МНОГОФАКТОРНАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

*Минаков В.Ф., Шепелёва О.Ю., Лобанов О.С.**

Ключевые слова: *угрозы, опасности, несанкционированный доступ, модель, эффективность.*

Аннотация.

Цель работы: *разработка математической модель и интегральной оценки вероятности обеспечения безопасного состояния информационных ресурсов компании в условиях угроз и опасностей несанкционированного доступа к коммерческой конфиденциальной информации.*

Методы: *комплексные аналитические и экспертные методы систематизации и математическое моделирование экономических отношений в цифровой экономике.*

Результаты: *представленная модель отличается учетом влияния ресурсных факторов обеспечения информационной безопасности, а также фактора времени. На основе предложенной математической модели построена зависимость вероятности обеспечения защищенного состояния информационных ресурсов компании в заданном диапазоне временных и ресурсных показателей. Установлена высокая эффективность совместного использования факторов времени и ресурсов для повышения вероятности безубыточной работы компании посредством снижения рисков возникновения ущербов в результате несанкционированного доступа к конфиденциальной коммерческой информации. Обоснована возможность использования модели в задачах стратегического управления деятельностью компании.*

DOI: 10.21681/1994-1404-2020-1-40-46

Введение

Современные процессы цифровизации распространяются не только на локальные технологические операции предприятий, но и на взаимодействие субъектов экономики [1—3]. Это процедуры формирования предложений товаров, работ и услуг производителями, их выбор потребителями и формирование запросов на их приобретение. Таким образом, посредством цифровых ресурсов обеспечивается управление потоками материальных и трудовых ресурсов [4, 5]. Оплата товаров и услуг также производится чаще по безналичному расчету (электронными платежами). Для этого используются как банковские услуги: платежные системы, дистанционное банковское обслуживание в системах «клиент-банк», посредством банковских карт и т. д., так и сервисы замкнутых платежных систем «Яндекс-Деньги», Web-Money и др. Доля безналичных расчетов примерно равна доле наличных, причем у обладателей банковских карт эта доля составляет 90% (по данным Центробанка России). Важно также, что цифровые технологии трансформировали экономические процессы. Информационно-коммуникационные технологии (ИКТ) играют системообразующую роль. Так, финансовые, транспортные, маркетинговые агрегаторы стали фактором сближения и конвергенции участников экономических процессов. Именно цифровые платформы агрегаторов обеспечивают согласование интересов потребителей и производителей товаров и услуг, обеспечивая принятие и исполнение решений о сделках, запуске бизнес-процессов, управлении ресурсами хозяйственной деятельности [6, 7].

В таких условиях растут возможности несанкционированного доступа к материальным и финансовым ресурсам, и, соответственно, число компьютерных

* ***Минаков Владимир Фёдорович,*** *доктор технических наук, профессор кафедры информатики, Санкт-Петербургский государственный экономический университет, Российская Федерация, г. Санкт-Петербург.*
E-mail: m-m-m-m-m@mail.ru

Шепелёва Ольга Юрьевна, *ассистент кафедры информатики, Санкт-Петербургский государственный экономический университет, Российская Федерация, г. Санкт-Петербург.*
E-mail: shepeleva-olga@list.ru

Лобанов Олег Сергеевич, *кандидат экономических наук, доцент кафедры информатики, Санкт-Петербургский государственный экономический университет, Российская Федерация, г. Санкт-Петербург.*
E-mail: thelobanoff@gmail.com

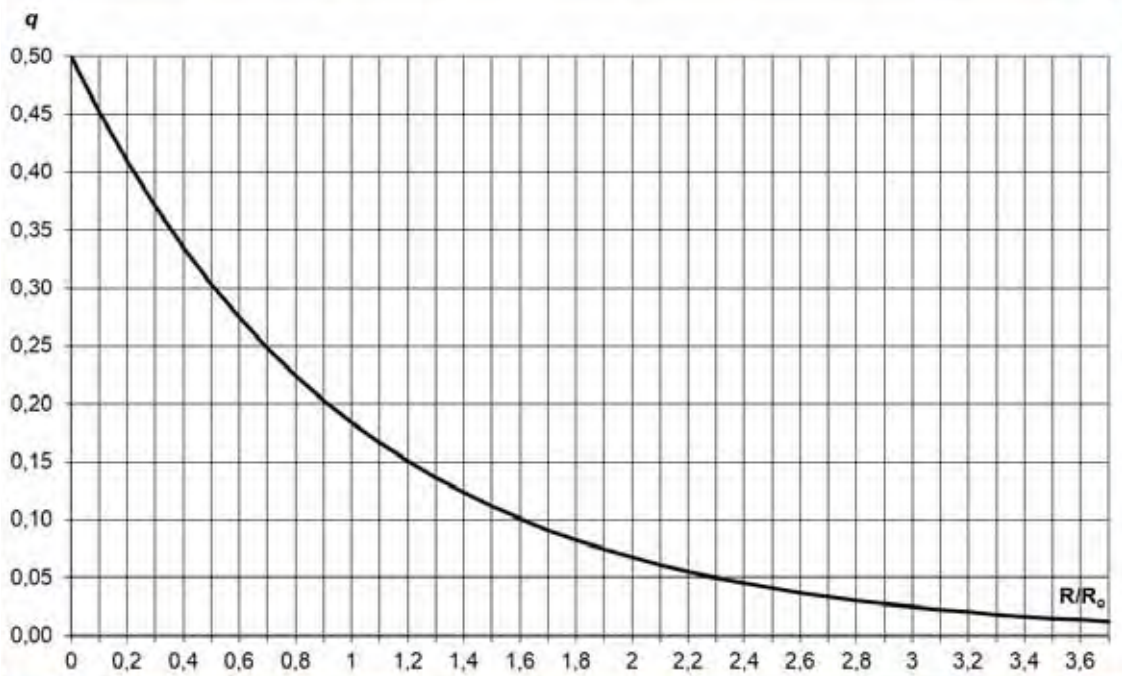

Рис. 1. Зависимость вероятности компьютерных преступлений от затрат на средства обеспечения информационной безопасности

преступлений в отношении управления перечисленными ресурсами [8—10]. Только прямой финансовый ущерб от компьютерных преступлений за 2018 год, по расчетам специалистов компании McAfee, составил свыше 600 миллиардов долларов США, а ущерб с учетом потерь репутации, срыва сделок и, соответственно, упущенной выгоды — 3 триллиона долларов США. Следовательно, актуальность обеспечения информационной безопасности в экономике возрастает [11, 12]. Не случайно так растет интерес к прорывным информационным технологиям: например, распределенным реестрам (блокчейн) и криптовалютам, их эмитентам и платежам с их использованием. Аналогичные процессы наблюдаются в системах смарт-контрактов.

Целью данного исследования стала разработка модели ресурсного динамического обеспечения безопасности в цифровой экономике. Надежность системы безопасности информационных ресурсов экономических объектов предопределяется функционированием средств защиты в условиях угроз и опасностей несанкционированного доступа. Анализ таких средств [8—14] позволяет установить, что они направлены на решение задач a) выявления; b) предотвращения; c) нейтрализации; d) пресечения; e) локализации; f) уничтожения; g) отражения; h) локализации последствий. Каждая из функциональных информационных систем, решающая названный класс задач, требует от предприятия затрат на приобретение, внедрение и сопровождение средств компьютерной безопасности.

Следовательно, для решения каждой задачи необходимы инвестиции. Очевидно, класс средств защиты снижает вероятность q компьютерного преступления в *k* раз:

$$q_1(R) = q_0/k(R_1), q_2(R) = q_0/k(R_1)/k(R_2)\ldots \quad (1)$$

где R-стоимость средств безопасности.

Для средневзвешенного значения затрат

$$R = (R_1 + R_2 + \ldots + R_n)/N\ , \quad (2)$$

имеем среднее значение k и, следовательно, получаем в общем виде

$$q(R) = q_0/k^R = q_0 \cdot k^{-R} \quad (3)$$

Выразим кратность через фиксирование основание натурального логарифма e через соотношение

$$k^{-R} = e^{-R/R_o} \quad (4)$$

где R_o — численное значение затрат, обеспечивающее снижение вероятности q в e раз:

$$q(R) = q_0 \cdot e^{-R/R_o} \quad (5)$$

Характер зависимости $q(R)$ представлен на рис. 1.

Рисунок 1 показывает, что затраты на информационную безопасность асимптотически снижают вероятность киберпреступлений. Действительно, добиться абсолютной безопасности с нулевым значением вероятности совершения злоумышленных действий в виртуальном пространстве невозможно [15].

Учитывая, что сумма вероятностей безопасной работы информационных ресурсов p и вероятности реализации компьютерных преступлений q:

$$q(R) + p(R) = 1\ , \quad (6)$$

получаем

$$p(R) = 1 - q(R), \quad (7)$$

Таким образом, показатель надежности — вероятность безотказной работы системы защиты — описывается зависимостью от объема ресурсного обеспечения средствами безопасности: программным и аппаратным обеспечением, разработкой новых методов, организационными механизмами и пр. [16]. Это можно выразить формулой:

$$p(R) = p_{max1} \cdot \left(1 - e^{-R/R_0}\right), \quad (8)$$

где $e \approx 2{,}71828$,

p, p_{max1} — вероятности (текущее и максимально возможное значение) успешного противодействия угрозам и опасностям совершения компьютерного преступления и, соответственно, вызванного им экономического ущерба при базовом варианте обеспечения информационной безопасности.

Очевидно, что использование дополнительных средств защиты в виде инновационных решений, для которых не созданы средства взлома в силу неизвестности принципа действия и характеристик нововведений, повышает вероятность состояния защищенности на некоторую величину p_{max2}, причем $p_{max1} + p_{max2} = p_{max}$. Иначе: $p_{max} = p_{max} \cdot (a_1 + a_2)$. В [14, с. 54] получена «зависимость вероятности обеспечения защиты» во времени в форме сигмоиды. Представим сигмоиду вероятностей функцией вида

$$p(t) = \frac{p_{max2}}{1 + e^{d - t/T}} \quad (9)$$

где T постоянная времени изменения эффекта защиты в условиях эксплуатации средства безопасности;

$e \approx 2{,}71828$,

d — число постоянных времени смещения медианного значения сигмоиды относительно начала времени отсчета.

Теперь с учетом одновременного влияния ранее использованных средств защиты и инновационных решений получим результирующую вероятность обеспечения защиты в виде суммы компонент (в качестве примера использованы: постоянная времени T=2 года как средний период между обновлениями программного обеспечения в системе информационной безопасности, R_0=4, $a_1 = 0{,}5$; $a_2 = 0{,}5$):

$$p(t,R) = \frac{0{,}5}{1 + e^{4 - t/2}} + 0{,}5 \cdot \left(1 - e^{-R/4}\right), \quad (10)$$

На рис. 1 визуализирован эффект повышения вероятности противодействия ущербам от несанкционированных доступов к коммерческой конфиденциальной информации. Как видно из рисунка, рост вероятности защищенности цифровых ресурсов существенно зависит от соотношения времени и ресурсного обеспечения информационной безопасности. Это позволяет закладывать проектные решения на основе решения задачи обеспечения требуемого уровня рисков, определяя такое соотношение ресурсов (а следовательно, и затрат) и времени реализации проекта, которое в наибольшей степени отвечает целям компании, возможностям реализации проекта в соответствии со стратегией ее деятельности [17—19]. Более того, полученная зависимость является инструментом построения поля сценариев для принятия управленческих решений по обеспечению безопасного состояния не только информационных, но и финансовых, а также материальных ресурсов компании [20—22]. Очевидно, что соотношение между эффектами повышения вероятности предотвращения несанкционированного доступа a_1 и a_2 может на основе полученной модели выбираться и оптимизационным путем, когда модель может использоваться в интегральных показателях деятельности компании в течение определенного времени.

Важно отметить, что развитие парадигмы ресурсно-затратного вида на обеспечение информационной безопасности фактором влияния времени приводит

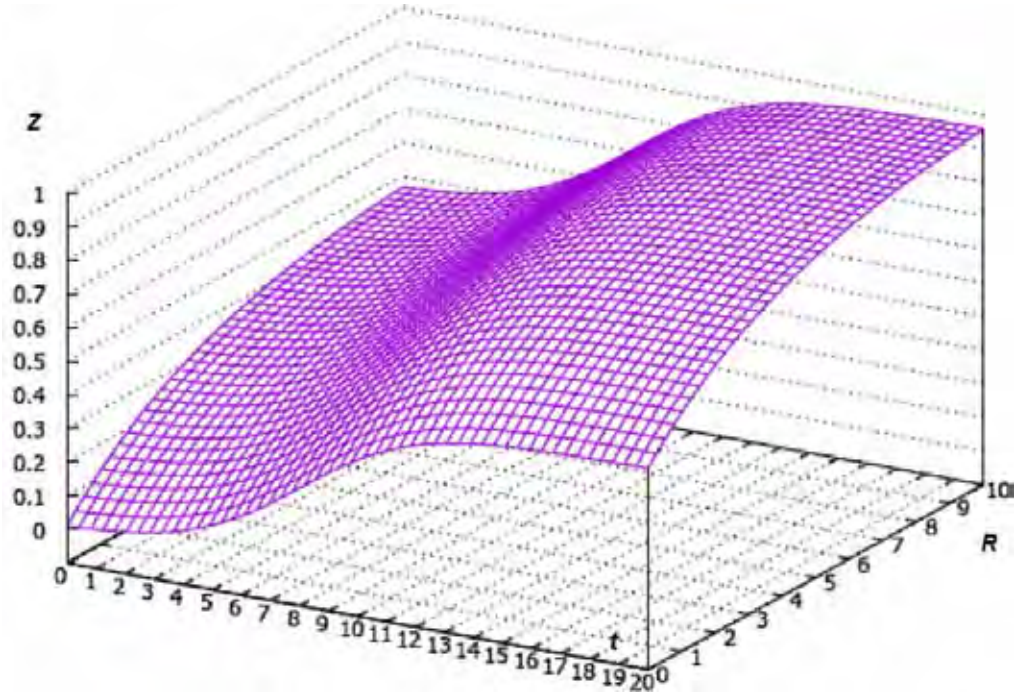

Рис. 2. Влияние ресурсов (R) ***и времени*** (t) ***на вероятность обеспечения безопасного состояния***

к обобщенной модели. Действительно, подстановка в предложенную модель единственного численного значения времени (например, текущего момента времени) приводит к частному случаю решения задачи обеспечения информационной безопасности, например, при оперативном управлении. Для задач тактического управления в среднесрочной перспективе задаются интервалы времени, определяемые тактическими целями. Для разработки стратегии развития системы безопасности предприятия модель может быть использована на длительных временных интервалах, в течение которых требуется достижение долгосрочный целей.

Кроме того, фиксируя расчетный момент времени, получаем модель вариативных решений в части выбора целесообразных инвестиций в ресурсы информационной безопасности, — например, для выбора альтернативных проектов, предлагаемых аутсорсерами информационной безопасности [16].

Модель аналитического вида выгодно отличается от представления процессов управления информационной безопасностью системами дифференциальных уравнений, во-первых, возможностью ее практического использования. Действительно, офисные приложения (включая облачные) позволяют любому пользователю выполнить расчеты, используя стандартные функции, например, табличных процессоров, и на их основе оценить альтернативные варианты решений проблемы обеспечения информационной безопасности. Важно, что, независимо от вида средств защиты, используемых в них методов, конечным показателем, оцениваемым моделью, является результат в форме оценки достигаемой вероятности безопасной работы информационных ресурсов предприятий, их объединений, органов государственной власти и многих других структур. Модель инвариантна к видам их деятельности, отраслям экономики, формам собственности и прочим особенностям.

Свойство инвариантности расширяет границы применимости предложенной модели. Она остается справедливой к новым, не представленным на современном рынке, разработкам. Это свойство имеет особую ценность в связи с беспрецедентной динамикой рынка информационно-коммуникационных систем и технологий. Во-первых, согласно закономерности, установленной Гордоном Муром применительно к концентрации активных ключей в аппаратной части микропроцессоров и дополненной Давидом Хаусом наблюдениями за динамикой роста производительности вычислительных средств, каждые 18 и 24 месяца вдвое возрастают соответственно первый и второй показатели. Следовательно, использование злоумышленниками более мощных вычислительных мощностей даже на основе метода простого перебора снижает вероятность сохранения защищенного состояния информационных систем предприятий. Во-вторых, сформировались и стремительно развиваются инновационные направления цифровизации экономики на основе смарт-технологий, обработки больших объемов данных, технологий M2M, интеллектуальных систем, облачных сервисов, платформ и инфраструктур и ряд других. Эволюция таких информационных технологий делает непредсказуемыми новые критические для экономических процессов места уязвимостей. Вместе с тем разработки адекватных методов и средств защиты информации и цифровых бизнес-процессов ведутся с учетом новых видов угроз и опасностей информационной безопасности в режиме реального времени. Компании-разработчики таких средств всегда делают предложения потребителям с указанием сроков разработки и внедрения средств защиты информации, а также ценой продуктов. Названные показатели и являются исходными данными для разработанной модели. А ее использование позволяет на основе прямых расчетов получить количественные оценки достигаемого результата в части информационной безопасности.

Модель также может быть использована в дополнение к методам анализа иерархий, деревьев решений и многих других в системах поддержки принятия решений. Важно, что развитие названных методов существенно развивает принципы обоснованного принятия управленческих решений учетом фактора времени. Данное обстоятельство имеет решающее значение для обеспечения устойчивости предприятий, их развития.

Очевидно, что фактор времени играет решающую роль в управлении изменениями. Его количественный учет позволяет изменить парадигму тактического и стратегического управления деятельностью предприятия. Вместо отслеживания происходящих изменений и следования им с лагом по времени, представляется возможность формирования изменений, обеспечивая предприятию конкурентные преимущества за счет первенства осуществления изменений. Не менее важно, что данная парадигма хорошо согласуется с методологиями проектного управления. Отметим, что традиционная парадигма проектного управления приводит, как показывает практика, к низкой реализуемости проектов. А инвестиции в разработку и реализацию проектов в хозяйственной деятельности предприятий существенно превосходят инвестиции в средства обеспечения информационной безопасности.

Выводы

Предложена модель интегральной оценки вероятности обеспечения безопасного состояния информационных ресурсов компании в условиях угроз и опасностей несанкционированного доступа к коммерческой конфиденциальной информации. Отличительной особенностью модели является учет фактора времени при использовании инновационных решений обеспечения информационной безопасности в дополнение к ресурсным факторам ее повышения, основанных на повышении затрат. Установлена достаточно высокая степень повышения вероятности безубыточной работы компании, превышающая в конкретном рассмо-

тренном примере эффект от ресурсного подхода к снижению рисков. Показана возможность использования модели в задачах стратегического управления деятельностью компании, управления проектами обеспечения информационной безопасности, а также оптимизации издержек. Достоверность предложенной модели подтверждается доказательством справедливости модели и строгими математическими выкладками.

Рецензент: ***Марков Алексей Сергеевич****, доктор технических наук, старший научный сотрудник, МГТУ им. Н.Э. Баумана, г. Москва, Россия.*
E-mail: a.markov@bmstu.ru

Литература

1. Бочков С.И., Макаренко Г.И., Федичев А.В. Об Окинавской хартии глобального информационного общества и задачах развития российских систем коммуникации // Правовая информатика. 2018. № 1. С. 4—14.
2. Минаков В.Ф., Шепелёва О.Ю., Шепелёв П.Ю. Феномен конвергенции информационных и материальных потоков в экономических процессах // Правовая информатика. 2018. № 3. С. 70—74.
3. Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V., Petrenko A.S. About Readiness for Digital Economy. In: Proceedings of the 2017 IEEE II International Conference on Control in Technical Systems, IEEE, CTS, 2017, pp. 96-99. DOI: 10.1109/CTSYS.2017.8109498.
4. Kravchenko N.A., Glinskiy V.V., Serga L.K., Anokhin N.V. Sources of high-tech business financing: experience of empirical research. Academy of Accounting and Financial Studies Journal, 2017, v. 21, No. 3, pp. 12-14.
5. Ивантер В.В., Белоусов Д.Р., Блохин А.А. и др. Структурно-инвестиционная политика в целях модернизации экономики России // Проблемы прогнозирования. 2017. № 4 (163). С. 3—16.
6. Glinskiy V., Serga L., Khvan M. Assessment of environmental parameters impact on the level of sustainable development of territories. In: Procedia CIRP 13. Ser. 13th Global Conference on Sustainable Manufacturing -- Decoupling Growth from Resource Use, 2016, pp. 626-631.
7. Glinskiy V., Serga L., Chemezova E., Zaykov K. Clusterization economy as a way to build sustainable development of the region. In: Procedia CIRP 13. Ser. 13th Global Conference on Sustainable Manufacturing -- Decoupling Growth from Resource Use, 2016, pp. 324-328.
8. Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети Интернет // Мониторинг правоприменения. 2016. № 1 (18). С. 41—53.
9. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18—23.
10. Степанов О.А. Правовое регулирование отношений в сфере безопасного функционирования и развития систем искусственного интеллекта: доктринальные аспекты // Правовая информатика. 2019. № 1. С. 56—63.
11. Dorofeev A.V., Markov A.S., Tsirlov V.L. Social media in identifying threats to ensure safe life in a modern city. Communications in Computer and Information Science, 2016, v. 674, pp. 441-449.
12. Maximov R., Krupenin A., Sharifullin S., Sokolovsky S. Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines. Voprosy kiberbezopasnosti [Cybersecurity issues], 2019, No. 1 (29), pp. 10-17, DOI: 10.21681/2311-3456-2019-1-10-17.
13. Астраханцев Р.Г., Лось А.Б., Мухамадиева Р.Ш. Анализ современных тенденций развития технологии «блокчейн» и цифровых валют // Вопросы кибербезопасности. 2019. № 5 (33). С. 57—62.
14. Мальцев Г.Н., Панкратов А.В., Лесняк Д.А. Исследование вероятностных характеристик изменения защищенности информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. 2015. № 1 (74). С. 50—58. DOI: 10.15217/issn1684-8853.2015.1.50.
15. Probabilistic Modeling in System Engineering. By ed. A. Kostogryzov, London: IntechOpen, 2018. 278 p.
16. Минаков В.Ф., Шепелёва О.Ю., Лобанов О.С. Ресурсно-временная модель повышения защищенности конфиденциальных данных // Сборник трудов Десятой международной научно-технической конференции «Безопасные информационные технологии» (Москва, 3—4 декабря 2019 г.). М. : МГТУ им. Н.Э. Баумана, 2019. С. 301—304.
17. Glinskiy V., Serga L., Zaykov K. Identification method of the russian federation arctic zone regions statistical aggregate as the object of strategy development and a source of sustainable growth. Procedia Manufacturing, 2017, v. 8, pp. 308-314.
18. Litvintseva G.P., Glinskiy V.V., Stukalenko E.A. Interregional differentiation of population incomes in the Russian Federation in the post-crisis period. Academy of Strategic Management Journal, 2017, v. 16, No. 4.
19. Glinskiy V., Serga L., Novikov A., Bulkina A., Litvintseva G. Investigation of correlation between the regions sustainability and territorial differentiation. Procedia Manufacturing, 2017, v. 8, pp. 323-329.

20. Borisov V.N., Kuvalin D.B., Pochukaeva O.V. Improving the factor efficiency of machinery in the regions of the Russian Federation. Studies on Russian Economic Development, 2018, v. 29, No. 4, pp. 377-386.
21. Borisov V.N., Pochukaeva O.V. Investment and innovative technological efficiency: Case study of the Arctic project. Studies on Russian Economic Development, 2017, v. 28, No. 2, pp. 169-179.
22. Ivanter V.V., Belkina T.D., Belousov D.R., Blokhin A.A., Borisov V.N. et al. Recovery of economic growth in Russia. Studies on Russian Economic Development, 2016, v. 27, No. 5, pp. 485-494.

A MULTI-FACTOR MODEL FOR ENSURING CONFIDENTIAL DATA SECURITY

Vladimir Minakov, *Dr.Sc. (Technology), Professor at the Department of Informatics, Saint Petersburg State University of Economics, Saint Petersburg, Russian Federation.*
E-mail: m-m-m-m-m@mail.ru

Ol'ga Shepeleva, *Assistant Professor at the Department of Informatics, Saint Petersburg State University of Economics, Saint Petersburg, Russian Federation.*
E-mail: shepeleva-olga@list.ru

Oleg Lobanov, *Ph.D. (Economics), Associate Professor at the Department of Informatics, Saint Petersburg State University of Economics, Saint Petersburg, Russian Federation.*
E-mail: thelobanoff@gmail.com

Keywords: *threats, dangers, unauthorised access, model, efficiency.*

Abstract.

Purpose of the work: *working out a mathematical model and integrated estimate of the probability of ensuring a safe state of the company's information resources under the condition of threats and danger of unauthorised access to commercial confidential information.*

Method used: *complex analytical and expert methods of systematisation and mathematical modelling of economic relations in digital economy.*

Results obtained: *the presented model is notable for taking into account the influence of resource factors for ensuring information security as well as the time factor. Based on the proposed mathematical model, the relationship of the probability of ensuring a protected state of the company's information resources in a given range of time and resource indicators is built. A high efficiency of the joint use of time and resource factors for increasing the probability of the company's profitable operation by means of reducing the risk of damages arising from unauthorised access to confidential commercial information is established. A justification is given for the feasibility of using the model in tasks of strategic management of the company.*

References

1. Bochkov S.I., Makarenko G.I., Fedichev A.V. Ob Okinavskoi khartii global'nogo informatsionnogo obshchestva i zadachakh razvitiia rossiiskikh sistem kommunikatsii. Pravovaia informatika, 2018, No. 1, pp. 4-14.
2. Minakov V.F., Shepeleva O.Iu., Shepelev P.Iu. Fenomen konvergentsii informatsionnykh i material'nykh potokov v ekonomicheskikh protsessakh. Pravovaia informatika, 2018, No. 3, pp. 70-74.
3. Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V., Petrenko A.S. About Readiness for Digital Economy. In: Proceedings of the 2017 IEEE II International Conference on Control in Technical Systems, IEEE, CTS, 2017, pp. 96-99. DOI: 10.1109/CTSYS.2017.8109498.
4. Kravchenko N.A., Glinskiy V.V., Serga L.K., Anokhin N.V. Sources of high-tech business financing: experience of empirical research. Academy of Accounting and Financial Studies Journal, 2017, v. 21, No. 3, pp. 12-14.
5. Ivanter V.V., Belousov D.R., Blokhin A.A. i dr. Strukturno-investitsionnaia politika v tseliakh modernizatsii ekonomiki Rossii. Problemy prognozirovaniia, 2017, No. 4 (163), pp. 3-16.
6. Glinskiy V., Serga L., Khvan M. Assessment of environmental parameters impact on the level of sustainable development of territories. In: Procedia CIRP 13. Ser. 13th Global Conference on Sustainable Manufacturing -- Decoupling Growth from Resource Use, 2016, pp. 626-631.
7. Glinskiy V., Serga L., Chemezova E., Zaykov K. Clusterization economy as a way to build sustainable development of the region. In: Procedia CIRP 13. Ser. 13th Global Conference on Sustainable Manufacturing -- Decoupling Growth from Resource Use, 2016, pp. 324-328.

8. Dorofeev A.V., Markov A.S. Strukturirovannyi monitoring otkrytykh personal'nykh dannykh v seti Internet. Monitoring pravoprimeneniia, 2016, No. 1 (18), pp. 41-53.
9. Kartskhiia A.A., Makarenko G.I., Sergin M.Iu. Sovremennye trendy kiberugroz i transformatsiia poniatiia kiberbezopasnosti v usloviiakh tsifrovizatsii sistemy prava. Voprosy kiberbezopasnosti, 2019, No. 3 (31), pp. 18-23.
10. Stepanov O.A. Pravovoe regulirovanie otnoshenii v sfere bezopasnogo funktsionirovaniia i razvitiia sistem iskusstvennogo intellekta: doktrinal'nye aspekty. Pravovaia informatika, 2019, No. 1, pp. 56-63.
11. Dorofeev A.V., Markov A.S., Tsirlov V.L. Social media in identifying threats to ensure safe life in a modern city. Communications in Computer and Information Science, 2016, v. 674, pp. 441-449.
12. Maximov R., Krupenin A., Sharifullin S., Sokolovsky S. Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines. Voprosy kiberbezopasnosti [Cybersecurity issues], 2019, No. 1 (29), pp. 10-17, DOI: 10.21681/2311-3456-2019-1-10-17.
13. Astrakhantsev R.G., Los' A.B., Mukhamadieva R.Sh. Analiz sovremennykh tendentsii razvitiia tekhnologii "blokchein" i tsifrovykh valiut. Voprosy kiberbezopasnosti, 2019, No. 5 (33), pp. 57-62.
14. Mal'tsev G.N., Pankratov A.V., Lesniak D.A. Issledovanie veroiatnostnykh kharakteristik izmeneniia zashchishchennosti informatsionnoi sistemy ot nesanktsionirovannogo dostupa narushitelei. Informatsionno-upravliaiushchie sistemy, 2015, No. 1 (74), pp. 50-58, DOI: 10.15217/issn1684-8853.2015.1.50.
15. Probabilistic Modeling in System Engineering. By ed. A. Kostogryzov, London: IntechOpen, 2018. 278 pp.
16. Minakov V.F., Shepeleva O.Iu., Lobanov O.S. Resursno-vremennaia model' povysheniia zashchishchennosti konfidentsial'nykh dannykh. Sbornik trudov Desiatoi mezhdunarodnoi nauchno-tekhnicheskoi konferentsii "Bezopasnye informatsionnye tekhnologii" (Moskva, 3-4 dekabria 2019 g.), M. : MGTU im. N.E. Baumana, 2019, pp. 301-304.
17. Glinskiy V., Serga L., Zaykov K. Identification method of the russian federation arctic zone regions statistical aggregate as the object of strategy development and a source of sustainable growth. Procedia Manufacturing, 2017, v. 8, pp. 308-314.
18. Litvintseva G.P., Glinskiy V.V., Stukalenko E.A. Interregional differentiation of population incomes in the Russian Federation in the post-crisis period. Academy of Strategic Management Journal, 2017, v. 16, No. 4.
19. Glinskiy V., Serga L., Novikov A., Bulkina A., Litvintseva G. Investigation of correlation between the regions sustainability and territorial differentiation. Procedia Manufacturing, 2017, v. 8, pp. 323-329.
20. Borisov V.N., Kuvalin D.B., Pochukaeva O.V. Improving the factor efficiency of machinery in the regions of the Russian Federation. Studies on Russian Economic Development, 2018, v. 29, No. 4, pp. 377-386.
21. Borisov V.N., Pochukaeva O.V. Investment and innovative technological efficiency: Case study of the Arctic project. Studies on Russian Economic Development, 2017, v. 28, No. 2, pp. 169-179.
22. Ivanter V.V., Belkina T.D., Belousov D.R., Blokhin A.A., Borisov V.N. et al. Recovery of economic growth in Russia. Studies on Russian Economic Development, 2016, v. 27, No. 5, pp. 485-494.