Ахметов Б.С., Лахно В.А., Досжанова А.А., Картбаев Т.С., Сабит Б. Модели для адаптивной экспертной системы по выявлению киберугроз. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVIII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2018. – С. 84-90.

УДК 004.056

МОДЕЛИ ДЛЯ АДАПТИВНОЙ ЭКСПЕРТНОЙ СИСТЕМЫ ПО ВЫЯВЛЕНИЮ КИБЕРУГРОЗ

Б.С. Ахметов, В.А. Лахно, А.А. Досжанова, Т.С. Картбаев, Б. Сабит

MODELS FOR THE ADAPTIVE EXPERT SYSTEM FOR DETECTING CYBERHOUROSIS

B.S. Akhmetov, V.A. Lakhno, A.A. Doszhanova, T.S. Kartbayev, B. Sabit

Аннотация. В данной статье рассмотрена актуальность внедрения адаптивной экспертной системы (АЭС) для решения задач интеллектуального распознавания сложных аномалий и прогнозирования, возникающих киберугроз, которая является одним из перспективных вариантов повышения эффективности принятия решений в области защиты информации (ЗИ) и кибербезопасности как в Республике Казахстан, так и во всем мире. Также затронуты принципы стандартной постановки задачи распознавания киберугроз, аномалий и кибератак (объекты распознавания - ОБР) и задачи АЭС. Отмечена эффективность применения дискретных процедур распознавания угроз в проектируемой адаптивной экспертной системе.

Ключевые слова: кибербезопасность, защита информации, распознавание угроз, аномалии, экспертная система, система поддержки принятия решений.

Abstract. In this article, the relevance of the introduction of an adaptive expert system (AES) for solving problems of intellectual recognition of complex anomalies and prediction of emerging cyberthreats is considered, which is one of the promising options for increasing the efficiency of decision-making in the field of information security (IS) and cybersecurity both in the Republic of Kazakhstan and and all over the world. Also, the principles of the standard statement of the problem of recognition of cyberthreats, anomalies and cyber attacks (objects of recognition - OBR) and the tasks of nuclear power plants are also touched upon. The efficiency of discrete detection procedures for threats in the projected adaptive expert system is noted.

Keywords: cybersecurity, information protection, threat recognition, anomalies, adaptive expert system, decision support system.

По мере развития информационных технологий и систем, без которых сегодня невозможно представить прогресс ни в одной области человеческой деятельности, все более актуальной становится проблема обеспечения кибербезопасности (КрБ) для различных объектов информатизации (ОБИ) [1, 2]. Учитывая постоянное возрастание многообразия потенциальных и сложности реальных киберугроз, одним из вариантов повышения эффективности принятия решений в области защиты информации (ЗИ) и кибербезопасности стало внедрение разнообразных интеллектуальных (или интеллектуализированных) программно-аппаратных комплексов в данной области. В частности, в работах [3–5] были предложены различные модели для интеллектуализированных экспертных и систем поддержки принятия решений (ЭС и ИСППР) в области кибербезопасности. Подобные ЭС и ИСППР могут достаточно эффективно обеспечить поддержку решений аналитиками служб ЗИ и КрБ в самых разных вопросах, начиная с задач выбора рациональных стратегий инвести-

рования в средства КрБ ОБИ и заканчивая задачами адаптивного распознавания киберугроз, аномалий и кибератак на информационно-коммуникационные системы ОБИ.

По мере усложнения сценариев кибератак стало очевидно, что традиционные сигнатурные методы не всегда в состоянии обеспечить должный уровень защиты ОБИ. Именно последним обстоятельством и продиктовано стремительное развитие интереса исследователей [3–6] к интеллектуализации технологий распознавания киберугроз, аномалий и кибератак (далее – объекты распознавания (ОБР)), в частности для ИСППР в задачах кибербезопасности.

Неполнота информации о киберугрозах для ОБИ имеет двоякое свойство. С одной стороны, часто отсутствует априорная информация, например, на уровне представления о структуре всего атакуемого объекта [2, 6, 7]. С другой стороны, службы информационной безопасности не всегда могут располагать сведениями, необходимыми для идентификации угроз, которые принадлежат конкретному классу. Зачастую заранее известно лишь общее множество угроз для КрБ и способов их осуществления. В подобной ситуации первостепенный приоритет имеет возможность стороны защиты ОБИ использовать доступные данные обо всех потенциальных угрозах. Умение стороны защиты ОБИ использовать для достижения КрБ все возможные данные, которые поступают в процессе функционирования ОБИ, связано с таким термином, как «адаптация» систем КрБ [8–10].

Адаптация на системном уровне в задачах ЗИ и Крб ОБИ – это способность систем КрБ (СКрБ, в частности, ИСППР) вырабатывать правильную стратегию поведения для защитных механизмов в процессе воздействия внешних и внутренних факторов, в том числе и компьютерных атак на ОБИ. Адаптация может быть представлена, например, специальными аппаратно-программными механизмами или путем перераспределения нагрузки на элементы ОБИ [8–10], см. рис. 1.

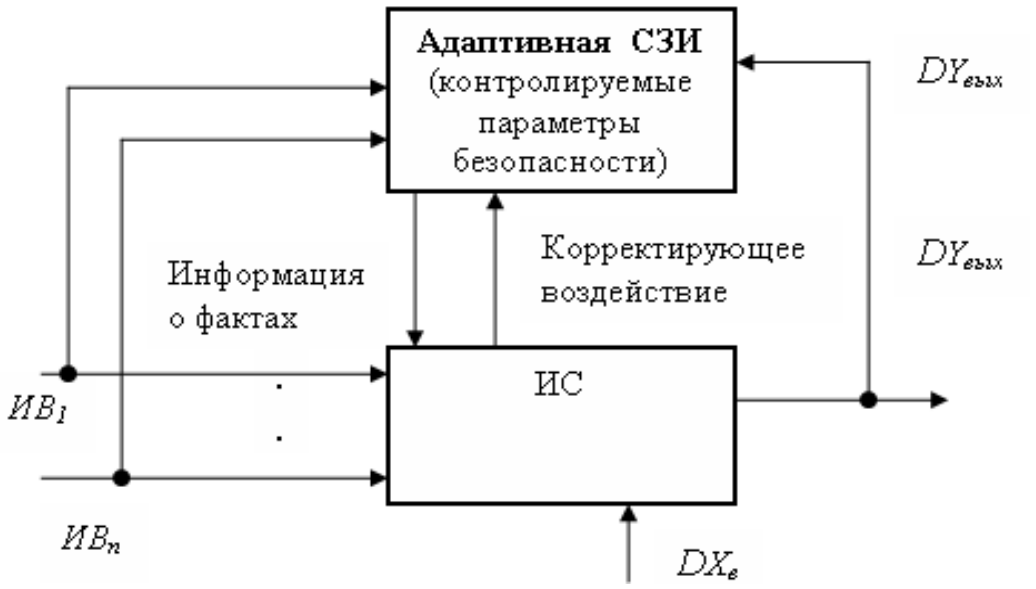

Рис. 1. Схема адаптивной системы защиты информации АИСТП

Полагаем, что основная задача адаптивной системы защиты информации (АСЗИ) или адаптивной системы КрБ (АСКрБ) для ОБИ заключается в выработке управляющих или корректирующих воздействий. Последние формируются на основе информационных воздействий, а также заданных метрик КрБ ОБИ. Цель

АСЗИ (АСКрБ) – поддержание $DY_{вых}$ в пределах допустимых заданных значений метрик КрБ. Полагаем, что разрабатываемая нами ИСППР в задачах кибербезопасности является составной частью АСЗИ (АСКрБ).

Стандартную постановку задачи распознавания киберугроз, аномалий и кибератак (ОБР) можно сформулировать так. Исследуется PA – число возможных целей для атаки. Объекты PA можно описать, используя систему признаков $\{pa_1,..., pa_n\}$. Полагаем, что PA математически можно описать как объединение непересекающихся классов (подмножеств) ОБР. Также для адаптивной экспертной системы по выявлению киберугроз (АЭС) должна существовать конечная подборка объектов $\{pa_{ax1},..., pa_{axn}\}$. Кажный объект – это прецедент. О прецедентах есть данные, к каким классам ОБР они относятся. Иными словами, на начальном этапе работы АЭС мы имеем в своем распоряжении так называемые объекты, используемые для обучения, – ОИО.

Задача АЭС – по минимальной представленной подборке значений признаков (зачастую может отсутствовать информация, к какому классу принадлежит ОБР) определить этот класс. Следовательно, распознав класс конкретной угрозы, аномалии или кибератаки, можно более эффективно выстроить работу всех контуров или рубежей, обеспечивающих кибербезопасности ОБИ.

В наших предшествующих публикациях [1, 3, 4, 6] были детально описаны используемые модели и алгоритмы для АЭС в задачах обеспечения КрБ различных ОБИ. В частности, дискретные процедуры распознавания угроз (ДПРПУ) [1, 3, 4] в ОБИ, основанные на использовании аппарата логических выражений. Это позволяет реализовать данные алгоритмы как программно, так и аппаратно.

Ключевая особенность подхода, который используется в проектируемой АЭС, – применение ДПРПУ. Это позволило получать довольно высокие результаты в ходе тестовых экспериментов по распознаванию разновариантных угроз, аномалий и кибератак. Особенно в ситуациях, когда отсутствуют данные о закономерностях распределения значений признаков и есть небольшие первоначальные выборки для ОИО. Кроме того, отсутствует необходимость задавать метрики в областях описания ОБР. Последнее достигается путем определения для каждого признака бинарной функции близости между его значениями ОИР. Это позволило четко разграничивать ОБР и фрагменты их описаний (подописания) [1].

Целевое задание в ходе конструирования ДПРПУ – отыскать информативные подописания (или фрагменты описаний) ОБР для различных классов угроз, аномалий и кибератак [1].

Сравнивая с широко используемыми в системах выявления вторжений (кибератак) методами и моделями (последовательный перебор признаков, статистические алгоритмы состояний), модели, которые в своей основе содержали ДПРПУ, а также разнообразные ОИО, дали значительный эффект. Так, в частности, сократился объем необходимых правил для распознавания ОБР. Например, в рамках класса сокращение правил составило 2,5–12 раз (зависит от класса ОБР – аномалия, кибератака, киберугроза), рис. 2.

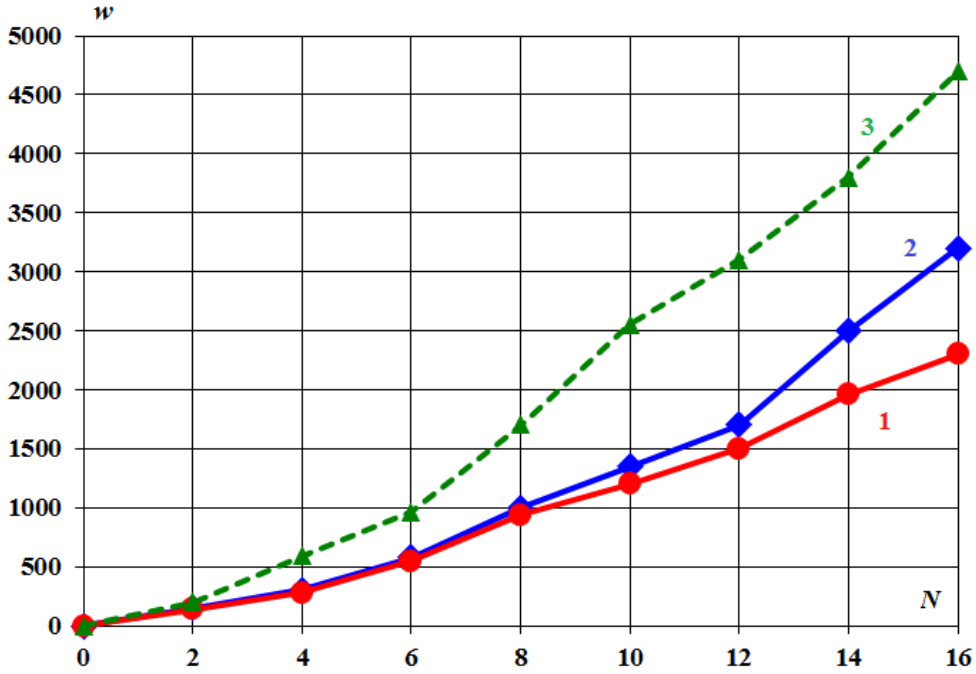

Рис. 2. Сравнительная эффективность предложенной модели для КрБ систем SCADA (N – количество признаков; w – количество шагов обучения АЭС)

Следовательно, возможно добиться существенного снижения времени выявления аномалий, кибератак или угроз, а также последующей оценки их последствий для ОБИ. В ходе тестирования прототипа АЭС рациональное число шагов обучения ОИО составляло $w \approx 3000..3050$ для известных классов ОБР. Для более сложных случаев атак или аномалий – $w \approx 3500...4500$.

Библиографический список

1. Ахметов Б.Б. Совершенствование киберзащиты информационно-коммуникационных систем транспорта за счет минимизации обучающих выборок в системах выявления вторжений // Захист інформації. 2018, том 20. № 1. С. 12-17.

2. Барсуков В.С., Водолазкий В.В. Современные технологии безопасности: интегральный подход. М.: Нолидж, 2000. 496 с.

3. Akhmetov B., Lakhno V. Korchenko A., Alimseitova Zh. System of decision support in weakly formalized problems of transport cybersecurity ensuring. Journal of theoretical and applied information technology. 2018 Vol. 96 No 8, pp. 2184-2196.

4. Akhmetov, B., Lakhno, V., Boiko, Y., & Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Eastern-European Journal of Eenterprise Technologies, (1 (2)), pp. 4-15.

5. Домарев В.В. Безопасность информационных технологий. Системный поход. К.: ТОВ «ТВД ДС», 2004. 992 с.

6. Лахно В.А., Петров А.С. Обеспечение защищенности автоматизированных информационных систем транспортных предприятий при интенсификации перевозок. Луганск: ВНУ им. В.Даля, 2010. 280 с.

7. Лахно В.А. Обеспечение информационной безопасности корпоративных систем на железнодорожном транспорте // Известия Волгоградского государственного технического университета. Серия - Актуальные проблемы управления, вычислительной техники и информатики в технических системах. Волгоград, 2014. Выпуск 20. № 6 (133). С. 131–136.

8. Al Hadidi M. M. et al. Intelligent Systems for Monitoring and Recognition of Cyber Attacks on Information and Communication Systems of Transport //International Review on Computers and Software (IRECOS). 2016. T. 11. №. 12. С. 1167-1177.

9. Atighetchi M., Adaptive Cyberdefense for Survival and Intrusion Tolerance/ Atighetchi M., Pal P., Webber F., Schantz R., Jones C., Loyall J. // Internet Computing. 2004. Vol. 8, No.6. P.25-33.

10. Lakhno V. A. Development of a support system for managing the cyber security, Radio Electronics, Computer Science, Control, 2017, No. 2, pp. 109–116.

Ахметов Бахытжан Сражатдинович
Казахский национальный
педагогический университет
имени Абая,
г. Алматы, Казахстан
E-mail: bakhytzhan.akhmetov.54@mail.ru

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

Лахно Валерий Анатольевич
Европейский университет,
г. Киев, Украина
E-mail: Valss21@ukr.net

Lakhno V.A.
European University,
Kiev, Ukraine

Досжанова Алия Амантаевна
Алматинский университет
энергетики и связи,
г. Алматы, Казахстан
E-mail: d_alia.81@mail.ru

Doszhanova A.A.
Almaty University
of Energy and Communication,
Almaty, Kazakhstan

Картбаев Тимур Саатдинович
Алматинский университет
энергетики и связи,
г. Алматы, Казахстан
E-mail: kartbaev_t@mail.ru

Kartbayev T.S.
Almaty University
of Energy and Communication,
Almaty, Kazakhstan

Сабит Ботакоз
Алматинский университет
энергетики и связи,
г. Алматы, Казахстан
E-mail: sabit_botakoz@mail.ru

Sabit Botakoz
Almaty University
of Energy and Communication,
Almaty, Kazakhstan