Russian Technological Journal.
2021;9(6):16–25

ISSN 2782-3210 (Print)
ISSN 2500-316X (Online)

УДК 004.9
https://doi.org/10.32362/2500-316X-2021-9-6-16-25

НАУЧНАЯ СТАТЬЯ

Разработка моделей аналитической системы обработки данных для мониторинга ИБ объекта информатизации, использующего облачную инфраструктуру

В.А. Сизов,
А.Д. Киров @

Российский экономический университет имени Г.В. Плеханова, Москва, 117997 Россия
@ *Автор для переписки, e-mail: kirov.ad@rea.ru*

Резюме. Статья посвящена разработке аналитической системы обработки данных (АСОД) для мониторинга информационной безопасности (ИБ) в рамках системы менеджмента ИБ современных компаний, ведущих свою основную деятельность в киберпространстве и использующих облачную инфраструктуру. На основе анализа современных информационных технологий (ИТ) и наиболее востребованных продуктов обеспечения ИБ облачных инфраструктур, а также существующих научных подходов предложен формализованный подход к синтезу АСОД для мониторинга ИБ такого объекта информатизации. Этот подход учитывает полезность используемых ИТ с позиции ИБ. Представлена общая модель структуры информационного обеспечения АСОД для мониторинга ИБ, а также модель зависимости полезности ИТ от времени и соотношения уровня квалификации специалиста по ИБ и злоумышленника. В качестве критерия в первой оптимизационной модели используется качество системы мониторинга ИБ. В качестве ограничений предлагаются следующие: ограничение на время принятия решения на инцидент; ограничение на степень качества анализа событий ИБ аналитической системой обработки данных и ограничение на совместимость функций анализа данных с типами данных о событиях ИБ. Приведенные результаты исследования второй модели показывают логически непротиворечивую зависимость полезности ИТ от времени и соотношения уровня квалификации специалиста по ИБ к уровню квалификации злоумышленника. Представлены частные модели структуры информационного обеспечения АСОД, позволяющие определить рациональную структуру информационного обеспечения АСОД по частным критериям. В качестве частных критериев используются следующие: максиминный критерий полезности информационного обеспечения АСОД для мониторинга ИБ объекта информатизации в облачной инфраструктуре и критерий максимума актуальности информационного обеспечения, распределенного по узлам облачной инфраструктуры для систем с невысокой степенью централизации управления.

Ключевые слова: информационная безопасность, аналитическая система обработки данных, облачная инфраструктура, компьютерное моделирование, математическое моделирование, мониторинг ИБ, объект информатизации

• **Поступила:** 25.03.2021 • **Доработана:** 11.05.2021 • **Принята к опубликованию:** 25.07.2021

Для цитирования: Сизов В.А., Киров А.Д. Разработка моделей аналитической системы обработки данных для мониторинга ИБ объекта информатизации, использующего облачную инфраструктуру. *Russ. Technol. J.* 2021;9(6):16–25. https://doi.org/10.32362/2500-316X-2021-9-6-16-25

Прозрачность финансовой деятельности: Никто из авторов не имеет финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

RESEARCH ARTICLE

The development of models of an analytical data processing system for monitoring information security of an informatization object using cloud infrastructure

Valerii A. Sizov,
Aleksey D. Kirov @

Plekhanov Russian University of Economics, Moscow, 117997 Russia
@ *Corresponding author, e-mail: kirov.ad@rea.ru*

Abstract. The article is devoted to the problem of developing an analytical data processing system for monitoring information security within the information security management system of modern companies conducting their main activities in cyberspace and using cloud infrastructure. Based on the analysis of modern information technologies related to ensuring information security of cloud infrastructure and the most popular products for ensuring information security of cloud infrastructures, as well as existing scientific approaches, a formalized approach to the synthesis of an analytical data processing system for monitoring the information security of an informatization object using cloud infrastructure is proposed. This approach takes into account the usefulness of the used information technologies from the viewpoint of information security. A general model of the structure of information support of an analytical data processing system for monitoring information security, as well as a model of the dependence of the usefulness of information technology on time and the ratio of the skill level of an information security specialist and an attacker are presented. The quality of the information security monitoring system is used as a criterion in the first optimization model. The following limitations are suggested: limitation on the time of making a decision on an incident; limitation on the degree of quality of analysis of information security events by the analytical data processing system and limitation on the compatibility of data analysis functions with data types about information security events. The cited results of the study of the second model show a logically consistent dependence of the usefulness of information technology on time and the ratio of the skill level of an information security specialist to the skill level of an attacker. The particular models of the structure of the information support of ASOD are presented. They make it possible to determine the rational structure information support of ASOD according to particular criteria. The following particular criteria are used: the maximin criterion of the usefulness of the information support of ASOD for monitoring the information security of an informatization object in the cloud infrastructure; the criterion for the maximum relevance of information support distributed over the nodes of the cloud infrastructure for systems with a low degree of centralization of management.

Keywords: information security, analytical data processing system, cloud infrastructure, computer modeling, mathematical modeling, information security monitoring, object of informatization

• **Submitted:** 25.03.2021 • **Revised:** 11.05.2021 • **Accepted:** 25.07.2021

For citation: Sizov V.A., Kirov A.D. The development of models of an analytical data processing system for monitoring information security of an informatization object using cloud infrastructure. *Russ. Technol. J*. 2021;9(6):16–25 (in Russ.). https://doi.org/10.32362/2500316X-2021-9-6-16-25

Financial disclosure: The authors have no a financial or property interest in any material or method mentioned.

The authors declare no conflicts of interest.

ВВЕДЕНИЕ

Аналитические системы обработки данных (АСОД) для мониторинга ИБ – большой формирующийся класс систем, функционирующих в системе менеджмента ИБ (СМИБ) современных компаний.

Современные компании, ведущие свою основную деятельность в киберпространстве с использованием облачной инфраструктуры, построенной на технологиях сервис-провайдеров облачных инфраструктур, используют эти системы для управления ИБ и для совершенствования процессов, реализующих методы ИБ, включая процессы мониторинга, протекающие в реальном масштабе времени. Особенности технической реализации таких аналитических систем обуславливают особые требования к удобству их использования инженером по защите информации, оперативности, безошибочности и качеству обработки данных в реальном времени. Кроме этого, потенциальные затраты компании-пользователя облачных услуг на переход от одного поставщика этих услуг к другому характеризуются соотношением последствий в области ИБ, возникающих в результате кибератак, системных сбоев, ошибок пользователей, других внешних факторов и разницы в классах технологий кибербезопасности провайдеров. Поэтому предоставляемый поставщиком облачных услуг уровень ИБ подвержен тем же жестким условиям двусторонней рыночной конкуренции, которые определяют цены поставщика облачных услуг и его стратегию обеспечения ИБ клиентов.

Новые информационные технологии (ИТ) актуализируют проблему обеспечения безопасности и защиты информации перед их разработчиками, вендорами и потребителями. В настоящее время считается, что наиболее эффективным путем обеспечения ИБ объектов информатизации компании и/или используемой ею облачной инфраструктуры является путь разработки и внедрения безопасных ИТ. Их использование в облачных инфраструктурах позволяет дополнительно сократить расходы на обслуживание корпоративных информационных систем. Большое количество современных ИТ, используемых в облачной инфраструктуре, направлено на комплексное решение задачи повышения эффективности использования имеющихся ресурсов (табл. 1).

Облачная инфраструктура, используемая для размещения корпоративных информационных систем, все чаще принимает гибридную форму. Часть данных, наиболее критичных для функционирования бизнес-процессов, размещается внутри собственной инфраструктуры компании с использованием универсальных облачных технологий, формируя «частное облако компании». Другие данные, в свою очередь, обрабатываются в «публичных облаках», в которых инфраструктура предоставляется поставщиками облачных услуг

Таблица 1. Содержание современных ИТ, связанных с обеспечением ИБ облачной инфраструктуры

№ п/п	Наименование ИТ	Содержание
1	Сетевые решения для центров обработки данных (ЦОД) (DCN) [1]	Сетевое оборудование, позволяющее автоматически распределять нагрузку на локальные вычислительные сети (ЛВС) облачной инфраструктуры (как на само облачное сетевое оборудование, так и на каналы связи), предоставляемое как сервис
2	Проактивное распределение ресурсов [2]	Технология, позволяющая автоматически распределять ресурсы облачной инфраструктуры (аппаратные ресурсы в виде облачных серверов и рабочих мест и программные ресурсы в виде программного обеспечения, включая средства его разработки и отладки), предоставляемые как сервис, на основе предсказания ожидаемой нагрузки
3	Самодиагностика программного обеспечения [3]	Технология, предназначенная для автоматического выявления и коррекции ошибок, возникающих при эксплуатации программного обеспечения и реализации его функций
4	Шифрование данных в облачных инфраструктурах [4]	Технология, предназначенная для распределенного шифрования данных без использования единого распределяющего и удостоверяющего центра

Таблица 2. Назначение современных продуктов обеспечения ИБ облачных инфраструктур

№ п/п	Наименование продукта защиты информации в облачных инфраструктурах	Производитель продукта защиты информации в облачных инфраструктурах	Назначение
1	MVision Cloud	McAfee	Создание «динамического периметра защиты», способного адаптироваться к динамическим условиям внешней среды. Создание политик безопасности и их применение к SaaS, PaaS, IaaS-решениям, контейнерам и компонентам виртуальных облачных сред
2	Cisco Cloud Security	Cisco	Защита пользователей, данных и приложений в облаке от атак через взломанные учетные записи, от вредоносного ПО и утечки данных независимо от их местоположения и от того, откуда осуществляется доступ в Интернет. Нейтрализация вредоносного ПО до того, как оно распространится на сеть или оконечные устройства и сокращение времени на восстановление после заражения
3	FortiGate-VM	FortiNet	Для защиты данных используются высокоскоростные VPN-подключения. Политики безопасности реализуются во всех средах. Центр облачной безопасности служит для обеспечения централизованной и согласованной реализации мер безопасности корпоративной сети и обмена данными и поддерживает безопасное подключение сетей, расположений, облаков и центров обработки данных
4	Kaspersky Security для виртуальных и облачных сред	Лаборатория Касперского	Одновременная реализация как защиты рабочей среды, так и концепции «безопасность как код», которая обеспечивает непрерывную интеграцию рабочих процессов и восполнение пробелов в кибербезопасности сред разработки
5	CheckPoint CloudGuard	CheckPoint	Поддержка самого широкого спектра облачных инфраструктур, включая AWS, Microsoft Azure и Azure Stack, Google Cloud Platform, VMware Cloud on AWS и другие. Автоматическая подготовка и автоматическое масштабирование вместе с автоматическим обновлением политик гарантируют, что средства защиты не отстают от всех изменений в вашем облаке. Единая унифицированная консоль обеспечивает согласованную видимость, управление политиками, ведение журналов, создание отчетов и контроль во всех облачных средах и сетях

согласно моделям «Инфраструктура как услуга», «Платформа как услуга» либо «Программное обеспечение как услуга». Это обуславливает необходимость использования современных технологий обеспечения безопасности данных в облачных инфраструктурах. Будучи интегрированными с современными технологиями обработки данных, такие технологии превращаются в полноценные высокотехнологичные продукты, предлагаемые ведущими компаниями на рынке продуктов обеспечения ИБ облачных инфраструктур. Примеры таких продуктов представлены в табл. 2.

Анализ представленных технологий свидетельствует об их сложности. Для их развития и совершенствования необходимо применять научный подход, включающий методы математического и компьютерного моделирования.

В [5] представлен обзор моделей зрелости возможностей и показателей безопасности систем. Отмечается, что эти модели в основном являются реактивными, а не проактивными и, следовательно, не обеспечивают адекватных мер для оценки общей безопасности облачной системы. Поэтому в этой работе предложена модель зрелости возможностей облачной безопасности (CSCMM), которая расширяет существующие модели кибербезопасности с помощью метрики безопасности. В [6] представлена методология, позволяющая определить лучшие меры безопасности для мультиоблачных приложений, компоненты которых развернуты в гетерогенных облаках. Методология

основана на декомпозиции приложений и моделировании угроз по компонентам с последующим анализом рисков вместе с фиксацией требований облачного бизнеса и безопасности. Однако в этих работах недостаточное внимание уделяется процессам и технологиям мониторинга ИБ, которые в значительной степени влияют на качество его выходной информации (полнота, актуальность, своевременность и др.).

Выходная информация, генерируемая АСОД, представляет собой совокупность данных, полученных в результате выполнения наборов функций аналитики данных, входящих в его состав с определенной структурой или несколькими возможными видами структур. Такие совокупности данных могут быть использованы либо в текущей системе, либо перенаправляться в иные системы, присутствующие в данной облачной инфраструктуре. Качество выходной информации АСОД представляет собой степень ее пригодности для применения в целях выявления и расследования инцидентов ИБ офицером безопасности.

В качестве одного из основных методов, предложенных для повышения качества данных, получаемых в результате анализа данных мониторинга ИБ с применением АСОД, выступает компьютерное моделирование.

ПОСТАНОВКА ЗАДАЧИ

Современные системы мониторинга ИБ (СМИБ) создаются с целью обеспечения возможности адекватного и своевременного реагирования на кибератаки, направленные на информационную инфраструктуру СЭД и управления ИБ компании, что является главным компонентом, необходимым для оперативного и стратегического реагирования на актуальные угрозы в соответствии с политикой ИБ компании. Такая инфраструктура может быть построена на основе технологий ЛВС, составляя «частное облако компании» и/или в виде облачных инфраструктур, предоставляемых провайдерами облачных услуг, составляя «публичное облако компании».

Для создания эффективной системы управления информационной безопасностью компании требуется в максимальной степени автоматизировать ее функции управления с учетом современных требований к мониторингу ИБ и особенностей гибридных облачных инфраструктур.

Таким образом, задача разработки моделей аналитической системы обработки данных для мониторинга ИБ объекта информатизации, использующего облачную инфраструктуру, является актуальной. Данную задачу целесообразно разделить на ряд подзадач.

Первая подзадача состоит в разработке общей модели структуры информационного обеспечения аналитической системы обработки данных для мониторинга ИБ. Решение данной задачи позволяет определить рациональные решения, близкие к оптимальному, представляющие собой определенные совокупности информационных элементов, распределенные по узлам вычислительной сети АСОД.

Вторая подзадача представляет собой определение характера и степени зависимости полезности ИТ от времени и соотношения уровня квалификации специалиста по ИБ и уровня квалификации злоумышленника. Решение данной задачи позволяет выявить условия, при которых полезность ИТ будет наилучшей.

Третья подзадача представляет собой разработку совокупности частных моделей структуры информационного обеспечения АСОД для мониторинга ИБ объекта информатизации в облачной инфраструктуре. Решение данной задачи позволяет определить рациональную структуру информационного обеспечения АСОД по частным критериям [7, 8].

РАЗРАБОТКА ОБЩЕЙ МОДЕЛИ СТРУКТУРЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ АНАЛИТИЧЕСКОЙ СИСТЕМЫ ОБРАБОТКИ ДАННЫХ ДЛЯ МОНИТОРИНГА ИБ

Пусть:

$$\theta = F(\delta, t), \quad (1)$$

где θ – качество системы мониторинга ИБ; F – функция качества системы мониторинга ИБ; $\delta = G(R)$, где δ – степень качества анализа событий ИБ АСОД; t – время, необходимое аналитической системе обработки данных для принятия решения относительно того, насколько вероятно, что конкретное событие ИБ или их совокупность является инцидентом ИБ; G – функция качества анализа событий ИБ АСОД;

$$R = H(S),$$

где R – степень совместимости процедур анализа данных с типами данных о событиях ИБ; H – функция степени совместимости процедур анализа данных с типами данных о событиях ИБ; S – структура информационного обеспечения АСОД (совокупности информационных элементов, распределенные по узлам вычислительной сети АСОД: данные о событиях ИБ, дополнительные данные для анализа и расследования инцидентов ИБ).

Тогда общая модель структуры информационного обеспечения аналитической системы обработки данных для мониторинга ИБ имеет следующий вид:

Найти $\max\limits_{\{S\}} \theta$ при ограничениях:

$$t1 < t2;\ \delta1 < \delta < \delta2;\ R1 < R < R2, \quad (2)$$

где $t1 - t2$ – период времени, за который необходимо принять решение относительно того, насколько вероятно, что конкретное событие ИБ или их совокупность является инцидентом ИБ для наиболее эффективного противодействия данному инциденту и его расследования;

$\delta1 - \delta2$ – пределы степени качества анализа событий ИБ аналитической системой обработки данных, позволяющие принять решение относительно того, насколько вероятно, что конкретное событие ИБ или их совокупность является инцидентом ИБ с требуемой степенью достоверности;

$R1 - R2$ – пределы степени совместимости функций анализа данных с типами данных о событиях ИБ, в которых возможно принятие решения относительно того, насколько вероятно, что конкретное событие ИБ или их совокупность является инцидентом ИБ.

РАЗРАБОТКА МОДЕЛИ ЗАВИСИМОСТИ ПОЛЕЗНОСТИ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ ОТ ВРЕМЕНИ И СООТНОШЕНИЯ УРОВНЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗЛОУМЫШЛЕННИКА

Для разработки модели зависимости полезности ИТ от времени и соотношения уровня квалификации специалиста по ИБ и злоумышленника предлагается использовать аналитическую модель на основе статистического распределения Рэлея [9]. В качестве параметра масштаба распределения Рэлея выступает отношение уровня квалификации специалиста по ИБ, устраняющего уязвимости в программном и аппаратном обеспечении, к уровню квалификации злоумышленника, атакующего программное и аппаратное обеспечение, реализующее ИТ.

Оценка зависимости полезности ИТ от времени и соотношения уровней квалификации указанных категорий имеет следующий вид:

$$P(t,\sigma) = 1 - \frac{t}{\sigma^2} e^{-\frac{t}{2\sigma^2}}, \; t \geq 0, \; \sigma > 0, \qquad (3)$$

где P – уровень полезности ИТ в момент времени t; σ – отношение количественной оценки уровня квалификации специалиста по ИБ к уровню квалификации злоумышленника.

Соответствие количественных и качественных оценок уровней квалификации специалиста по ИБ и злоумышленника приведено в табл. 3 и 4 соответственно. В случае, когда противоборствующие стороны – группы людей, к ним необходимо применять групповые количественные оценки уровня их квалификации [10]. Итоговая матрица отношений количественных оценок уровней квалификации специалиста по ИБ и уровня квалификации злоумышленника представлена в табл. 5.

Таблица 3. Соответствие количественных и качественных оценок уровней квалификации специалиста по ИБ

Класс специалиста по ИБ	Качественная оценка уровня квалификации специалиста по ИБ	Количественная оценка уровня квалификации специалиста по ИБ
Высококвалифицированный специалист	Высокий	1
Обычный специалист	Средний	2
Низкоквалифицированный специалист	Низкий	3

Таблица 4. Соответствие количественных и качественных оценок уровней квалификации злоумышленника

Класс злоумышленника	Качественная оценка уровня квалификации злоумышленника	Количественная оценка уровня квалификации злоумышленника
Высококвалифицированный специалист	Высокий	3
Обычный специалист	Средний	2
Низкоквалифицированный специалист	Низкий	1

Таблица 5. Итоговая матрица отношений количественных оценок уровней квалификации специалиста по ИБ и уровня квалификации злоумышленника

Класс специалиста по ИБ / Класс злоумышленника	Высококвалифицированный специалист	Обычный специалист	Низкоквалифицированный специалист
Высококвалифицированный специалист	0.33	0.5	1
Обычный специалист	0.66	1	2
Низкоквалифицированный специалист	1	1.5	3

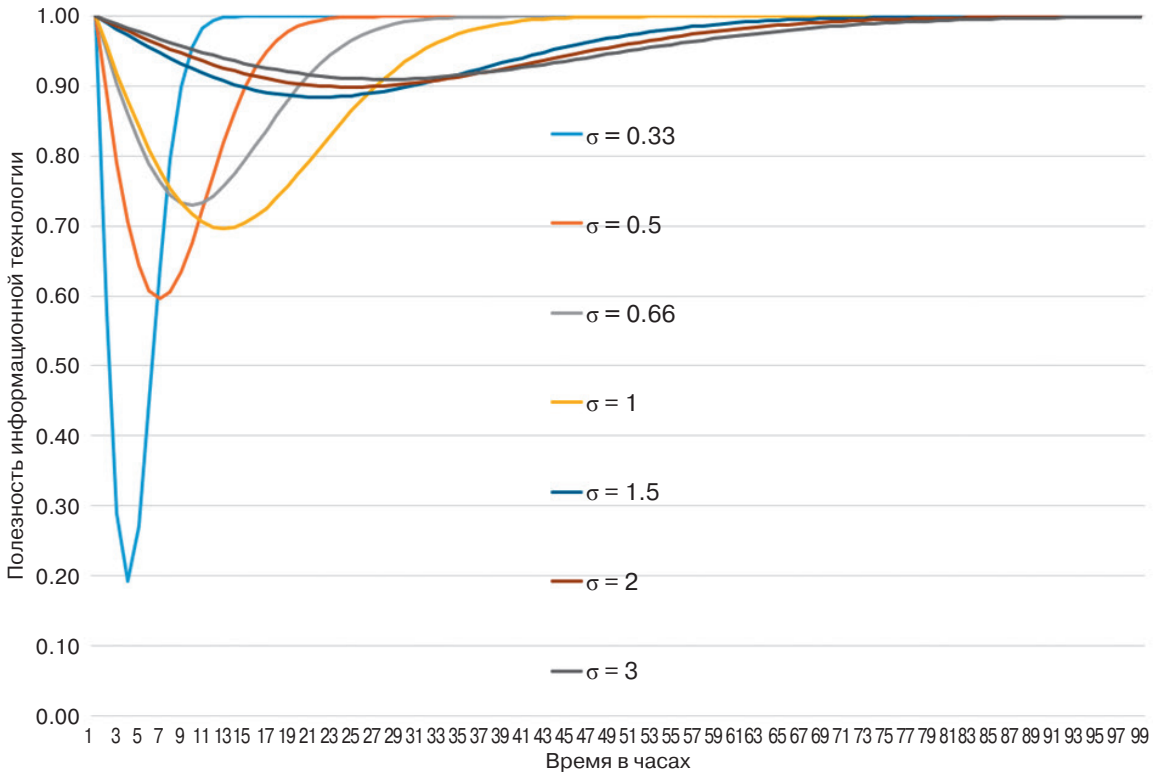

Рис. 1. Графики зависимости полезности ИТ от времени и соотношения уровня квалификации специалиста по ИБ и злоумышленника

Анализ представленных на рис. 1 графиков показывает, что с повышением уровня квалификации злоумышленника полезность ИТ для пользователей падает быстрее, а с повышением уровня квалификации специалиста по ИБ полезность ИТ для пользователей быстрее возвращается к максимальному значению, что соответствует реальности.

РАЗРАБОТКА ЧАСТНЫХ МОДЕЛЕЙ СТРУКТУРЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ АНАЛИТИЧЕСКОЙ СИСТЕМЫ ОБРАБОТКИ ДАННЫХ ДЛЯ МОНИТОРИНГА ИБ ОБЪЕКТА ИНФОРМАТИЗАЦИИ В ОБЛАЧНОЙ ИНФРАСТРУКТУРЕ

В настоящее время в области управления информационной безопасностью современных объектов информатизации в облачных инфраструктурах выделяется группа задач менеджмента инцидентов ИБ, которая включает следующие основные задачи: мониторинг событий ИБ объектов информатизации в облачных инфраструктурах и выявление инцидентов ИБ; регистрация инцидентов ИБ; анализ инцидентов ИБ; информирование администрации сервис-провайдеров облачных инфраструктур обо всех случаях нарушений ИБ; сбор свидетельств и доказательств для реагирования по случаям инцидентов ИБ в облачных инфраструктурах и другие. С практической точки зрения одним из наиболее эффективных подходов создания мониторинга ИБ считается применение систем класса SIEM [11–14].

Решения класса SIEM (Security Information and Event Management) предназначены для обеспечения следующих функций:

- управление информацией и событиями безопасности, в том числе в облачных инфраструктурах;
- сбор и хранение зарегистрированных событий безопасности;
- обработка и анализ хранящихся во внутренних базах данных событий ИБ с применением системы правил, создаваемой и управляемой офицером безопасности и уникальной для каждой облачной инфраструктуры.

Реализация этих функций позволяет осуществлять выявление и разбор инцидентов, а также проверку соответствия системы управления ИБ существующим требованиям и нормам, являющимся частью стандартов, рекомендаций, приказов и других нормативных и руководящих документов в этой области [15]. Реализация вышеприведенных функций предполагает наличие в системах класса SIEM АСОД, принципы построения которой были указаны ранее, или, по крайней мере, ее ключевых компонентов.

Однако основным недостатком таких систем является сравнительно длительный период времени, необходимый для анализа данных и принятия решения о том, является данное событие ИБ или их совокупность инцидентом ИБ или нет [16–18].

В основе этого недостатка лежит противоречие между распределенным характером источников информации о событии ИБ в облачных инфраструктурах (как правило, этими источниками являются средства защиты информации, объединенные в облачных инфраструктурах) и централизованным способом принятия решения на действия с инцидентами ИБ. Для разрешения указанного противоречия необходимо, с одной стороны, обеспечить процесс принятия решения наиболее полной информацией, а с другой стороны, эта информация должна быть актуальной. С учетом больших объемов данных о событиях ИБ в АСОД необходимо оптимизировать структуру информационного обеспечения АСОД с учетом структуры и технических характеристик ЛВС.

Особенности функционирования АСОД для мониторинга ИБ объекта информатизации на базе облачной инфраструктуры позволяют для решения задач повышения качества выходной информации при помощи компьютерного моделирования использовать методы теории полезности, позволяющие оценить полезный эффект от размещения информационных элементов в тех или иных вычислительных узлах облачной инфраструктуры [17]. Современные АСОД позволяют устанавливать степень достоверности информации, учитывая не только степень полноты и точности данных (достаточности данных для решения поставленной задачи и соответствия структуры и содержания данных системам, использование которых является оптимальным для решения поставленных задач), но и степень актуальности данных (способность информации отражать реальное состояние объектов на текущий момент времени).

Метод определения оптимальных с точки зрения мониторинга ИБ вычислительных узлов облачной инфраструктуры для размещения в них тех или иных типов информационных элементов и распределения этих элементов по узлам основан на компьютерном моделировании облачной инфраструктуры, в которой проводится мониторинг ИБ и применении методов теории полезности для оценки степени соответствия типов информационных элементов вычислительным узлам облачной инфраструктуры. Специфика управления инцидентами ИБ предполагает работу с массивами данных, что позволяет выделить необходимые наборы данных, которые могут быть распределены по узлам облачной инфраструктуры на основе модели [16–19]. Следовательно, частные модели должны быть использованы, в том числе, для определения структуры и объемов информационного обмена между узлами облачной инфраструктуры. В состав информационного обеспечения АСОД для мониторинга ИБ объекта информатизации в облачной инфраструктуре могут входить как сами данные о состоянии ИБ объекта информатизации в облачной инфраструктуре, полученные непосредственно от средств защиты информации, развернутых внутри облачной инфраструктуры, так их копии и/или предыстории, полученные в узлах облачной инфраструктуры в местах их использования АСОД для мониторинга ИБ объекта информатизации. В качестве частных критериев этих моделей целесообразно использовать: максиминный критерий полезности информационного обеспечения АСОД для мониторинга ИБ объекта информатизации в облачной инфраструктуре; критерий максимума актуальности информационного обеспечения, распределенного по узлам облачной инфраструктуры для сложных, комплексных систем с невысокой степенью централизации управления [7, 8].

Результатом решения задачи разработки структуры информационного обеспечения аналитической системы обработки данных для мониторинга ИБ объекта информатизации является оптимальный по заданным критериям состав компонентов информационного обеспечения АСОД и их размещение по узлам облачной инфраструктуры.

ЗАКЛЮЧЕНИЕ

В статье рассмотрена задача определения рациональной структуры информационного обеспечения АСОД для мониторинга ИБ объекта информатизации в облачной инфраструктуре. При этом рассмотрены СМИБ, построенные на основе современных SIEM-систем, и предложен формализованный подход на базе разработки и использования методов математического и компьютерного моделирования.

В основу формализации и решения этой задачи положены методы теории полезности и исследования операций, которые позволяют с помощью компьютерного моделирования определить оптимальный состав компонентов информационного обеспечения АСОД и их распределение по узлам облачной инфраструктуры с точки зрения общей полезности информации с учетом используемых в этих узлах аналитических информационных технологий для выявления инцидентов ИБ.

В целом такой подход позволяет повысить оперативность процедуры выявления инцидентов ИБ за счет организации рационального обмена информацией между узлами облачной инфраструктуры (средствами защиты информации) с учетом характеристик аналитических процедур обработки данных, и, в целом, качество системы мониторинга ИБ.

Вклад авторов. Все авторы в равной степени внесли свой вклад в исследовательскую работу.

Authors' contribution. All authors equally contributed to the research work.

СПИСОК ЛИТЕРАТУРЫ

1. Liu Z., Zhao A., Liang M. A port-based forwarding load-balancing scheduling approach for cloud datacenter networks. *J. Cloud Comp*. 2021;10(1):13. https://doi.org/10.1186/s13677-021-00226-w
2. Chen J., Wang Y., Liu T. A proactive resource allocation method based on adaptive prediction of resource requests in cloud computing. *J. Wireless Com. Network*. 2021;24. https://doi.org/10.1186/s13638-021-01912-8
3. Wang J., Zhang G., Wang W., Zhang K., Sheng Y. Cloud-based intelligent self-diagnosis and department recommendation service using Chinese medical BERT. *J. Cloud Comp.: Advances, Systems and Applications*. 2021;10(1):4. https://doi.org/10.1186/s13677-020-00218-2
4. Chen Y., Liu H., Wang B., Sonompil B., Ping Y., Zhang Z. A threshold hybrid encryption method for integrity audit without trusted center. *J. Cloud Comp.: Advances, Systems and Applications*. 2021;10(1):3. https://doi.org/10.1186/s13677-020-00222-6
5. Ngoc T.L., Doan B.H. Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing: Practice and Experience*. 2017;18(4):277–290. https://doi.org/10.12694/scpe.v18i4.1329
6. Afolaranmi S.O., Moctezuma L.E.G., Rak M., Casola V., Rios E., Lastra J.L.M. Methodology to Obtain the Security Controls in Multi-cloud Applications. In: *Proceedings of the 6th International Conference on Cloud Computing and Services Science* (*CLOSER 2016*). 2016. V.1. p. 327–332. http://doi.org/10.5220/0005912603270332
7. Сизов В.А. Разработка моделей повышения эффективности сохранности данных в распределенной вычислительной среде на основе динамического резервирования данных. В сб.: *Advances in Science and Technology*: *сб. статей XXI международной научно-практической конференции*. М.: «Актуальность. РФ», 2019. С. 96–100.
8. Сизов В.А. Модели и методы виртуально-восстановительного резервирования данных автоматизированных информационно-управляющих систем в условиях чрезвычайных ситуаций. *Автоматика и телемеханика*. 1998;7:176–184.
9. Arce D.G. Cybersecurity and platform competition in the cloud. *Computers & Security*. 2020;93:101774. https://doi.org/10.1016/j.cose.2020.101774
10. Джинчарадзе Г.Р. Методические аспекты организации процедуры оценки персонала. *Инженерный Вестник Дона*. 2012;2(20):340–345. URL: https://cyberleninka.ru/article/n/metodicheskie-aspekty-organizatsii-protsedury-otsenki-personala
11. Сизов В.А., Киров А.Д. Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности. *Открытое образование*. 2020;24(1):69–79. https://doi.org/10.21686/1818-4243-2020-1-69-79
12. Lee J., Kim Y.S., Kim J.H., Kim I.K. Toward the SIEM architecture for cloud-based security services. In: *2017 IEEE Conference on Communications and Network Security* (*CNS*). https://doi.org/10.1109/CNS.2017.8228696

REFERENCES

1. Liu Z., Zhao A., Liang M. A port-based forwarding load-balancing scheduling approach for cloud datacenter networks. *J. Cloud Comp*. 2021;10(1):13. https://doi.org/10.1186/s13677-021-00226-w
2. Chen J., Wang Y., Liu T. A proactive resource allocation method based on adaptive prediction of resource requests in cloud computing. *J. Wireless Com. Network*. 2021;24. https://doi.org/10.1186/s13638-021-01912-8
3. Wang J., Zhang G., Wang W., Zhang K., Sheng Y. Cloud-based intelligent self-diagnosis and department recommendation service using Chinese medical BERT. *J. Cloud Comp.: Advances, Systems and Applications*. 2021;10(1):4. https://doi.org/10.1186/s13677-020-00218-2
4. Chen Y., Liu H., Wang B., Sonompil B., Ping Y., Zhang Z. A threshold hybrid encryption method for integrity audit without trusted center. *J. Cloud Comp.: Advances, Systems and Applications*. 2021;10(1):3. https://doi.org/10.1186/s13677-020-00222-6
5. Ngoc T.L., Doan B.H. Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing: Practice and Experience*. 2017;18(4):277–290. https://doi.org/10.12694/scpe.v18i4.1329
6. Afolaranmi S.O., Moctezuma L.E.G., Rak M., Casola V., Rios E., Lastra J.L.M. Methodology to Obtain the Security Controls in Multi-cloud Applications. In: *Proceedings of the 6th International Conference on Cloud Computing and Services Science* (*CLOSER 2016*). V.1. 2016, p. 327–332. http://doi.org/10.5220/0005912603270332
7. Sizov V.A. Development of models for improving the efficiency of data safety in a distributed computing environment based on dynamic data reservation. In: *Advances in Science and Technology*: *Collection of articles of the XXI International Scientific and Practical Conference*. 2019, p. 96–100. (in Russ.).
8. Sizov V.A. Models and methods of virtual-recovered redundancy of data of automatic information-control systems under extreme conditions. *Autom. Remote Control*. 1998;59(7):1047–1053.
[Sizov V.A. Models and methods of virtual-recovered redundancy of data of automatic information-control systems under extreme conditions. *Automat. i Telemekh*. 1998;(7):176–184 (in Russ.).]
9. Arce D.G. Cybersecurity and platform competition in the cloud. *Computers & Security*. 2020;93:101774. https://doi.org/10.1016/j.cose.2020.101774
10. Dzhincharadze G.R. Methodological aspects of the organization of the personnel assessment procedure. *Inzhenernyi Vestnik Dona = Engineering journal of Don*. 2012;2(20):340–345 (in Russ.). Available from URL: https://cyberleninka.ru/article/n/metodicheskie-aspekty-organizatsii-protsedury-otsenki-personala
11. Sizov V.A., Kirov A.D. Problems of implementation SIEM-systems in the practice of managing information security of economic entities. *Otkrytoe obrazovanie = Open Education*. 2020;24(1):69–79 (in Russ.). https://doi.org/10.21686/1818-4243-2020-1-69-79
12. Lee J., Kim Y.S., Kim J.H., Kim I.K. Toward the SIEM architecture for cloud-based security services. In: *2017 IEEE Conference on Communications and*

13. Granadillo G.G., El-Barboni M., Debar H. New types of alert correlation for security information and event management systems. In: *2016 8th IFIP International Conference on New Technologies, Mobility and Security* (*NTMS*). 2016. https://doi.org/10.1109/NTMS.2016.7792462
14. Kavanagh M., Rochford O. *Magic Quadrant for Security Information and Event Management.* Gartner technical report. 2015. 15 p.
15. Марков А.С., Цирлов В.Л. Структурное содержание требований информационной безопасности. *Мониторинг правоприменения*. 2017;1(22):53–61.
16. Nabil M., Soukainat S., Lakbabi A., Ghizlane O. SIEM selection criteria for an efficient contextual security. In: *2017 International Symposium on Networks, Computers and Communications* (*ISNCC*). 2017. https://doi.org/10.1109/ISNCC.2017.8072035
17. Кирсанов К.К. Теория полезности в период смены концептуальных положений. *Науковедение* (*Вестник Евразийской науки)*. 2015;7(2):38. URL: http://naukovedenie.ru/PDF/37EVN215.pdf
18. 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):2–16. https://doi.org/10.21681/2311-3456-2017-5-2-16
19. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2. *Труды СПИИРАН*. 2016;6(49):208–225. https://doi.org/10.15622/sp.49.11

Network Security (CNS). https://doi.org/10.1109/CNS.2017.8228696
13. Granadillo G.G., El-Barboni M., Debar H. New Types of Alert Correlation for Security Information and Event Management Systems. In: *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. 2016. https://doi.org/10.1109/NTMS.2016.7792462
14. Kavanagh M., Rochford O. *Magic Quadrant for Security Information and Event Management.* Gartner technical report. 2015. 15 p.
15. Markov A.S., Tsirlov V.L. Structured content of information security requirements. *Monitoring pravoprimeneniya = Monitoring of Law Enforcement*. 2017;1(22):53–61 (in Russ.). https://doi.org/10.21681/2412-8163-2017-1-53-61
16. Nabil M., Soukainat S., Lakbabi A., Ghizlane O. SIEM selection criteria for an efficient contextual security. In: *2017 International Symposium on Networks, Computers and Communications (ISNCC)*. https://doi.org/10.1109/ISNCC.2017.8072035
17. Kirsanov K.K. The theory of utility in the period of change of conceptual provisions. *Naukovedenie* (*The Eurasian Journal*). 2015;7(2):38 (in Russ.). Available from URL: http://naukovedenie.ru/PDF/37EVN215.pdf
18. Kotenko I.V., Fedorchenko A.V., Saenko I.B., Kushnerevich A.G. Big data technologies for security event correlation based on event type accounting. *Voprosy kiberbezopasnosti = Cybersecurity issues*. 2017;5(24):2–16 (in Russ.). https://doi.org/10.21681/2311-3456-2017-5-2-16
19. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. An Analysis of Security Event Correlation Techniques in SIEM-Systems. Part 2. *Trudy SPIIRAN = SPIIRAS Proceedings*. 2016;6(49):209–225 (in Russ.). https://doi.org/10.15622/sp.49.11

Об авторах

Сизов Валерий Александрович, д.т.н., профессор, кафедра Прикладной информатики и информационной безопасности Института математики, информационных систем и цифровой экономики ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова» (117997, Россия, Москва, Стремянный пер., 36). E-mail: sizov.va@rea.ru. https://orcid.org/0000-0002-4844-4714

Киров Алексей Дмитриевич, специалист, специализированная учебно-научная лаборатория по информационному противоборству в бизнесе, кафедра Прикладной информатики и информационной безопасности Института математики, информационных систем и цифровой экономики ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова» (117997, Россия, Москва, Стремянный пер., 36). E-mail: kirov.ad@rea.ru. https://orcid.org/0000-0002-8424-3071

About the authors

Valerii A. Sizov, Dr. Sci. (Eng.), Professor, Department of Applied Informatics and Information Security, Institute of Mathematics, Information Systems and Digital Economy, Plekhanov Russian University of Economics (36, Stremyanny per., Moscow, 117997 Russia). E-mail: sizov.va@rea.ru. https://orcid.org/0000-0002-4844-4714

Aleksey D. Kirov, Specialist, Specialized Educational and Scientific Laboratory on Information Confrontation in Business, Department of Applied Informatics and Information Security, Institute of Mathematics, Information Systems and Digital Economy, Plekhanov Russian University of Economics (36, Stremyanny per., Moscow, 117997 Russia). E-mail: kirov.ad@rea.ru. https://orcid.org/0000-0002-8424-3071