§1 УПРАВЛЕНИЕ И ОБЕСПЕЧЕНИЕ СИСТЕМ БЕЗОПАСНОСТИ

Тумбинская М.В.

МОДЕЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ИНТЕРНЕТ-БАНКИНГА

Аннотация. *Исследование данной статьи посвящено информационной безопасности современных систем интернет-банкинга. Автор рассматривает эффективность и качество принятия управленческих решений по защите конфиденциальной информации в процессе реализации атак злоумышленников. Особое внимание в статье уделено математическому моделированию. Предложенные модели позволят минимизировать количество атак киберпреступников, оптимизировать и совершенствовать комплексную систему информационной безопасности организаций экономической и социальной сферы, повысить эффективность использования защищенной информационной системы интернет-банкинга, выбрать правильную стратегию развития услуги интернет-банкинга. В процессе исследования использовались методы системного анализа, математического моделирования, анализа иерархий, теории оптимизации, вероятностей и математической статистики. Предложена обобщенная структурная схема информационной системы интернет-банкинга, системная модель информационной системы интернет-банкинга, которая позволит оценить уровень защищенности системы, определяемый путем решения задачи поддержки принятия решений в слабо структурированной предметной области, характеризующейся разнотипными показателями. Предложена теоретико-множественная модель поддержки принятия решений при управлении информационной безопасностью информационных систем интернет-банкинга, позволяющая накапливать аналитическую информацию о реализуемых угрозах киберпреступниками, обеспечить автоматизированную поддержку принятия решений по вопросам нейтрализации атак киберпреступников, обеспечения мер защиты конфиденциальной информации, облегчить процесс выработки управляющих воздействий. Представлена формализация модели киберпреступника, характеризующаяся личностными па-*

DOI: 10.7256/2073-8560.2016.2.14211

раметрами нарушителя и сценариями действий по хищению конфиденциальной информации в информационной системе интернет-банкинга.

Ключевые слова: *защита информации, информационная система, интернет-банкинг, киберпреступник, поддержка принятия решений, моделирование, оптимизация, угрозы и атаки, управляющие воздействия, эффективностьtic security, World War I, National interests, National development priorities, Immaterial factors, Institutional theory, Geopolitics, Strategical branches, State regulation.*

Abstract. *The study of this paper is devoted to information security of modern systems of Internet banking. The author examines the efficiency and quality of management decision-making for the protection of confidential information in the course of implementation of malicious attacks. Particular attention is paid to mathematical modeling. The proposed model will minimize the number of cybercriminals, optimize and improve the comprehensive system of information security organizations of economic and social development, improve the efficiency of secure information systems Internet banking, choose the right strategy for the development of Internet banking services. The study used methods of system analysis, mathematical modeling, analytic hierarchy process, optimization theory, probability and mathematical statistics. A generalized block diagram of an information system of Internet banking, systemic model of information system Internet banking, which will assess the level of security of the system, determined by solving the problem of decision support in poorly structured domain, characterized by heterogeneous characteristics. Proposed a set-theoretic model of decision support in Information Security Management Information Systems Internet banking, allowing accumulate analytical information about ongoing threats cybercriminals provide automated support for decisions on matters of neutralization cybercriminals, measures to ensure the protection of confidential information, facilitate the development of operating influences. Formalization of the model is represented by cybercriminals, characterized by personal parameters offender and scenarios for the theft of confidential information in the information system of Internet banking.*

Key words: *optimization, modeling, decision support, cybercriminals, Internet banking, information system, information security, threats and attacks, efficiency, control actions.*

В настоящее время происходит масштабная информатизация и глобализация. Современные web-технологии дают возможность пользователям использовать online сервисы для распределения и оптимизации своих ресурсов, повышения качества жизнедеятельности, получения нового вида услуг.

Интернет-банкинг – новый вид услуги современной социально-экономической сферы, которая обладает множеством преимуществ и за ней большое будущее. Популярность данной услуги не вызывает сомнения. Анализ литературных источников [1, 3-6] показал, что существует прямая зависимость между полнотой функциональных возможностей и удобством использования информационных систем интернет-банкинга (чем больше функционала предлагает система интернет-банкинга, тем более дружественнее ее интерфейс). Обладатели (банковские организации) заинтересованы в совершенствовании, повышении качества обслуживания, расширении функциональных возможностей, информационной безопасности систем интернет-банкинга. Рисунок 1 [2] иллюстрирует заинтересованность банковских организаций в развитии собственных систем интернет-банкинга.

Массовое использование информационных систем интернет-банкинга порождает проблему киберпреступлений. Интернет-банкинг – легкая «добыча» для киберпреступников. Первые попытки кибероперацій по хищению денежных средств были сделаны мошенниками еще в 2009 году. Киберпреступники находят все более оригинальные алгоритмы по реализации атак на информационные системы интернет-банкинга и хищению денежных средств. На сегодняшний день при удачной атаке киберпреступник может получить практически неограниченные возможности по управлению уязвимой информационной системы интернет-банкинга. Анализ источников [7-12] свидетельствует о том, что, несмотря на интенсивные исследования в области разработки систем защиты информации, проблема обеспечения информационной безопасности остается чрезвычайно актуальной, требует разработки новых подходов к ее решению.

DOI: 10.7256/2073-8560.2016.2.14211

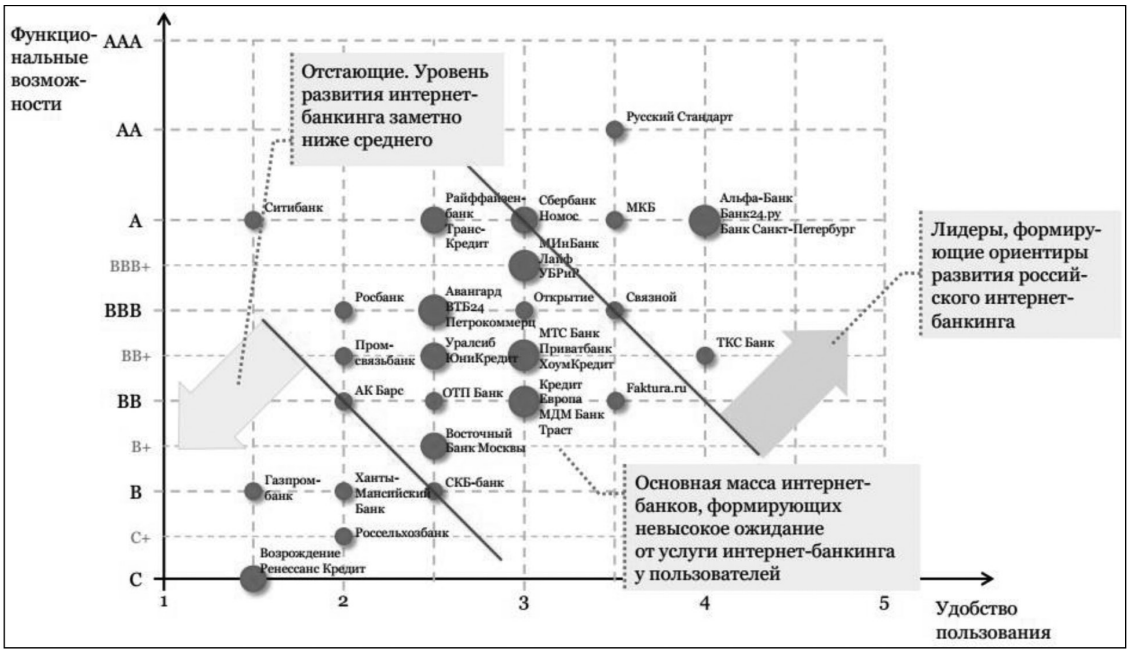

Рис. 1. Распределение банковский организаций по качеству систем интернет-банкинга

Анализ web-портала [4] показал, что киберпреступления в системах интернет-банкинга имеют тенденцию роста. Динамика статистических данных за 2014 год представлена на рисунке 2. Среднее значение количества персональных компьютеров, атакованных вредоносным программным обеспечением при использовании информационных систем интернет-банкинга составило 244380 шт.

Потенциальных нарушителей можно разделить на внутренних нарушителей из числа сотрудников банковской организации и внешних нарушителей – киберпреступников информационной системы интернет-банкинга. Предполагается, что потенциальный киберпреступник обладает высокой квалификацией, знаниями в IT-сфере, программно-аппаратными средствами реализации атаки.

В связи с этим возникает необходимость в грамотном выборе мер и средств обеспечения защиты информации в системах интернет-банкинга от умышленного разрушения, кражи, порчи, несанкционированного доступа, чтения и копирования киберпреступниками.

Предлагается модель системы поддержки принятия решений при управлении информационной безопасностью в информационных системах интернет-банкинга, использование которой обеспечит противодействие атакам киберпреступников, оптимизацию и совершенствование информационной безопасности, повышение

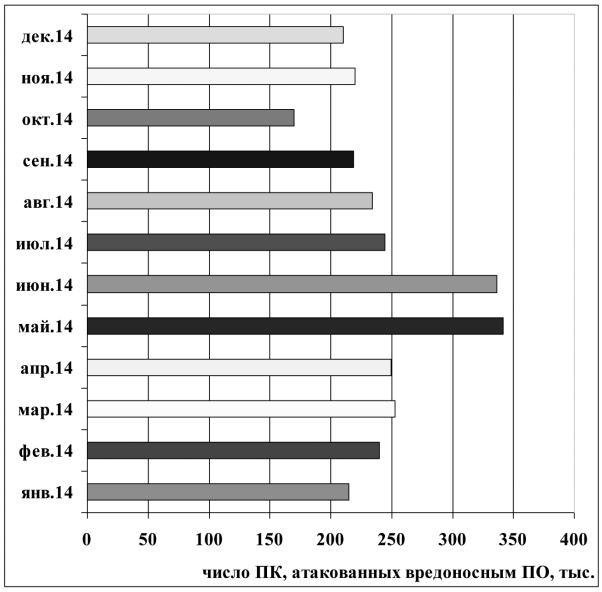

Рис. 2. Динамика статистических данных за 2014 год

эффективности использования защищенной информационной системы интернет-банкинга.

Программная реализация модели системы поддержки принятия решений может являться автономным модулем информационной системы интернет-банкинга, которая позволит вырабатывать рекомендации по обеспечению информационной безопасности системы интернет-банкинга. Модель системы поддержки принятия решений взаимодействует с моделью угроз, моделью киберпреступника на базе существующих (действующих) средств защиты

DOI: 10.7256/2073-8560.2016.2.14211

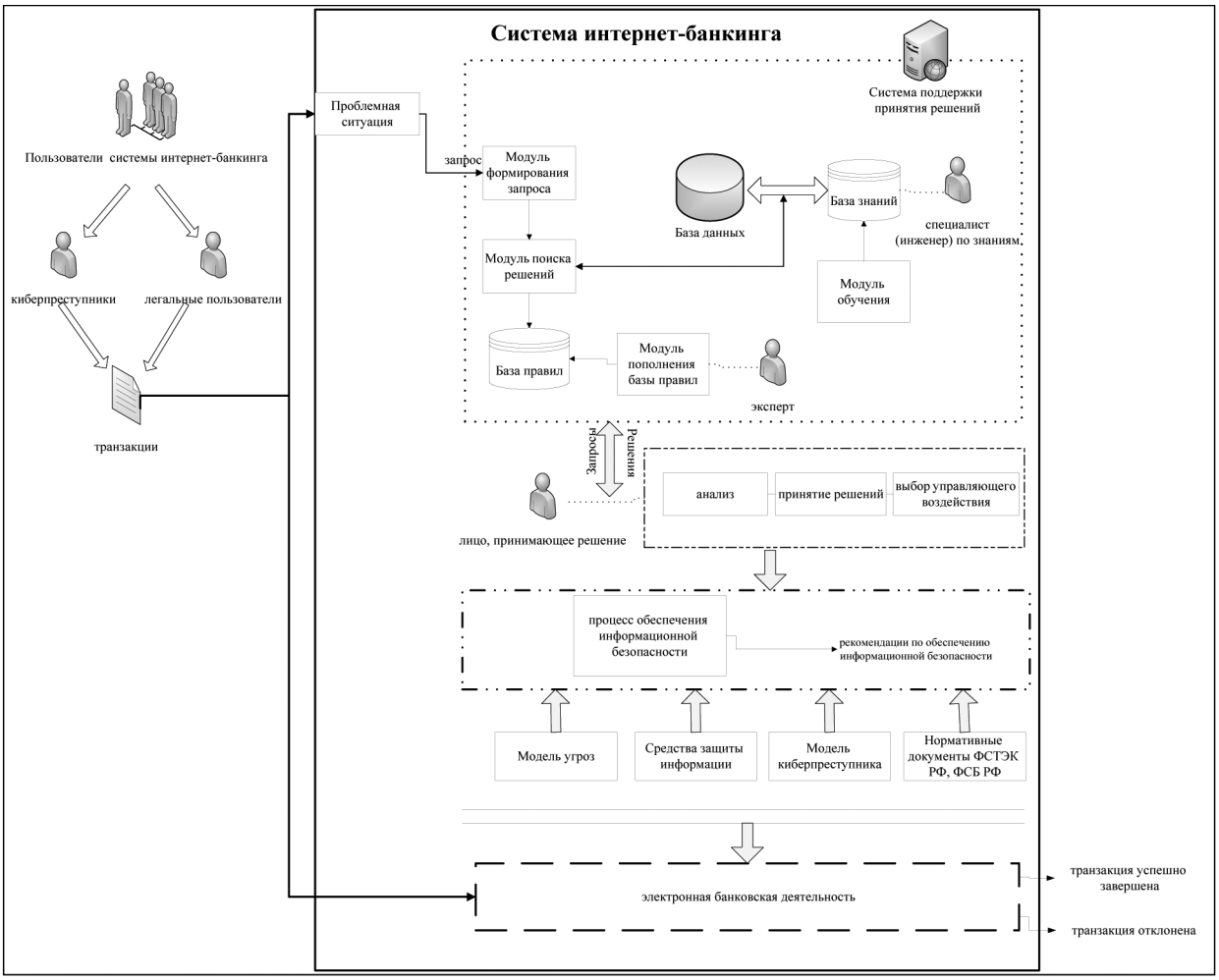

Рис. 3. Структурная схема информационной системы интернет-банкинга

информации и нормативных документов ФСБ РФ и ФСТЭК РФ. Структурная схема информационной системы интернет-банкинга представлена на рисунке 3.

Системную модель информационной системы интернет-банкинга можно представить в виде:

$$S^{ib} = \left\langle User, Tr, M^p, Pr, T_r^u \right\rangle, (1)$$

где $User$ – пользователи (клиенты) информационной системы интернет-банкинга,

$User = user_i \cup user_j$,

$user_i = \{user_1, user_2, ..., user_m\}$ – легальные пользователи информационной системы интернет-банкинга, $user_j = \{user_1, user_2, ..., user_s\}$ – киберпреступники информационной системы интернет-банкинга, $Tr = \{tr_1, tr_2, ..., tr_g\}$ – множество транзакций от пользователей $User$, Pr – параметр, характеризующий электронную банковскую деятельность, $T_r^u = \{0; 1\}$ – выходной параметр S^{ib}, $T_r^u = 1$ в случае, если транзакция выполнена успешно, $T_r^u = 0$ в противном случае, M^p – теоретико-множественная модель поддержки принятия решений при управлении информационной безопасностью информационных систем интернет-банкинга:

$$M^p = \left\langle L, N, \tilde{} \right\rangle, (2)$$

где L – входной параметр модели M^p, N – обобщенный параметр модели M^p, характеризующий процесс поддержки принятия решений, $\tilde{}$ – выходной параметр модели M^p – рекомендации по обеспечению информационной безопасности информационной системы интернет-банкинга, $\tilde{} = \left\{ q_f \mid f = \overline{1, w} \right\}$, q_1 – рекомендации по совершенствованию аппаратной защиты информации, q_2 – рекомендации по совершенствованию программной защиты информации, θ_3 – рекомендации по совершенствованию организационно-правовой части защиты информации, q_4 – рекомендации по совершенствованию физической защиты информации.

DOI: 10.7256/2073-8560.2016.2.14211

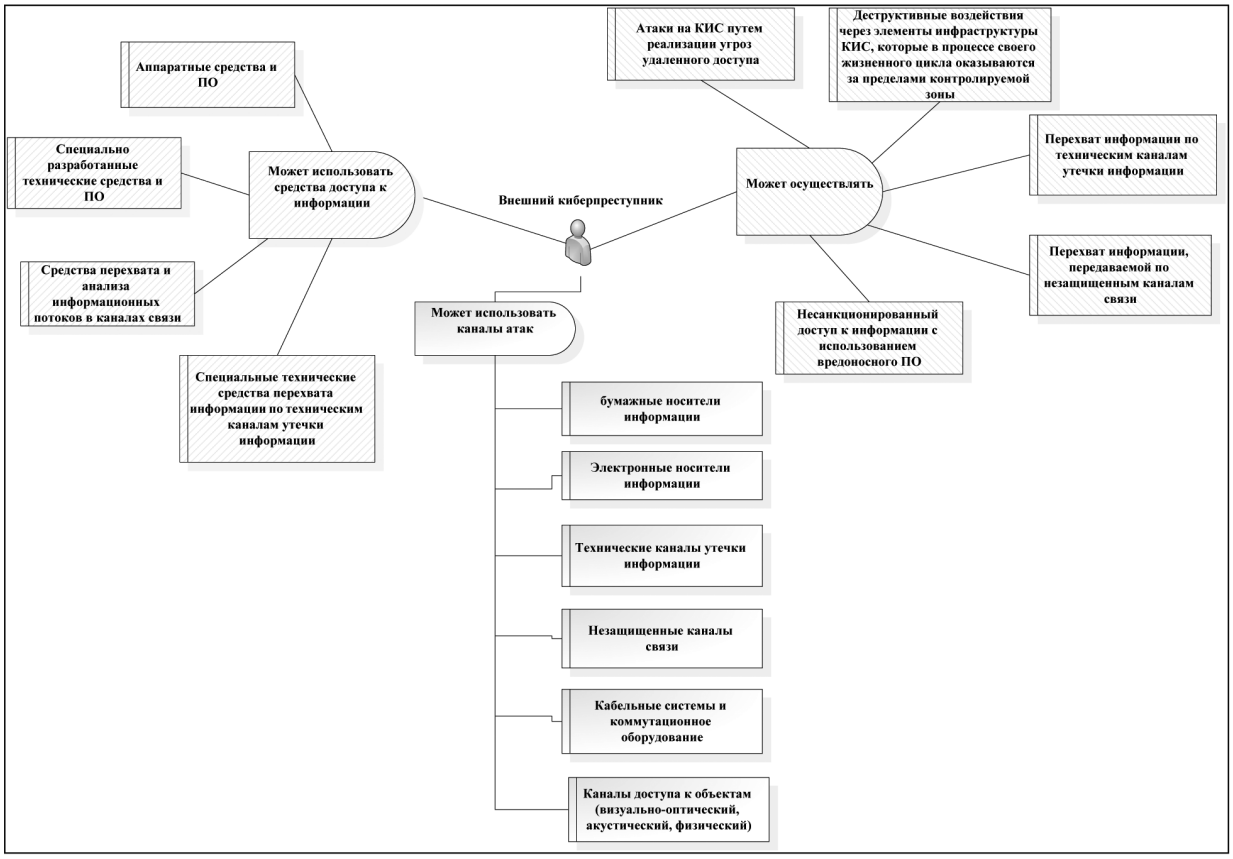

Рис. 4. Возможности внешнего киберпреступника

Входной параметр модели M^p можно представить в виде выражения (3).

$$L = \left\langle Z^{user}, M^{ug}, S_z, Y, M^k, ND \right\rangle, (3)$$

где Z^{user} – запрос (проблемная ситуация), M^{ug} – модель угроз, на основе которой определяется вероятность реализации угроз p^j в информационной системе интернет-банкинга, $b: M^{ug} \to p^j$, $p^j = \{p^1, p^2, p^3\}$, $p^1 = \{0;1\}$, $p^1 = 1$ в случае, если вероятность угроз в информационной системе интернет-банкинга очень высокая, $p^1 = 0$ в случае, если вероятность угроз в информационной системе интернет-банкинга очень низкая, $p^2 = \{0;1\}$, $p^2 = 1$ в случае, если вероятность угроз в информационной системе интернет-банкинга высокая, $p^2 = 0$ в случае, если вероятность угроз в информационной системе интернет-банкинга низкая, $p^3 = \{0;1\}$, $p^3 = 1$ в случае, если вероятность угроз в информационной системе интернет-банкинга соответствует среднему значению, $p^3 = 0$ в случае, если вероятность угроз в информационной системе интернет-банкинга соответствует ниже среднего значения, S_z – наличие средств защиты информации, $S_z = \{s_{z_1}, s_{z_2}, s_{z_3}\}$, где s_{z_1} – средства защиты информации имеются в достаточном объеме, s_{z_2} – средства защиты информации имеются в ограниченном объеме, s_{z_3} – средства защиты информации отсутствуют, Y – предполагаемый ущерб от реализации угроз в информационной системе интернет-банкинга, $x: M^{ug} \times M^k \to Y$, M^k – модель киберпреступника, в основу которой заложены типовые образы киберпреступника, позволяющие определить потенциального нарушителя в информационной системе интернет-банкинга, $ND = \{nd_i \mid i = \overline{1,t}\}$ – нормативные документы ФСТЭК РФ, ФСБ РФ.

Обобщенный параметр N модели M^p можно представить в виде выражения (4):

$$N = \left\langle M^{sp}, B^{sp}, Z, R, User^{sp} \right\rangle, (4)$$

где, $M^{sp} = \{M^z, M^{pr}, M^{pbp}, M^{ob}\}$ множество модулей модели M^p, где M^z – модуль формирования запроса, M^{pr} – модуль поиска решений, M^{pbp} – модуль пополнения базы правил, M^{ob} – модуль обучения, $B^{sp} = \{B^d, B^z, B^p\}$ множество баз данных, правил и знаний модели M^p, B^d – база данных, B^z – база знаний, B^p – база правил, $Z = \{z_f \mid f = \overline{1,s}\}$ – запросы, $R = \{r_a \mid a = \overline{1,w}\}$ – решения, $User^{sp} = \{user_1^{sp}, user_2^{sp}, user_3^{sp}\}$ – пользователи системы поддержки принятия

DOI: 10.7256/2073-8560.2016.2.14211

решений, где $user_1^{sp}$ – специалист (инженер) по знаниям, $user_2^{sp}$ – эксперт, $user_3^{sp}$ – лицо, принимающее решение, $c: Z^{user} \to M^z$, $d: M^z \times M^{pr} \to B^p$, $e: M^{pbp} \times user_2^{sp} \to B^p$, $j: M^{ob} \times user_1^{sp} \to B^z$, $s: B^z \to B^d$, $y: B^z \times \left(B^d \times M^{ob}\right) \to M^{pr}$, $user_3^{sp} = \{h, t, s\}$, где h – процесс анализа, t – процесс принятия решений, s – процесс выбора управляющего воздействия, $p: Z \times h \times t \times s \to R$, $A: R \to \tilde{}$.

При использовании информационной системы интернет-банкинга будем рассматривать только внешнего киберпреступника, который может реализовать атаки на систему различными алгоритмами с использованием современных методов и средств получения конфиденциальной информации (рис. 4).

Модель киберпреступника можно представить в виде выражения (5):

$$M^k = \left\langle P^l, A^{ck}, Obr \right\rangle, \quad (5)$$

где P^l – личностные параметры киберпреступника, A^{ck} – сценарий действий хищения информации в информационных системах интернет-банкинга, Obr – образ киберпреступника, $i: P^l \times A^{ck} \to Obr$,
$P^l = \{V^k, W^k, Ch^k, Risk^k, OR^k, Rs^k\}$, где V^k – возраст, W^k – пол, Ch^k – мотивация, $Risk^k$ – риск, OR^k – опыт работы (знания) в IT-сфере, Rs^k – доступные ресурсы для реализации угрозы, $A^{ck} = \{a_1^{ck}, a_2^{ck}, ..., a_f^{ck},\}$ – множество сценариев хищения информации в S^{ib}, $Obr = \{obr_1, obr_2, ..., obr_y\}$.

Предложенные системная модель информационной системы интернет-банкинга, теоретико-множественная модель поддержки принятия решений при управлении информационной безопасностью информационных систем интернет-банкинга, модель киберпреступника позволит усовершенствовать систему защиты информации, рационально использовать современные методы и средства защиты информации, за счет которых увеличится мощность информационной безопасности информационной системы интернет-банкинга, увеличится эффективность и качество принятия управленческих решений по защите конфиденциальной информации.

БИБЛИОГРАФИЯ

1. ДБО-Системы дистанционного банковского обслуживания. [Электронный ресурс]: http://www.tadviser.ru (дата обращения 04.01.2015).
2. Лаборатория Касперского. Развитие информационных угроз. [Электронный ресурс]: http://securelist.ru/analysis/ (дата обращения 04.01.2015).
3. Щеглов К. А., Щеглов А. Ю. Защита от атак на повышение привилегий // Вестник компьютерных и информационных технологий. №1, 2015.
4. Царегородцев А.В. Анализ рисков безопасности данных в корпоративных сетях кредитно-финансовых организаций на основе облачных вычислений // Национальные интересы: приоритеты и безопасность. 2013. № 39.
5. Игонина Л.Л. Экономическая безопасность России в системе макроэкономических инвестиционных критериев // Национальные интересы: приоритеты и безопасность. 2013. № 2.
6. Крутиков В.К., Зайцев Ю.В., Огай Г.Р. Возникновение внутренних угроз: неразрывная связь экономической и социально-психологической безопасности // Национальные интересы: приоритеты и безопасность. 2014. № 37.
7. В.М. Елин. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. №2(24).
8. Я.Н. Лаврушина, А.А. Макарова, А.В. Куликов. Построение модели количественной оценки операционного риска (технический риск – сбой в предоставлении IT-услуг) в статистически некорректной среде // Бизнес-информатика. 2012. № 2(20).
9. Крупные компании не защищены даже от неквалифицированных киберпреступников [Электронный ресурс]: http://www.crn.ru/news/detail.php?ID=87552 (дата обращения 10.01.2015).
10. Бородин А.В. Архитектура информационной системы поддержки принятия решений по управлению персоналом розничной подсистемы коммерческого банка // Программные системы и вычислительные методы. – 2014. – 2. – С. 174 – 190. DOI: 10.7256/2305-6061.2014.2.12331.
11. Загузов Г.В. Административно-правовые средства обеспечения информационной безопасности и защиты информации в Российской Федерации // Административное и муниципальное право. – 2010. – 5. – С. 44 – 47.

DOI: 10.7256/2073-8560.2016.2.14211

12. Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В. Сценарный анализ эффективности управления региональной безопасностью // Национальная безопасность / nota bene. – 2014. – 2. – С. 188 – 206. DOI: 10.7256/2073-8560.2014.2.11319.
13. Смирнов В.И. Оценки защищенности речевой информации в выделенном помещении с помощью инструментально-расчетного метода // Кибернетика и программирование. – 2012. – 2. – С. 18 – 24. URL: http://www.e-notabene.ru/kp/article_13869.html
14. Коробейников А.Г., Гришенцев А.Ю., Кутузов И.М., Пирожникова О.И., Соколов К.О., Литвинов Д.Ю. Разработка математической и имитационной моделей для расчета оценки защищенности объекта информатизации от несанкционированного физического проникновения // Кибернетика и программирование. – 2014. – 5. – С. 14 – 25. DOI: 10.7256/2306-4196.2014.5.12889. URL: http://www.e-notabene.ru/kp/article_12889.html

REFERENCES

1. DBO-Sistemy distantsionnogo bankovskogo obsluzhivaniya. [Elektronnyi resurs]: http://www.tadviser.ru (data obrashcheniya 04.01.2015).
2. Laboratoriya Kasperskogo. Razvitie informatsionnykh ugroz. [Elektronnyi resurs]: http:// securelist.ru/analysis/ (data obrashcheniya 04.01.2015).
3. Shcheglov K. A., Shcheglov A. Yu. Zashchita ot atak na povyshenie privilegii // Vestnik komp'yuternykh i informatsionnykh tekhnologii. №1, 2015.
4. Tsaregorodtsev A.V. Analiz riskov bezopasnosti dannykh v korporativnykh setyakh kreditno-finansovykh organizatsii na osnove oblachnykh vychislenii // Natsional'nye interesy: prioritety i bezopasnost'. 2013. № 39.
5. Igonina L.L. Ekonomicheskaya bezopasnost' Rossii v sisteme makroekonomicheskikh investitsionnykh kriteriev // Natsional'nye interesy: prioritety i bezopasnost'. 2013. № 2.
6. Krutikov V.K., Zaitsev Yu.V., Ogai G.R. Vozniknovenie vnutrennikh ugroz: nerazryvnaya svyaz' ekonomicheskoi i sotsial'no-psikhologicheskoi bezopasnosti // Natsional'nye interesy: prioritety i bezopasnost'. 2014. № 37.
7. V.M. Elin. Moshennichestvo v sfere komp'yuternoi informatsii kak novyi sostav prestupleniya // Biznes-informatika. 2013. №2(24).
8. Ya.N. Lavrushina, A.A. Makarova, A.V. Kulikov. Postroenie modeli kolichestvennoi otsenki operatsionnogo riska (tekhnicheskii risk – sboi v predostavlenii IT-uslug) v statisticheski nekorrektnoi srede // Biznes-informatika. 2012. № 2(20).
9. Krupnye kompanii ne zashchishcheny dazhe ot nekvalifitsirovannykh kiberprestupnikov [Elektronnyi resurs]: http://www.crn.ru/news/detail.php?ID=87552 (data obrashcheniya 10.01.2015).
10. Borodin A.V. Arkhitektura informatsionnoi sistemy podderzhki prinyatiya reshenii po upravleniyu personalom roznichnoi podsistemy kommercheskogo banka // Programmnye sistemy i vychislitel'nye metody. – 2014. – 2. – С. 174 – 190. DOI: 10.7256/2305-6061.2014.2.12331.
11. Zaguzov G.V. Administrativno-pravovye sredstva obespecheniya informatsionnoi bezopasnosti i zashchity informatsii v Rossiiskoi Federatsii // Administrativnoe i munitsipal'noe pravo. – 2010. – 5. – С. 44 – 47.
12. Shul'ts V.L., Kul'ba V.V., Shelkov A.B., Chernov I.V. Stsenarnyi analiz effektivnosti upravleniya regional'noi bezopasnost'yu // Natsional'naya bezopasnost' / nota bene. – 2014. – 2. – С. 188 – 206. DOI: 10.7256/2073-8560.2014.2.11319.
13. Smirnov V.I. Otsenki zashchishchennosti rechevoi informatsii v vydelennom pomeshchenii s pomoshch'yu instrumental'no-raschetnogo metoda // Kibernetika i programmirovanie. – 2012. – 2. – С. 18 – 24. URL: http://www.e-notabene.ru/kp/article_13869.html
14. Korobeinikov A.G., Grishentsev A.Yu., Kutuzov I.M., Pirozhnikova O.I., Sokolov K.O., Litvinov D.Yu. Razrabotka matematicheskoi i imitatsionnoi modelei dlya rascheta otsenki zashchishchennosti ob"ekta informatizatsii ot nesanktsionirovannogo fizicheskogo proniknoveniya // Kibernetika i programmirovanie. – 2014. – 5. – С. 14 – 25. DOI: 10.7256/2306-4196.2014.5.12889. URL: http://www.e-notabene.ru/kp/article_12889.html

DOI: 10.7256/2073-8560.2016.2.14211