17. *Mukhacheva E.A., Mukhacheva A.S.* Tekhnologiya blochnykh struktur lokal'nogo poiska optimuma v zadachakh pryamougol'noy upakovki [Technology of block structures for local optimal search in rectangular packing problems], *Novye tekhnologii. Informatsionnye tekhnologii. Prilozhenie* [New technologies. Information Technology. Application], 2004, No. 5, pp. 19-31.
18. *Fadel G. Sinha G., McKee A.* Packing optimization using a rubberband analogy, *Design Engineering Technical Conference and Computers and Information in Engineering Conference, Pittsburgh, PA (ASME)*, 2001, Vol. 2, pp. 409-415.
19. *Bova V.V., Kureychik V.V., Lezhebokov A.A.* Problemno orientirovannyy geneticheskiy algoritm upakovki raznogabaritnykh elementov [Problem-oriented genetic algorithm for packing multisized elements], *Vestnik Rostovskogo gosudarstvennogo universiteta putey soobshcheniya* [Bulletin of the Rostov State Transport University], 2014, No. 3 (55), pp. 52-59.
20. *Zhukov L.A., Korchevskaya O.V.* Metod ploskostey: chislennyy eksperiment dlya zadach dvukh i trekhmernoy ortogonal'noy upakovki [Method of planes: numerical experiment for two- and three-dimensional orthogonal packing problems], *Informatsionnye tekhnologii* [Information technologies], 2008, No. 11, pp. 41-45.

Статью рекомендовала к опубликованию д.т.н., профессор Л.С. Лисицина.

Курейчик Владимир Викторович – Южный федеральный университет; e-mail: vkur@sfedu.ru; г. Таганрог, Россия; тел.: 88634383451; кафедра систем автоматизированного проектирования; зав. кафедрой САПР; д.т.н.; профессор.

Бова Виктория Викторовна – e-mail: vvbova@yandex.ru; тел.: 88634371651; кафедра систем автоматизированного проектирования; доцент.

Халенков Александр Юрьевич – e-mail: halenkov@sfedu.ru; тел.: 88634371651; кафедра систем автоматизированного проектирования; аспирант.

Kureichik Vladimir Victorovich – Southern Federal University; e-mail: vkur@sfedu.ru; Taganrog, Russia; phone: +78634371651; the department of computer aided design; head of CAD department; dr. of eng. sci.; professor.

Bova Victoria Victorovna – e-mail: vvbova@yandex.ru; phone: +78634371651; the department of computer aided design; associate professor.

Halenkov Alexander Yuryevich – e-mail: halenkov@sfedu.ru; phone: +78634371651; the department of computer aided design; graduate student.

УДК 004.056 DOI 10.18522/2311-3103-2023-5-66-81

А.А. Олейникова, В.В. Золотарев

КОНЦЕПЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ ЦИКЛА НЕПРЕРЫВНОГО ДЕТЕКТИРОВАНИЯ И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Для динамически изменяющихся объектов управления в задаче управления информационной безопасностью возникают новые задачи, такие как изменение подходов к сбору и анализу данных, разработка динамических сценариев реагирования на угрозы безопасности информации. Они должны быть решены через создание применимых в указанной задаче алгоритмов, моделей, методик и подходов управления безопасностью, в том числе на уровне организации процессов, работы с данными и формирования архитектуры информационной безопасности организации. Кроме того, для разработки и формирования инструментов непрерывного детектирования и реагирования необходимо предложить новые способы интеграции указанных алгоритмов в структуру объекта управления. При этом создание систем реагирования на базе новой концепции предполагает и изменение алгоритмов управления безопасностью таких систем в особых случаях, таких как децентрализованное

управление, тестирование на устойчивость, облачные сервисы безопасности и других, требующих отдельного исследования. При этом реагирование на инциденты информационной безопасности должно предполагать учет непрерывно меняющегося ландшафта угроз и реконфигурации инфраструктуры организации. Также на развитие представленной в статье новой концепции повлияла концепция объектно-ориентированного программирования в части основных положений. Настоящая работа содержит описание концепции управления на основе цикла непрерывного детектирования и реагирования, приводит некоторые алгоритмы и процессы, отличающие реализацию показанной концепции, а также примеры их реализации. Приведенные в статье практические примеры касаются таких вопросов, как формирование окрестности инцидента, и позволяют формировать контекст управления информационной безопасностью. Кроме того, показан подход к автоматизации процессов управления информационной безопасностью. Результаты работы могут быть использованы как для имитационных моделей, так и для реализации в виде набора процессов управления информационной безопасностью в практических задачах. Кроме того, полученные результаты могут быть интегрированы в средства оркестрации для систем защиты информации, что повышает эффективность реагирования на инциденты информационной безопасности.

Управление информационной безопасностью; процессный подход; алгоритм управления безопасностью; управление на основе данных; непрерывное детектирование и реагирование.

A.A. Oleynikova, V.V. Zolotarev

THE CONCEPT OF INFORMATION SECURITY MANAGEMENT BASED ON A CYCLE OF INFORMATION SECURITY INCIDENTS CONTINUOUS DETECTION AND RESPONSE

For dynamically changing management objects, new tasks arise in the task of information security management, such as changing approaches to data collection and analysis, developing dynamic scenarios for responding to information security threats. They should be solved through the creation of algorithms, models, methods and approaches of security management applicable to this task, including at the level of organizing processes, working with data and forming the organization's information security architecture. In addition, for the development and formation of continuous detection and response tools, it is necessary to propose new ways of integrating these algorithms into the structure of the control object. At the same time, the creation of response systems based on the new concept also involves changing the security management algorithms of such systems in special cases, such as decentralized management, stability testing, cloud security services and others that require separate research. At the same time, responding to information security incidents should take into account the continuously changing threat landscape and reconfiguration of the organization's infrastructure. Also, the development of the new concept presented in the article was influenced by the concept of object-oriented programming in terms of the main provisions. This work contains a description of the control concept based on a continuous detection and response cycle, provides some algorithms and processes that distinguish the implementation of the concept shown, as well as examples of their implementation. The practical examples given in the article relate to issues such as the formation of the incident neighborhood, and allow you to form the context of information security management. In addition, an approach to automation of information security management processes is shown. The results of the work can be used both for simulation models and for implementation as a set of information security management processes in practical tasks. In addition, the results obtained can be integrated into orchestration tools for information security systems, which increases the effectiveness of responding to information security incidents.

Information security management; process approach; security management algorithm; data-based management; continuous detection and response.

Введение. Управление информационной безопасностью в современных условиях – непрерывно совершенствующаяся область, содержащая как минимум средства и методы управления безопасностью инфраструктурных решений, про-

цессы и процедуры, а также соответствующие им политики и средства управления. Стандартизированные решения также предполагают опору на циклы совершенствования, контроля и анализа, а также постоянное обновление применимых политик и требований.

В настоящий момент имеет место переход от модели управления информационной безопасностью, основанной на процессной модели, к модели непрерывного детектирования и реагирования на динамически формирующийся ландшафт угроз, что приводит к изменению базовых основ управления информационной безопасностью от уровня инфраструктуры до уровня разработки сценариев реагирования на инциденты информационной безопасности. Также сформирована потребность в обширной автоматизации бизнес-процессов и применении современных подходов к интеграции. Так, эксперты ведущих компаний отмечают, что уже к 2025 году 90% рабочих процессов по обеспечению безопасности будут автоматизированы и управляться в виде кода [1].

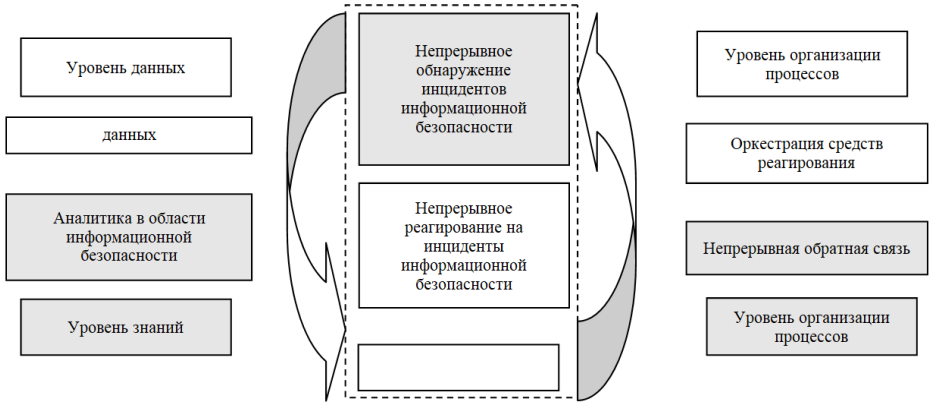

Рис. 1. Концепция CD/CR с учетом уровней развертывания

Кроме того, очевидной тенденцией является расширение области автоматизации в области информационной безопасности до фреймворков, содержащих как анализируемые объекты, так и наборы инструментов, процедур и процессов, реализующих типовые операции [2–4]. Автоматизация часто является необходимостью уже потому, что при традиционном процессном подходе количество атомарных задач реагирования на угрозы безопасности информации (задач, декомпозиция которых нецелесообразна) может достигать сотен тысяч и миллионов [5].

Внутри задач автоматизации привычным является наличие стандартных, статичных планов реагирования, которые представляют собой либо разветвленные и содержащие множество условий графы, сложные алгоритмы действий, покрывающие большое количество ситуаций, либо множество небольших алгоритмов реагирования с описанием их реализации (плейбуков), специализированных под конкретный тип инцидента.

При этом инфраструктура предприятия – живой организм, который постоянно меняется: добавляются новые устройства, сегменты сети, меняются политики работы критичных активов, добавляются новые средства защиты информации, в том числе и с уникальными характеристиками и настройками. По этой причине в организациях с развитым уровнем информационной безопасности регулярно проводятся аудит и инвентаризация, которые помогают актуализировать информационную модель предприятия.

Ключевой проблемной ситуацией в этом случае является следующее: существует ли способ в процессе инцидента подстраиваться под текущую ситуацию как в инфраструктуре, так и в способе исполнения атакующей техники?

Вопрос целесообразности реализации таких способов реагирования также зависит от уровня зрелости системы управления информационной безопасностью в организации. Здесь и далее предполагается, что организация, применяющая описанную в работе концепцию управления информационной безопасностью, как минимум стандартизировала и автоматизировала основные процессы управления информационной безопасностью, в том числе процесс управления инцидентами, и нуждается именно в оптимизации детектирования и реагирования, а не в первичной реализации этого процесса.

Следующий аспект, влияющий на эффективность защиты – динамика внешнего окружения. В текущих реалиях техники реализации атак эволюционируют, усложняются, затрагивают новые типы данных инфраструктуры, используют новые механизмы и способы посткомпрометации. Например, программы-вымогатели «ransomeware» теперь не только шифруют данные организации и требуют оплату за восстановление доступа, но могут так же реализовать утечку данных организации, для реализации сценария шантажа организации в обмен на неразглашение информации властям, конкурентам или общественности.

В силу динамического ландшафта угроз и способов их реализации, плейбуки систем реагирования тоже должны изменяться, чтобы не устаревать на фоне меняющегося поведения злоумышленников.

В рамках развития подхода с 2022 года ведущими организациями начали на практике применяться модели, развивающие идеи непрерывного обнаружения и реагирования на инциденты информационной безопасности. В частности, операционная модель ASO [1] (рис. 1) основана на создании непрерывных циклов обратной связи в основных областях обнаружения и реагирования на инциденты. Ее совмещение с уровнями развертывания по четырехуровневой модели управления информационной безопасности, ранее предложенной авторами, также учтено [6].

Исследователями также оценивается возможность комплексного измерения безопасности на базе оценки зрелости [7, 8], а также различные аналитические модели реагирования на угрозы безопасности, основанные на привязке к бизнес-процессам организации и возможностям оркестрации средств защиты информации [9, 10].

Следовательно, **что целью предлагаемых изменений** в целом является переход к концепции управления информационной безопасностью на основе цикла непрерывного детектирования и реагирования (CD/CR), учитывающей возможность непрерывного управления с реализацией обратной связи на основе данных от управляемого объекта, но при этом основанной на автоматизации всех рабочих процессов и быстром развертывании в инфраструктуре независимо от ее характеристик и особенностей.

Цели, задачи и ограничения. Итак, в настоящем исследовании предлагается концепция управления информационной безопасностью на основе цикла непрерывного детектирования и реагирования на инциденты информационной безопасности, базис которой составляют три условия:

1) Ориентация на управляемый объект;

2) Ориентация на данные;

3) Независимость от физической инфраструктуры.

Целью разработки концепции является обоснование нового подхода к автоматизации управления информационной безопасностью **на основе цикла непрерывного детектирования и реагирования на инциденты информационной**

безопасности в виде автоматизация-как-код и формирование основы для изменения политик безопасности и сценариев реагирования, учитывающих особенности этого подхода.

Проблемы, возникающие при этом, это:

1) **эксфильтрация данных и действий**,

2) создание **синтетических данных** для задач непрерывного детектирования и реагирования,

3) управление знаниями, а именно **сценарии динамического реагирования** на инциденты информационной безопасности.

Проблема **эксфильтрации данных** возникает при обмене данными между участниками процессов и объектами, содержащими необходимые им данные (узлами документооборота, внешними и внутренними агрегированными базами данных). При этом возникающие потоки данных могут быть нарушающими принятые политики безопасности в отношении информационного обмена, а коммуникации – скрытыми, неявными или слабоконтролируемыми [11].

При реализации управления на основе данных добавляется сложность контроля автоматизированных и автоматических коммуникаций и коннекторов, существующих как элемент автоматизации бизнес-процессов информационной безопасности и роботизированных программных решений. Эти коммуникации могут быть либо не полностью контролируемыми с позиций распространения конфиденциальной информации (или иных типов информации, контроль над которыми может представлять интерес для организации), либо находиться в состоянии неполного контроля в определенных переходных состояниях организационных и информационных систем.

Проблема **эксфильтрации действий** возникает при работе автоматизированного процесса в области информационной безопасности тогда, когда требуется воздействие на объект, задействованный другими процессами, или на другие процессы. Такие действия могут быть злоумышленными, а также не полностью контролируемыми, что создает опасность неконтролируемого изменения как самих процессов, так и операционной среды.

Проблема **управления знаниями** для задач автоматизации и управления в виде кода возникает из-за формирования баз знаний, содержащих сценарии с чувствительной информацией и удаленным доступом к ним, а также непрерывным изменением и распространением знаний в процессах управления информационной безопасностью. В частности, примерами проявления такой проблемы является обмен данными об индикаторах компроментации или применение сценариев реагирования на инциденты в децентрализованных системах.

Общая схема концепции управления информационной безопасностью на основе цикла непрерывного детектирования и реагирования на инциденты информационной безопасности. На уровне общей схемы и работы с данными добавляется также следующее условие: существует необходимость получить доступ к как можно большему количеству источников для сбора, анализа, валидации и верификации информации; с точки зрения информационной безопасности это будет нарушением принципа минимизации полномочий и локализации объектов защиты информации в инфраструктуре организации, если не будут приняты соответствующие усилия по формированию дополнений в политику информационной безопасности организации. Причина такого противоречия в том, что эффективность управления с увеличением количества источников данных должна возрастать [12], а сложность реализации систем защиты информации для подобных решений может становиться неприемлемой из-за возможных неполных или нецелесообразных подходов и решений. Важны также и форматы собираемых данных [13].

Итак, концепция должна на базовом уровне учитывать:

1. Работу с источниками данных.
2. Работу с политиками управления данными, применимыми в области информационной безопасности.
3. Работу с автоматизированными процессами и управляемыми объектами.

Кроме того, можно отметить, что существуют недостатки реально применяемых схем реализации детектирования и реагирования на инциденты информационной безопасности, связанные с низким уровнем зрелости процессов реагирования в организациях, даже если применены подходы по автоматизированному реагированию и сценарии реагирования на инциденты информационной безопасности реализованы в схеме автоматизация-как-код (рис. 2).

Указанная схема уже предлагает улучшения по сравнению с традиционным подходом на основе системы обеспечения информационной безопасности, основанной на процессной модели. В частности, появление сервисно-ориентированной модели управления безопасностью, шаблонов (паттернов) безопасности и отдельного управления сервисами безопасности (этап I) декларирует повышение управляемости на уровне организации процессов информационной безопасности.

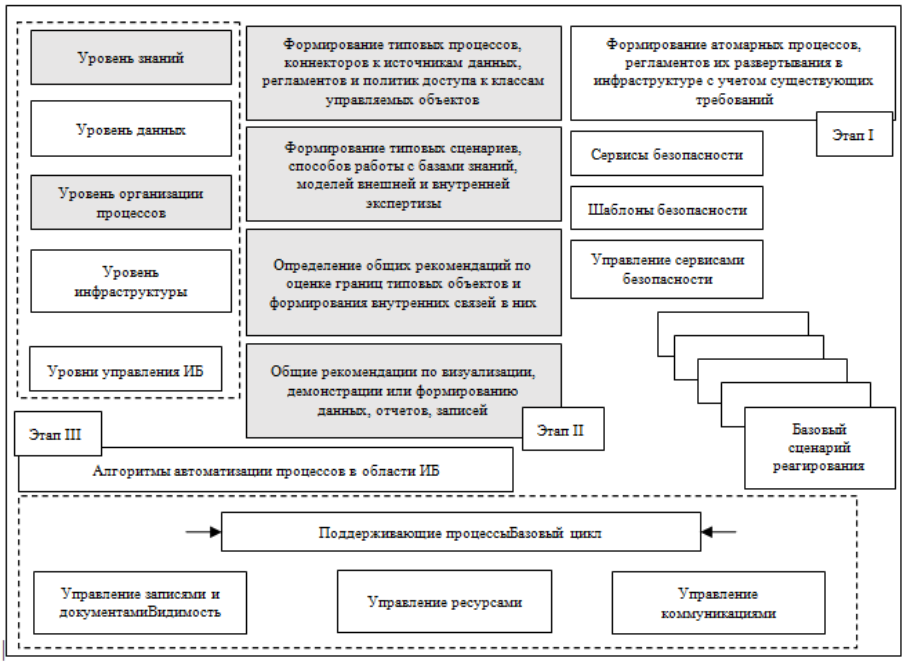

Рис. 2. Недостатки схемы реагирования на низком уровне зрелости

Вместе с тем имеются следующие недостатки, которые ограничивают эффективность предлагаемой схемы:

- предполагается, что данных, полученных на этапе II, достаточно для реагирования на угрозы информационной безопасности. Это не вполне соответствует эмпирически полученным результатам. В частности, примеры извлечения информации о динамически меняющемся ландшафта угроз [14] сигнализируют о возможной неэффективности указанной схемы в случае непрерывного изменения атак и неполной информации о деструктивных действиях,

♦ предполагается, что может существовать стабильный механизм противодействия угрозам безопасности, привязанный к инфраструктуре. По-видимому, это не так, поскольку динамически меняющийся ландшафт угроз приведет к неэффективности подобного механизма, даже реализованного на этапе III в рамках сервисной модели,

♦ границы области анализа и рекомендации по визуализации данных также требуют учета динамики развития реагирования на угрозы безопасности, поскольку указанные выше недостатки говорят о необходимости формирования дополнительных (синтетических) данных для обогащения информации об объекте управления, а также постоянном мониторинге инфраструктуры с учетом полученных данных.

Основываясь на этом, можно сформировать основные **принципы** предлагаемой концепции:

0) Предварительно должно учитываться условие, что любой автоматизированный и управляемый как код процесс будет использовать множество источников данных и баз знаний и управляемый объект не должен быть причиной утечки информации во время такого использования. Следовательно, должны быть предъявлены отдельные требования к операционной среде. Кроме того, должен существовать изолированный репозиторий, содержащий все необходимые для управления данные объекта, и политика управления доступом к указанному репозиторию на всех этапах его жизненного цикла.

1) Все данные и знания, ключевые для выполнения операций над управляемым объектом, должны быть связаны с ним и храниться в общей для объекта и автоматизированного процесса управления операционной среде. Этот принцип может предполагать управление объектом как микросервисом, контейнеризацию, формирование песочниц или иных виртуальных сред, а также облачные решения. Таким образом, данные и знания должны быть инкапсулированы в объект.

В качестве дополнения необходимо отметить, что управляемый объект абстрагируется от физической инфраструктуры. Границы управляемого объекта и область управления должны быть определены согласно требованиям автоматизированного процесса управления информационной безопасности, разворачиваемого с определенными конфигурационными параметрами, а также требований коннекторов и иных средств извлечения данных. Управление знаниями должно осуществляться в рамках границ управляемого объекта.

Внешние запросы к данным и знаниям должны быть контролируемыми и не должны изменять накопленные данные и знания извне.

Данные и знания, необходимые для динамического изменения алгоритмов реагирования и составляющие контекст безопасности для конкретного управляемого объекта, группы объекта или системы в целом, могут и должны быть синтезированы на этапе анализа объекта и привязки к физической инфраструктуре. При этом может иметься как статический, так и динамический набор алгоритмов синтеза и обогащения контекста безопасности. Интерес может представлять также интепретация внешних источников данных на этапе синтеза и обогащения контекста.

Также в рамках обогащения контекста могут и должны (если такая возможность существует) использоваться ретроданные, то есть данные о предыдущих состояниях управляемого объекта и (если такая возможность существует) связанных объектов.

2) Процесс может управлять группой объектов, используя общую конфигурацию автоматизированного управления. Наследование характеристик управления в рамках концепции предполагает как использование отдельных методов и процедур контроля, применимых для конкретного управляемого объекта, так и форми-

рование общей операционной модели для классов объектов, таких, например, как автоматизированные системы управления технологическими процессами. Каждый способ унификации характеристик должен предполагать безопасный алгоритм обращения к данным и знаниям, унифицированный в части источников данных и знаний, в том числе внешних, а также правил доступа к ним.

3) Разные типы данных, получаемые из источников данных объекта, должны обрабатываться универсальными способами. При этом должны поддерживаться как основанные на API способы сбора данных, так и способы, позволяющие собирать данные без прямого доступа, в том числе и свидетельства из косвенных источников. Тем не менее, даже свидетельства из косвенных источников должны быть цифровыми и собираться автоматизированно.

Кроме того, должен существовать универсальный способ обращения к ретроданным для целей обогащения контекста безопасности. Это предполагает либо существование накопленной статистики данных, либо формирование такой статистики с момента внедрения концепции, основываясь на указанных выше принципах.

Далее рассмотрена общая схема работы в рамках данной концепции, учитывающая четырехуровневую модель управления информационной безопасностью [6] (рис. 3), а также схема работы с автоматизированными бизнес-процессами управления информационной безопасностью на уровне данных и знаний (рис. 4).

Вспомогательные процессы в данной схеме должны обеспечить работу с записями, документами и регистрационными данными.

Задачей вспомогательных процессов также может быть формирование и поддержка операционных средств, включая управление облачными или виртуальными средствами, регламенты и алгоритмы их контроля, а также создание защищенных интерфейсов и баз данных для служебной (технологической) информации.

Рис. 3. Общая схема управления информационной безопасностью на основе предлагаемой концепции

Кроме того, необходимо рассмотреть высокоуровневую автоматизацию процессов управления информационной безопасностью, которая должна содержать базовые (типовые) алгоритмы и процессы реагирования, использующие только доступные извне данные управляемых объектов (рис. 4). Типовые алгоритмы и процессы могут использоваться в различных задачах, таких как быстрое развертывание в рамках инфраструктуры-как-код, обучение и демонстрационные стенды, а также для исследовательских задач и формирования новых специальных алгоритмов реагирования на угрозы информационной безопасности.

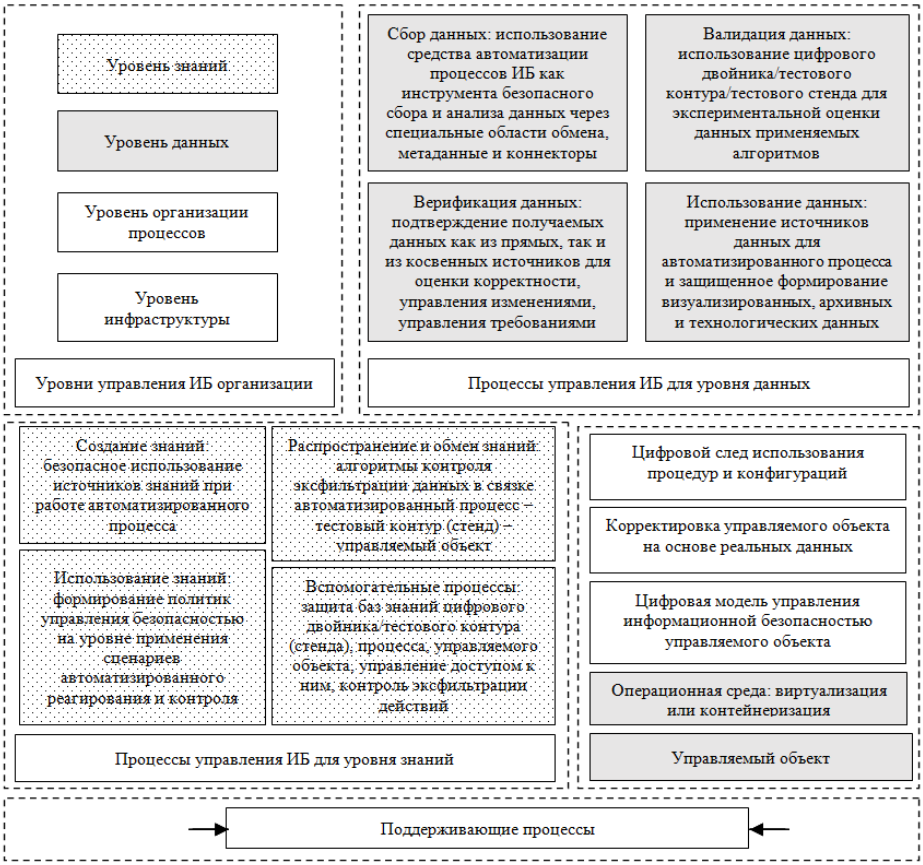

Рис. 4. Схема работы с автоматизированными бизнес-процессами управления информационной безопасностью на уровне данных и знаний

Таким образом (рис. 4) также создается и основа для быстрой разработки автоматизированных фреймворков, содержащих наборы типовых алгоритмов для различных задач и их защищенные модификации.

Пример реализации предложенной концепции. Принцип эксперимента в следующем: проверяется возможность оценки работы с объектом на описанных в концепции принципах для реальной системы класса SOAR. Для решения первой задачи (учета динамики изменений инфраструктуры) был разработан подход на основе предложенной концепции (рис. 5), который заключается в применении лучших практик CD/CR к выстраиванию процессов информационной безопасности (ИБ). Первыми об этой технологии как о перспективной разработке, как уже упоминалось выше, заявила корпорация Google [1]. В разрезе их исследований

предлагается разбить процессы и процедуры информационной безопасности до атомарных функций, которые можно переспользовать и которые являются по сути небольшими унифицированными процессами по выполнению операции. Атомарные унифицированные процессы хранятся в репозитории; функция выполняется единственным экземпляром рабочего процесса, который правится в одном месте разными заинтересантами (таким образом, соблюдается консистентность) и, когда возникает необходимость, этот процесс стандартным образом включается в плейбук за счет унифицированного input/ouput.

Примером унифицированного процесса может быть процедура сбора аутентификационных сессий с хоста. Она может быть выполнена разными способами и разными средствами в зависимости от типа хоста, политик использования хоста или закрывающего средства защиты информации. Но, если все эти вариации обрабатываются в рамках одного универсального процесса сбора аутентификаций с одним стандартным input/ouput, то строить процессы ИБ проще. Атомарный процесс, ко всему прочему, будет переиспользован в совершенно разных процессах ИБ: не только при построении динамических плейбуков в процессе управления инцидентами, но еще и в управлении активами, управлении учетными записями и т.д.

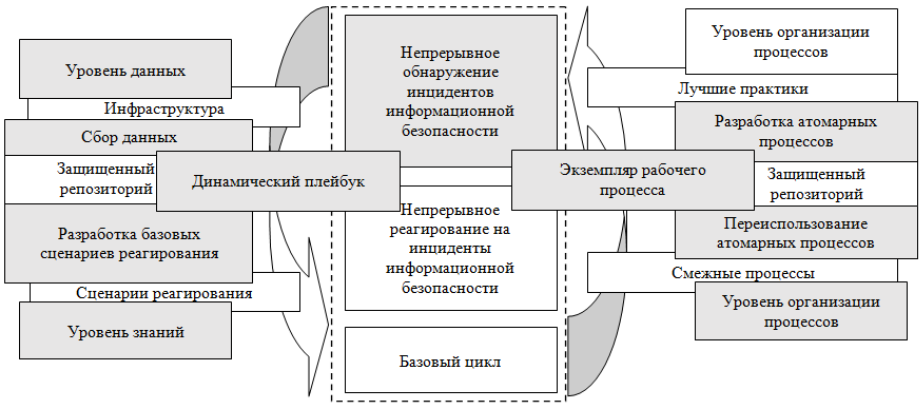

Рис. 5. Применение концепции на практике с учетом уровней развертывания

Набор таких унифицированных процессов дает нам возможность формировать уникальный подход к конкретной инфраструктуре или конкретному ее состоянию.

Выше (рис. 5) рассмотрен только способ решения первой части проблемы – учета актуального состояния инфраструктуры. Так же нам нужно решить проблему обфускации проведения атак [15], что по сути своей является уже дедуктивным расследованием, которое сложно покрыть корреляционным анализом. Дополнительно необходимо учесть, что атакующие могут применять множество дополнительных возможностей, таких как боковые перемещения, эксфильтрацию данных и прочее [16], что дополнительно осложняет детектирование и анализ. В какой-то степени отклонения от поведения можно покрыть через анализ аномалий (UEBA) [17] и все равно это не дает полной информации об инциденте: поиск аномалий в поведении устройств/человека и отклонения в исполнении атак – это разные вещи. Таким образом, на данном этапе необходимо работать над поиском признаков компрометаций устройств или учетных записей, используя технологию threat hunting (построение гипотез об угрозах безопасности информации по поиску подозрительной активности). И действительно, контролирование изменчивости про-

ведения техник атак через распространенные признаки компрометации устройств – одна из задач, решаемых аналитиками третьей линии, специализирующихся на поиске угроз.

Если использовать подходы threat hunting в применении к окрестностям инцидента, то мы можем найти дополнительные обьекты, которые были скомпрометированы, несмотря на то, что ранее техника проведения атаки их не затрагивала. Например, эксплуатация уязвимости не компрометировала учетную запись или вредоносное программное обеспечение не подгружало какой-то хакерский tool set.

Алгоритм формирования окрестности инцидента, то есть автоматизированного формирования контекста инцидента, может включать (но не обязательно состоит только из них) следующие шаги:

Этап 1. Внутреннее сетевое сканирование и попытки эксплуатации уязвимостей внутри сети автоматизированными средствами анализа защищенности и/или специальными инструментальными средствами для тестирования на проникновение.

Этап 2. Детектирование подозрительной сетевой активности системных утилит (rundll32, regsvr32, mshta, certutil).

Этап 3. Детектирование запуска командных интерпретаторов (powershell, cmd, wscript, cscript) офисными приложениями (word, excel).

Этап 4. Мониторинг процесса записи в ключи реестра, отвечающие за автозагрузку либо за изменение системных настроек операционной системы.

Этап 5. Мониторинг создания служб, задач планировщика с powershell, а также LOLbins утилитами.

Этап 6. Детектирование запуска пользователем нерегламентированного ПО (утилиты администрирования, VPN-клиенты, TOR, torrent-клиенты и т.д.).

Рассмотрим также более подробно сбор данных об инциденте (рис. 5) на примере. Очевидно, что алгоритм формирования окрестности инцидента может быть дополнен, если появляется типовой способ детектирования конкретного или типового инцидента или его индикаторов компрометации.

Далее, если наложить это на практические аспекты формирования окрестности инцидента, можно заметить, что, к примеру, подозрительные процессы находятся по подозрительным родителям системных процессов, то есть логика наследования соблюдается и в области детектирования (рис. 6).

Рис. 6. Дополнительные данные об инциденте

Расширяя пример использования, можно показать, что в командной строке можно найти код powershell с «полезной нагрузкой» в base64, что означает обфускацию кода, скрывающую дополнительный объект, потенциально используемый злоумышленником (рис. 7). Таким образом, расширяется количество данных, используемых для анализа инцидента.

На этом этапе очевидно, что такой подход может дать существенно расширенный набор дополнительной информации и новые объекты, затронутые в ходе реализации инцидента.

Если поиск этих объектов может быть встроен в анализ инцидента, динамический плейбук будет базироваться на реальном актуальном контексте атаки, то есть на всех объектах, включая расширенный набор (рис. 5-7), связанный с инцидентом.

По итогу формируется **расширенная область, затронутая инцидентом**, по которой из репозитория процессов можно начать собирать динамический процесс реагирования по следующему алгоритму:

Этап 1. Выбор набора возможных атомарных процессов реагирования для внутренних хостов.

Этап 2. Выбор набора атомарных процессов реагирования для скомпрометированной (ых) учетных записей.

Этап 3. Выбор набора атомарных процессов реагирования для дополнительных объектов (почтового сервера, объектов, подвергшихся воздействию ВПО и т.п.).

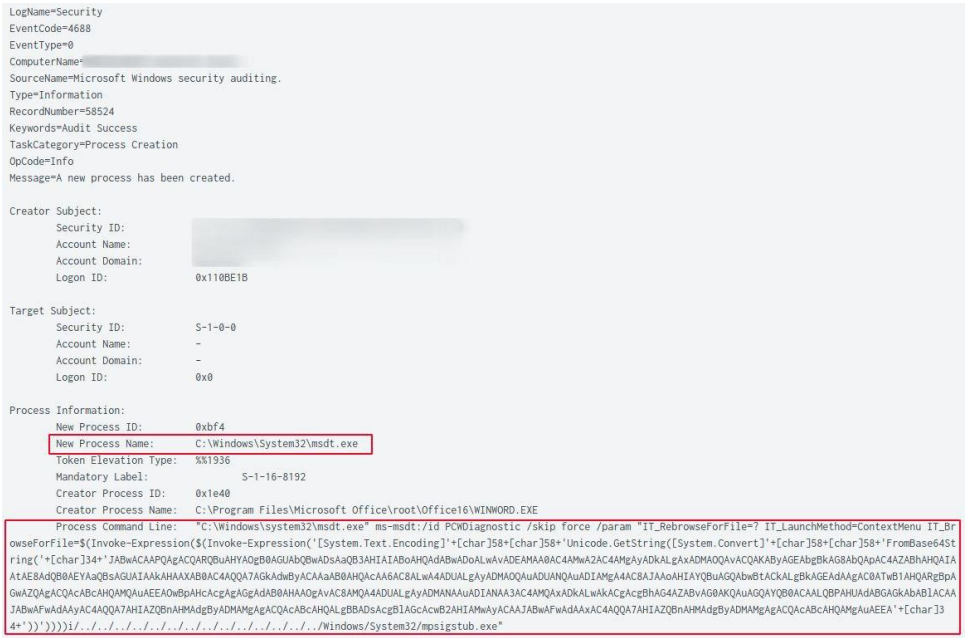

Рис. 7. Расширенный анализ данных об инциденте

Из результатов указанного алгоритма начинает выстраивается динамический плейбук: если появляется конкретный тип объекта появился, процесс добавляется в процесс реагирования. Множество унифицированных процессов реагирования на множестве объектов ограничивается рекомендациями по выполнению конкретных действий, в зависимости от техники атаки, определенной в процессе классификации инцидента. Следовательно, динамика плейбука заключается в изменении состава действий реагирования в зависимости от пораженных объектов и техники атаки. Этот подход позволяет создавать связанный набор действий, актуальный конкретной ситуации.

Расширяя пример использования далее, можно заметить, что возможно дополнить (сформировать) не только окрестность инцидента, но и выстроить цепочки атаки (*kill chain*) [18] из отдельных инцидентов в связанную историю, отобра-

жающую ландшафт атаки, растянутой по периметру, времени и способам исполнения. В действительности атаки становятся все более комплексными и сложными, из инцидентов с различными техниками, которые еще и связаны между собой неочевидными параметрами или свойствами (например, наличием в инцидентах одного и того же процесса, либо использование однотипного *named pipes*).

Подобные ситуации не покрываются стандартными планами реагирования, но, если добавить в стандартные подходы динамическую составляющую, то инциденты могут быть связаны по идентичным объектам и контексту: запуски аналогичных подозрительных процессов, сетевых аутентификаций, задействованных учетных записей, корреляция имен задействованных хостов в разных инцидентах, скорее всего, говорят о принадлежности к одному и тому же *kill chain*. При таком подходе инциденты становятся связанными, а динамические плейбуки выстраиваются в последовательность работы над атакой, то есть переходят на более высокий (стратегический) уровень планов реагирования.

Если проанализировать собранную информацию через классификацию по угрозам *Mitre Att@ck* [19] или БДУ ФСТЭК [20], то этапы *kill chain* могут быть преобразованы автоматизированно в последовательность тактик, применяемых нарушителем, на которые со стороны защищаемой организации динамически выстраивается контекстный ответ.

Заключение. Исследование сосредоточено на формировании пригодных в практике рекомендаций по построению процессной модели управления информационной безопасности, построенной на предлагаемой концепции управления информационной безопасностью. Особенностью подхода является привязка автоматизации и детектирования угроз безопасности к управляемому объекту, а не к инфраструктуре или отдельному процессу. При текущей волатильности в информационной безопасности, сложной динамике процессов управления информационной безопасностью и контекста инцидентов, в том числе и поведения нарушителей, состояния состояния защищаемых инфраструктур, необходимо соответствующие, симметричные динамике ситуации, динамичные подходы к детектированию и реагированию на инциденты информационной безопасности.

Представлены также некоторые условия управления информационной безопасностью при применении предлагаемой концепции, такие как контроль эксфильтрации данных.

Подобное расширение может быть полезно при развертывании разных типов экспертных и советующих систем, систем поддержки принятия решений, ситуационных центров и особенно интересно для задач управления знаниями в области создания и улучшения динамически формируемых сценариев реагирования на угрозы информационной безопасности, опирающихся на описанную концепцию, которые возможно рассмотреть в отдельных исследованиях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ghanizada I.* IT prediction: the vast majority of security operations workloads will be automated. – URL: https://cloud.google.com/blog/products/identity-security/it-prediction-vast-majority-of-security-operations-workloads-will-be-automated.
2. *Королев И.Д., Литвинов Е.С., Маркин Д.И.* Повышение уровня автоматизации процессов сбора данных о выявленных событиях и инцидентах информационной безопасности // Инженерный вестник Дона. – 2021. – Т. 82, № 10. – С. 140-151.
3. *Котенко И.В., Саенко И.Б., Юсупов Р.М.* Новое поколение систем мониторинга и управления инцидентами безопасности // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2014. – № 3 (198). – С. 7-18.

4. *Богданов В.В., Домуховский Н.А., Савин М.В.* SOAR: автоматизация работы с инцидентами информационной безопасности // Защита информации. Инсайд. – 2021. – № 3 (99). – С. 13-17.
5. *Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г.* Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. – 2017. – № 5 (24). – С. 2-16. – DOI: 10.21681/2311-3456-2017-5-2-16.
6. *Золотарев В.В., Лапина М.А.* Модель и алгоритм управления информационной безопасностью образовательной организации высшего образования с учетом требований управления на основе данных // Прикаспийский журнал: управление и высокие технологии. – 2022. – № 4 (60). – С. 107-118. – DOI: 10.54398/20741707_2022_4_107.
7. *Bailey K.* Detection Engineering Maturity Matrix. – URL: https://detectionengineering.io/.
8. *Велигодский С.С., Милославская Н.Г.* Подход к оценке уровня зрелости центров управления сетевой безопасностью // Системы высокой доступности. – 2023. – Т. 19, № 2. – С. 25-37. – DOI: 10.18127/j20729472-202302-02.
9. *Королев И.Д., Попов В.И., Коноваленко С.А.* Методика аналитической обработки распределенных во времени инцидентов информационной безопасности // Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12, № 5. – С. 53-61. – DOI: 10.36724/2409-5419-2020-12-5-53-61.
10. *Сагиров Р.А.* Применение нейронных сетей для автоматизации задач в области информационной безопасности // Защита информации. Инсайд. – 2019. – № 5 (89). – С. 56-59.
11. *Золотарев В.В.* Алгоритм контроля эксфильтрации данных с учетом требований управления на основе данных // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 4 (64).
12. *Иванов А.В., Никрошкин И.В., Огнев И.А., Киселев М.А.* Применение средств экспертизы Blue Team в процессе мониторинга информационных систем на примере платформы TI (Threat Intelligence) // Безопасность цифровых технологий. – 2023. – № 2 (109). – С. 34-51. – DOI: 10.17212/2782-2230-2023-2-34-51.
13. *Савин М.В., Стойчин К.Л., Некрасов А.В., Комаров Н.В.* Обзор стандартов и форматов представления автоматизированных сценариев реагирования на инциденты компьютерной безопасности // Защита информации. Инсайд. – 2022. – № 4 (106). – С. 14-19.
14. *Rahman R., Hezaveh R., Williams L.* What Are the Attackers Doing Now? Automating Cyberthreat Intelligence Extraction from Text on Pace with the Changing Threat Landscape: A Survey // ACM Comput. Surv. – December 2023. – 55, 12, Article 241. – 36 p. – https://doi.org/10.1145/3571726.
15. *Ерохин В.* Поиск вредоносных сценариев powershell с использованием синтаксических деревьев // Безопасность информационных технологий. – 30 (3). – P. 77-89. – DOI: http://dx.doi.org/10.26583/bit.2023.3.05.
16. Follina Exploit Leads to Domain Compromise. – URL: https://thedfirreport.com/2022/10/31/follina-exploit-leads-to-domain-compromise/.
17. *Salitin M.A., Zolait A.H.* The role of User Entity Behavior Analytics to detect network attacks in real time // 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain, 2018. – P. 1-5. – DOI: 10.1109/3ICT.2018.8855782.
18. *Hutchins E.M., Cloppert M.J., Amin R.M.* Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains // Lockheed Martin Corporation. – URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
19. MITRE ATT&CK. – URL: https://attack.mitre.org/.
20. Банк данных угроз безопасности информации / Федеральная служба по техническому и экспортному контролю, Государственный научно-исследовательский испытательный институт проблем технической защиты информации. – URL: https://bdu.fstec.ru/.

REFERENCES

1. *Ghanizada I.* IT prediction: the vast majority of security operations workloads will be automated. Available at: https://cloud.google.com/blog/products/identity-security/it-prediction-vast-majority-of-security-operations-workloads-will-be-automated.

2. *Korolev I.D., Litvinov E.S., Markin D.I.* Povyshenie urovnya avtomatizatsii protsessov sbora dannykh o vyyavlennykh sobytiyakh i intsidentakh informatsionnoy bezopasnosti [Increasing the level of automation of data collection processes on identified events and incidents of information security], *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don], 2021, Vol. 82, No. 10, pp. 140-151.
3. *Kotenko I.V., Saenko I.B., Yusupov R.M.* Novoe pokolenie sistem monitoringa i upravleniya intsidentami bezopasnosti [A new generation of security incident monitoring and management systems], *Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Tele-kommunikatsii. Upravlenie* [Scientific and Technical Bulletin of St. Petersburg State Polytechnic University. Computer science. Telecommunications. Management], 2014, No. 3 (198), pp. 7-18.
4. *Bogdanov V.V., Domukhovskiy N.A., Savin M.V.* SOAR: avtomatizatsiya raboty s intsidentami informatsionnoy bezopasnosti [SOAR: automation of work with information security incidents], *Zashchita informatsii. Insayd* [Information protection. Inside], 2021, No. 3 (99), pp. 13-17.
5. *Kotenko I.V., Fedorchenko A.V., Saenko I.B., Kushnerevich A.G.* Tekhnologii bol'shikh dannykh dlya korrelyatsii sobytiy bezopasnosti na osnove ucheta tipov svyazey [Big data technologies for the correlation of security events based on the types of connections], *Voprosy kiberbezopasnosti* [Issues of cybersecurity], 2017, No. 5 (24), pp. 2-16. DOI: 10.21681/2311-3456-2017-5-2-16.
6. *Zolotarev V.V., Lapina M.A.* Model' i algoritm upravleniya informatsionnoy bezopasnost'yu obrazovatel'noy organizatsii vysshego obrazovaniya s uchetom trebovaniy upravleniya na osnove dannykh [Model and algorithm of information security management of an educational organization of higher education taking into account the requirements of data-based management], *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: management and high technologies], 2022, No. 4 (60), pp. 107-118. DOI: 10.54398/20741707_2022_4_107.
7. *Bailey K.* Detection Engineering Maturity Matrix. Available at: https://detectionengineering.io/.
8. *Veligodskiy S.S., Miloslavskaya N.G.* Podkhod k otsenke urovnya zrelosti tsentrov upravleniya setevoy bezopasnost'yu [An approach to assessing the level of maturity of network security management centers], *Sistemy vysokoy dostupnosti* [High availability systems], 2023, Vol. 19, No. 2, pp. 25-37. DOI: 10.18127/j20729472-202302-02.
9. *Korolev I.D., Popov V.I., Konovalenko S.A.* Metodika analiticheskoy obrabotki raspredelennykh vo vremeni intsidentov informatsionnoy bezopasnosti [Methodology of analytical processing of information security incidents distributed in time], *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli* [High–tech technologies in Earth space research], 2020, Vol. 12, No. 5, pp. 53-61. DOI: 10.36724/2409-5419-2020-12-5-53-61.
10. *Sagirov R.A.* Primenenie neyronnykh setey dlya avtomatizatsii zadach v oblasti informatsionnoy bezopasnosti [Application of neural networks for automation of tasks in the field of information security], *Zashchita informatsii. Insayd* [Information protection. Inside], 2019, No. 5 (89), pp. 56-59.
11. *Zolotarev V.V.* Algoritm kontrolya eksfil'tratsii dannykh s uchetom trebovaniy upravleniya na osnove dannykh [Algorithm of data exfiltration control taking into account the requirements of data-based management], *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: management and high technologies], 2023, No. 4 (64).
12. *Ivanov A.V., Nikroshkin I.V., Ognev I.A., Kiselev M.A.* Primenenie sredstv ekspertizy Blue Team v protsesse monitoringa informatsionnykh sistem na primere platformy TI (Threat Intelligence) [The use of Blue Team expertise tools in the process of monitoring information systems on the example of the TI (Threat Intelligence) platform], *Bezopasnost' tsifrovykh tekhnologiy* [Security of digital technologies], 2023, No. 2 (109), pp. 34-51. DOI: 10.17212/2782-2230-2023-2-34-51.
13. *Savin M.V., Stoychin K.L., Nekrasov A.V., Komarov N.V.* Obzor standartov i formatov predstavleniya avtomatizirovannykh stsenariev reagirovaniya na intsidenty komp'yuternoy bezopasnosti [Review of standards and formats for the presentation of automated scenarios for responding to computer security incidents], *Zashchita informatsii. Insayd* [Information protection. Inside], 2022, No. 4 (106), pp. 14-19.
14. *Rahman R., Hezaveh R., Williams L.* What Are the Attackers Doing Now? Automating Cyberthreat Intelligence Extraction from Text on Pace with the Changing Threat Landscape: A Survey, *ACM Comput. Surv.*, December 2023, 55, 12, Article 241, 36 p. Available at: https://doi.org/10.1145/3571726.

15. *Erokhin V.* Poisk vredonosnykh stsenariev powershell s ispol'zovaniem sintaksicheskikh derev'ev [Searching for malicious powershell scripts using syntax trees], *Bezopasnost' informatsionnykh tekhnologiy* [Information Technology Security], 30 (3), pp. 77-89. DOI: http://dx.doi.org/10.26583/bit.2023.3.05.
16. Follina Exploit Leads to Domain Compromise. Available at: https://thedfirreport.com/2022/10/31/follina-exploit-leads-to-domain-compromise/.
17. *Salitin M.A., Zolait A.H.* The role of User Entity Behavior Analytics to detect network attacks in real time, *2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain, 2018*, pp. 1-5. DOI: 10.1109/3ICT.2018.8855782.
18. *Hutchins E.M., Cloppert M.J., Amin R.M.* Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, *Lockheed Martin Corporation.* Available at: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
19. MITRE ATT&CK. Available at: https://attack.mitre.org/.
20. Bank dannykh ugroz bezopasnosti informatsii [Data bank of information security threats], Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu, Gosudarstvennyy nauchno-issledovatel'skiy ispytatel'nyy institut problem tekhnicheskoy zashchity informatsii [Federal Service for Technical and Export Control, State Research and Testing Institute of Problems of Technical Protection of Information]. Available at: https://bdu.fstec.ru/.

Статью рекомендовал к опубликованию д.т.н., профессор А.В. Боженюк.

Олейникова Анна Алексеевна – ООО «Интеллектуальная безопасность»; e-mail: ana.oleynikova@gmail.com, г. Москва, Россия; тел.: 83912227639.

Золотарев Вячеслав Владимирович – Сибирский государственный университет науки и технологий; e-mail: amida.2@yandex.ru; г. Красноярск, Россия; тел.: 83912227639; к.т.н.; доцент.

Oleynikova Anna Alekseevna – Intellectual Security LLC; e-mail: ana.oleynikova@gmail.com; Moscow, Russia; phone: +73912227639.

Zolotarev Vyacheslav Vladimirovich – Siberian State University of Science and Technology; e-mail: amida.2@yandex.ru; Krasnoyarsk, Russia; phone: +73912227639; cand. of eng. sc.; associate professor.

УДК 004.89 DOI 10.18522/2311-3103-2023-5-81-92

В.С. Усатюк, С.И. Егоров, А.П. Локтионов, Е.А. Титенко, И.Е. Чернецкая

АРХИТЕКТУРА НЕЙРОННЫХ СЕТЕЙ НА ОСНОВЕ КОДОВ НА ГРАФАХ

Одним из важных достижений теории помехоустойчивого кодирования является открытие кодов на графах и их важного подмножества низкоплотностных кодов (LDPC-кодов). Используя проверочную матрицу кода на графе, можно получить марковское случайное поле. LDPC-код может быть вложен в модель Изинга (разновидность марковского случайного поля) путем использования топологии тора с отрицательной кривизной. При этом кодовые слова соответствуют седловым точкам (экстремумам) в модели, а треппин-сеты соответствуют локальным минимумам. Использование LDPC-кодов с увеличенным кодовым расстоянием позволяет максимально разнести седловые точки, и таким образом повысить устойчивость нейронной сети к шуму и мощность представления. При этом блочная и разряженная структура, характерная для тора отрицательной кривизны, упрощает мультиплексирование и снижает число обучаемых параметров нейронной сети. Целью исследования являются снижение вычислительной сложности и увеличение точности нейронных сетей за счёт применения априорных структурных (квазициклических) разряженных графов для широкого класса задач машинного обучения на марковских случайных полях. В работе представлен новый подход, позволяющий осуществ-