rho_n$),

W_m – выгода нарушителя в случае успешной реализации компьютерной атаки,

W_i – текущий доход нарушителя от легальной деятельности,

F – тяжесть наказания в случае разоблачения нарушителя (в денежном эквиваленте).

В качестве функции полезности $U(\xi)$ в ТПК для нарушителя, не склонного к риску, традиционно, используют классическую функцию, предложенную Бернулли [13]:

$$U(\xi) = b\ln\left(\frac{a+\xi}{a}\right), \quad (3)$$

где a, b – константы.

3. Анализ зависимости ожидаемой полезности от параметров функции

Будем считать, что нарушитель системы ИБ, как любой рациональный человек, стремится максимизировать ожидаемую полезность. Следовательно, в предположении о том, что значения всех за исключением одной переменной c в (2) известны, значение

$$c = \arg\max U(C)$$

есть решение уравнения:

$$\frac{\partial EU(c)}{\partial c} = 0. \quad (4)$$

Для анализа зависимости функции (2) от параметров ρ_n, W_m, F используем эластичность функции, представляющую собой предел отношения относительного изменения значения функции к относительному изменению переменной, когда последнее стремится к нулю [15]:

$$\eta_c^{EU} = \lim_{\Delta c \to 0}\left(\frac{\Delta EU}{EU} : \frac{\Delta c}{c}\right) = \frac{c}{EU}\lim_{\Delta c \to 0}\frac{\Delta EU}{\Delta c} = c\frac{\partial EU/\partial c}{EU},$$

[3]Закон убывающей предельной полезности

Выбор данной характеристики обусловлен тем, что по ее значению можно оценивать степень зависимости вероятности принятия нарушителем решения о проведении атаки от вероятности разоблачения нарушителя ρ_n и тяжести наказания *F*.

Подставляя (2) в (5), находим абсолютную величину эластичности ожидаемой полезности от вероятности разоблачения нарушителя ρ_n:

$$\left|\eta_{\rho_n}^{EU}\right| = \left|\rho_n \frac{\partial EU/\partial \rho_n}{EU}\right| = \left|\frac{U\left(W_m + W_i - F\right) - U\left(W_m + W_i\right)}{EU}\right| = \left|\frac{\rho_n F}{EU}\right| \left|\frac{U\left(W_m + W_i - F\right) - U\left(W_m + W_i\right)}{F}\right| \quad (6)$$

и абсолютную величину эластичности ожидаемой полезности от тяжести наказания:

$$\left|\eta_F^{EU}\right| = \left|F \frac{\partial EU/\partial F}{EU}\right| = \left|\frac{U'\left(W_m + W_i - F\right)}{EU}\right| = \left|\frac{\rho_n F}{EU}\right| \left|U'\left(W_m + W_i - F\right)\right|. \quad (7)$$

Из (6), (7) видно, что $\left|\eta_{\rho_n}^{EU}\right|$, $\left|\eta_F^{EU}\right|$ с точностью до множителя $\left|\rho_n F / EU\right|$ равняются, соответственно, тангенсу угла наклона прямой, соединяющей точки $U\left(W_m + W_i - F\right)$ и $U\left(W_m + W_i\right)$, и тангенсу угла наклона касательной к графику функции $U\left(W_m, W_i, F\right)$ в точке $W_m + W_i - F$. Следовательно, $\left|\eta_{\rho_n}^{EU}\right| > \left|\eta_F^{EU}\right|$, когда $U''(W_m - F) > 0$, т.е. функция возрастает ускоренно, и $\left|\eta_{\rho_n}^{EU}\right| < \left|\eta_F^{EU}\right|$, когда $U''(W_m - F) < 0$, т.е. функция возрастает замедленно.

Из (3) так же видно, что в случае нарушителя, не склонного к риску, эластичность ожидаемой полезности от вероятности разоблачения меньше эластичности ожидаемой полезности от тяжести наказания. Это означает, что для нарушителя, не склонного к риску, тяжесть наказания более существенный сдерживающий фактор, в то время как для нарушителя, склонного к риску, при принятии решения об атаке вероятность наказания более существенна. Отметим, что на практике можно реализовать дифференцированный контроль склонности к риску внутренних нарушителей, являющихся сотрудниками данной организации. Для этого можно использовать одну из известных методик, например, HCR-20 («Historical Clinical Risk»), PCL («Psychopathy Checklist»), имеющей несколько различных модификаций, VRAG («Violence Risk Appraisal Guide») или тест RSK Шуберта [16].

Абсолютные величины эластичности ожидаемой полезности от выгоды нарушителя и эластичности ожидаемой полезности от дохода нарушителя от легальной деятельности вычисляются по соответствующим формулам:

$$\left|\eta_{W_m}^{EU}\right| = \left|W_m \frac{dEU/dW_m}{EU}\right| = \left|W_m \frac{(1-p_n)U'\left(W_m + W_i\right) + p_n U'\left(W_m + W_i - F\right)}{EU}\right|, \quad (8)$$

$$\left|\eta_{W_i}^{EU}\right| = \left|W_i \frac{dEU/dW_i}{EU}\right| = \left|W_i \frac{(1-p_n)U'\left(W_m + W_i\right) + p_n U'\left(W_m + W_i - F\right)}{EU}\right|. \quad (9)$$

Из (8) и (9) видно, что ожидаемая полезность компьютерной атаки будет определяться, в первую очередь, выгодой нарушителя в случае успешной реализации компьютерной атаки W_m, если текущей доход нарушителя от легальной деятельности

меньше выгоды нарушителя от реализации компьютерной атаки, т.е. $W_m > W_i$, то и наоборот. Результаты проведенного анализа подтверждаются доступными статистическими данными [17, 18], анализ которых показал:

– большую часть атак осуществляют преступные кибергрупировки, которые работают длительное время [18], в их легальный доход близок к нулю.

– по данным прокуратуры наибольшее число задержанных за компьютерные атаки нарушителей – это люди со средним образованием или студенты, не имеющие постоянного заработка [17, 18].

В том случае, когда доходы от легальной деятельности нарушителя существенно больше выгоды нарушителя в случае успешной реализации компьютерной атаки $(W_i > W_m)$ влияние тяжести наказания на ожидаемую полезность становится больше, чем выгода от компьютерной атаки. Таким образом, вероятность разоблачения нарушителя ρ_n напрямую влияет на ожидаемую полезность от компьютерной атаки, в то время как выгода нарушителя W_m влияет опосредовано.

Из проведенного анализа можно сделать следующие выводы:

– Значение ожидаемой полезности, при прочих равных условиях, определяется, в первую очередь, вероятностью разоблачения нарушителя (вероятность проведения незаметной атаки) для нарушителя, склонного к риску, и тяжестью наказания, для нарушителя, не склонного к риску. Следовательно, нужно строить дифференцированную систему защиты ИБ в зависимости от типа нарушителя.

– Можно ожидать, что увеличение доходов от легальной деятельности специалистов в области ИБ приведет к значительному сокращению числа нарушителей.

– Количество компьютерных атак за определенный период времени зависит от вероятности проведения незаметной компьютерной атаки, тяжести наказания, наличия и величины альтернативных доходов (выгод).

4. Обоснование возможности описания динамики изменения функции полезности

Обоснования необходимости учета динамки изменения вероятности атаки при оценке эффективности системы ИБ приведены в [6, 7]. Для описания изменения значения выгоды от компьютерной атаки во времени в терминах ТПК можно использовать формулу Эрлиха [19]:

$$W(t) = W_0 + W_m(t_m) + W_i(t_i) - F(t_m), \quad (10)$$

где W_0 – благосостояние нарушителя в начале рассматриваемого периода времени *t*,

$W_m(t_m)$ – выгода нарушителя в случае успешной реализации атаки за период времени *t*,

$W_i(t_i)$ – доход нарушителя от легальной деятельности за период времени *t*,

$F(t_m)$ – тяжесть наказания в случае разоблачения нарушителя (в денежном эквиваленте) за период времени *t*,

t_m – время, потраченное в период времени *t* на подготовку и реализацию атаки,

t_i – время, потраченное в период времени *t* на легальную деятельность.

Период времени *t* в этом случае описывается следующим образом:

$$t = t_m + t_i + t_c, \quad (11)$$

где t_c – время, потраченное в период времени t на потребление (досуг, отдых и т.п.).

Так как ожидаемая полезность (2) зависит от дополнительной единицы выгоды, используя в (2) вместо переменной W_m функцию (10), получаем функцию, описывающую зависимость ожидаемой полезности от времени, максимальное значение которой находится из условия $\frac{dEU(t)}{dt} = 0.$

5. Обоснование выбора источников первичной информации для расчета ожидаемой полезности от киберпреступления

Возможность использования статистической информации для оценки вероятности компьютерной атаки нарушителем обоснована в [6, 7]. При расчете вероятности проведения незаметной компьютерной атаки следует учитывать, что предложенная модель строится с точки зрения нарушителя. При «формировании» ожидаемой полезности нарушитель в первую очередь опирается на свои знания, и, следовательно, на открытые источники информации о правонарушениях. В этой связи для расчета вероятности проведения незаметной компьютерной атаки целесообразно использовать результаты анализа статей новостного агрегатора о количестве громких судебных дел [20], а также статистику Генпрокуратуры РФ [18] о количестве зарегистрированных преступлений и данные ФинЦЕРТ [21, 22] о блокировке фишинговых ресурсов и телефонных номеров.

Оценить вероятность проведения незаметной компьютерной атаки можно по следующей формуле:

$$\rho_m = \frac{A_m - A_{mf}}{A_m}, \qquad (12)$$

где A_m – количество выявленных компьютерных атак данного типа, A_{mf} – количество выявленных компьютерных атак, закончившихся арестом (наказанием преступника).

Отметим, что при оценке рисков международные стандарты рекомендуют учитывать ценность активов организации [1]. Однако нарушитель, в отличие от сотрудников организации, не знает реальной ценности активов, поэтому он может оперировать только предполагаемой величиной и потенциальной величиной выгоды, которую может получить (например, выплата за расшифровку данных после компьютерной атаки с помощью шифровальщика). Следовательно, потерянная ценность актива для организации в ходе успешной компьютерной атаки нарушителем не равна выгоде, получаемой нарушителем.

Нарушитель, выбирая методы и объекты компьютерной атаки, планирует получить определенную выгоду, величину которой, как и настоящую ценность активов атакуемой организации, он не может знать предварительно. Следовательно, на практике в качестве оценки W_m может быть использована средняя выручка нарушителя от рассматриваемого типа атак [6, 7]. Для финансового сектора средние значения выручки за 2017–2018 гг. от наиболее распространенных атак были рассчитаны в [6, 7]. Расчеты для других отраслей и типов компьютерных атак можно провести аналогичным образом.

Компьютерные преступления, в отличие от других правонарушений, требуют от нарушителя наличия специальных навыков, знания методов и наличие возможности совершить компьютерную атаку. Следовательно, наибольшую выгоду от законной деятельности нарушитель получит, работая в сфере информационных технологий и информационной безопасности, поэтому W_i может быть рассчитана как средняя зарплата в сфере информационных технологий и ИБ в регионе проживания нарушителя за

рассматриваемый период. В этой связи, чем выше компетентность нарушителя, тем больше у него может быть заработная плата и, соответственно, тем более эффективная компьютерная атака может быть им реализована. Таким образом, при определении функциональной зависимости дохода от времени, можно предположить, что функциональные зависимости $W_m(t_m)$ и $W_i(t_i)$ будут одинаковыми.

В Уголовном кодексе РФ предусмотрены штрафы за совершение компьютерных атак, а также лишение свободы, поэтому при расчете тяжести наказания в денежном эквиваленте следует учитывать как величину штрафа, так и величину потерь за период времени отбывания наказания, а потери, связанные с отбыванием наказания, можно рассчитывать, как потерю легального и не легального заработка за срок заключения.

Заключение

В статье на основе теории принятия решений, общей практики выявления и предупреждения правонарушений, ИТ-подходов к выявлению уязвимостей предложена и математически обоснована функция, описывающая связь между вероятностью компьютерной атаки и ключевыми факторами атаки. Проведен анализ предложенной функции, результаты которого позволят сделать следующие обоснованные выводы:

– осуществление защиты от компьютерных атак возможно за счет изменения восприятия преступником возможностей (в том числе соотношения между выгодой и потерями) совершения преступления;

– необходимо разрабатывать дифференцированные системы ИБ, уменьшающие вероятности компьютерных атак, наиболее опасных для данной ИС, которые будут являться для нарушителей, адекватно оценивающих риски, возникающие вследствие проводимой атаки, и учитывающих тяжесть наказания за совершаемое им деяние, предусмотренное действующим законодательством РФ, сдерживающим фактором;

– нарушитель, безнаказанно совершивший результативную компьютерную атаку, продолжит в будущем предпринимать попытки реализации компьютерных атак;

– количество компьютерных атак за определенный период времени зависит от вероятности того, что компьютерная атака пройдет не заметно, тяжести наказания, наличия и величины альтернативных доходов (выгод) у нарушителя;

– можно ожидать, что увеличение доходов от легальной деятельности специалистов в области ИБ существенно сократит количество нарушителей.

СПИСОК ЛИТЕРАТУРЫ:

1. Международный стандарт ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2013. – 23 с.
2. J. Stuckman, J. Walden and R. Scandariato, "The Effect of Dimensionality Reduction on Software Vulnerability Prediction Models," in IEEE Transactions on Reliability, Vol. 66, No. 1. P. 17–37, March 2017. DOI: http://dx.doi.org/10.1109/TR.2016.2630503.
3. Scandariato R., Walden J., Hovsepyan A., Joosen W. Predicting Vulnerable Software Components via Text Mining. IEEE Transactions on Software Engineering. 2014. Vol. 40, No 10. P. 993–1006. DOI: http://dx.doi.org/10.1109/TSE.2014.2340398
4. Yasasin E., Prester J., Wagner G., Schryen G. Forecasting IT security vulnerabilities – An empirical analysis // Computers and Security. 2020. Vol. 88. DOI: http://dx.doi.org/10.1016/j.cose.2019.101610.
5. Deb A., Lerman K., Ferrara E. Predicting Cyber-Events by Leveraging Hacker Sentiment. Information. Vol. 9, No 11. 2018. – 18 p. DOI: http://dx.doi.org/10.3390/info9110280.
6. Макарова, Ольга С.; Поршнев, Сергей В. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями. Безопасность информационных технологий, [S.l.], Т. 27, № 1. С. 6–18, mar. 2020. ISSN 2074-7136.

URL: <https://bit.mephi.ru/index.php/bit/article/view/1248> (дата обращения: 27.04.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.01.
7. Makarova O.S., Porshnev S.V. Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information // Доклады конференции.2020. DOI: http://dx.doi.org/10.26583/bit.2020.1.01
8. А.В. Андрейчиков, О.Н. Андрейчикова Методы и интеллектуальные системы принятия решений для проведения ФОРСАЙТ-исследований // Cloud of science. 2014. №3. URL: https://cyberleninka.ru/article/n/metody-i-intellektualnye-sistemy-prinyatiya-resheniy-dlya-provedeniya-forsayt-issledovaniy (дата обращения: 27.04.2020).
9. Cody T., Adams S., Beling P.A. A utilitarian approach to adversarial learning in credit card fraud detection. Institute of Electrical and Electronics Engineers Inc. Conference paper «Systems and Information Engineering Design Symposium», 2018. P. 237–242. DOI: http://dx.doi.org/10.1109/SIEDS.2018.8374743.
10. Pasquier R., Goulet J., Smith I.F. Measurement system design for civil infrastructure using expected utility. Elsevier Ltd. Advanced Engineering Informatics. 2017. Vol. 32. P. 40–51. DOI: http://dx.doi.org/10.1016/j.aei.2016.12.002.
11. Hausken K., Moxnes J.F The dynamics of crime and punishment // International Journal of Modern Physics C. 2005. Vol. 16, № 11. P. 1701-1732. DOI: http://dx.doi.org/10.1142/S0129183105008229.
12. Becker G.S. The economics of crime // Cross Sections, Federal Reserve Bank of Richmond. 1995. Vol. 12. P. 8–15. URL: https://ideas.repec.org/a/fip/fedrcs/y1995ifallp8-15nv.12no.3.html (дата обращения: 27.04.2020).
13. Бернулли Д. Опыт новой теории измерения жребия. Теория потребительского поведения и спроса // Вехи экономической мысли. СПб.: Экономическая школа, 1999. Т. 1. С. 11–27.
14. Данилов Н.Н. Курс математической экономики // СПб.: Лань.2016. С. 116–118.
15. Ганичева, А.В. Математические модели и методы оценки событий, ситуаций и процессов // СПб.: Лань. 2017. С. 107–110.
16. Dolan M., Doyle M. Violence risk prediction: Clinical and actuarial measures and the role of the Psychopathy Checklist. The British Journal of Psychiatry. 2000. Vol. 177, No 4. P. 303–311. DOI: http://dx.doi.org/10.1192/bjp.177.4.303.
17. Генпрокуратура составила портрет типичного российского хакера. vedomosti.ru URL:https://www.vedomosti.ru/technology/news/2018/12/11/788967-sostavila/ (дата обращения: 27.04.2020).
18. Киберпреступность и киберконфликты // TADVISER.RU/ URL: http://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Россия/ (дата обращения: 27.04.2020).
19. Ehrlich I. Participation in illegitimate activities: theoretical and empirical investigation //J. of Publ. Econ. 1973. Vol. 81. No 3. C. 521—565.
20. Потери банков от киберпреступности // TADVISER.RU/ URL: http://www.tadviser.ru/index.php/ Статья: Потери_банков_от_киберпреступности / (дата обращения: 27.04.2020).
21. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 1.09.2017 – 31.08.2018 // CRB.RU/ URL: https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf/ (дата обращения: 27.04.2020).
22. Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году // CRB.RU/ URL: https://cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf/ (дата обращения: 27.04.2020).

REFERENCES:

[1] International Standard ISO/IEC 27001: 2013. Information technology – Security techniques – Information security management systems – Requirements. M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2013. – 23 p. (in Russian).
[2] J. Stuckman, J. Walden and R. Scandariato, "The Effect of Dimensionality Reduction on Software Vulnerability Prediction Models," in IEEE Transactions on Reliability, Vol. 66, No. 1. P. 17–37, March 2017. DOI: http://dx.doi.org/10.1109/TR.2016.2630503.
[3] Scandariato R., Walden J., Hovsepyan A., Joosen W. Predicting Vulnerable Software Components via Text Mining. IEEE Transactions on Software Engineering. 2014. Vol. 40, No 10. P. 993–1006. DOI: http://dx.doi.org/10.1109/TSE.2014.2340398.
[4] Yasasin E., Prester J., Wagner G., Schryen G. Forecasting IT security vulnerabilities – An empirical analysis. Computers and Security. 2020. Vol. 88. DOI: http://dx.doi.org/10.1016/j.cose.2019.101610.
[5] Deb A., Lerman K., Ferrara E. Predicting Cyber-Events by Leveraging Hacker Sentiment. Information. Vol. 9, No 11. 2018. – 18 p. DOI: http://dx.doi.org/10.3390/info9110280.

[6] Makarova, Olga S.; Porshnev, Sergey V. Assessment of probabilities of computer attacks based on the method of analysis of hierarchies with dynamic priorities and preferences. IT Security (Russia), [S.l.], Vol. 27, No. 1. P. 6–18, mar. 2020. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1248> (accessed: 27.04.2020). DOI:http://dx.doi.org/10.26583/bit.2020.1.01 (in Russian).
[7] Makarova O.S., Porshnev S.V. Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information. Conference paper .2020. DOI: http://dx.doi.org/10.26583/bit.2020.1.01.
[8] Andreichikov A.V., Andreichikova O.N. Methods and intelligent decision-making systems for conducting FORSIGHT research. Electronic journal. Cloud of Science. 2014. №3. URL: https://cyberleninka.ru/article/n/metody-i-intellektualnye-sistemy-prinyatiya-resheniy-dlya-provedeniya-forsayt-issledovaniy (accessed: 27.04.2020) (in Russian).
[9] Cody T., Adams S., Beling P.A. A utilitarian approach to adversarial learning in credit card fraud detection. Institute of Electrical and Electronics Engineers Inc. Conference paper «Systems and Information Engineering Design Symposium», 2018. P. 237–242. DOI: http://dx.doi.org/10.1109/SIEDS.2018.8374743.
[10] Pasquier R., Goulet J., Smith I.F. Measurement system design for civil infrastructure using expected utility. Elsevier Ltd. Advanced Engineering Informatics. 2017. Vol. 32. P. 40–51. DOI: http://dx.doi.org/10.1016/j.aei.2016.12.002.
[11] Hausken K., Moxnes J.F The dynamics of crime and punishment // International Journal of Modern Physics C. 2005. Vol. 16, № 11. P. 1701-1732. DOI: http://dx.doi.org/10.1142/S0129183105008229.
[12] Becker G.S. The economics of crime. Cross Sections, Federal Reserve Bank of Richmond. 1995. Vol. 12. P. 8–15. URL: https://ideas.repec.org/a/fip/fedrcs/y1995ifallp8-15nv.12no.3.html (accessed: 27.04.2020).
[13] Bernoulli D. Experience of a new theory of measurement of lots. Theory of consumer behavior and demand. Milestones of economic thought. SPb.: School of Economics. 1999. Vol. 1, P.11–27.
[14] Danilov N.N. The course of mathematical economics. St. Petersburg: Lan. 2016. P. 116–118.
[15] Ganicheva, A.V. Mathematical models and methods for assessing events, situations and processes. St. Petersburg: Lan. 2017. P. 107–110.
[16] Dolan M., Doyle M. Violence risk prediction: Clinical and actuarial measures and the role of the Psychopathy Checklist. The British Journal of Psychiatry. 2000. Vol. 177, No 4. P. 303–311. DOI: http://dx.doi.org/10.1192/bjp.177.4.303.
[17] The Prosecutor General's Office compiled a portrait of a typical Russian hacker vedomosti.ru URL:https://www.vedomosti.ru/technology/news/2018/12/11/788967-sostavila/ (accessed: 27.04.2020) (in Russian).
[18] Cybercrime and cyberconflicts. TADVISER.RU URL: http://www.tadviser.ru/index.php/Article:Cybercrime_and_kiberconflicts_:_Russia/ (accessed: 27.04.2020) (in Russian).
[19] Ehrlich I. Participation in illegitimate activities: theoretical and empirical investigation. J. of Publ. Econ. 1973. Vol. 81. No 3. P. 521—565.
[20] Losses of banks from cybercrime. TADVISER.RU URL: http://www.tadviser.ru/index.php/Article:Losses_of_banks_from cybercrime (accessed: 27.04.2020) (in Russian).
[21] Report of the Center for Monitoring and Response to Computer Attacks in the Credit and Financial Sphere of the Information Security Department of the Bank of Russia 1.09.2017 – 08.31.2018. CRB.RU. URL: https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf/ (accessed: 27.04.2020) (in Russian).
[22] Overview of the main types of computer attacks in the financial sector in 2018. CRB.RU. URL: https://cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf/ (accessed: 27.04.2020) (in Russian).

Поступила в редакцию – 27 апреля 2020 г. Окончательный вариант – 25 мая 2020 г
Received – April 27, 2020. The final version – May 25, 2020.