УДК 004.056.5

В.М. Заичкин, С.П. Серёдкин

Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

РОЛЬ ПОЛИТИКИ БЕЗОПАСНОСТИ В ОБЕСПЕЧЕНИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ

Аннотация. *В статье обоснована необходимость формирования и внедрения политики информационной безопасности на предприятии в виду роста киберпреступлений за последние годы. Представлен анализ практических подходов при создании политик безопасности, а также описаны решения, предлагаемые компания, работающими в сфере информационной безопасности, помогающие создавать комплексную многоуровневую систему защиты информации. Дано формальное описание модели политики информационной безопасности на разных уровнях представления и обоснована необходимость ее реализации в виде виртуальной модели перед запуском на реальном объекте, если он входит в состав критически важной информационной инфраструктуры (КИИ). Проведен анализ требований руководящих документов для объектов КИИ, определяющих особенности разрабатываемых для них политик информационной безопасности. С целью оценки эффективности разработанных политик предлагается их тестирование на Национальных киберполигонах и оценка в соответствии с выбранной комплексной методикой оценки защищенности объекта КИИ.*
Ключевые слова: *информационная безопасность, политика информационной безопасности*.

V.M. Zaichkin, S.P. Seryodkin

Irkutsk State Transport University, Irkutsk, the Russian Federation

THE ROLE OF SECURITY POLICY IN ENSURING THE PROTECTION OF INFORMATION RESOURCES OF THE ENTERPRISE

Abstract. *The article substantiates the need for the formation and implementation of an information security policy at the enterprise in view of the growth of cybercrimes in recent years. The analysis of practical approaches to the creation of security policies is presented, as well as the solutions offered by companies working in the field of information security, helping to create a complex multi-level information protection system, are described. A formal description of the information security policy model at different levels of representation is given and the need for its implementation in the form of a virtual model before launching on a real object, if it is part of a critical information infrastructure (CII), is justified. The analysis of the requirements of the guidance documents for the CII objects defining the features of the information security policies developed for them is carried out. In order to assess the effectiveness of the developed policies, it is proposed to test them on National cyberpolygons and evaluate them in accordance with the selected comprehensive methodology for assessing the security of the CII object.*

Введение

Анализируя тенденцию роста киберпреступлений в Российской Федерации, можно сделать вывод, что злоумышленники постоянно усовершенствуют известные методы реализации кибератак или используют их совокупность с целью нанесения максимального ущерба информационным ресурсам системообразующих компаний с последующим блокированием их работы. Только за первые восемь месяцев 2019 года количество зарегистрированных киберпреступлений в России показало годовой рост на 66,8 % по данным Генпрокуратуры [1]. Зафиксированная негативная тенденция подтверждается увеличением с 4,4 % в 2017 г. до 25,8 % в 2021 г. удельного веса таких преступлений в общем числе зарегистрированных [2]. Таким образом, устойчивая и надежная работа предприятия невозможна при отсутствии функционирования на нем эффективной системы защиты информации и требует серьезного и профессионального подхода для ее реализации. Данная система включает в себя подсистему защиты информации от несанкционированного доступа, подсистему защиты информации от несанкционированных воздействий и подсистему антивирусной защиты, а также персонал, который управляет данными подсистемами в целом. Исходя из этого с каждым годом растёт потребность в специалистах в сфере информационной безопасности (далее по тексту –

ИБ), так как только высоко квалифицированные кадры, имеющие практический опыт в работе каждой из выше сказанных подсистем, могут добиться требуемого уровня защищенности информации. Начиная свою трудовую деятельность на предприятии, специалист по защите информации должен создать план, в котором определить последовательность своих действий в условиях производственной деятельности организации. Первостепенным мероприятием по реализации данного плана является разработка организационно-распорядительной документации или создания политики информационной безопасности (далее по тексту – ПИБ).

Роль ПИБ на предприятии и предлагаемые отечественные решения для ее обеспечения

Под ПИБ понимают формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области ИБ, которыми руководствуется организация в своей деятельности. Во многих организациях, которые заинтересованы в обеспечении ИБ, формируется иерархическая структура. На верхнем уровне данной структуры расположена концепция информационной безопасности. Содержание концепции раскрывается в частных ПИБ и других документах, обеспечивающих детальное разъяснение ее положений для персонала и контрагентов компании [3]. В работе [4] дается определение ПИБ как комплекса организационных, административных и технических мер, за каждое из которых несет ответственность отдельное подразделение.

Частные ПИБ могут быть одинаковые, пересекающиеся или дополняющие друг друга требования и процедуры. Последовательность и содержание этапов создания ПИБ являются типовыми и описаны в работе [5]. В работе [6] авторами утверждается, что использование ПИБ позволяет модернизировать многие направления деятельности предприятий и сделать их работу более эффективной, при этом в соответствии с требованиями международных стандартов в области ИБ содержание ПИБ должно в себя включать определенный перечень данных.

В сложившейся ситуации для предприятия наиболее проблемным является реализация второго (выбор оптимальных, экономически выгодных и внедряемых решений защиты ИБ) и пятого (проверка качества работы систем безопасности, их аудит и совершенствование) этапов, так как требуется адаптация к современным реалиям: закупить зарубежное сертифицированное программное обеспечение не представляется возможным, поэтому требуется переход на использование отечественных продуктов. В качестве лидеров в данном сегменте является «Лаборатория Касперского» и «Код безопасности».

Так на 9-м Национальном форуме информационной безопасности в Сочи в 2022 году «Лаборатория Касперского» представила программный продукт, объединяющий в себе функциональность средства антивирусной защиты и SIEM-системы, образуя многоэшелонированную систему защиты информации и контроля ее пользователей [7]. Таким образом, одна компания может оказывать полный спектр услуг по формированию оригинальных ПИБ для каждого предприятия индивидуально. Кроме того, статистика, приведенная в [8], показала, что основной причиной киберинцидентов является человеческая ошибка. Для решения данной проблемы также «Лаборатория Касперского» предлагает использование фишингового симулятора, позволяющего обучить персонал предприятия соблюдению ПИБ с последующим их контролем.

Формальное описание формирования ПИБ

Если рассматривать формирование ПИБ с формальной точки зрения, то каждая из них, принадлежащая множеству $P = \{p_1, p_2, ..., p_q\}, Q = \overline{1,q}$, при этом данное множество состоит из двух подмножеств $P = \{p_1, p_2, ..., p_n\}, N = \overline{1,n}$, где P_1 – подмножество ПИБ на уровне приложений, P_2 – подмножество ПИБ на сетевом уровне. Каждый p_q элемент множества формируется на основе взаимодействия между собой подмножества субъектов $S = \{s_1, s_2, ..., s_i\}, I = \overline{1,i}$ и информационных объектов $O = \{o_1, o_2, ..., o_j\}, J = \overline{1,j}$,при этом опре-

делены множества правил $R = \{r_1, r_2, ..., r_k\}, K = \overline{1,k}$, в соответствии с которыми для каждого из них существует хотя бы одно сюръективное отображение: $\exists r_k : O \to P, S \to P$.

При рассмотрении информационных объектов на сетевом уровне, то их взаимодействие можно представить в виде информационных потоков, которые устанавливаются между множеством сетевых узлов *N*. Формально описание данного взаимодействия можно представить в виде матрицы $M : O \to N$, где ее элементы могут быть, например, номера портов для функционирования конкретных приложений. В работе [9] утверждается, что к матричному виду может быть приведена любая формальная политика безопасности, так как контроль информационных потоков позволяет контролировать дискреционный и мандатный методы управления доступом.

Тестирование и оценка качества ПИБ на объектах критической информационной инфраструктуры

Вместе с этим в [10] предлагается на основе формальных моделей создавать виртуальные модели ПИБ, так как благодаря поэтапному тестированию данных моделей, учитывающих соответствующие потребности компаний, что позволяет сформировать новые виды ПИБ и проверить их работоспособность перед применением на реальных информационных объектах. Особенно актуальным является формирование виртуальных моделей на объектах критической информационной инфраструктуре (КИИ), так как в условиях проведения специальной военной операции данные объекты являются первостепенной целью для киберпреступников в виду возможности своими действиями нанести максимальный ущерб государству и обществу. Исходя из этого, система защиты информации на объектах КИИ должна создаваться на основе ПИБ, максимально приближенных и адаптированных к современным агрессивным условиям.

Для реализации выше сказанного требования правительство РФ обновила или же выпустила новые нормативно-правовые документы в области ИБ. Данные изменения включают в себя:

1. Правительство РФ своим постановлением № 2360 от 20.12.2022 приняло поправки в правила категорирования объектов КИИ и перечень показателей критериев значимости. Ряд изменений вступил в силу с 20 декабря 2022 года [11].

2. В России ввели административную ответственность за предоставление недостоверных сведений ФСТЭК России о результатах категорирования объектов КИИ. (№ 518-ФЗ от 19.12.2022) [12].

3. ФСБ России своим приказом № 543 от 01.11.2022 [13] утвердила трехлетний переходный период, в течение которого допускается осуществлять мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты в интересах субъектов КИИ на основании заключенных с НКЦКИ соглашений о сотрудничестве. По истечении этого периода, согласно Указу Президента РФ от 1 мая 2022 г. № 250, для проведения таких работ организации смогут подключать только аккредитованные центры ГосСОПКА. Предполагается, что за время переходного периода регулятор разработает необходимую нормативную правовую базу и проведет аккредитацию центров ГосСОПКА [14].

Эти наиболее важные изменения должны определять состав ПИБ и требования к категорированию объектов КИИ. Ведь степень категории значимости объектов определяет, состав требуемого класса средств защиты информации и степень ответственности за исполнение требований законодательства по обеспечению ИБ объектов КИИ. Чем выше категория значимости, тем более продвинутой должна быть система безопасности организации.

Таким образом, грамотно разработанные и своевременно обновляемые в соответствии с изменяющимися условиями ПИБ отражают мнение руководства по вопросу информационной безопасности и описывают реализацию методов защиты информации, позволяют разработать единые стандарты, регламентируют работу персонала. ПИБ являются незаменимой точкой старта, фундамента для дальнейшей разработки разного рода видов докумен-

тации по обеспечению безопасности на предприятии. Вместе с этим, для реализации 5 этапа по формированию ПИБ требуется проведение оценки качества предлагаемых решений.

С целью выработки конкретных рекомендаций для повышения защищенности объектов КИИ целесообразно тестирование ПИБ в масштабе киберполигонов, функционирующих на базе российских вузов, число которых к 2024 г. должно вырасти до 15 единиц [15]. В рамках данной работы в виду того, что тестированию подвергаются средства защиты информации обособленно, а не вся система в целом, предлагается новая методика экспериментальной оценки уровня защищенности информационных систем от компьютерных атак. Согласно разработанной методике рассчитывается интегральный качественный или количественный показатели уровня защищенности. Вместе с этим для применения данной методики требуются специалисты, имеющие опыт в создании и реализации сценарием компьютерных атак, осуществляемых хакерскими группировками в реальном мире. За рубежом в настоящее время уже известен опыт применения так называемых «этичных хакеров». Так, компания SIX утверждает, что деятельность данных специалистов позволяет выявить уязвимости в системе еще до того, как данные уязвимости обнаружат настоящие хакеры [16].

Таким образом, формирование и реализация ПИБ на предприятиях на основе отечественных решений и их тестирование с помощью киберполигонов на основе известной методики оценки позволит достичь требуемого законодательством РФ требуемого уровня защищенности.

Заключение

В данной статье рассмотрены подходы к созданию политики информационной. Представлено формальное описание процесса формирования ПИБ. Сделан вывод о необходимости использования на основе формальных моделей виртуальных моделей ПИБ. С целью обеспечения требуемого уровня безопасности компании для объектов КИИ необходимо строго руководствоваться требованиями нормативно-правовых актов РФ в сфере обеспечения информационной безопасности. С целью оценки качества разрабатываемых ПИБ целесообразно применять комплексную методику оценки защищенности информационных ресурсов на основе тестирования данных политик на инфраструктуре национальных киберполигонов. Кроме того, предложенный авторами статьи практический подход по созданию политики безопасности может быть полезен как студентам, так и сотрудникам предприятий, работающих в сфере защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басыня, Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия / Е. А. Басыня // Безопасность информационных технологий. – 2018. – Т. 25, № 4. – С. 42-51. – EDN YQNKOD.

2. Гончар, В. В. Основные проблемы расследования киберпреступлений и пути их решения / В. В. Гончар // Информационные технологии в деятельности органов внутренних дел: материалы Всероссийской научно-практической конференции, Москва, 13 октября 2022 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2022. – С. 75-78. – EDN RZGIBW.

3. Зайцев, С. Е. Политики информационной безопасности в системах информационной безопасности / С. Е. Зайцев // Научный вестник Московского государственного технического университета гражданской авиации. – 2008. – № 137. – С. 37-44. – EDN LPCYLL.

4. Ориова, Г. А. Разработка политики информационной безопасности компании / Г. А. Орипова, Э. Г. Харисова // Матрица научного познания. – 2020. – № 11-2. – С. 163-167. – EDN ALZBYT.

5. Михалева, М. Г. Разработка политики информационной безопасности компании / М. Г. Михалева // StudNet. – 2020. – Т. 3, № 3. – С. 374-379. – EDN XWGIUD.

6. Петренко, С. А. Политики безопасности компании при работе в Интернет / Петренко С.А., Курбатов В.А., - 3-е изд., (эл.) - Москва: ДМК Пресс, 2018. - 397 с.: ISBN 978-5-93700-

057-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/983161 (дата обращения: 23.11.2023). – Режим доступа: по подписке.

7. ИНФОФОРУМ-СОЧИ | 5-6 ИЮЛЯ 2022 9-Й ЮЖНЫЙ ФОРУМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ / [Электронный ресурс] // Инфофорум Национальный форум информационной безопасности: [сайт]. — URL: https://infoforum.ru/infoforum-sochi-2022 (дата обращения: 23.11.2023).

8. Кибепреступления: разнообразие и уголовное преследование / [Электронный ресурс] // securitymedia.org: [сайт]. — URL: https://securitymedia.org/info/kibeprestupleniya-raznoobrazie-i-ugolovnoe-presledovanie.html#:~:text=Статистика%20киберпреступлений%20за%202022%20год,их%20число%20составило%2010%20тысяч (дата обращения: 23.11.2023).

9. Ерохин, С. Д. Формальные методы построения многоуровневой политики безопасности / С. Д. Ерохин, А. Н. Петухов, П. Л. Пилюгин // Информационная безопасность: вчера, сегодня, завтра: Сборник статей по материалам V Международной научно-практической конференции, Москва, 14 апреля 2022 года. – Москва: Российский государственный гуманитарный университет, 2022. – С. 40-47. – EDN QMVDLM.

10. Шабалин, А. М. Построение виртуальной модели защиты корпоративной информации с использованием системы Infowatch Traffic Monitor / А. М. Шабалин, Е. А. Калиберда // Вестник кибернетики. – 2020. – № 1(37). – С. 35-42. – DOI 10.34822/1999-7604-2020-1-35-42. – EDN AMEUII.

11. Российская Федерация· Законы· Постановление Правительства Российской Федерации от 20 декабря 2022 г. № 2360 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127». https://www.garant.ru/products/ipo/prime/doc/405890219/

12. Российская Федерация. Законы. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон № 518-ФЗ [Принят государственной думой 13 декабря 2022 года: одобрен Советом Федерации 14 декабря 2022 года] / Доступен по адресу URL: http://publication.pravo.gov.ru/Document/View/0001202212190005.

13. Российская Федерация. Законы. Об определении переходного периода, предусмотренного подпунктом "б" пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. N 250: Приказ ФСБ России от 1 ноября 2022 г. N 543 [Зарегистрировано в Минюсте РФ 01.12.2022 N 71291]

14. Российская Федерация. Законы. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 1 мая 2022 № 250 / Доступен по адресу URL:http://www.kremlin.ru/acts/bank/47796.

15. Сизоненко, А. Б. Методика экспериментальной оценки уровня защищенности информационных систем от компьютерных атак на базе киберполигона / А. Б. Сизоненко, И. С. Рудь, А. О. Титарев // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2022. – № 6. – С. 52-66. – EDN HLFMRP.

16. Этичные хакеры на страже финансов: глава компании SIX представляет свой метод борьбы со злом / [Электронный ресурс] // SecurityLab.ru: [сайт]. — URL: https://www.securitylab.ru/news/543837.php (дата обращения: 23.11.2023).

REFERENCES

1. Basy`nya, E. A. Distributed system for collecting, processing and analyzing information security events of the enterprise network infrastructure / *Bezopasnost` informacionny`x texnologij* [Information technology security] – 2018. – vol. 25, no. 4. – pp. 42-51.

2. Gonchar, V. V. The main problems of cybercrime investigation and ways to solve them / *Informacionny`e texnologii v deyatel`nosti organov vnutrennix del: materialy` Vseros-sijskoj nauchno-prakticheskoj konferencii* [Information technologies in the activities of internal affairs bodies: materials of the All-Russian Scientific and Practical Conference] Moscow: Moscow Uni-

versity of the Ministry of Internal Affairs of the Russian Federation named after V.Ya. Kikot, 2022. – pp. 75-78.

3. Zajcev, S. E. Information security policies in information security systems / *Nauchny`j vestnik Moskovskogo gosudarstvennogo texnicheskogo universiteta grazhdanskoj aviacii* [Scientific Bulletin of the Moscow State Technical University of Civil Aviation] – 2008. – vol. 137. – pp. 37-44.

4. *Oriova, G. A., Kharisova E. G.* Development of the company's information security policy */ Matricza nauchnogo poznaniya* [The matrix of scientific knowledge] – 2020. – vol. 11-2. – pp. 163-167.

5. Mixaleva, M. G. Development of the company's information security policy / StudNet. – 2020. – vol. 3, no. 3. – pp. 374-379.

6. Petrenko, S. A., Kurbatov V.A Company's security policies when working on the Internet / 3rd ed., (e-mail) - Moscow: DMK Press, 2018. - 397 p.: ISBN 978-5-93700-057-6.

7. INFOFORUM-SOChI | 5-6 IYuLYa 2022 9-J YuZhNY`J FORUM INFORMACIONNOJ BEZOPASNOSTI (INFOFORUM-SOCHI | JULY 5-6, 2022 9TH SOUTHERN INFORMATION SECURITY FORUM) Available at: https://infoforum.ru/infoforum-sochi-2022 (accessed 23 November 2023).

8. Kibeprestupleniya: raznoobrazie i ugolovnoe presledovanie (Cybercrime: diversity and criminal prosecution) Available at: https://securitymedia.org/info/kibeprestupleniya-raznoobrazie-i-ugolovnoe-presledovanie.html#:~:text=Статистика%20киберпреступлений%20за%202022%20год,их%20число%20составило%2010%20тысяч (accessed 23 November 2023).

9. Eroxin, S. D., Petukhov A. N., Pilyugin P. L. Formal methods for building a multi-level security policy / Information security: yesterday, today, tomorrow: Collection of articles based on the materials of the V International Scientific and Practical Conference, Moscow, April 14, 2022. – Moscow: Russian State University for the Humanities, 2022. – pp. 40-47.

10. Shabalin, A. M., Kaliberda E. A. Building a virtual model of corporate information protection using the Infowatch Traffic Monitor system / Vestnik kibernetiki [Bulletin of Cybernetics]. – 2020. – vol. 1, no. 37. – pp. 35-42. – DOI 10.34822/1999-7604-2020-1-35-42.

11. The Russian Federation. Laws. Resolution of the Government of the Russian Federation of December 20, 2022 No. 2360 "On Amendments to the Resolution of the Government of the Russian Federation of February 8, 2018 No. 127". https://www.garant.ru/products/ipo/prime/doc/405890219.

12. The Russian Federation. Laws. On Amendments to Certain Legislative Acts of the Russian Federation: Federal Law No. 518-FZ [Adopted by the State Duma on December 13, 2022: approved by the Federation Council on December 14, 2022] / Accessed at URL: http://publication.pravo.gov.ru/Document/View/0001202212190005.

13. Russian Federation. Laws. On the definition of the transition period provided for by subparagraph "b" of paragraph 5 of the Decree of the President of the Russian Federation of May 1, 2022 N 250: Order of the FSB of Russia of November 1, 2022 N 543 [Registered with the Ministry of Justice of the Russian Federation 01.12.2022 N 71291].

14. Russian Federation. Laws. On additional measures to ensure information security of the Russian Federation: Decree of the President of the Russian Federation No. 250 dated May 1, 2022 / Available at URL:http://www.kremlin.ru/acts/bank/47796.

15. Sizonenko, A. B., Rud′ I. S. , A. O. Titarev The method of experimental assessment of the level of protection of information systems from computer attacks based on cyberpolygon / *Elektronnyy setevoy politematicheskiy zhurnal "Nauchnyye trudy KubGTU"* [Electronic network polythematic journal "Scientific works of KubSTU"] – 2022. – vol. 6. – pp. 52-66.

16. Etichnyye khakery na strazhe finansov: glava kompanii SIX predstavlyayet svoy me-tod bor′by so zlom (Ethical hackers on guard of finance: the head of SIX company presents his method of fighting evil) Available at: https://www.securitylab.ru/news/543837.php 2022 (accessed 23 November 2023).

Информация об авторах

Заичкин Владислав Михайлович – Студент 1-го курса магистратуры по специальности Информационная безопасность. Безопасность информационных систем и технологий, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: vlad_zaya99@mail.ru

Серёдкин Сергей Петрович – к. э. н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sseryodkin2008@yandex.ru.

Information about the authors

Zaichkin Vladislav Mikhailovich is a 1st–year Master's student in the specialty Information Security. Security of information systems and technologies, Irkutsk State Transport University, Irkutsk, e- mail: vlad_zaya@mail.ru

Seryodkin Sergei Petrovich – Ph. D. in Economics, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: sseryodkin2008@yandex.ru.