МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ВСЕРОССИЙСКАЯ ГРУППА ТЕОРИИ ИНФОРМАЦИИ IEEE
АКАДЕМИЯ ИНФОРМАТИЗАЦИИ ОБРАЗОВАНИЯ
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ООО «ОТКРЫТЫЕ РЕШЕНИЯ»
ОБЩЕСТВО «ЗНАНИЕ» РОССИИ
ПРИВОЛЖСКИЙ ДОМ ЗНАНИЙ

XXII Международная
научно-техническая конференция

ПРОБЛЕМЫ ИНФОРМАТИКИ В ОБРАЗОВАНИИ, УПРАВЛЕНИИ, ЭКОНОМИКЕ И ТЕХНИКЕ

Сборник статей

Декабрь 2022 г.

Пенза

УДК 004
ББК 32.81я43+74.263.2+65.050.2я43
П781

П781 **ПРОБЛЕМЫ ИНФОРМАТИКИ В ОБРАЗОВАНИИ, УПРАВЛЕНИИ, ЭКОНОМИКЕ И ТЕХНИКЕ :**
сборник статей XXII Международной научно-технической конференции. – Пенза: Приволжский Дом знаний, 2022. – 356 с.

ISBN 978-5-8356-1800-2
ISSN 2311-0406

Под редакцией ***В.И. Горбаченко,*** доктора технических наук, профессора;
В.В. Дрождина, кандидата технических наук, профессора

Информация об опубликованных статьях предоставлена в систему Российского индекса научного цитирования (РИНЦ) по договору № 573-03/2014К от 18.03.2014.

ISBN 978-5-8356-1800-2
ISSN 2311-0406

XXII International
scientific and technical conference

PROBLEMS OF INFORMATICS IN EDUCATION, MANAGEMENT, ECONOMICS AND TECHNICS

December, 2022

Penza

так и к группе лиц. Информационная защита обязана развиваться в разы быстрее, чем вся индустрия информационных войн, иначе мировых катастроф не избежать.

Абашкина Алиса Юрьевна
Яковлева Светлана Сергеевна
Поволжский государственный университет телекоммуникаций и информатики,
г. Самара, Россия

Abashkina A. Yu.
Yakovleva S. S.
Povolzhsky State University of Telecommunications and Informatics,
Samara, Russia

УДК 004

ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ РЕСУРСАМИ КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Ж.К. Алимсеитова, Б.С. Ахметов

DYNAMIC RESOURCE MANAGEMENT OF CYBER SECURITY OF INFORMATION OBJECTS

Zh.K. Alimseitova, B.S. Akhmetov

Аннотация. Рассматриваются вопросы повышения уровня защищенности объектов информатизации за счет оптимального распределения ресурсов защиты информации между объектами защиты с учетом действий злоумышленника. Полученные результаты и методология исследования могут быть использованы другими организациями для оптимального распределения ресурсов защиты информации между объектами защиты с учетом действий злоумышленника с целью повышения уровня защищенности объекта информатизации.

Ключевые слова: информационная безопасность, кибернетическая безопасность, защита информации, объект информатизации, объект защиты.

Abstract. The issues of increasing the level of security of informatization objects due to the optimal distribution of information protection resources between the objects of protection, taking into account the actions of an intruder, are considered. The results obtained and the methodology of the study can be used by other organizations for the optimal distribution of information

protection resources between the objects of protection, taking into account the actions of the attacker in order to increase the level of security of the informatization object.

Key words: information security, cyber security, information security, informatization object, protection object.

Одним из актуальных направлений, которое активно развивается в последнее десятилетие в сфере информационной и кибернетической безопасности (далее соответственно, ИБ и КБ) является выявление кибератак и предотвращения вторжений в информационно-коммуникационные системы объектов информатизации со стороны неавторизованной стороны. Как показывают ежегодные аналитические отчеты ведущих компаний, специализирующихся на проблематике кибербезопасности [1, 2], атаки на распределенные информационно-коммуникационные системы объектов информатизации с каждым годом становятся все совершеннее. Современные кибернетические атаки стали глобальными [1]. А периодичность крупных целевых (так называемых таргетированных) атак становится более частой, чем, например, это фиксировалось 10–15 лет назад.

Массированные кибернетические атаки породили целую волну инновационных исследований в области обеспечения информационной и кибернетической безопасности различных объектов информатизации. А также инициировали разработку и создание специальных средств защиты информации. Для обнаружения сетевых вторжений специалисты в области кибербезопасности сегодня используют целый арсенал современных методов [1, 3], моделей [3], средств [4], программного обеспечения [5]. Широко стали применяться и комплексные технические решения [6]. Перспективным и достаточно новым направлением исследований в этой области стали работы по развитию методов, моделей и программных комплексов систем поддержки принятия решений (СППР) [7] и экспертных систем в области ИБ и КБ.

Такое увеличение и усложнение средств защиты информации приводит к увеличению стоимости ресурсов стороны защиты, что, в свою очередь, актуализирует проблему их эффективного распределения и оптимального использования.

Анализ научных работ [2-4] в области моделирования управления ресурсами стороны защиты информации показывает, что основные усилия сосредоточены на определении объема инвестиций в защиту. Вопросам распределения этих инвестиций между объектами защиты посвящены единичные исследования. Кроме того, существующие разработки редко учитывают влияние возможных действий злоумышленника и их последствий на

изменение показателей и характеристик ИС на ОБИ. Такими показателями могут быть доля потерянной информации, которая определяет эффективность системы защиты, прибыль от внесения инвестиций в защиту информации, их рентабельность и тому подобное.

Таким образом, для построения эффективной СЗИ необходимо учитывать достаточно большое количество показателей, которые в комплексе и определяют ее эффективность. В результате мы приходим к многокритериальной задаче. Решение подобной задачи – это всегда компромисс в удовлетворении требований по отдельным показателям. При решении подобных многокритериальных задач, всегда стоит дилемма выбора алгоритмов решения [7]. Особенно это касается задач, связанных с защитой информации, поскольку действия стороны защиты в большинстве происходят в условиях неопределенности. Заметим, при нечетком подходе недостаточная осведомленность может привести к тому, что решение не будет получено, а поставленная цель защиты ОБИ не может быть обеспечена в достаточной степени при заданных ограничениях.

Распределение ограниченных ресурсов стороны защиты (материальных, людских, финансовых и др.) надлежащим образом составляет сущность многих направлений исследования в области кибернетической (КБ) или информационной безопасности (ИБ) [6]. Эта задача имеет несколько аспектов и требует определенных знаний о ситуации, которая предопределяет выбор методики решения и конечный результат. К таким знаниям о каждом из объектов защиты относятся: количество, качество и значимость информационных ресурсов (далее ИР); имеющийся уровень защищённости ИР; количество ресурсов (материальных, финансовых, людских, др.), которые может направить сторона (или стороны) нападения с учетом ожидаемой вероятности события; количество ресурсов, необходимых для достаточной защищенности ИР; количество ресурсов, которые может выделить сторона защиты объекта информатизации (ОБИ); допустимый уровень риска потери ИР.

Проблематика динамического управления ресурсами стороны защиты ОБИ – это не только чисто техническая задача, которая решается путем увеличения числа компонентов защиты в контурах кибербезопасности ОБИ [6-7]. Но это также и управленческая задача. Причем вторая составлявшая задачи связана с таким понятием как менеджмент ИБ и КБ, основной задачей которого является оптимизация не только технических, но экономических показателей эффективности функционирования СЗИ для ОБИ.

Критерием оптимальности может быть один (или несколько) показателей информационной (кибернетической) безопасности – величина ущерба от реализации угроз информации, общие расходы, которые включают ущерб от утечки информации и затраты на ее защиту, прибыль от

инвестиций в защиту информации, их рентабельность и тому подобное. Одновременно достичь оптимальных значений различных показателей из-за противоречивости их требований достаточно сложно, а зачастую и невозможно. В результате мы приходим к многокритериальной задаче.

Особую актуальность приобретает разработка вопросов оптимизации показателей средств защиты информации в условиях динамического противостояния с атакующей стороной [5]. В условиях неопределенности, когда действия соперника можно предположить лишь с определенной вероятностью, поиск оптимального распределения ограниченных ресурсов между объектами ЗИ за счет использования теоретико-игровых методов и учета динамики изменения условий противостояние, позволит свести величину причиненного вреда от реализации угроз информации к минимуму. Основанием для исследования является гипотеза о возможности повышения уровня защищенности ОБИ путем решения задачи многокритериальной оптимизации при выборе СЗИ для многоконтурных СЗИ ИКС. При этом представляется целесообразным сосредоточить внимание на развитии эволюционных методов и генетических алгоритмов для генерации множества решений в ходе поиска оптимальных конфигураций многоконтурных систем ЗИ и КБ для ОБИ, а также применения ГА для решения задачи по динамическому перераспределению ресурсов стороны защиты, исходя из актуальности существующих угроз.

На основании вышеизложенного можно оценить важность и релевантность планируемых исследований для повышения уровня защищенности ОБИ за счет оптимального распределения ресурсов защиты информации между объектами защиты с учетом действий злоумышленника. Полученные результаты и методология исследования могут быть использованы другими организациями для оптимального распределения ресурсов защиты информации между объектами защиты с учетом действий злоумышленника с целью повышения уровня защищенности объекта информатизации.

Библиографический список

1. Petit, J., Shladover, S.E. (2015). Potential Cyberattacks on Automated Vehicles, IEEE Transactions on Intelligent Transportation Systems, Vol. 16, Iss. 2, P. 546 – 556. DOI: 10.1109/TITS.2014.2342271

2. Sawik, T. (2013). Selection of optimal countermeasure portfolio in it security planning, Decision Support Systems, Vol. 55, Iss. 1, P. 156–164. http://dx.doi.org/10.1016/j.dss.2013.01.001

3. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. (2016). Decision support approaches for cyber security investment, Decision Support Systems, Vol. 86, P. 13–23. http://dx.doi.org/10.1016/j.dss.2016.02.012

4. Kanatov, M., Atymtayeva, L., Yagaliyeva, B. (2014). Expert systems for information security management and audit, Implementation phase issues, Soft Computing and Intelligent Systems (SCIS), Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), P. 896 – 900. DOI:10.1109/SCIS-ISIS.2014.7044702

5. Lee, K.-C., Hsieh, C.-H., Wei, L.-J., Mao, C.-H., Dai, J.-H., Kuang, Y.-T. (2016). Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation, Soft Computing, P. 1–14. doi:10.1007/s00500-016-2265-0

6. Lakhno, V., Kazmirchuk, S., Kovalenko, Y., Myrutenko, L., Zhmurko, T. (2016). Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features, Eastern-European Journal of Enterprise Technologies, No 3/9 (81), P. 30–38. DOI: 10.15587/1729-4061.2016.71769

7. Perlovsky, L. Shevchenko, O. (2014). Dynamic Logic Machine Learning for Cybersecurity, Chapter Cybersecurity Systems for Human Cognition Augmentation of the series Advances in Information Security, Vol. 61, P. 85–98. DOI: 10.1007/978-3-319-10374-7_6

Алимсеитова Ж.К.
Казахский национальный исследовательский университет им. К.И.Сатпаева,
Алматы, Казахстан

Ахметов Б.С.
Казахский национальный педагогический университет имени Абая,
Алматы, Казахстан

Alimseitova Zh.K.
Kazakh National Research University. K.I. Satpaeva,
Almaty, Kazakhstan

Akhmetov B.S.
Kazakh National Pedagogical University named after Abay,
Almaty, Kazakhstan