© Beketova G., Akhmetov B., Korchenko A., Lakhno A. Design of a model for intellectual detection of cyber-attacks, based on the logical procedures and the coverage matrices of features // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 3, p. 242-254.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

DOI: 10.18372/2225-5036.22.11096

РАЗРАБОТКА МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНОГО РАСПОЗНАВАНИЯ АНОМАЛИЙ И КИБЕРАТАК С ИСПОЛЬЗОВАНИЕМ ЛОГИЧЕСКИХ ПРОЦЕДУР, БАЗИРУЮЩИХСЯ НА ПОКРЫТИЯХ МАТРИЦ ПРИЗНАКОВ

Гулжанат Бекетова[1], Берик Ахметов[2], Александр Корченко[3], Валерий Лахно[4]

[1]Казахский национальный исследовательский технический университет им. К.И.Сатпаева, Казахстан
[2]Международный казахско-турецкий университет им. Ясави, Казахстан
[3]Национальный авиационный университет, Украина
[4]Европейский университет, Украина

БЕКЕТОВА Гулжанат Сакитжановна

Год и место рождения: 1984 год, г. Кызылорда, Кызылординская обл., Казахстан.
Образование: Кызылординский государственный университет им. Коркыт Ата, 2005 г.
Должность: докторант кафедры компьютерной и программной инженерии с 2014 г.
Научные интересы: защита информации, информационная безопасность, биометрия, криптография
Публикации: около 20 научных статей.
E-mail: beketova_gs@mail.ru

АХМЕТОВ Берик Бахытжанович, к.т.н.

Год и место рождения: 1985 год, г. Алматы, Казахстан.
Образование: Казахский национальный университет имени аль-Фараби, 2009 г.
Должность: Вице-президент по учебно-методической работе.
Научные интересы: информационная безопасность, бизнес-аналитика, применение ИКТ в образовании.
Публикации: более 40 научных статьей в национальных и международных базах.
E-mail: berik.akhmetov@ayu.edu.kz

КОРЧЕНКО Александр Григорьевич, д.т.н.

Год и место рождения: 1961 год, г. Киев, Украина.
Образование: Киевский институт инженеров гражданской авиации, 1983 г.
Должность: заведующий кафедрой безопасности информационных технологий НАУ.
Научные интересы: информационная и авиационная безопасность: экспертиза в области информационной безопасности, риски информационной безопасности, квантовая криптография, защита гражданской авиации от киберугроз
Публикации: более 300 печатных научных работ, среди которых монографии, словари и энциклопедии, учебники и пособия.
E-mail: agkorchenko@gmail.com

ЛАХНО Валерий Анатольевич, д.т.н.

Год и место рождения: 1964 год, г. Луганск, Украина
Образование: Ворошиловградский машиностроительный институт
Должность: Заведующий кафедрой кибербезопасности и управление защитой информационных систем
Научные интересы: информационная безопасность, безопасность информационно-коммуникационных систем
Публикации: более 100 научных статей.
E-mail: valss21@ukr.net

Аннотация. *Глобальное развитие критически важных компьютерных систем (КВКС) в энергетике, промышленности, связи и на транспорте, объектах инфраструктуры крупных мегаполисов и т. п. требует постоянного отслеживания киберугроз, а также уязвимостей технических компонентов и программного обеспечения. Несовершенство существующих методов киберзащиты, а также изменяющийся характер действий атакующей стороны, диктует необходимость продолжать исследования в области математического и алгоритмического развития систем защиты информации, способных своевременно обнаруживать кибератаки, аномалии и угрозы. Таким образом, актуальность исследований, направленных на дальнейшее развитие моделей и методов защиты на основе интеллектуального распознавания угроз КВКС и обеспечения их информационной безопасности, является одной из ключевых проблем киберзащиты критической инфраструктуры государства. В статье предложена схема адаптивной системы защиты информации КВКС и описана модель построения системы киберзащиты на основе логических процедур и матриц признаков кибератак, аномалий и угроз.*

Ключевые слова: *кибератака, информационная безопасность, критически важные компьютерные системы, интеллектуальное распознование, система защиты информации, системы обнаружения аномалий.*

Введение

Повсеместное применение компьютерных систем и информационно-коммуникационных технологий (ИКТ) способствует повышению производительности труда, снижению материально-сырьевых затрат, улучшению качества продукции и уровня жизни. Критически важные компьютерные системы (КВКС) и ИКТ играют ключевую роль в развертывании, эксплуатации и техническом обслуживании жизнено важных инфраструктур, ответственных за своевременную доставку потребителям энергоресурсов, воды, продуктов питания, предоставление транспортных услуг и связи. Чтобы гарантировать высокую работоспособность, надежность и безопасность КВКС, необходимо превентивно решать проблемы, связанные с их информационной безопасностью (ИБ) и киберзащитой (КЗ). Активное расширение сфер применения КВКС, особенно в сегменте мобильных, распределенных и беспроводных ИКТ, сопровождается возникновением новых угроз для ИБ, о чем свидетельствует стремительный рост числа инцидентов, связанных с ИБ и КЗ КВКС, а также выявленных уязвимостей в их программном обеспечении (ПО). Таким образом, актуальность исследований, направленных на дальнейшее развитие моделей и методов защиты на основе интеллектуального распознавания угроз КВКС и обеспечения их ИБ, является одной из ключевых проблем КЗ критической инфраструктуры государства.

Цель работы: дальнейшее развитие моделей и методов защиты критически важных компьютерных систем на основе интеллектуального распознавания киберугроз в условиях постоянного увеличения количества дестабилизирующих воздействий на конфиденциальность, целостность и доступность информации.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Разработать метод интеллектуального распознавания угроз, аномалий и кибератак, позволяющий обеспечить кибербезопасность КВКС на основе применения инновационных интеллектуальных систем киберзащиты для повышения устойчивости КВКС к кибератакам.

2. Разработать модель интеллектуального распознавания аномалий и кибератак с использованием логических процедур, базирующуюся на покрытиях матриц признаков (МП) и понятии элементарного классификатора (ЭК).

Обзор предшествующих исследований

По данным различных источников [1-3], за период с 2009 по 2015 год количество киберинцидентов, том числе, кибератак направленных на информационные системы государств, входящих в тор 20, выросло в среднем в 15 раз (рис. 1). Причем зафиксирована тенденция устойчивого роста количества киберинцидентов и кибератак, что, в частности, объясняется ростом количества КВКС подключенным к глобальным сетям (рис. 2).

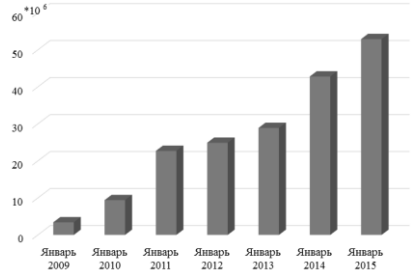

Рис. 1. Динамика киберинцидентов в КВКС за период с 2009 по 2015 г. [1, 4, 5]

После того, как в промышленных, энергетических и транспортных КВКС были выявлены столь сложные вирусы как Stuxnet (2010), Duqu (2011), Flame (2012), Careto (2014), произошел резкий скачок интереса к ИБ критически важных автоматизированных систем управления (АСУ или SCADA).

В итоге в период с 2011 по 2015 г. В компонентах критически важных SCADA было выявлено более 130 уязвимостей [1, 3-5] (рис. 3). Самое большее количество уязвимостей (42) за период с 2011 по 2015 г. было выявлено в компонентах КВКС компании Siemens [3, 6].

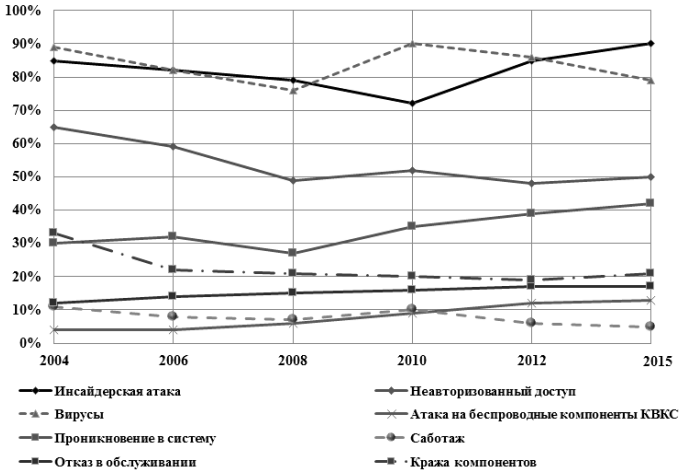

Рис. 2. Динамика киберугроз для КВКС предприятий [1-3, 6]

Представляют интерес для злоумышленников и такие компоненты КВКС и SCADA, как человеко-машинные интерфейсы (HMI). В них за период с 2004 г. по 2015 г. было обнаружено более 120 уязвимостей [1-3] (рис. 4).

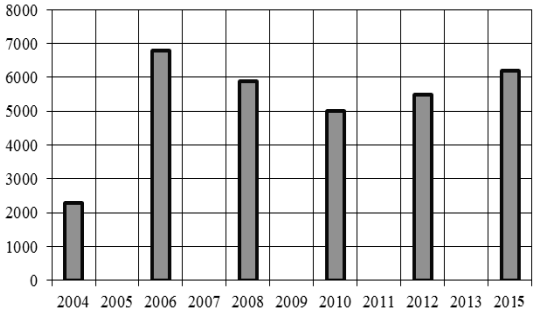

Рис. 3. Динамика роста уязвимостей в КВКС [1-4]

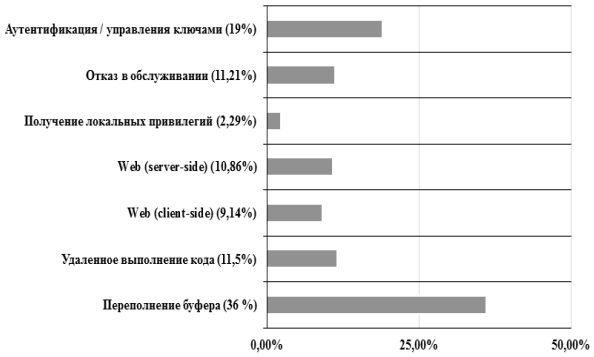

Рис. 4. Типы уязвимостей КВКС [3, 6-10]

По данным, представленным в [3, 5, 11-13] рост количества уязвимостей в КВКС в период с 2004 по 2015 г. Составил приблизительно 600%. Кроме того, как показали исследования [9, 14-16], сформировалась устойчивая тенденция снижения требований к уровню сложности успешно реализованных кибератак на КВКС. Внешние киберугрозы для КВКС, могут привести к реальным авариям или даже катастрофами, см. табл. 1 [3, 12, 17-19].

Факты вмешательства в работу КВКС различных отраслей Таблица 1

№	Год	Государство	Событие	Описанные последствия
Связь и Интернет				
1	2002	Великобритания (ВБ)	НСД к служебной телефонной связи железной дороги и системы управления семафором.	Отключен от связи диспетчерский пункт железной дороги, сбой в системе включения семафоров [20].
2	2014	США-Сирия	Хакеры отключили 84 блока сирийских IP-адресов	В результате атаки вся Сирия внезапно потеряла связь с интернетом [3].
Городские коммуникации				
3	2011	США	Хакеры отключили компьютеры системы водоснабжения (СВС) в Хьюстоне, штат Техас.	Потеря контроля над работой насосов, СВС [21].
4	2011	США	Хакеры отключили компьютеры СВС Спрингфилде, штат Иллинойс.	Потеря контроля над СВС на несколько часов [21-23].
Транспорт				
5	2003	Швеция, Гетеборг	Проникновение в АСУ движением городских автобусов и такси.	Потеря контроля над графиком движения на несколько часов [8].

Продолжение табл. 1

6	2014	РФ	Вирус отключил видеокамеры фиксации скоростного режима «Стрелка-СТ» в Москве и области.	Камеры выведены из строя на несколько дней [3, 22].
7	2003	США	Вирус SQL Slammer нарушает работу АСК авиакомпании «Continental Airlines»	Отмена рейсов [22].
Энергетический сектор				
8	2009	США	Выявлен вредоносный код в компьютерах энерго генерирующих компаний	В течении нескольких месяцев собиралась конфиденциальная информация [19, 22].
9	2010	Иран	Выявлен вирус Stuxnet в системах энергосектора	Несколько месяцев осуществлялся кибершпионаж за ядерной программой Ирана [24].
10	2011	США	SQL инъекция аккаунтов VPN компаний энергосектора	Кибершпионаж [24].
11	2012	Иран	Атаки на АСУ нефтяного комплекса	Работа АСУ приостановлена на двое суток [22, 24].
12	2012	РФ, Нидерланды, ВБ, США	Хакерская группа Anonymous совершила кибератаки на серверы «Газпром», «Роснефть», Shell, BP Global и ExxonMobil	В свободном доступе оказались тысячи почтовых аккаунтов сотрудников данных компаний [3, 10, 22].
13	2013-2014	Сомали, США, ВБ, Норвегия и др.	Обнародован отчет компании Rapid7 о фактах вмешательства со стороны преступных группировок в работу GPS систем нефтедобывающих платформ, танкеров и контейнеровозов в персидском заливе и Аденском проливе.	Зафиксированы факты выхода из строя программного обеспечения на буровых платформах на 19 суток [3, 10, 22].
14	2015	Украина	Хакерская атака на энерго распределительные подстанции	Отключение от электрообеспечения нескольких областей Украины

Следует отметить, что подходы к созданию систем обнаружения вторжений (кибернападений) (СОВ), реализующие классические алгоритмы [8, 18, 25-27] хороши для строго определенного количества угроз. В том случае, если возникает новая уязвимость или класс кибератак, которые не блокируется СЗИ, следует предусмотреть возможность изменения архитектуры базовой СОВ. Кроме того, что в настоящий момент большинство рассмотренных в работах [28-34] моделей угроз для КВКС не учитывают риски возникновения новых уязвимостей и угроз. То есть: $YZ_{1D_{СЗИ}} + YZ_{2D_{СЗИ}} = YZ_{3D_{СЗИ}} \neq YZ_{12D_{СЗИ}}$, где $YZ_{iD_{СЗИ}}$ – уязвимость уровней СЗИ для КВКС.

Таким образом, одним из наиболее важных аспектов обеспечения киберзащиты КВКС являются ее адаптационные возможности, проявляющиеся в условиях изменения среды эксплуатации.

Адаптация КВКС определяется, прежде всего, способностью системы вырабатывать правильную стратегию поведения в связи с изменением условий существования (внешних и внутренних факторов, в том числе и кибератак). Адаптация может быть представлена, например, специальными аппаратно-программными механизмами типа кластеризации и динамического перераспределения (балансировки) нагрузки [27, 35, 56]. При этом адаптивные СЗИ, в том числе СОВ, во многих исследованиях рассматриваются как неотъемлемая часть КВКС [27, 32-35, 56].

Достаточно большое количество работ за последние десятилетия посвящены и проблематике развития интеллектуальных СОВ [36-39]. В частности, в работах [23, 38] представлены обзоры методов обнаружения аномалий, предложены принципы классификации методов обнаружения, базирующиеся машинном обучении и статистическом анализе. Обзор современных методов машинного обучения для систем распознавания кибератак (СРКА) достаточно полно представлен в работах [2, 26, 40]. Однако, за рамками этих публикаций остались некоторые методы, например, метод k-средних [41], и его модификации [42]. Методы обнаружения кибератак на основе конечных автоматов (КА) достаточно подробно изложены в работах [43, 44]. Другим перспективным направлением развития адаптивных СОВ, часто упоминаемым в работах зарубежных авторов, является направление, связанное с обнаружения злоупотреблений на основе состояний КВКС [9, 45, 46].

Методы вычислительного интеллекта, в частности нейронные сети (НС) для задач обнаружения кибератак, описаны в работах [24, 47, 48]. В [49-51] описаны модели и методы адаптации генетических алгоритмов для задачи обнаружения кибератак. В работах [16, 45, 48] описаны вычислительные иммунные системы, которые можно использовать для задачи построения СРКА.

Типичный недостаток большинства СРКА, описанных в [35, 52, 53] – ошибочные срабатывания, поскольку в них почти всегда задействована только одна технология обнаружения (как правило, идентификация атак). По мнению многих авторов [23, 50, 51, 54-56], самым перспективным направлением развития методов обнаружения кибератак и аномалий является объединение существующих подходов в адаптивных или гибридных СРКА, обладающих способностью к самообучению.

Среди методов, которые применяются в СРКА, исследователи выделили следующие направления: 1) обнаружение аномалий в системе (системы обнаружения аномалий – СОА); 2) обнаружение злоупотреблений [5, 57]. В работах [58-60] рассматривались особенности функционирования СРКА, в которых применялись различные методы и модели. Прикладные аспекты коммерческих СРКА – IDES, NIDES, EMERLAND, JiNao, HayStack и др., рассмотрены в работах [61].

Методы обнаружения аномалий (МОА), дают возможность стороне защиты выполнить распознавание с высокой степенью точности и сделать обоснованное заключение о причине изменений в состоянии КВКС. Для создания МОА принято использовать: 1) контролируемое обучение; 2) неконтролируемое обучение [24, 62]. Различие между подходами состоит в том, что в контролируемом обучении применяют дискретный набор признаков, а продолжительность обучения заранее определена. Для неконтролируемого обучения совокупность признаков, как правило, меняется с течением времени, и обучение может продолжаться по мере совершенствования системы. Сегодня в коммерческих СОМ применяют только контролируемое обучение [57, 63].

Большинство современных СРКА и СОА базируется на моделях и методологиях, основанных на теории распознавания образов [64, 65, 73-75].

Сложность имплементации в существующие модели СРКА формализованного аппарата теории распознавания, заключается в том, что конкретный информационный комплекс для КВКС, включающий в себя зачастую уникальные ПО и информационные массивы, а также собственную подсистему ИБ, состоит из разнородных компонентов. Однако, проводимая в рамках настоящего исследования, конкретизация задач распознавания кибератак и применения моделей, позволяющих минимизировать количество обучающих выборок в форме матриц признаков, а также элементарных классификаторов (ЭК) для каждого из моделируемых классов кибератак, позволит оптимизировать работу СРКА.

В ходе исследования, учитывая особенности предметной области и сформулированных задач, использовались: булева алгебра, теория нечетких множеств, методы и средства имитационного моделирования.

Модель интеллектуального распознавания аномалий и кибератак с использованием логических процедур, базирующуюся на покрытиях матриц признаков

Ниже остановимся на предлагаемой в работе модели логических процедур распознавания киберугроз для КВКС.

Пусть существует набор киберугроз для КВКС. Показатель опасности каждой киберугрозы зависит от показателей набора факторов, повышающих или понижающих защищенность КВКС от данной угрозы [6, 8, 23, 26, 28, 33, 34 40, 66-71]. Для обеспечения однозначности, полноты и целостности классификации, введем следующие требования к классификации киберугроз: непересекающиеся классы угроз (определяет однозначность выбора класса на основе внешнего правила, позволяющего принять решение); применимость (добавление класса не должно вызывать дробления более одного класса на две части); объективность (наличие или отсутствие класса должно подтверждаться известными классификациями); расширяемость (добавление класса возможно путем дробления существующих классов); количество классов конечно.

Базисом для построения ЭК объектов распознавания (ОР - аномалии, атаки и пр.) для СРКА, могут стать различные данные, например, описательная информация которая представлена в форме двоичного представления трудно объяснимых признаков кибератаки или угрозы для ИБ – $\{p_{ax1},...,p_{axn}\}$ в КВКС. Также могут быть использованы: диапазоны пороговых значений и параметры входящего и исходящего трафика, непредусмотренные адреса пакетов, атрибутов, временных параметров, запросов и т. д.

Примем: MI – общее число киберугроз для КВКС; PA – число возможных целей нарушителя в защищаемой КВКС; B_{p_a} – множество номеров киберугроз, реализуемых нарушителем при достижении p_a - й цели, например, в ходе атаки на КВКС.

Обобщенную категорийную модель интеллектуального распознавания аномалий и кибератак с использованием логических процедур, базирующуюся на покрытиях матриц признаков, в графической интерпретации можно представить так, см. рис. 5.

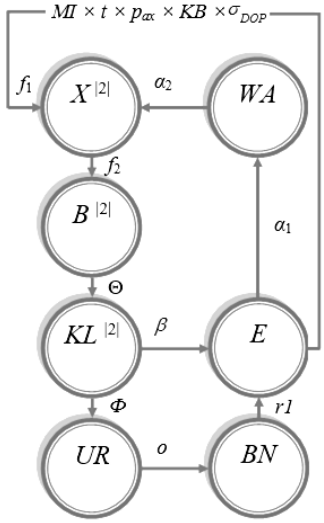

Рис. 5. Категорийная модель распознавания аномалий и кибератак с использованием логических процедур, базирующуюся на покрытиях матриц признаков

Квантор $\Theta: B^{|2|} \to KL^{|2|}$ позволяет разбить пространство признаков ОР (аномалий, кибератак или угроз) на классы $KL^{|2|}$ (пара: эталон – ОР). Проверка гипотезы о принадлежности ОИО к классу KL, реализуется оператором Φ. Точность распознавания контролируется параметром BN (оператором о). Множество UR учитывает количество статистических гипотез при формировании ОИО. Оператор $r1$ формирует множество E для оценки результативности применения ОИО для класса KL. Оператор β используется в процессе оптимизации системы контрольных отклонений ОИО. Схема последовательно

замыкается множеством WA, включающим операторы $\alpha_1 : E \to WA$ и $\alpha_2 : WA \to X^{|2|}$, которые отслеживают реализацию ОИО в процессе обучения адаптивной СРКА.

В категорийной модели принято: t – множество моментов времени, в ходе которых происходит снятие параметров «слепков» ИБ; p_a – признаки ОР; MI – множество ОР (аномалии, атаки угрозы), которые влияют на информационную безопасность (ИБ) КВКС; G_{DOP} – ЭК, используемые в алгоритмах формирования ОИО; KB – база знаний (ОИО и др.) для идентификации ОР; $X^{|2|}$ – матрица эталон; $B^{|2|}$ – бинарная учебная матрица; f_1, f_2 – процедуры формирования матрицы признаков в ее описательном и бинарном представлении, соответственно.

Реализация модели предполагает следующие этапы:

Этап 1. Исследуется множество объектов РА – число возможных целей нарушителя при атаке на КВКС. Объекты, которые можно отнести к данному множеству, характеризуются совокупностью признаков $\{p_{ax1},...,p_{axn}\}$. Известно, что множество РА представлено в виде объединения подмножеств (классов) киберугроз для КВКС – $(KL_1,...,KL_l)$ или $(B_{p_{a1}},...,B_{p_{al}})$ которые не пересекаются. Предположим, что существует конечная группа объектов $\{sp_{a1},...,sp_{am}\}$ из РА, о которых известно, к каким классам аномалий, атак или угроз их можно отнести (это прецеденты, т.е. объекты, используемые для обучения – ОИО). СРКА необходимо по имеющемуся множеству параметров (признаков), т. е. используя описание ОР sp_{an} из РА, классифицировать этот ОР. Затем, по итогам классификации выстраивается работа СЗИ для КВКС. СРКА изначально неизвестно к какому классу относится ОР.

Будем полагать, что классификация ОР (кибератак или аномалий), представляет собой множества потенциальных вариантов действий источника угроз. Кроме того, будем учитывать множество существующих методов реализации атак с использованием уязвимостей, которые, в конечном счете, могут привести к достижению целей нападающей стороны.

Этап 2. Построение ЛППРУ. Парадигмой построения ЛППРУ является отыскания информативных подописаний (или фрагментов описаний) ОР [23, 25, 33, 34, 73]. Эти фрагменты при создании, конкретных проектных решений для СРКА, например, на основе, нейросетей, конечных или клеточных автоматов, позволят в будущем однозначно делать вывод о наличии (или отсутствии) атаки (аномалии, угрозы) в рамках класса.

Информативными положим фрагменты, отражающие характерные закономерности при описании ОР, используемого в ходе обучения СРКА. Тогда, наличие (отсутствие) фрагмента(тов) в описании ОР, проходящего классификацию, дает возможность отнести его к определенному классу. В ЛППРУ информативным положим фрагмент(ты), который имеется в описаниях ОР рассматриваемого класса кибератак, но отсутствует в описании других классов.

При построении ЛППРУ для СРКА используются предложенные рядом авторов [17, 23, 72] элементарные классификаторы (ЭК). ЭК – это фрагмент описывающий объект, используемый для обучения СРКА. Для каждого класса кибератак (киберугроз, аномалий, уязвимостей и т.п.) $(KL_1,...,KL_l)$ выполняется построение множества ЭК с заранее заданными параметрами.

При этом сделаем следующие допущения для ЭК: используются ЭК, которые присутствуют в описаниях объектов анализируемого в данный момент класса, но их нет в описании объектов других классов; описательный наборов показателей (признаков) задан в двоичной форме (0010101). При этом ОИО характеризуют все объекты данного класса. А, следовательно, ОИО имеют большую информативность. Для повышения эффективности ЛППРУ, актуальной является проблематика использования в них свойства «невстречаемости» групп из приемлемых значений показателей ОР. Кроме того, необходимо, имплементировать в алгоритм распознавания «решающее правило» $DR(p_{axi})$ [23, 73], для класса атаки (аномалии или угрозы) в СРКА с минимальным количеством ошибок в его работе.

Следующая проблема при проектировании атапривных СРКА – присутствие в выборке ОИО, с характеристиками, лежащими на стыке различных классов кибератак $(KL_1,...,KL_l)$, например, DOS/DDoS или переполнение буфера. Подобный ОИО является атипичным для своего класса. Это объясняется схожестью информативных подописаний, т.к. показатели, представленные в двоичной форме в целом близки. Присутствие в обучающей выборке (ОВ) атипичных ОИО, увеличивает длину информативных подописаний. Таким образом, станет возможным различать ОР из разных классов.

При решении заданий, связанных с проектированием эффективных СРКА для КВКС корректные данные о структуре всех целей атаки (РА), чаще всего, отсутствуют. Следовательно, изначально, при синтезе ЛППРУ не гарантируется корректность их использования на новых ОР, которые отличны от $\{sp_{a1},...,sp_{am}\}$. При этом, ОИО обладают показателями характерными для анализируемого множества $\{sp_{a1},...,sp_{am}\}$, то алгоритм, который работает безошибочно на этапе учебы СРКА, обеспечит приемлемые результаты и на неклассифицированных sp_{an}, которые не входили в выборку ОИО. В связи с этим, в работах [48, 73] уделялось проблематике корректности алгоритмов, используемых для распознавания в СРКА. Алгоритм корректен, если он верно распознает объекты из тестовой выборки.

Этап 3. Проверка работоспособности метода, основанного на ЛППРУ и матрицах информативных признаков объектов распознавания.

Проверка метода или соответствующего алгоритма может быть проверена при помощи следующей процедуры. Анализируемый объект sp_{an}, например, описательные показатели (ОП) аномалии или кибератаки, киберугрозы и т.п., сопоставляется с каждым ОИО из $\{sp_{a1},...,sp_{am}\}$. В случае если ОП sp_{an}

тождественны с ОП ОИО sp_{ai}, его относят к классу, к которому принадлежит sp_{ai}. Иначе алгоритмом будет выдано сообщение об отказе от распознавания. Алгоритм работоспособен [71, 72, 76], но он не адоптирован распознать ни один объект sp_{ai}, ОП которого не тождественны с ОП ОИО, имеющихся в репозитории.

Выполненный в [2, 23, 26, 40, 75] анализ разновидностей кибератак, аномалий и типов НСД (т.е. классов) к ресурсам КВКС, показал, что вопрос о расстоянии между sp_{ai} и sp_{aj}, а также принадлежности их к рассматриваемому классу, например, кибератакам, можно решать элементарным сравнением заданных множеств информационных подописаний sp_{ai} и, однако, возникает проблема корректного выбора поднаборов информационных показателей (ИП), используемых алгоритмом распознавания для сравнения ОР. В работах [23, 71, 75] был предложен термин – алгоритм расчета оценок (АРО), который может быть задействован в предлагаемой модели.

Например, рассмотрим задачу классификации для двух классов киберугроз $B_{p_{a1}}, B_{p_{a2}}$. Предположим, что аналитик службы ИБ КВКС располагает данными, которые характеризуют нормальную активность пользователей по узлам КВКС, и совокупность примеров классов атак (т.н. шаблоны атак). Полагаем, что рассматриваемые классы не пересекаются. Очевидно, что имеется вектор VE и число $ЧХ$, для которых справедливы следующие отношения, $(p_{ax_1}, VE) > ЧХ$ при $p_{ax_1} \in P_{ax_1}$ и $(p_{ax_1}, VE) < ЧХ$ при $p_{ax_2} \in P_{ax_2}$, где P_{ax_1}, P_{ax_2} – количественное измерение объекта или пространство показателей.

Предлагается более удобный способ динамического распознавания ОР, при котором можно выполнить переход от исходного пространства описаний объектов P_{ax_j}, в форме двоичного представления признаков, к новому пространству NEP_{ax} с помощью преобразования $P_{ax_j} \to NEP_{ax}$. Примем, что NP_{p_a} – некоторая подборка из r_{p_a}, $r_{p_a} \le MI$ несходных дискретных показателей (угрозы, аномалии, кибератаки и т.п.) вида $\{p_{aj_1}, ..., p_{aj_r}\}$. Расстояние между объектами $sp'_a = (\alpha p'_{a1}, \alpha p'_{a2}, ..., \alpha p'_{aMI})$ и $sp''_a = (\alpha p''_{a1}, \alpha p''_{a2}, ..., \alpha p''_{aMI})$ из РА по набору NP_{p_a} оценим величиной:

$$BN(sp'_a, sp''_a, NP_{pa}) = \begin{cases} 1, & если \quad \alpha p'_{j_{ti}} = \alpha p''_{j_{ti}} \quad при \quad ti = 1,2,...,r_{p_a}, \\ 0 & в \quad противном \quad случае. \end{cases} \qquad (1)$$

В системе показателей ОИО $\{p_{a_1}, ..., p_{a_{jMI}}\}$ выделим совокупность подмножеств вида $NP_{p_a} = \{p_{aj_1}, ..., p_{a_{MI}}\}$, $r_{p_a} \le MI$. Выделенные подмножества будем полагать опорными (ОМ) АРО [23, 76-78]. Всю их совокупность обозначим – ΩMI.

Зададим следующие дополнительные параметры: po_{sp_a} – параметр, характеризующий значимость цели (объекта) sp_{ai}, $i = 1,2,..., PA$; $po_{NP_{pa}}$ – параметр, характеризующий значимость объекта ОМ $NP_{p_a} \in \Omega MI$.

Выполним расчет оценки, сравнивая объект sp_{an} с каждым ОИО по каждому ОМ.

Для каждого класса кибератак на КВКС KL, $KL \in \{KL_1, ..., KL_l\}$, вычислим оценку принадлежности $\Gamma(sp_a, KL)$ объекта sp_a классу KL:

$$\Gamma(sp_a, \mathrm{KL}) = \frac{1}{|\mathrm{LW_{KL}}|} \sum_{sp_{ai} \in KL} \sum_{NP_{Pa} \in \Omega MI} po_{sp_a} \cdot po_{NP_{pa}} \cdot BN(sp_a, sp_{ai}, NP_{p_a}), \Gamma(sp_a, KL), \text{ где } |LW_{KL}| = |KL \cap \{sp_{a1}, ..., sp_{aMI.}\}|. \qquad (2)$$

Объект sp_{an} отнесен к классу, обладающему max оценкой. Если имеется множество таких классов, то алгоритм отказывается от последующего распознавания. Для повышения корректности алгоритма необходимо решить следующую систему неравенств:

$$\Gamma(\mathrm{sp_{a1}}, KL_1) > \Gamma(\mathrm{sp_{a1}}, KL_2), \Gamma(\mathrm{sp_{aMI_1}}, KL_1) > \Gamma(\mathrm{sp_{aMI_1}}, KL_2), \Gamma(\mathrm{sp_{aMI}}, KL_2) > \Gamma(\mathrm{sp_{aMI}}, KL_1). \qquad (3)$$

Для решения системы (3) необходимо выбрать параметры $po_{sp_{ai}}$, $i = 1,2,..., PA$ и $po_{NP_{pa}}$, $NP_{p_a} \in \Omega MI$. Когда система несовместна, необходимо найти для нее максимальную совместимую подсистему. Затем из решения этой подсистемы определить значения $po_{sp_{ai}}$ и $po_{NP_{pa}}$.

Альтернативным способом повысить корректность работы метода является путь подборки системы достоверных ОМ для того, чтобы распознать и классифицировать объекты (аномалии, угрозы, уязвимости или кибератаки). Например, выбрать подборку таким образом, чтобы для любого ОИО $sp'_a \notin KL$ выполнялось условие. Кроме того, для любого ОИО $sp''_a \in KL$, выполнялось неравенство $\Gamma(sp''_a, KL) > 0$. Реализовать это можно следующим образом. Положим $NP_{p_a} = \{p_{aj_1}, ..., p_{a_{MI}}\}$ является ОМ. Совокупность показателей (или признаков) NP_{p_a} будем считать удовлетворяющей требованиям теста, если для каждого ОИО sp'_a, sp''_a, и при этом, относящихся к несходным классам, выполняется условие $BN(sp'_a, sp''_a, NP_{pa}) = 0$. Таким образом, наш тест – это группа (подборка) показателей, по которому различаются только любые два объекта из разных классов.

Введем обозначение: MC – множество всех ЭК, полученных по совокупности признаков из $\{s_{ax1}, ..., s_{axn}\}$, т.е. $MC = (\sigma_{DOP}, NP_{sa})$, где $NP_{sa} \subseteq \{s_{ax1}, ..., s_{axn}\}$, $\sigma_{DOP} = (\sigma_{DOP_1}, ..., \sigma_{DOP_r})$, $\sigma_{\mathrm{DOP_i}} \in NP_{s_{aj}}$, $при \ i = 1,2,..., r_{s_a}$.

Учитывая, что в результате процесса обучения сформирована матрица бинарных признаков, можно для каждого проверяемого объекта, выполнить анализ принадлежности к классу на основании определения величины $BN(\sigma_{\text{DOP}}, sp_a, NP_{sa})$.

$$S = \begin{pmatrix} s_{ax_{11}} & s_{ax_{12}} & \dots & s_{ax_{1i}} & \dots & s_{ax_{1n}} \\ s_{ax_{21}} & s_{ax_{22}} & \dots & s_{ax_{2i}} & \dots & s_{ax_{2n}} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_{ax_{l1}} & s_{ax_{l2}} & \dots & s_{ax_{li}} & \dots & s_{ax_{ln}} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_{ax_{Z1}} & s_{ax_{Z2}} & \dots & s_{ax_{Zi}} & \dots & s_{ax_{Zn}} \end{pmatrix},$$

или

$$S = \begin{pmatrix} 0 & 1 & \dots & 1 & \dots & 1 \\ 1 & 0 & \dots & - & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ - & 1 & \dots & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & - & \dots & 0 \end{pmatrix}.$$

Каждый алгоритм, задействованный в процедуре распознавания кибератак или аномалий обозначим – *AL*. Для соответствующего класса объекта распознавания в СРКА рассматривается подмножество $MC^{AL}(KL)$ множества *MC*.

Обозначим $\text{MC}^{\text{AL}} = \bigcup_{j=1}^{l} MC^{AL}(KL_j)$. Анализ объекта sp_{an} осуществляется на основе определения величины $BN(\sigma_{\text{DOP}}, sp_a, NP_{sa})$ для каждого элемента $(\sigma_{\text{DOP}}, NP_{sa})$ множества $MC^{AL}(KL)$, $KL \in \{KL_1,...,KL_l\}$. При этом для каждого элемента выполняется вычисление оценки (sp'_a, KL), определяющей принадлежность sp_a классу *KL*. Алгоритмы (*AL*) задействованные в СРКА характеризуются совокупностью ЭК $MC^{AL}(KL)$ и порядком расчетов $\Gamma(sp'_a, KL)$.

Классификаторы, используемые в алгоритмах $\sigma_{DOP} = (\sigma_{DOP_1},...,\sigma_{DOP_r})$, сформированы как совокупность информационных признаков NP_{sa}. При этом, каждый ЭК, должен обладать как минимум одним из перечисленных ниже свойств: 1) фрагмент группы (sp_a, NP_{sa}), где $sp_a \in KL$, совпадает с $\sigma_{DOP} = (\sigma_{DOP_1},...,\sigma_{DOP_r})$; 2) только часть фрагментов (sp_a, NP_{sa}), где $sp_a \in KL$, совпадает с $\sigma_{DOP} = (\sigma_{DOP_1},...,\sigma_{DOP_r})$; 3) фрагменты группы (sp_a, NP_{sa}), где $sp_a \in KL$, не совпадают с $\sigma_{DOP} = (\sigma_{DOP_1},...,\sigma_{DOP_r})$.

Синтез ЭК σ_{DOP_i} для класса (кибератаки, аномалий и пр.) базируется репликации покрытий матриц σ_{DOP_i}, которое образовано описаниями ОИО для KL. Поставим в соответствие ЭК объекта – $(\sigma_{\text{DOP}}, NP_{sa})$, где $\sigma_{DOP} = (\sigma_{DOP_1},...,\sigma_{DOP_r})$, NP_{sa} – набор признаков с номерами $j_1,...j_{r_{sa}}$ элементарную конъюнкцию $\Re = s_{axj_1}^{\sigma_{DOP_1}} ... s_{axj_{r_{pa}}}^{\sigma_{DOP_{r_{pa}}}}$. Если $sp_a = (\alpha s_{a1},...,\alpha s_{aQ})$ – объект из множества *PA*, следовательно, $BN(\sigma_{\text{DOP}}, sp_a, NP_{sa}) = 1$ тогда и только тогда, когда $(\alpha\alpha_{a1},...,\alpha._{aQ}) \in NI_{\Re}$, где $NI_{\Re}$ – интервал истинности элементарной конъюнкции $\Re$.

При создании ЛПРУ, следует учесть, что определение множества ЭК сводится к отысканию допустимых и максимальных конъюнкций для отличительной функции класса объекта *KL* (аномалии, кибератаки и т. п). Данная функция является булевой. При этом она принимает различные значения на ОИО из KL_l и $\overline{KL_l}$.

Тогда процедура распознавания объекта sp_a, например, кибератаки в КВКС, выполняется на основании результатов расчета по элементарным конъюнкциям ($\Re$). При этом характеристическая функция (ХФ) класса KL_l будет представлена как ФАЛ (функция алгебры логики) F_{KL}, которая равна нулю (0) на информационных описаниях sp_{an} из KL_l и равна единице (1) на оставшихся наборах признаков из E_{KL}^{MI}, где E_{KL}^{MI} – совокупность наборов, имеющих длину r_{s_a}. Следовательно, покрытию класса соответствует допустимое для $F_{\overline{KL}}$ значение $\Re$. Тупиковому покрытию соответствует – максимальное наначение $\Re$ для $F_{\overline{KL}}$. Допустимая $\Re$ в матрицах признаков объектов определит принадлежность конкретного объекта sp_{an} к классу CT_i, если выполняется условие – $(\alpha s_{a1},...,\alpha s_{aQ}) \notin \text{NI}_{\Re}$.

Принимая во внимание выше сказанное, необходимо получить сокращенную дизъюнктивную нормальную форму (СДНФ) функции для F_{KL}. СДНФ равна 0 на наборах из $B_{F_{\overline{CT}}}$ и 1 на остальных наборах E_{KL}^{MI}. После того как СДНФ для $F_{\overline{KL}}$ получена, из нее необходимо удалить конъюнкции $\Re$, которые не обладают свойством $NI_{\Re} \cap A_{F_{KL}} \neq 0$.

Например, получить СДНФ логической функции можно путем преобразования конъюнктивной функции вида $\text{D}_1 \wedge \text{D}_2 \wedge ... \wedge \text{D}_\text{u}$, где $\text{D}_\text{i} = s_{ax1}^{\overline{\beta_{i1}}} \vee s_{ax2}^{\overline{\beta_{i2}}} \vee ... \vee s_{axQ}^{\overline{\beta_{iQ}}}, i = 1,2,..,mu$ реализует функцию F_{KL}, β_{iMI} – элементы набора $B_{F_{\overline{KL}}}$.

Обозначим: $\overline{\text{s}_{\text{ax}}^{\ \alpha}} = \bigvee_{\beta_i \neq \alpha_i} \text{s}_{\text{ax}}^{\ \beta}$. Тогда конъюнктивная функция принимает вид принимает вид $\text{D}^*_1 \wedge \text{D}^*_2 \wedge ... \wedge \text{D}^*_\text{u}$, где

$$\text{D}^*_\text{i} = \bigvee_{t \neq \beta_{i1}} s_{ax1}^{\eta} \vee \bigvee_{t \neq \beta_{i2}} s_{ax2}^{\eta} \vee ... \vee \bigvee_{t \neq \beta_{iQ}} s_{axQ}^{\eta}, i = 1,2,..,u. \quad (4)$$

Таким образом, синтез ЛППРУ и ЭК выполняется следующим образом: 1) задаем ХФ; 2) находим СДНФ, реализующую данную ХФ; 3) находим допустимую (максимальную) конъюнкцию $\Re$, определяющую принадлежность объекта к рассматриваемому классу.

Т.к. ЭК и ОИО ограничены по объему, приняты следующие правила обучения ОИО. Задана учебная матрица ОИО – $\left\| s_{axi}^{(j)} \right\|, i = \overline{1,N},\ j = \overline{1,n},$ где N,n – количество признаков распознавания (например, атаки) и испытаний (тестов), соответственно. Модификация учебной матрицы ОИО при условии минимизации количества признаков, ее столбцов и строк, выполняется при соблюдении следующих правил:

$$EN_{1,m}^{(k)}[0]=0;\ EN_{2,m}^{(k)}[0]=0;$$

$$s_{ax_{m,i}}^{(j)} = \begin{cases} 1,\ if\ \ \zeta_b \le \Delta_{m,i}^{(j)} \le \zeta_t; \\ 0,\ if\ \ else. \end{cases} \quad (5)$$

$$I(s_{ax_i}) = 1 + \sum_{i=1}^{G} (P_i \cdot \sum_{ct=1}^{CT} P_{i,ct} \cdot \log_{ct}\ P_{i,ct}); \quad (6)$$

$$\begin{aligned} &if\ \ s_{ax_m}^{(j)} \in KL_m^0 \\ &then\quad EN_{1,m}^{(k)}[j] := EN_{1,m}^{(k)}[j-1]+1; \\ &if\ \ s_{ax_c}^{(j)} \in KL_m^0 \\ &then\quad EN_{2,m}^{(k)}[j] := EN_{2,m}^{(k)}[j-1]+1, \end{aligned} \quad (7)$$

где $EN_{1,m}^{(k)}$, $EN_{2,m}^{(k)}$ – количество событий, характеризующих принадлежность реализаций ОИО к совокупности признаков для ЭК рассматриваемого класса объектов (аномалий, кибератак) и количество событий, характеризующих принадлежность реализаций ОИО к совокупности признаков для ЭК «чужого» класса объектов, соответственно; ζ_b, ζ_t – нижний и верхний контрольные допуски для признака; $\Delta_{m,i}^{(j)}$ – выборочное среднее значение i –го признака в векторах ОИО базового класса объекта; $I(s_{ax_i})$ – информативность признака в рамках класса объекта; G – количество градаций признака объекта; P_i – вероятность i-той градации признака; $P_{i,ct}$ – вероятность появления i-той градации признака в классе объектов KL.

Таким образом, предложенная модель, основанная на построении множества ЭК и ЛППРУ, построенных на допустимых и максимальных конъюнкциях для характеристической функции класса ОР (аномалий, кибератак и киберугроз), позволяет создавать не только программные, но и аппаратные адаптивные СРКА.

Результаты имитационного моделирования

Предложенная модель ЛППРУ, была реализована в среде MatLab 7 (см. рис. 6). На рис. 7-11 показаны основные результаты, полученные в ходе моделирования информативности значений показателей попыток НСД к информационным ресурсам КВКС. На рис. 6 показан пример простой матрицы идентифицированных источников угроз и уязвимостей для 2 классов компьютерных атак (атака на уровне СУБД при нарушении политики паролей и атака на уровне сетевого ПО при отсутствии аутентификации). На рис. 7 приведена структура блока «Chart», позволяющего оценить взаимодействие рассматриваемых угроз и уязвимостей. На рис. 8–9 представлены результаты моделирования. Исследования показали, что в модели «голосования» по представительным наборам (ПН) при решении задач анализа киберугроз для КВКС достаточно ограничиться ПН из 3 признаков. Для большей длины наборов эффективность алгоритма оказывалась такой же. При добавлении ПН меньшей длины эффективность алгоритма понижалась.

На диаграммах показано распределение информативности показателей. На гистограмме 8 видно, что объекты из принадлежащие к разным классам ИБ, трудно сложно отделить друг от друга. Это объясняет неэффективность классических алгоритмов распознавания для задач, решаемых в СРКА.

Как следует из рис. 9, в задачах анализа кибератак на КВКС часть значений показателей имеют информативность близкую нулю. Однако достаточно много показателей обладающих большой информативностью.

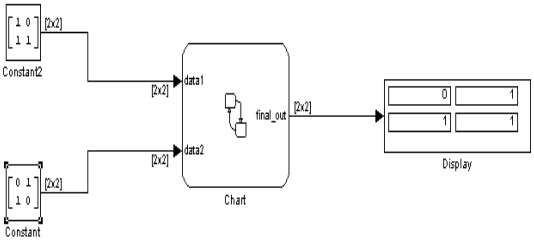

Рис. 6. Пример матрицы идентифицированных источников угроз и уязвимостей для 2 классов компьютерных атак

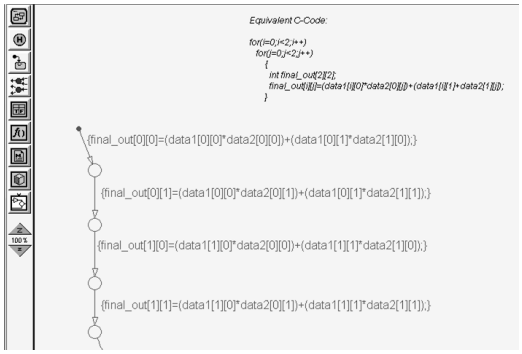

Рис. 7. Структура блока «Chart»

Решение задач распознавания угроз, аномалий и кибератак на основе ПН, целесообразно выполнять при условии отклонения в алгоритме требований тупиковости. Это связано со значительным увеличением времени решения задачи, а, следовательно, значительно снижает скорость работы алгоритма. В тестах применялись ПН, обладающие ограниченной длиной. Максимальная длина набора признаков составила 3. Для меньшего количества признаков в наборе для ряда классов атак оказалось про-

блематично включить в набор все информативные фрагменты. Если количество признаков в наборе увеличить до 4-5, это ведет к увеличению времени работы алгоритма.

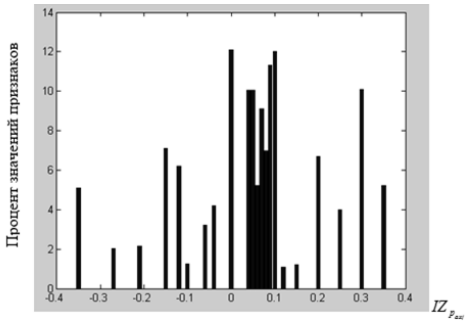

Рис. 8. Распределение типичности значений информативности показателей (признаков) для возможных каналов утечки информации

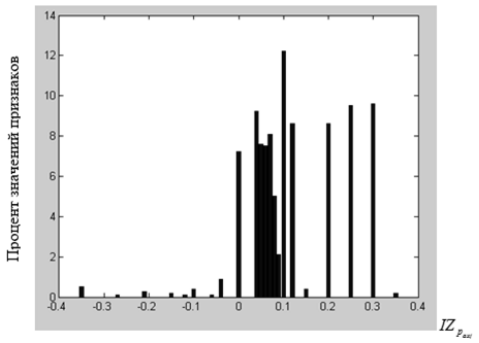

Рис. 9. Распределение типичности значений информативности показателей (признаков) для задачи компьютерной атаки

Таким образом, в работе показано, что применение компонентов интеллектуальной адаптивной защиты информации КВКС, может быть основано на использовании логических процедур и понятии элементарного классификатора для аномалий, киберугроз и уязвимостей КВКС. Изложенные основные подходы к конструированию ЛПРУ с использованием аппарата логических функций, позволят на практике создавать эффективные аналитические, схемотехнические и программные решения СЗИ для КВКС.

Выводы

В результате проведенных исследований, сделаны следующие выводы.

1. Показано, что для проведения эффективной политики ИБ для КВКС, выбору и внедрению СЗИ, поставить в соответствие описание, анализ и моделированием киберугроз и уязвимостей для системы в целом.

2. Разработан метод формирования решающего правила для отнесения рассматриваемых аномалий и кибератак к определенному классу объектов распознавания на основе дискретных процедур, матриц учитывающих информативность признаков, а также, анализе критичности отдельных элементов КВКС. Предложенный метод и модель позволяют выполнять распознавание аномалий и кибератак с минимальным количеством ошибок.

3. Впервые показано, что построение множества элементарных классификаторов для рассматриваемых классов угроз сводится к нахождению допустимых и максимальных конъюнкций для характеристической функции класса объектов распознавания.

Литература

[1] Основная статистика за 2015 год [Электронный ресурс]. – Режим доступа: https://securelist.ru/files/2015/12/KSB_2015_ Stats_FINAL_RU.pdf

[2] Jasiul B. Detection and Modeling of Cyber Attacks with Petri Nets / B. Jasiul, M. Szpyrka, J. Śliwa //Entropy. – 2014. – 16(12). – P. 6602–6623.

[3] 2015 Attacks Statistics [Електронний ресурс]. – Режим доступу: http://www.hackmageddon.com/2016/01/11/2015 – cyber-attacks-statistics/

[4] OSVDB: The Open Source Vulnerability Database. [электронный ресурс] – Режим доступа: http://www.osvdb.org/

[5] Results of internet SSL usage published by SSL Labs. [Електронний ресурс]. – Режим доступу: http://webappsec.org

[6] Creating trust in the digital world EY's Global Information Security Survey 2015. [Електронний ресурс]. – Режим доступу: http://www.ey.com/ Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

[7] Бочков М.В. Активный аудит действий пользователей в защищенной сети / М.В.Бочков, В.А. Логинов, И.Б. Саенко // Защита информации. Конфидент. – 2002. – № 45. – С. 94–98.

[8] Норткат С. Анализ типовых нарушений безопасности в сетях. / Норткат С. – М.: «Вильямс», 2006. – 424 с.

[9] Jyothsna V. A review of anomaly based intrusion detection systems / V. Jyothsna, R. Prasad // International Journal of Computer Applications. – 2011. – Vol. 28, No. 7. – P. 26–35.

[10] MITRE Research Program. [Електронний ресурс]. – Режим доступу: http://www.mitre.org

[11] Анализ и оценивание рисков информационной безопасности [Текст] : монография / А. Г. Корченко, А.Е. Архипов, С.В. Казмирчук. – К. : Лазурит–Полиграф, 2013. – 275 с.

[12] Ахмад Д.М. Защита от хакеров корпоративных сетей / Дубровский И., Флинн Х. пер. с англ. – 2–е изд. – М.: Компаний АйТи; ДМК – Пресс, 2005. – 864 с.

[13] Балтабай А.Г. Применение искусственных нейронных сетей в рамках обеспечения информационной безопасности / А.Г. Балтабай, А.Е. Абдыгаметова, А.А. Жаманкулова // Труды II Международной научно-практической конференции «Информационные и телекоммуни-кационные технологии: образование, наука, практика», Алматы, Казакстан, 3–4 декабря, 2015 года. – С. 60–63.

[14] Heckerman D. A tutorial on learning with bayesian networks / D. Heckerman //Innovations in Bayesian Networks. – 2008. – Vol. 156. – P. 33–82.

[15] ISO/IEC IS 27001:2005 Information technology. Security techniques. Information security management systems. Requirements.

[16] Komar M. Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification. / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov // IEEE 7th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems. – 2013. –Vol. 2. – P. 665–668.

[17] Колегов Д. Н. ДП–модель компьютерной системы с функционально и параметрически ассоциированными с субъектами сущностями / Д. Н. Колегов // Вестник Сибирского государственного аэрокосмического университета имени академика М. Ф. Решетнева. –2009. – № 1(22), Ч. 1. – С. 49–54.

[18] Комаров А.А. Тесты на проникновение: методики и современные подходы / А.А.Комаров // Журнал «IT–спец». – 2009. – № 2. – С. 48–53.

[19] Walk, T. Cyber-attack protection for pipeline SCADA systems [Text] / T. Walk //Pipelines International digest. – 2012. – Vol. 2. – P. 5–8.

[20] Smith Roger. Counter–terrorism Modeling and Simulation: A New Type of Decision Support Tool. [Електронний ресурс]. – Режим доступу: http://www.modelbenders. com/papers /Signal_ 2001_12.pdf.

[21] The Web Hacking Incidents Database 2008: Annual Report. [Електронний ресурс]. – Режим доступу: http://www.breach.com/confirmation /2008WHID.html

[22] Курило А.П. Обеспечение информационной безопасности бизнеса / Курило А.П. – М.: Альпина Паблишер, 2011. – 512 с.

[23] Лахно В.А. Обеспечение защищенности автоматизированных информационных систем транспортных предприятий при интенсификации перевозок [Текст] / В.А. Лахно, А.С. Петров. – Луганск: ВНУ им. В. Даля, 2010. – 280 с.

[24] Vinchurkar D.P. A review of intrusion detection system using neural network and machine learning technique / D.P. Vinchurkar, A. Reshamwala // International Journal of Engineering Science and Innovative Technology.– 2012.–Vol. 1, № 2.–P. 54–63.

[25] Карпінський М.П. Інтегрована модель представлення кризових ситуацій та формалізована процедура побудови еталонів ідентифікуючих параметрів / М.П. Карпінський, А.О. Корченко, А.І. Гізун // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2015. – В.1 (29). – С. 76-85.

[26] Chi S.–D. Network Security Modeling and Cyber At–tack Simulation Methodology / Chi S.–D., Park J.S., Jung K.–C. //LNCS. – 2001. – Vol. 2119. – P. 1-7.

[27] Khan L. A new intrusion detection system using support vector machines and hierarchical clustering / L. Khan, M. Awad, B.Thuraisingham // The International Journal on Very Large Data Bases. – 2007. – Vol. 16, Iss. 4. – P. 507–521.

[28] Казмирчук С.В. Анализ и оценивания рисков информационных ресурсов в нечетких условиях / С.В. Казмирчук // Защита информации – 2013. – Том 15 №2 (59). – С. 133-140.

[29] Норткат С. Обнаружение вторжения в сеть. / Норткат С., Новак Жд. пер. с англ. – М.: Издательство «Лори», 2001. – 384 с.

[30] Пюкке С. М. Размышления по традиционной проблеме / С. М. Пюкке // Защита информации. –2002. –№ 4–5. – С. 22–25.

[31] Мустафина А.К. Тестирование объектно-ориентированных систем / А.К.Мустафина, Алибиева Ж.М., А.У.Утегенова, А.Б.Берлибаева // Вестник Национальной Академии Наук Республики Казахстан. –2015. – № 6. – С. 3–46.

[32] Исмухамедова А. М. Анализ уязвимостей в различных операционных системах / Исмухамедова А. М., Сатимова Е. Г. // Труды II Международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика», Алматы, Казакстан, 3-4 декабря, 2015 года. – С. 191–195.

[33] Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко – К. : «МК-Пресс», 2006. – 320 с.

[34] Мельников В.В. Безопасность информации в автоматизированных системах. / Мельников В.В. – М.: Финансы и статистика, 2003. – 368 с.

[35] Герасименко В.А. Защита информации в автоматизированных системах обработки данных / Герасименко В.А. В 2–х кн. – М.: Энергоатомиздат, 1994. Т1. – С. 132–138.

[36] Скопа О. О. Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем / О. О. Скопа, Н. Ф. Казакова // Системи обробки інформації. – 2009. – Вип. 7. – С. 48–53.

[37] Терейковский И. А. Безопасность программного обеспечения, созданного с использованием семейства технологий COM, DCOM, COM+ / И. А. Терейковский // Захист інформації. – 2006. – № 1. – С. 55–67.

[38] Al–Jarrah O. Network Intrusion Detection System using attack behavior classification. Information and Communication Systems / O. Al–Jarrah, A. Arafat //5th International Conference. – 2014. – P. 1–6.

[39] Atighetchi M. Building Auto–Adaptive Distributed Applications: The QuO–APOD Experience / Atighetchi M., Pal P.P., Jones C.C., Rubel P. // Proceedings of 3rd International Workshop Distributed Auto–adaptive and Reconfigurable Systems (DARES). Providence, USA. – 2003. – P. 74–84.

[40] Chapman C. Project Risk Management: processes, techniques and insights. / C. Chapman, S. Ward. NY – 2003. –Vol. 1210. – P.1-34.

[41] Li W. A New intrusion detection system based on knn classification algorithm in wireless sensor network / W. Li, P. Yi, Y. Wu, L. Pan, J. Li // Journal of Electrical and Computer Engineering. – 2014. – Vol. 2014. – P. 17-25.

[42] Ranjan R. A new clustering approach for anomaly intrusion detection / R. Ranjan, G. Sahoo // International Journal of Data Mining Knowledge Management Process (IJDKP). – 2014. –Vol. 4, No. 2. – P. 29–38.

[43] Iglun K. State Transition Analysis: A Rule–Based Intrusion Detection System / Iglun K., Kemmerer R. A., Porras P. A. //IEEE Transactions on Software Engineering. –1995. – N 21(3). – P. 17–28.

[44] Jha S. Minimization and reliability analysis of attack graphs. Tech–nical Report CMU–CS–02–109 /

Jha S., Sheyner O., Wing J. – Carnegie Mellon University, 2002.

[45] Y. Immunity–Based Systems A Design Perspective. / Ishida Y. – Springer Verlag, 2004. – 192 p.

[46] Knight J. The Willow Architecture: Comprehensive Survivability for Large–Scale Distributed Applications / Knight J., Heimbigner D., Wolf A.L., Carzaniga A., Hill J., Devanbu P., Gertz M. // Proceedings of International Conference Dependable Systems and Networks (DSN 02). Bethesda, MD, USA. – 2002. – P. 17–26.

[47] Selim S., Hashem M., Nazmy T. M. Detection using multi–stage neural network. International Journal of Computer Science and Information Security (IJCSIS). – 2010. –Vol. 8, No. 4. – P. 14–20.

[48] Zhou Y.P. Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection / Y.P. Zhou // Asia–Pacific Conference on Information Processing. – 2009. –Vol. 1. – P. 21–24.

[49] Negoita M. Computational Intelligence Engineering of Hybrid Systems. / Negoita M., Neagu D., Palade V. – Springer Verlag. 2005. – 213 p.

[50] Pawar S.N. Intrusion detection in computer network using genetic algorithm approach: a survey/ S.N. Pawar // International Journal of Advances in Engineering Technology. – 2013. –Vol. 6, Iss. 2. –P. 730–736.

[51] Raiyn J. A survey of Cyber Attack Detection Strategies / J. Raiyn // International Journal of Security and Its Applications. –2014. –Vol.8, No. 1. – P. 247–256.

[52] Городецкий В.И. Концептуальные основы стохастического моделирования в среде Интернет / Городецкий В.И., Котенко И.В. // Труды института системного анализа РАН. – 2005. N. 9. – С. 168–185.

[53] Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : РУТА, 2010. – 280 с.

[54] Котенко И.В. Модели противоборства команд агентов по реализации и защите от распределенных атак «Отказ в обслуживании». // Тр. междунар. научно–технич. конф. IEEE AIS'03 и CAD–2003. –2003. – т. 1. – С. 422 – 428.

[55] Mirkovic J. Internet Denial of Service: Attack and Defense Mechanisms. / Mirkovic J., Dietrich S., Dittrich D., Reiher P. – Prentice Hall PTR, 2004.– P. 400.

[56] Omar S. Machine learning techniques for anomaly detection: an overview / S. Omar, A. Ngadi, H.H. Jebur // International Journal of Computer Applications. – 2013. – Vol. 79, No. 2. – P. 33–41.

[57] Silva F. Mickunas M.D. Modeling Dynamic Adaptation of Distributed Systems / Silva F., Endler M., Kon F., Campbell R.H., // Technical Report UIUCDCS–R–2000–2196, Department of Computer Science, University of Illinois at Urbana–Champaign. – 2000. –70 p.

[58] Горяйнов В.В. О предельных распределениях вероятностей для докритических ветвящихся процессов. / Горяйнов В.В., Полковников А.А. // Теория вероятностей и ее применение.– 1996. – Т.41, вып.2. – С. 417–424.

[59] Иванов К.В. Расчет буферной памяти и времени задержки кадров в коммутаторе OptiSwitch / Иванов К.В. // КГТУ – 2007. – № 4. – С. 57–60.

[60] Templeton S. J. Requires/Provides Model for Computer Attacks. / Templeton S. J., Levitt K. A. Proc. of the New Security Paradigms Workshop, 2000. p. 274.

[61] Tsai C.–F., Hsub Y.–F., Linc C.–Y., Lin W.–Y. Intrusion detection by machine learning: a review. Expert Systems with Applications. –2009. – Vol. 36, Iss. 10. – P. 11994–12000.

[62] Unsupervised adaptive filtering. V. 1, 2. Edited by S. Haykin. – New York: John Willey & Sons, Inc, 2000.

[63] Wu S.X., Banzhaf W. The use of computational intelligence in intrusion detection systems: a review. Applied Soft Computing. – 2010. – Vol. 10, Is. 1. – P. 1–35.

[64] Ameziane E., Hassani, A., Abou El Kalam, A., Bouhoula, A., Abassi, R., Ait Ouahman, A. Integrity–OrBAC: a new model to preserve Critical Infrastructures integrity. International Journal of Information Security. – 2014. – 14 (4). – P. 367–385.

[65] Guitton C., Korzak E. The Sophistication Criterion for Attribution. The RUSI Journal. – 2013. – Vol.158, Iss. 4. – P. 62–68.

[66] Минаев В.А. Информационно – аналитические системы обеспечения безопасности: проблемы и решения. / Минаев В.А. // Системы безопасности связи и телекоммуникаций. – 2001. –№ 42(6). – С. 20–24.

[67] Галатенко В. А. Оценка безопасности автоматизированных систем. Обзор и анализ предлагаемого проекта технического доклада ISO/IEC PDTR 19791. – Jet info. – 2005. – № 7 (146). –С.16 –21.

[68] Гроздов Г.Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы / Гроздов Г.Г. Монография. – Киев: ГУИКТ, 2009. – 132 с.

[69] Козиол Дж. Искусство взлома и защиты систем. / Козиол Дж., Личфилд Д., Эйтэл Д. и др. – СПб.: Питер, 2006. – 416 с.

[70] Яремчук Ю.Е. Модель классификации топологических структур в мультиагентных сетях системы принятия решений при управлении / Яремчук Ю.Е., Шиян А.А., Бекетова Г.С. // Труды II Международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика», г. Алматы, 3-4 декабря, 2015. – С. 295–299.

[71] Баскакова Л.В. Модель распознающих алгоритмов с представительными наборами и системами опорных множеств. / Баскакова Л.В., Журавлев Ю.И. // Журн. Выч. матем. и матем. физики. – 1981. –Т. 21, №5. – С. 1264–1275.

[72] Вайнцвайг М.Н. Алгоритм обучения распознавания образов «Кора». М.: Сов. радио, 1973. – С. 91.

[73] Логинов В.А. Методика активного аудита действий субъектов доступа в корпоративных вычислительных сетях на основе аппарата нечетких множеств / Логинов В.А. //Сб. докл. VI Междунар. конф. SCM'2003. – СПб.: СПГЭТУ. – 2003. – т. 1. – С. 240–243.

[74] Xiang Y. A Survey of Active and Passive Defence Mechanisms against DDoS Attacks. / Xiang Y., Zhou W., Chowdhury M. // Technical Report, TR C04/02, School of Information Technology, Deakin University, Australia. – March 2004.

[75] Mukkamala S., Sung A.H., Abraham A., Ramos V. Intrusion detection systems using adaptive regression splines. Sixth International Conference on Enterprise Information Systems. – 2013. – Part 3. – P. 211–218.

[76] Дмитриев А.И. О математических принципах классификации предметов и явлений / Дмитриев А.И., Журавлев Ю.И., Кренделев Ф.П. Дискретный анализ. – 1966. – Вып. 7. – С. 1–17.

[77] Chung M. Simulating Concurrent Intrusions for Testing Intrusion Detection Systems / Chung M, Mukherjee B., Olsson R. A., Puketza N. //Proc. of the 18th NISSC. – 1995. – P.17.

[78] Harel D. Statecharts: A Visual Formalism for Complex Systems / Harel D.// Science of Computer Programming. – 1987. – Vol. 8. – P. 231–274.

УДК 004.056 (045)

Бекетова Г.С., Ахметов Б.Б., Корченко О.Г., Лахно В.А. Розробка моделі інтелектуального розпізнавання аномалій і кібератак з використанням логічних процедур, які базуються на покриттях матриць ознак

Анотація. *Глобальний розвиток критично важливих комп'ютерних систем (КВКЗ) в енергетиці, промисловості, зв'язку та на транспорті, об'єктах інфраструктури великих мегаполісів, і т.п. Вимагає постійного відстеження кіберзагроз, а також уразливостей технічних компонентів й програмного забезпечення. Недосконаліть існуючих методів кіберзахисту, а також змінний характер дій атакуючої сторони, диктує необхідність продовжувати дослідження в галузі математичного та алгоритмічного розвитку систем захисту інформації, здатних своєчасно виявляти кібератаки, аномалії та загрози. Таким чином, актуальність досліджень, спрямованих на подальший розвиток моделей і методів захисту на основі інтелектуального розпізнавання загроз КВКЗ і забезпечення їх інформаційної безпеки, є однією з ключових проблем кіберзахисту критичної інфраструктури держави. У статті запропоновано схему адаптивної системи захисту інформації КВКЗ і описано модель побудови системи кіберзахисту на основі логічних процедур і матриць ознак кібератак, аномалій і загроз.*

Ключові слова: *кібератака, інформаційна безпека, критично важливі комп'ютерні системи, інтелектуальне розпізнавання, система захисту інформації, системи виявлення аномалій.*

Beketova G., Akhmetov B., Korchenko A., Lakhno A. Design of a model for intellectual detection of cyber-attacks, based on the logical procedures and the coverage matrices of features

Abstract. *The results of studies aimed at further development of methods and algorithms for detection of cyber threats and the most common classes of anomalies and cyber attacks in critical information systems (CIS) are presented. First developed a method for intelligent recognition of threats based on the discrete procedures using the apparatus of logic functions and fuzzy sets, allowing you to create effective analysis, hardware and software solutions of the system of information protection CIS. First developed a model for making a decision rule proposed discrete procedures, which enables detection of threats, with a minimum number of errors. It is proved that the proposed approach allows solving complex problems of the CIS cyber defense control and can be used in the development of software solutions for cyber defense systems.*

Key words: *cyber attacks, information security, mission-critical computer systems, intelligent recognition protection system information, anomaly detection system.*

Отримано *3 жовтня 2016 року*, затверджено редколегією 17 *жовтня 2016 року*