DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.1.1

УДК 681.322
ББК 32.973

МОДЕЛЬ ПРОФИЛЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Светлана Сергеевна Козунова

Аспирант кафедры системы автоматизированного проектирования
и поискового конструирования,
Волгоградский государственный технический университет
cad@vstu.ru
просп. им. Ленина, 28, 400005 г. Волгоград, Российская Федерация

Аннотация. Рассматриваются аспекты управления угрозами информационной безопасности корпоративных информационных систем. Выделены уязвимости, характерные для корпоративных информационных систем. Определены источники угроз. Описаны потенциальные нарушители. Разработана уникальная модель профиля угроз информационной безопасности корпоративной информационной системы.

Ключевые слова: профиль угроз, задача классификации угроз, список угроз, источники угроз, уязвимости, корпоративная информационная система, управление, информационная безопасность.

Введение

Деятельность по обеспечению информационной безопасности (ИБ) в корпоративных информационных системах (КИС) приобретает большую популярность в современном обществе научно-технологического прогресса [8]. Актуальность построения защищенных КИС повышается из-за роста малых и больших предприятий, а также увеличения потребности в процедурах объединения организаций и предприятий в корпорации [8; 14]. Построение защищенных КИС основывается на оценке уровня ИБ в случае реализации угроз их информационным ресурсам [1; 4; 8]. Авторами работы [1] отмечено, что при реализации угроз ИБ предприятия несут материальные, репутационные и финансовые потери. Таким образом, базовой операцией при обеспечении ИБ КИС является разработка модели угроз, присущей данной КИС.

Связанные работы и предложенные решения

Изучением проблем управления угрозами ИБ КИС и их нейтрализации посвящены работы [2; 3; 6–11; 13]. Авторами публикации [2] описаны виды информационных угроз, на основании которых разработана классификация атак. Однако в работе [2] сделан акцент на SCADA-системах и сетевой безопасности. Авторы в исследовании [6] предлагают стратегию снижения уровня риска, основанную на менеджменте угроз. В частности, в [6] описаны следующие процедуры менеджмента угроз: уклонение от угрозы или ликвидация источника угрозы, снижение уровня уязвимостей за счет применения защитных мер, снижение негативных последствий от реализации угроз [6].

Впервые понятие профиля угроз было исследовано автором работы [3]. В [3] отмечено, что профиль угроз связан с жизненным циклом ИС и позволяет описать угрозы ИБ как качественно, так и формализовано. Анализ [7; 9; 13] показывает, что предпосылками к необходимости определения списка угроз является базовая процедура классификации информационный ресурсов (ИР). Так, для каждого ИР или группы ИР необходимо определить список угроз в соотношении конфиденциальности, целостности и доступности с целью выявления уязвимостей для каждой идентифицированной угрозы. Причиной этому является возможность реализации угрозы с использованием уязвимости [2; 11; 13]. Согласно исследованию [9], профиль угрозы описывается статичными атрибутами (принадлежность угрозы, способ реализации, объект защиты, источник угроз, уязвимость).

Задача классификации угроз ИБ корпоративной бизнес-системы особенно важна для систем, функционирующих на промышленных предприятиях и в конструкторских бюро [2; 13].

Таким образом, большинство проведенных исследований посвящены проблеме управления угрозами ИБ и их анализу в промышленных и информационных системах. Однако данная проблема в КИС практически не решена. Следовательно, существуют предпосылки в необходимости разработки профиля угроз, использование которого позволит реализовать риск-ориентированный подход [11]. Применяя список угроз ИБ, можно построить систему управления ИБ предприятия, что позволит инфраструктуре предприятия обладать свойством защищенности информации, использующейся в бизнес-процессах предприятия [13].

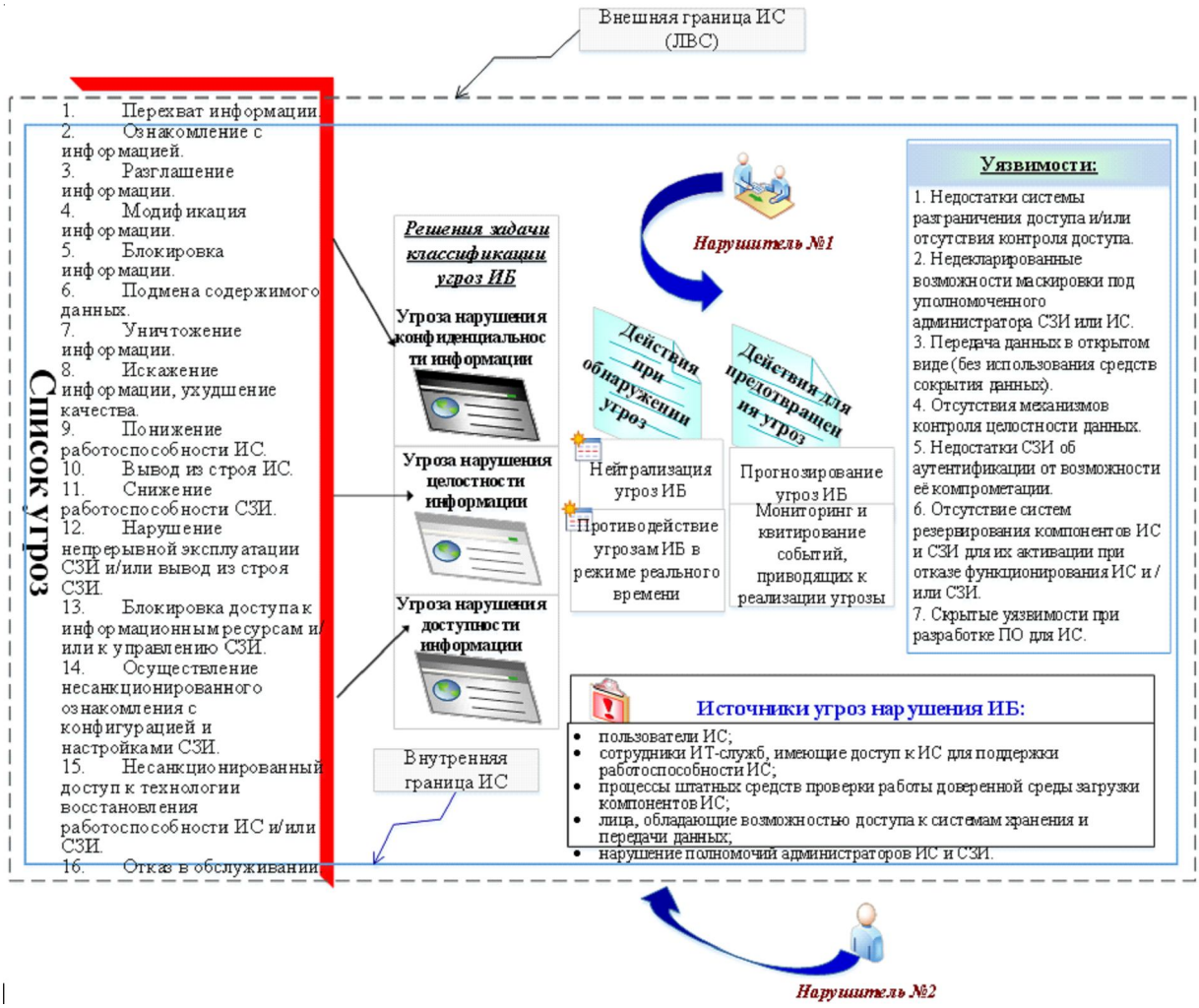
Предложенная модель

Авторами статьи предложена модель профиля угроз ИБ КИС (см. рисунок), основанная на объекте угроз и цели их реализации. Данное свойство угрозы описано авторами работы [8]. Целью реализации угроз (как единичной угрозы, так и совокупности угроз) является вывод из строя защитных механизмов КИС [8] и активация уязвимостей КИС [6; 12]. Исходя из этого, можно выделить основную цель функционирования системы защиты информации (СЗИ) КИС: противодействие угрозам безопасности КИС.

Модель (см. рисунок) описывает актуальные угрозы, характерные для КИС, используя компоненты: «список угроз», «источники угроз», «уязвимости». Данным угрозам сопоставимы семь уязвимостей, отталкиваясь от которых, злоумышленник может совершить атаку на КИС, ее компоненты и вычислительную сеть (ВС), в которой она функционирует. Профиль

угроз имеет поэтапное описание действий при необходимости обнаружить и предотвратить угрозы. В модели определены типы нарушителей: нарушитель № 1 – «внутренний», нарушитель № 2 – «внешний». Внутренний нарушитель – лицо, являющееся пользователем или администратором этой КИС. Внешним нарушителем могут быть сотрудники предприятия, не являющиеся пользователями КИС, или иные лица, не входящие в состав рабочего персонала предприятия. Область действия злоумышленников показана стрелкой (см. рисунок). Атакующие действия внешнего злоумышленника направлены на внешнюю границу КИС, в основном на ВС, информационные и коммуникационные технологии, СЗИ, расположенные на границе ВС для образования защищенной связи между ВС и КИС. Атакующие воздействия внутреннего злоумышленника производятся внутри КИС: на компоненты ИС, программные средства, прикладные приложения, базы данных, информационные ресурсы, средства разграничения доступа.

Направленность угроз ИБ формируется источником угроз. Для КИС характерны несколько таких источников, при разработке профилей защиты их было выделено пять: 1) пользователи информационной системы корпоративного типа или информационных систем, объединенные в единое звено управления; 2) сотрудники подразделений ИТ-служб, имеющие доступ к КИС для поддержки ее работоспособности; 3) функциональные процессы встроенных (штатных) средств проверки работы доверенной среды загрузки компонентов ИС; 4) лица, обладающие возможностью доступа к системам хранения и передачи данных; 5) нарушение полномочий администраторами ИС и СЗИ.



Модель профиля угроз информационной безопасности корпоративной информационной системы

Применение профиля угроз ИБ позволяет решить задачу классификации угроз ИБ путем их деления на три типа: нарушение целостности, доступности и конфиденциальности информации, что взаимосвязано с классификацией угроз безопасности, данной в работе [6], и позволяет выполнить рекомендации методики [14].

Заключение

От уровня обеспечения ИБ КИС зависит безопасность информационных активов предприятия, в котором внедрена КИС. Для защиты данных, обрабатываемых в КИС, целесообразно обеспечить ИБ самой системы, выделить и спрогнозировать угрозы нарушения ИБ. Такие меры обеспечат эффективное управление ИБ и качественное реагирование на угрозы КИС в режиме реального времени.

Таким образом, проведенные исследования проблем управления угрозами и обеспечения ИБ КИС позволили авторам статьи разработать модель профиля угроз ИБ КИС. Отличие от ранее предложенных моделей заключается в том, что предложенное решение определяет действия, которые необходимо предпринять при обнаружении угроз и для их предотвращения. Применение предложенной модели на практике позволит реализовать специальные процедуры менеджмента угроз ИБ предприятия, задействуя частные политики информационной безопасности для КИС.

СПИСОК ЛИТЕРАТУРЫ

1. Ажмухамедов, И. М. Оценка состояния защищенности данных организации в условиях возможности реализации угроз информационной безопасности / И. М. Ажмухамедов, О. М. Князева // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 3 (31). – С. 24–39.

2. Анализ информационных рисков в системах обработки данных на основе «туманных» вычислений / А. А. Финогеев, А. Г. Финогеев, И. С. Нефедова, Е. А. Финогеев, В. А. Камаев // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2015. – № 4. – С. 38–46.

3. Астахов, А. М. Искусство управления информационными рисками / А. М. Астахов. – М. : ДМК Пресс, 2010. – 314 с.

4. Бабенко, А. А. Information security model in the segment of corporate information system / А. А. Бабенко, С. С. Козунова // Информационные системы и технологии. – 2017. – № 1 (99). – С. 87–91.

5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : (выписка) : утв. заместителем директора ФСТЭК России 15 февр. 2008 г. – Электрон. текстовые дан. – Режим доступа: https://fstec.ru/component/attachments/download/289 (дата обращения: 06.02.2018). – Загл. с экрана.

6. Выборнова, О. Н. Синтез управленческих решений по снижению рисков в нечетких условиях при ограниченных ресурсах / О. Н. Выборнова, И. М. Ажмухамедов // Фундаментальные исследования. – 2016. – № 5 (ч. 1). – С. 18–22.

7. Козунова, С. С. Менеджмент угроз информационной безопасности информационных систем / С. С. Козунова // Концепции фундаментальных и прикладных научных исследований : сб. ст. по материалам Междунар. науч.-практ. конф. (г. Уфа, 9 дек. 2017 г.). В 6 ч. Ч. 3 / отв. ред.: А. А. Сукиасян. – Стерлитамак, 2017. – С. 69–71.

8. Козунова, С. С. Модель построения защищенной информационной системы корпоративного типа / С. С. Козунова, А. А. Бабенко // Информационные системы и технологии. – 2016. – № 3 (95). – С. 112–120.

9. Козунова, С. С. Управление рискоустойчивостью информационной системы конструкторского бюро / С. С. Козунова, А. Г. Кравец // Управление информационной безопасностью в современном обществе : материалы Всерос. молодежной науч. школы-конф. по проблемам информационной безопасности (г. Волгоград, 26–28 апр. 2017 г.) / редкол.: Е. А. Максимова, Ю. С. Бахрачева, В. В. Баранов. – Волгоград, 2017. – С. 203–207.

10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных : утв. заместителем директора ФСТЭК России 14 февр. 2008 г. – Электрон. текстовые дан. – Режим доступа: https://fstec.ru/component/attachments/download/290 (дата обращения: 06.02.2018). – Загл. с экрана.

11. Методы и модели оценки инфраструктуры системы защиты информации в корпоративных сетях промышленных предприятий : монография / П. П. Парамонов, А. Г. Коробейников, И. Б. Тронников, И. О. Жаринов. – СПб. : Студия «НП-Принт», 2012. – 115 с.

12. Моделирование сетевых атак злоумышленников в корпоративной информационной системе / В. А. Гнеушев, А. Г. Кравец, С. С. Козунова, А. А. Бабенко // Промышленные АСУ и контроллеры. – 2017. – № 6. – С. 51–60.

13. Нгуен, Т. Т. Система обмена сообщениями на основе протокола MQTT / Т. Т. Нгуен, А. Г. Кравец, Н. З. Буй // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства : материалы VI Всерос. науч.-практ. конф. (г. Волгоград, 27–28 апр. 2017 г.) / редкол.: Е. А. Максимова [и др.]. – Волгоград, 2017. – С. 133–138.

14. Шевцов, В. Ю. Особенности защищенного документооборота на предприятии / В. Ю. Шевцов, А. А. Бабенко, С. С. Козунова // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространтсва : материалы V Всерос. науч.-практ. конф. (г. Волгоград, 22–23 апр. 2016 г.). – Волгоград, 2016. – С. 237–341.

REFERENCES

1. Azhmukhamedov I.M., Knyazeva O.M. Otsenka sostoyaniya zashchishchennosti dannykh organizatsii v usloviyakh vozmozhnosti realizatsii ugroz informatsionnoy bezopasnosti [Assessment of the Condition of Data Security of the Organization in Terms of the Possibility of Implementing Threats to Information Security]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii*, 2015, no. 3 (31), pp. 24-39.

2. Finogeev A.A., Finogeev A.G., Nefedova I.S., Finogeev E.A., Kamaev V.A. Analiz informatsionnykh riskov v sistemakh obrabotki dannykh na osnove «tumannykh» vychisleniy [Analysis of Information Risks in Data Processing Systems Based on "Foggy" Calculations]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitelnaya tekhnika i informatika*, 2015, no. 4, pp. 38-46.

3. Astakhov A.M. *Iskusstvo upravleniya informatsionnymi riskami* [The Art of Information Risks Management]. Moscow, DMK Press, 2010. 314 p.

4. Babenko A.A., Kozunova S.S. Information security model in the segment of corporate information system. *Informatsionnye sistemy i tekhnologii*, 2017, no. 1 (99), pp. 87-91.

5. *Bazovaya model ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh (vypiska) utverzhdena zamestitelem direktora FSTEK Rossii 15 fevralya 2008 g.* [The Basic Model of Threats to Personal Data Security during Their Processing in Information Systems of Personal Data. Certified Extract Approved by the Deputy Director of FSTEC of Russia on February 15, 2008]. URL: https://fstec.ru/component/attachments/download/289 (accessed 6 February 2018).

6. Vybornova O.N., Azhmukhamedov I.M. Sintez upravlencheskikh resheniy po snizheniyu riskov v nechetkikh usloviyakh pri ogranichennykh resursakh [Synthesis of Managerial Decisions to Reduce Risks in the Conditions of Uncertainty at Limited Resources]. *Fundamentalnye issledovaniya*, 2016, no. 5 (part 1), pp. 18-22.

7. Kozunova S.S. Menedzhment ugroz informatsionnoy bezopasnosti informatsionnykh sistem [Management of Threats to Information Systems' Security]. Sukiasyan A.A., ed. *Kontseptsii fundamentalnykh i prikladnykh nauchnykh issledovaniy: sb. st. po mater. mezhdunar. nauch.-prakt. konf. (g. Ufa, 9 dek. 2017 g.). V 6 ch. Ch. 3* [Conceptions of Fundamental and Applied Scientific Research. Collected Proceedings of International Research and Practice Conference (Ufa, 9th December 2017). In 6 parts. Part 3]. Sterlitamak, Agency for International Research, 2017, pp. 69-71.

8. Kozunova S.S., Babenko A.A. Model postroeniya zashchishchennoy informatsionnoy sistemy korporativnogo tipa [The Model of Building a Secure Information System of Corporate Type]. *Informatsionnye sistemy i tekhnologii*, 2016, no. 3 (95), pp. 112-120.

9. Kozunova S.S., Kravets A.G. Upravlenie riskoustoychivostyu informatsionnoy sistemy konstruktorskogo byuro [Managing risk tolerance information systems design bureau]. Maksimova E.A., Bahracheva Yu.S., Baranov V.V., eds. *Upravlenie informatsionnoy bezopasnostyu v sovremennom obshchestve: mater. vseros. Molodezhnoy nauch. shkoly-konf. po problemam informatsionnoy bezopasnosti (g. Volgograd, 26-28 aprelya 2017 g.)* [Information Security Management in Modern Society: Proceedings of the All-Russian Youth Scientific School-Conference on the Problems of Information Security (Volgograd, April 26-28, 2017)]. Volgograd, Izd-vo VolGU, 2017, pp. 203-207.

10. *Metodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh utverzhdena zamestitelem direktora FSTEK Rossii 14 fevralya 2008 g.* [The Methodology for Determining Relevant Threats to Personal Data Security during Their Processing in Information Systems of Personal Data: Approved by the Deputy Director of FSTEC of Russia on 14 February 2008]. URL: https://fstec.ru/component/attachments/download/290 (accessed 6 February 2018).

11. Paramonov P.P., Korobeynikov A.G., Tronikov I.B., Zharinov I.O. *Metody i modeli otsenki infrastruktury sistemy zashchity informatsii v korporativnykh setyakh promyshlennykh predpriyatiy: monografiya* [Methods and Models for Assessing the Infrastructure of Information Security in Corporate Networks of Industrial Enterprises]. Saint Petersburg, NP-Print Publ., 2012. 115 p.

12. Gneushev V.A., Kravets A.G., Kozunova S.S., Babenko A.A. Modelirovanie setevykh atak zloumyshlennikov v korporativnoy informatsionnoy sisteme [Modeling of Malefactors' Network Attacks in the Corporate Information System]. *Promyshlennye ASU i kontrollery*, 2017, no. 6, pp. 51-60.

13. Nguen T.T., Kravets A.G., Buy N.Z. Sistema obmena soobshcheniyami na osnove protokola MQTT [The Messaging System Based on MQTT Protocol]. Maksimova E.A., Bahracheva Yu.S., Baranov V.V., eds. *Upravlenie informatsionnoy bezopasnostyu v sovremennom obshchestve: mater. vseros. Molodezhnoy nauch. shkoly-konf. po problemam informatsionnoy bezopasnosti (g. Volgograd, 26-28 aprelya 2017 g.)* [Information Security Management in Modern Society: Proceedings of the All-Russian Youth Scientific School-Conference on the Problems of Information Security (Volgograd, April 26-28, 2017)]. Volgograd, Izd-vo VolGU, 2017, pp. 133-138.

14. Shevtsov V.Yu., Babenko A.A., Kozunova S.S. Osobennosti zashchishchennogo dokumentooborota na predpriyatii [Features of Secure Document Management at the Enterprise]. *Aktualnye voprosy informatsionnoy bezopasnosti regionov v usloviyakh globalizatsii informatsionnogo prostrantsva: mater. V vseros. nauch.-prakt. konf. (g. Volgograd, 22-23 apr. 2016 g.)* [Relevant Issues of Information Security of Regions in the Globalization of Information Space: Proceedings of the 5th All-Russian Research and Practice Conference (Volgograd, 22-23 April 2016)]. Volgograd, 2016, pp. 237-341.

THE MODEL OF INFORMATION SECURITY THREAT PROFILE OF CORPORATE INFORMATION SYSTEM

Aleksey Aleksandrovich Babenko

Candidate of Sciences (Pedagogy), Associate Professor, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Svetlana Sergeevna Kozunova

Postgraduate Student, Department of Computer-Aided Design and Search Design,
Volgograd State Technical University
cad@vstu.ru
Prosp. Lenina, 28, 400005 Volgograd, Russian Federation

Abstract. The level of information security of corporate information systems depends on the security of information assets of the enterprise in which the enterprise information systems are implemented. To protect data processed in corporate information systems, it is advisable to ensure the information security of the system, to identify and predict threats to information security violations. Such measures will ensure effective management of information security and high-quality response to threats in corporate information systems in real time.

Thus, the research of threats management and information security of corporate information systems allows the authors to develop a model of threat profile. The difference from the previously proposed models is that the present solution defines the actions that need to be taken when threats are detected and to prevent them. Application of the proposed model will allow implementing special procedures of information security management of the enterprise, using private information security policies for corporate information systems.

The authors highlight the key aspects of managing threats to information security of corporate information systems. The vulnerabilities typical for corporate information systems have been allocated. The sources of threats have been formed, and the potential violators have been described. A unique model of the profile of threats to information security for corporate information system has been developed.

Key words: threat profile, the task of threats classification, list of threats, threat sources, vulnerabilities, corporate information system, control, information security.