ПЕРСПЕКТИВНЫЕ МЕТОДЫ АНАЛИЗА ИНФОРМАЦИОННЫХ ПОТОКОВ В СФЕРЕ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ МЧС РОССИИ (ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ОБЗОР – ЧАСТЬ 2)

А.С. Артамонов, кандидат физико-математических наук, профессор.
ООО «Биоклимат», г. Новосибирск.
А.Ю. Иванов, доктор технических наук, профессор.
Санкт-Петербургский университет ГПС МЧС России

Обоснована целесообразность использования новых подходов к обеспечению информационной безопасности автоматизированных систем МЧС России. Исследованы возможности применения перспективных методов обработки данных о деструктивных информационных воздействиях на указанные системы и противодействии им.

Ключевые слова: системный подход, аналитика больших данных, поведенческий анализ, экспертный анализ сетевой активности, когнитивная аналитика

ADVANCED METHODS OF ANALYSIS OF INFORMATION FLOWS IN THE SPHERE OF SECURITY OF THE AUTOMATED SYSTEMS OF EMERCOM OF RUSSIA (INFORMATION-ANALYTICAL REVIEW – PART 2)

A.S. Artamonov. Bioclimate Company Ltd, Novosibirsk.
A.Yu. Ivanov. Saint-Petersburg university of State fire service of EMERCOM of Russia

In the article the expedience of the use of new approaches to information security of the automated systems of EMERCOM of Russia. Researched the possibilities of application of the promising methods for processing data about destructive information influences on these systems and counteract them.

Keywords: systemic approach, big data analytics, behavioral analysis, expert analysis of the network activity, cognitive intelligence

Поведенческий анализ (User Behavioral Analytics)

Одним из наиболее важных уроков, извлеченных специалистами по информационной безопасности за последнее десятилетие, заключается в том, что как бы ни были важны технические средства зашиты информации, влияние человеческого фактора является еще более критичным. Ошибки администраторов и пользователей – нарушение стандартных процедур и инструкций безопасности, неправильная конфигурация сетей, несвоевременная доработка, обновление, модернизация в соответствие с последними стандартами – открывают широкие возможности киберпреступникам. Поэтому не удивительно, что в последнее время все большее внимание уделяется поведенческому анализу пользователей.

Поведенческий анализ стал широко использоваться в маркетинге на стыке прошедшего и настоящего веков, как инструмент понимания и выявления закономерностей в поведении клиентов. Особую популярность он приобрел с появлением клиент-ориентированной концепции (customer centric), пришедшей на смену продукт-ориентированной концепции (product centric), когда клиенты подбирались для данного продукта, а не продукты для данного клиента. С тех пор поведенческие модели

и соответствующие аналитические инструменты стали широко использоваться для решения различных бизнес-проблем, в том числе проблем информационной безопасности.

В 2015 г. компания Hewlett Packard выпустила приложение User Behavior Analytics (UBA) [18]. Оно осуществляет мониторинг поведения пользователей, накапливает большие объемы релевантных данных и использует инструменты поведенческого анализа больших данных для обнаружения инцидентов в сфере информационной безопасности. Аналитическое приложение Hewlett Packard UBA позволяет:

– анализировать различные события пользовательской активности, такие как: сохранение и передача информации, работа с аналитическими приложениями и программными продуктами, доступ к базам данных, файловым каталогам, работа в интернете, получение информации по электронной почте и т.п.;

– применять готовые математические модели для профилирования пользовательской активности на основе полученных событий, то есть определять нормальную активность данной организации и данного пользователя;

– использовать результаты моделирования для выявления аномальной активности в информационной системе и для идентификации инсайдеров.

Необходимо отметить, что профилирование пользовательской активности происходит автоматически на основе математических моделей. Это позволяет создавать профиль каждого пользователя, автоматически поддерживать и обновлять его. В случае обнаружения значительных отличий в активности пользователя от эталонного профиля система регистрирует инцидент, оценивает отрицательный потенциальный эффект аномального поведения и присваивает ему соответствующий уровень риска. Это позволяет ранжировать риски с целью первоочередного устранения наиболее опасных.

Системы UBA сами не предпринимают каких-либо действий, но предоставляют администратору безопасности возможность быстро понять суть проблемы и принять адекватное решение. Система также предлагает интерфейс анализа и визуализации данных для построения аналитики по множеству измерений.

Использование систем UBA позволяет более эффективно бороться с инцидентами, источником которых все чаще являются сами сотрудники организации. Так, по данным InfoWatch 62 % нарушений информационной безопасности внутри организации связаны с действиями инсайдеров, а 44 % – с халатностью персонала [19].

Экспертный анализ сетевой активности (Network Forensics)

Термин Network Forensics, который приписывают эксперту в области сетевых экранов Маркусу Рануму, заимствован из судебной и криминальной терминологии, где он означает судебную экспертизу.

Суть этого подхода заключается в сборе, регистрации и анализе сетевых событий с целью выявления источников кибератак и других релевантных инцидентов. Основными составляющими Network Forensics являются следующие [20].

1. Анализ активности электронной почты (Email Forensics). Электронная почта является наиболее популярным средством общения в киберпространстве. Она же представляет собой уязвимый элемент, который нарушители используют для получения конфиденциальной информации. Прикладные программные продукты, используемые для Email Forensics: eMailTrackerPro и SmartWhols.

2. Анализ интернет-активности (Web Forensics). Осуществляется для выявления киберугроз на основе истории просмотра Web-страниц. Используемые аналитические приложения: Web Historian и Index.datanalyzer.

3. Анализ компьютерного трафика (Packet Sniffers). Выполняется с использованием анализаторов трафика – снифферов – специализированных программных продуктов или устройств. Инженеры, администраторы и специалисты по информационной безопасности используют снифферы для мониторинга и сбора информации о различных коммуникациях

внутри сетей. Снифферы являются основным источником данных для систем обнаружения вторжений, предназначенных для выявления фактов неавторизованного доступа в компьютерную систему либо несанкционированного управления системой – в основном через интернет. В настоящее время предлагается множество снифферов для основных операционных систем – Microsoft Windows, UNIX и Linux.

4. Отслеживание IP-адресов (IP Traceback Techniques). Часто нарушители маскируют атаки с помощью подмены – спуфинга (spoofing), основанного на фальсификации данных на уровне *IP*- и *MAC*-адресов. Реконструкция траектории вторжения с целью отслеживания истинного источника часто затруднена, так как кибератака может осуществляться транзитом через несколько промежуточных узлов и осуществляться на различных уровнях стека протоколов *TCP*/*IP*.

5. Ловушки и сети (Honeypots and Honeynets). Они предназначены специально для привлечения внимания нарушителей с целью получения детальной информации об их методах и инструментах, а также для определения уязвимостей существующих или создаваемых компьютерных сетей. При этом могут применяться различные архитектуры сетей (как параллельные, так и последовательные), а также реальные и виртуальные компьютеры (IP-адреса).

Многообразие источников информации для анализа сетевой активности и объем анализируемой информации требуют инновационных решений в области аналитики. До недавнего времени экспертный анализ компьютерных сетей был искусством – привилегией квалифицированных специалистов. Однако исследовательские проекты, изначально инициированные в области телефонной связи, привели к тому, что в настоящий момент для целей Network Forensics существует ряд программных продуктов и аналитических инструментов (Network Forensic Analysis Tools) как лицензированных, так и распространяемых свободно [21].

Intelligence-Driven Information Security

В настоящее время не сформировался русскоязычный аналог для обозначения этого подхода.

Этот термин стал использоваться примерно в середине прошедшего десятилетия. Он начал применяться для обозначения аналитических подходов к обеспечению информационной безопасности, адекватных по сложности средствам нападения.

Существенное развитие концепция Intelligence-Driven Information Security и ей подобные – Intelligence-Driven Defense, Intelligence-Led Security, Cognitive Security – получили позже, в период становления концепции больших данных в результате стремительного прогресса компьютерных технологий и аналитики, основанной на алгоритмах машинного обучения. Это позволило обрабатывать огромные объемы информации практически в режиме реального времени. Данный подход определяют как «приобретение в реальном времени знаний об информационных угрозах и соответствующее позиционирование потенциала организации против этих угроз с целью предотвращения, детектирования и предсказания кибератак, оценки рисков и принятия решений, а также для оптимизации стратегии информационной безопасности и санкционирования соответствующих действий» [22]. В 2012 г. подход взяла на вооружение компания RSA – лидер в области безопасности. С этого момента он стал внедряться в системы информационной безопасности.

Отличие традиционного и рассматриваемого подходов к обеспечению информационной безопасности состоит в следующем (рис. 3).

Традиционный подход сфокусирован на предотвращении кибератак. При этом мониторингу и действиям в ответ на атаку уделяется значительно меньше внимания и ресурсов. Приоритеты Intelligence-Driven Information Security распределены равномерно [23].

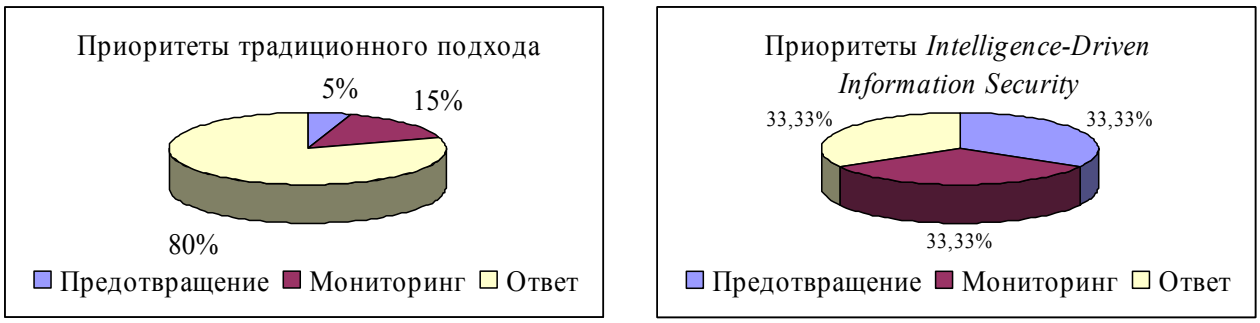

Рис. 3. **Приоритеты традиционного подхода и Intelligence-Driven Information Security**

Подход Intelligence-Driven Information Security строится на динамике детектирования, анализа и действий, в то время как традиционная стратегия в основном статична, пассивна и сфокусирована на определении того, что происходит на периферии защищаемой системы. Новая стратегия предоставляет дополнительные возможности – данные, аналитика и действие – для предотвращения/снижения потерь, вызванных неизбежными взломами защищаемых систем:

– данные в четырех ключевых сферах: риск (уязвимости, угрозы, защищенность) – для разработки оптимальной стратегии защиты и приоритетности действий; сетевая активность (от отдельных событий до упорядоченного набора данных временных сессий) – для последующего анализа с целью выявления аномалий; идентификация и активность пользователей – информация о тех, кто находится в данный момент в сети и об их активности; транзакции – события, происходящие на уровне ключевых приложений и продуктов, которые составляют основу деятельности организации;

– аналитика – обработка перечисленных данных для решения задач информационной безопасности: оценка рисков, выявление аномалий, ликвидация последствий кибератак, профилирование пользовательской активности и построение поведенческих моделей, предсказание инцидентов нарушений безопасности, оптимизация ресурсов;

– действие – реакция системы/службы информационной безопасности на кибератаку или инцидент нарушения. Быстрые и своевременные действия, например дополнительная идентификация или ограничение доступа, позволяют значительно уменьшить отрицательные последствия атак. Ключевым моментом здесь является обнаружение повторяющихся паттернов (закономерностей) с последующей операционализацией ответных действий.

Необходимо отметить, что Intelligence-Driven Information Security не сводится к приобретению знаний об угрозах на основе анализа и понимания их ландшафта, техники и методов, используемых киберпреступниками. Основная цель – управление рисками на основе полученных знаний. Это предполагает наличие инструментов видения будущего, с присущими ему неопределенностями, и методов решения возникающих при этом проблем. Эффективное управление рисками дает возможность принятия рациональных решений.

Аналитические методы обеспечения информационной безопасности

Аналитика – это искусство анализа, применимое во всех сферах человеческой жизни, основанное на выделении, сборе и обработке информации для выявления причинно-следственных связей и принятия решений. Применительно к задачам информационной безопасности аналитику можно определить как инструмент обработки данных для принятия эффективных решений и исполнения действий по защите информации. Несмотря на этимологию слова аналитика, синтез как процесс соединения или объединения ранее разрозненных вещей или понятий в целое является важной компонентой аналитики, без которой немыслим системный подход к информационной безопасности. Обычно выделяют три типа аналитики: описательную, предсказательную и предписательную (рис. 4).

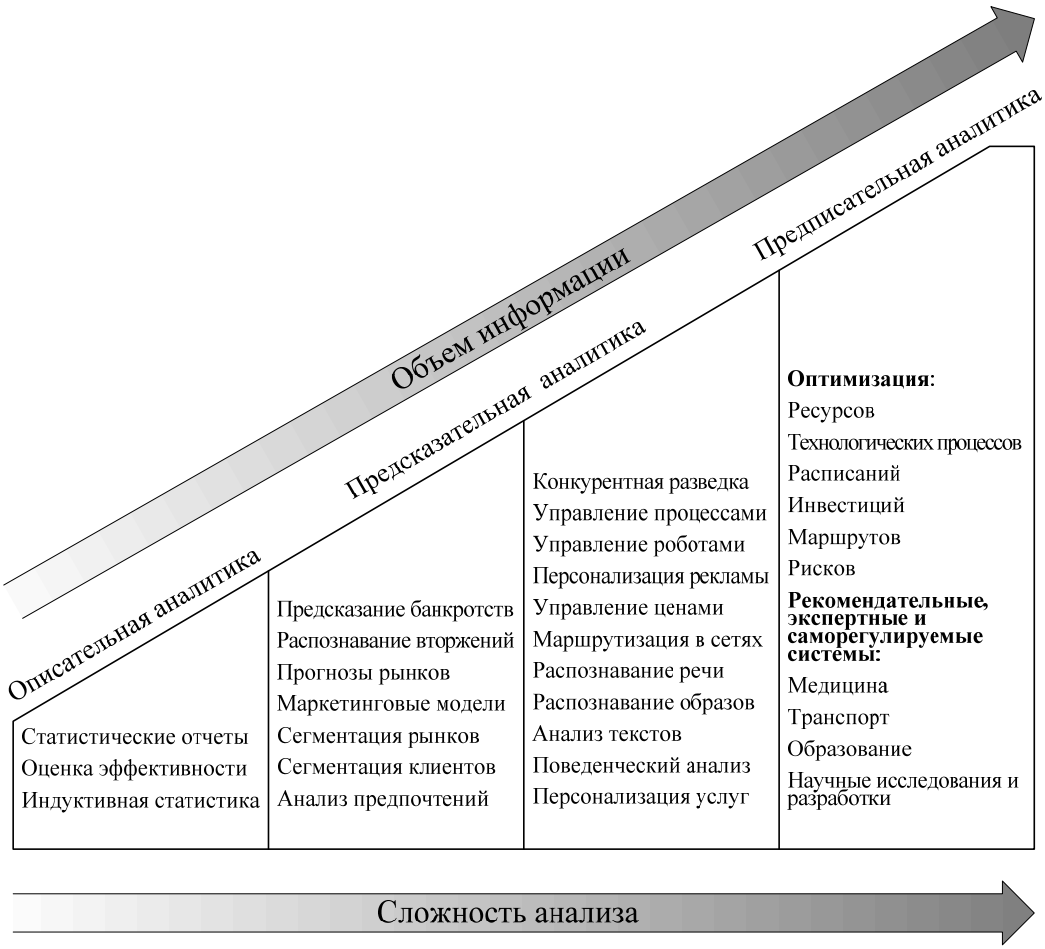

Рис. 4. **Эволюция аналитики**

Описательная аналитика, чаще именуемая описательной статистикой, предназначена для обработки эмпирических данных, их систематизации, представления в наглядном виде (визуализации), а также для количественного и качественного описания. Цель описательной аналитики – разработка отчетов, оценка эффективности и результативности, расчеты статистических показателей. На границе описательной и предсказательной аналитик находится индуктивная статистика, которая предполагает, что свойства и закономерности, выявленные при исследовании объектов выборки, также присущи генеральной совокупности.

Предсказательная аналитика использует статистические методы, алгоритмы машинного обучения, теорию игр и другие методы интеллектуального анализа для построения моделей и предсказания будущих событий на основе ретроспективных и текущих данных. Важным преимуществом моделей является то, что помимо прогнозирования они устанавливают связи между многими факторами и позволяют оценить риски и потенциальные возможности в зависимости от конкретного набора условий (значений/величины факторов) и, таким образом, через управление отдельными факторами достигать нужных результатов.

Предписательная аналитика. В некотором смысле она представляет собой предсказательную аналитику, дополненную методами исследования операций и теории принятия решений. Применительно к задачам информационной безопасности – это управление рисками, оптимизация ресурсов и структуры системы информационной безопасности, принятие адекватных противодействий в ответ на реальные или прогнозируемые киберугрозы.

Благодаря бурному прогрессу вычислительной техники и развитию концепции больших данных, аналитика превратилась в основной инструмент решения многих практических задач.

Сегодня можно констатировать, что аналитика информационной безопасности (Security Data Analytics) формируется как инновационный подход к проблемам зашиты информации на основе систем типа Business-Intelligence, которые обрабатывают огромные массивы информации как с целью защиты бизнеса (обнаружение мошенничества, нарушений, недобросовестного ведения бизнеса), так и для выявления новых возможностей. Основой систем и аналитики типа Security-Intelligence сегодня являются две наиболее разработанные области: экспертный анализ сетевой активности и поведенческий анализ, которые обрабатывают данные пользовательской и сетевой активности с целью определения трендов, паттернов нормальной и аномальной активности, выявления источников кибератак, детектирования и даже предсказания вторжений и других релевантных инцидентов.

Аналитические методы обработки данных

Существует множество аналитических подходов, моделей и алгоритмов обработки данных и получения новых знаний. Полный список аналитических методов приводится в обзоре компании McKinsey, посвященном теме больших данных [25]. Целесообразно рассмотреть примерный перечень методов, который может быть использован в области обеспечения информационной безопасности.

A/B/C... тестирование – статистические тесты для определения различия между группами статистических данных *A*, *B*, *C*, … Наиболее простой вариант – *t*-тест – устанавливает наличие различия между двумя группами данных; Более сложный – дисперсионный анализ (ANOVA) – для тестирования нескольких групп данных. Метод может быть использован для определения «загрязненности информации», обнаружения несанкционированного доступа путем сравнения текущих показателей ввода и использования информации пользователем относительно некоторых стандартов.

Анализ ассоциативных правил и его разновидности – ассоциативные правила позволяют находить закономерности между связанными событиями. В качестве таких событий могут выступать различного рода транзакции, последовательность действий пользователя, активность в компьютерной сети. Метод может быть использован для распознавания паттернов поведения нарушителя, определения вероятности возникновения событий, ведущих к искажению или разрушению информации.

Кластерный и сегментационный анализ – группа методов, относящихся к так называемым методам «обучение без учителя». С их помощью можно сгруппировать любые сущности – события, пользователей, нарушителей, ошибки базы данных в относительно однородные сегменты с подобными характеристиками, что позволяет лучше понять природу этих сущностей.

Методы классификации и регрессионного анализа – группа методов, которые относятся к так называемым методам «обучение с учителем». Они включают в себя: логистическую и линейную регрессии, искусственные нейронные сети, дерево принятия решений, байесовские классификаторы, метод опорных векторов и другие, а также их комбинации, реализуемые в виде ансамблей моделей. Эти методы подходят для выявления факторов, влияющих на поведение пользователей, на формирование ошибок в базе данных и, в конечном счете, на нарушение полноты и достоверности информации.

Анализ выбросов/аномалий – статистические модели и методы детектирования и распознавания редких событий. Имеет ряд применений: для уменьшения «шумов» при обработке данных, для обнаружения необычных банковских транзакций и выявления мошенничеств, для обнаружения вторжений в компьютерную сеть путем анализа трафика и выявления необычных записей и трендов в многомерном информационном потоке. В зависимости от характера аномалий используются различные модели: кластерные модели,

статистические модели экстремальных значений, информационно-теоретические модели и т.д.

Анализ текста (обработка естественного языка) – процесс получения высококачественной информации из текста на естественном языке. Как правило, для этого применяется статистическое обучение на основе шаблонов: входной текст разделяется с помощью шаблонов, затем осуществляется обработка полученных данных. Обычно для этого используются категоризация и кластеризация текста с последующей экстракцией сущностей. Методы могут быть использованы для анализа текста вводимого персоналом в процессе выполнения своих функциональных обязанностей, для анализа руководящих документов и инструкций, комплекса словарей и классификаторов, а также различного рода докладов о причинах возникновения критических ситуаций на предмет определения групп слов и выражений, ассоциирующихся с негативными последствиями.

Анализ временных рядов – совокупность математико-статистических методов анализа, предназначенных для выявления структуры временных рядов и для их прогнозирования – может использоваться для анализа активности в компьютерной сети (запросов, ответов, обращений к определенным компонентам информационной системы), для выявления и прогнозирования кибератак, а также для анализа и прогнозирования возникновения ошибок в базах данных.

Визуализация аналитических данных – представление статистических данных в виде таблиц, графиков и рисунков. Строго говоря, визуальное представление информации используется давно. Однако современные методы и средства визуализации статистических данных дают возможность реализовать динамическую связь графиков и таблиц с данными, что позволяет отображать данные в реальном времени: при обновлении данных одновременно происходит обновление визуальной информации. Не менее важно и то, что все компоненты визуальной информации могут быть связаны между собой в единое целое, например, выбирая определенный участок графика или таблицы, можно разложить ее составляющие на компоненты, представленные другим графиком, рисунком или таблицей. Визуализация является эффективным инструментом принятия своевременных и эффективных решений для организации оперативных действий по защите информации администратором безопасности.

Перспективы. Интеллектуальная аналитика

Каждый день в мире генерируется около 2,5 эксабайт ($2{,}5 \cdot 10^{18}$ байт) информации, 80 % из которых неструктурированны – в текстовом, аудио и видео форматах [26]. Обработка и осмысление этой информации лежат за пределами не только человеческих возможностей, но и традиционных баз данных и статистических методов. До недавнего времени это означало, что большая часть информации попросту игнорировалась. С развитием технологии и аналитики больших данных, а также алгоритмов машинного обучения ситуация быстро меняется: объемы обрабатываемой информации и скорость обработки растут, точность моделей и предсказаний увеличивается. Этот прогресс является наиболее впечатляющим там, где существуют вполне определенные алгоритмы решения проблемы, и требуется огромное быстродействие – несравнимо большее, чем возможности человека. В других областях, таких, как чтение текста, распознавание образов, объяснение содержания, не говоря уже о творческих функциях, которые традиционно считаются прерогативой человека, результаты использования современных подходов менее значительны. Успех решения «интеллектуальных» задач сегодня связывают с новым направлением в аналитике – когнитивной/познавательной аналитикой, которую можно определить как аналитику, основанную на когнитивных технологиях.

Когнитивные технологии – это сочетание науки и технологии искусственного интеллекта, с одной стороны, и теории и технологии обработки сигналов, с другой стороны. Здесь привлекаются алгоритмы машинного обучения, обработка естественного языка, распознавание речи, компьютерное зрение и многое другое. Когнитивные технологии

не новы, однако сегодня скорости компьютерной обработки позволяют использовать их более эффективно.

Исследования по применению когнитивной аналитики проводятся во многих областях: для визуализации данных, распознавания образов, анализа текстов, разработки систем идентификации и виртуальных агентов, рекомендательных систем и т.д. Подобные исследования проводятся и в области информационной безопасности. Так в 2016 г. компания IBM Security анонсировала использование облачной версии системы Watson (IBM Watson – суперкомпьютер фирмы IBM, оснащенный вопросно-ответной системой искусственного интеллекта) для кибербезопасности [26].

Дальнейшее развитие системы Watson Cyber Security корпорация IBM планирует осуществлять в сотрудничестве с восьмью университетами. Этот проект преследует амбициозные цели: развить принципиально новое поколение когнитивных систем, способных принимать разумные решения и постоянно обучаться на примерах новых киберугроз; систем, обладающих инстинктом и экспертными знаниями, способных анализировать Web-тексты, структурированные и неструктурированные данные, аналитические отчеты, то есть систем, подобных профессионалам в области информационной безопасности, но с возможностями несоизмеримо большими по сравнению с человеческими.

Другим примером инновационных разработок в области Cognitive Security может служить компания с одноименным названием – Cognitive Security [27], приобретенная Американской корпорацией Cisco в 2013 г. Линейка продуктов и сервисов компании Cognitive Security под названием Cognitive Analys, основана на использовании алгоритма, в котором реализованы новейшие достижения в области моделирования доверия и управления репутацией. В нем также используется многоступенчатый алгоритм для оценки степени доверия к используемым данным. Cognitive Analyst представляет собой интерактивный Web-интерфейс, позволяющий администратору непрерывно отслеживать состояние компьютерной сети, ускорять распознавание вторжений и предпринимать эффективные действия против киберпреступников.

Когнитивная аналитика и ее применение в области информационной безопасности еще находится на ранней стадии своего развития и пока еще не в состоянии заменить традиционные аналитические подходы. Однако тем организациям, которые нуждаются сейчас или предвидят необходимость в принятии решений на основании обработки огромных массивов информации в режиме времени, близком к реальному, уже сейчас следует задуматься о формировании базы для использования Cognitive Security.

Несомненно, в дальнейшем сфера информационного противоборства продолжит расширяться как с позиций охвата все большего числа жизненно важных (и не только) систем, так и в аспекте разработки новых технологий реализации кибератак и противодействия им. Поэтому весьма важным остается вопрос привлечения передовых теоретических методов для решения практических задач, связанных с защитой компьютерной информации. Возрастание сложности реализации таких разработок требует отыскания компромисса между стоимостью новейших средств защиты и эффективностью их применения в конкретной ситуации. Авторы статьи выражают надежду, что представленный информационно-аналитический обзор будет полезным для осуществления такого выбора.

Литература

18. Афонин Е. Поведенческий анализ помогает выявлять ИБ-инциденты // CNews Издание о высоких технологиях. URL: www.cnews.ru/articles/2016-01-26_hpe_kak_povedencheskij_analiz_pomogaet_vyyavlyat_ibintsidenty (дата обращения: 13.01.2017).

19. Восканян М. Злоумышленники – рядом // Intelligent Enterprise. 2005. № 131.

20. Natarajan Meghanathan, Sumanth Reddy Allam and Loretta A. Moore. Tools and techniques for network forensics // International Journal of Network Security & Its Applications (IJNSA). 2009. Vol. 1. No. 1. April.

21. Jay Bretzman. What Are the Best Network Forensics and Data Capture Tools? SecurityIntelligence. 2014. August 20. URL: https://securityintelligence.com/ what-are-the-best-network-forensics-and-data-capture-tools/ (дата обращения: 13.01.2017).

22. Sam Curry, Engin Kirda, Eddie Schwartz, William H. Stewart, Amit Yoran. Big data fuels intelligence-driven security. RSA Security Brief, January. 2013. URL: https:// www.emc.com/collateral/industry-overview/big-data-fuels-intelligence-driven-security-io.pdf. (дата обращения: 13.01.2017).

23. Adopting intelligence driven security. RSA Whitepaper. URL: https://www.emc.com/collateral/white-papers/h13235-wp-adopting-intelligence-driven-security.pdf. (дата обращения: 13.01.2017).

24. Roadmap to intelligence-driven information security // Security for business innovation council report RSA, The Security Division of EMC. URL: https://msisac. cisecurity.org/whitepaper/documents/5.pdf. (дата обращения: 13.01.2017).

25. Big data: The next frontier for innovation, competition, and productivity // McKinsey Glabal Institute. 2011. May. URL: www.mckinsey.com/mgi/piblications/ (дата обращения: 13.01.2017).

26. Marc van Zadelhoff. Cognitive Security=Security That Understands, Reasons And Learns. Forbes BrandVoice. 2016. May 10. URL: http://www.forbes.com/sites/ibm/ 2016/05/10/cognitive-security-security-that-understands-reasons-and-learns/#1fbcc9b314ab (дата обращения: 13.01.2017).

27. Gabriel Dusil. Cognitive Security – Positioning Network Behavior Analysis in the Security Ecosystem. 2012. June 30. URL: https://dusil.com/tag/cognitive-security/ (дата обращения: 13.01.2017).

References

18. Afonin E. Povedencheskij analiz pomogaet vyyavlyat' IB-incidenty // CNews Izdanie o vysokih tekhnologiyah. URL: www.cnews.ru/articles/2016-01-26_hpe_kak_povedencheskij _analiz_pomogaet_vyyavlyat_ibintsidenty (data obrashcheniya: 13.01.2017).

19. Voskanyan M. Zloumyshlenniki – ryadom // Intelligent Enterprise. 2005. № 131.

20. Natarajan Meghanathan, Sumanth Reddy Allam and Loretta A. Moore. Tools and techniques for network forensics // International Journal of Network Security & Its Applications (IJNSA). 2009. Vol. 1. No. 1. April.

21. Jay Bretzman. What Are the Best Network Forensics and Data Capture Tools? SecurityIntelligence. 2014. August 20. URL: https://securityintelligence.com/ what-are-the-best-network-forensics-and-data-capture-tools/ (data obrashcheniya: 13.01.2017).

22. Sam Curry, Engin Kirda, Eddie Schwartz, William H. Stewart, Amit Yoran. Big data fuels intelligence-driven security. RSA Security Brief, January. 2013. URL: https:// www.emc.com/collateral/industry-overview/big-data-fuels-intelligence-driven-security-io.pdf. (data obrashcheniya: 13.01.2017).

23. Adopting intelligence driven security. RSA Whitepaper. URL: https://www.emc.com/collateral/white-papers/h13235-wp-adopting-intelligence-driven-security.pdf. (data obrashcheniya: 13.01.2017).

24. Roadmap to intelligence-driven information security // Security for business innovation council report RSA, The Security Division of EMC. URL: https://msisac. cisecurity.org/whitepaper/documents/5.pdf. (data obrashcheniya: 13.01.2017).

25. Big data: The next frontier for innovation, competition, and productivity // McKinsey Glabal Institute. 2011. May. URL: www.mckinsey.com/mgi/piblications/ (data obrashcheniya: 13.01.2017).

26. Marc van Zadelhoff. Cognitive Security=Security That Understands, Reasons And Learns. Forbes BrandVoice. 2016. May 10. URL: http://www.forbes.com/sites/ibm/

2016/05/10/cognitive-security-security-that-understands-reasons-and-learns/#1fbcc9b314ab (data obrashcheniya: 13.01.2017).

27. Gabriel Dusil. Cognitive Security – Positioning Network Behavior Analysis in the Security Ecosystem. 2012. June 30. URL: https://dusil.com/tag/cognitive-security/ (data obrashcheniya: 13.01.2017).