УДК 004.056
doi:10.21685/2307-5538-2021-4-4

ПРОБЛЕМАТИКА ЭФФЕКТИВНОЙ ОЦЕНКИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАКЕТНО-КОСМИЧЕСКОЙ ОТРАСЛИ

В. А. Селифанов[1], А. В. Ляшенко[2], В. В. Мартыненко[3], М. А. Фролов[4]

[1, 2, 3, 4] АО «Российские космические системы», Москва, Россия
[1] selifanov.va@spacecorp.ru, [2] lyashenko.av@spacecorp.ru, [3] martynenko.vv@spacecorp.ru, [4] frolov.ma@spacecorp.ru

Аннотация. *Актуальность и цели.* При проектировании систем защиты информации важно организовать процесс управления инцидентами информационной безопасности (ИБ) максимально эффективным образом. Целью данной статьи является анализ проблематики эффективной оценки событий ИБ. *Материалы и методы.* Для проведения полноценного анализа в статье рассматривается отечественная и международная нормативно-методическая база в области управления событиями ИБ в ракетно-космической отрасли, а именно: государственные стандарты (ГОСТ Р) и международные стандарты ISO/IEC. Кратко описаны существующие модели управления событиями ИБ, такие как PDCA и PICERL. Для предотвращения возможных проблем оценки событий ИБ в ракетно-космической отрасли анализируется важность использования в информационных системах SIEM-решений, а также применяемые для этого методы настройки корреляции событий в SIEM-системах. *Результаты.* Ключевыми выводами являются следующие: отсутствует единая общепринятая методика, позволяющая построить унифицированную модель управления инцидентами в ракетно-космической отрасли; существующие модели построения процессов управления событиями ИБ в полной мере не описывают нюансы настройки технических решений, предназначенных для централизованного управления событиями ИБ, и не позволяют обеспечить оперативное реагирование на возможные инциденты ИБ, их обработку и разрешение последствий таких инцидентов в информационной системе в ракетно-космической отрасли. Результатом работы является определение и формулировка ключевых проблем управления событиями ИБ в ракетно-космической отрасли, возникающих при построении и эксплуатации систем защиты.

Ключевые слова: информационная безопасность, ракетно-космической отрасль, события ИБ, SIEM-система, PDCA, PICERL

Для цитирования: Селифанов В. А., Ляшенко А. В., Мартыненко В. В., Фролов М. А. Проблематика эффективной оценки событий информационной безопасности в ракетно-космической отрасли // Измерения. Мониторинг. Управление. Контроль. 2021. № 4. С. 32–40. doi:10.21685/2307-5538-2021-4-4

PROBLEMS OF EFFECTIVE ASSESSMENT OF INFORMATION SECURITY EVENTS IN THE ROCKET AND SPACE INDUSTRY

V.A. Selifanov[1], A.V. Lyashenko[2], V.V. Martynenko[3], M.A. Frolov[4]

[1, 2, 3, 4] Joint Stock Company "Russian Space Systems", Moscow, Russia
[1] selifanov.va@spacecorp.ru, [2] lyashenko.av@spacecorp.ru, [3] martynenko.vv@spacecorp.ru, [4] frolov.ma@spacecorp.ru

Abstract. *Background.* The organization of the information security incident management process is a very important aspect of the information security system design. The objective of the research was to analyze problems of effective assessment of information security events. *Materials and methods.* In the theoretical part of the article analyzed international and Russian standarts in the field of information security event management. For example, Russian GOST or international ISO/IEC. The article described such incident management models as PDCA and PICERL. The study proved the importance of using SIEM-solutions in information systems and methods for setting up event correlation. *Results.* The key thesis of this article are: there is no generally accepted method of incident management; models for building information security event management processes don't describe the nuances of configuring technical solutions and don't provide a quick response, analysis and resolution of information security incidents. The results of the study show the main problems of effective assessment of information security events.

Keywords: information security, rocket and space industry, information security events, SIEM-system, PDCA, PICERL

For citation: Selifanov V.A., Lyashenko A.V., Martynenko V.V., Frolov M.A. Problems of effective assessment of information security events in the rocket and space industry. *Izmereniya. Monitoring. Upravlenie. Kontrol' = Measurements. Monitoring. Management. Control*. 2021;(4):32–40. (In Russ.). doi:10.21685/2307-5538-2021-4-4

Введение

В связи с ежегодным увеличением мирового информационного пространства, объемов данных и усложнением глобальной архитектуры информационных систем растут и требования к системам защиты информации в ракетно-космической отрасли (РКО). Для получения максимально подробных данных о событиях информационной безопасности (ИБ), произошедших в информационной системе, необходима их агрегация из различных источников, таких как средства антивирусной защиты, журналы событий средств защиты, DLP-системы в части контроля действий всех пользователей и сканеры уязвимостей и т.д. Усложнение it-инфраструктуры в ракетно-космической отрасли влечет за собой увеличение числа событий ИБ, которые, в свою очередь, нуждаются в анализе и управлении, что невозможно без создания эффективной модели управления инцидентами ИБ в указанной отрасли[1].

Существующие стандарты

При проектировании систем защиты информации, а также построении модели управления событиями ИБ необходимо опираться как на отечественную нормативную базу, так и на международные стандарты.

К государственным стандартам России (ГОСТ Р), регламентирующим вопросы управления событиями ИБ, относятся:

1. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента ИБ. Требования.

Это основополагающий стандарт, устанавливающий требования к системам менеджмента ИБ, а также к процессу управления инцидентами. Данный документ рекомендует использование процессного подхода при организации системы менеджмента. Он заключается в том, что всю деятельность, функционирующую в организации, необходимо рассматривать как процесс. Для этого в стандарте вводится модель «Планирование (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (PDCA), используемая для структурирования процессов, влияющих на функционирование организации в целом[2].

Преимуществами этой модели является то, что произошедшие в информационной системе события и инциденты ИБ обрабатываются эффективным образом, особенно в части их классификации за счет тщательного анализа нежелательных происшествий минимизируются последствия от их повторного появления и ускоряется реакция по их предотвращению.

2. ГОСТ Р ИСО/МЭК 18044–2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов ИБ. Текущий стандарт предлагает использование структурного и планового подхода к реагированию на инциденты ИБ и построению менеджмента инцидентов в целом. Большое внимание уделяется этапам менеджмента инцидентов ИБ, соответствующим процессам модели PDCA.

3. ГОСТ Р ИСО/МЭК 27002–2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента ИБ. Текущий стандарт описывает ключевые меры и средства обеспечения ИБ информационной системы, в том числе защиту документов и данных компании, распределение обязанностей сотрудников, обучение персонала в области ИБ, менеджмент уязвимостей, непрерывности бизнеса и инцидентов

[1] ГОСТ Р ИСО/ МЭК 18044–2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

[2] ГОСТ Р ИСО/ МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

ИБ, а также документирование политики ИБ[1]. Также в стандарте уделяется особое внимание факту того, что не все, описываемые в документе средства, могут и должны быть применены в РКО.

4. Международные стандарты, описывающие порядок управления событиями ИБ, такие как ISO/IEC 27001:2013, ISO/IEC 27035:2011 и ISO/IEC 27002:2013, являются идентичными соответствующим отечественным стандартам в области управления информационными технологиями в целом, а также конкретизирующие область управления инцидентами ИБ. Проблема их использования путем перевода в отечественные заключается в том, что пока готовится и утверждается ГОСТ, международный документ может стать недействительным, поскольку произойдет его обновление[2]. Это вносит дополнительные неясности в правовую базу. Более наглядно это представлено в табл. 1.

Таблица 1

Актуальность российских стандартов

Российский стандарт	Актуальность	Международный стандарт	Актуальность
ГОСТ Р ИСО/МЭК 27001–2006	+	ISO/IEC 27001:2005	–
–	–	ISO/IEC 27001:2013	+
–	–	ISO/IEC 27001:2013/CD Amd 1	+
–	–	ISO/IEC 27001:2013/Cor 1:2014	+
–	–	ISO/IEC 27001:2013/Cor 2:2015	+
ГОСТ Р ИСО/МЭК 18044–2007	+	ISO/IEC 18044:2004	–
–	–	ISO/IEC 27035:2011	–
–	–	ISO/IEC 27035–1:2016 ISO/IEC 27035–2:2016	+
–	–	ISO/IEC 27035–3:2020	+
ГОСТ Р ИСО/МЭК 27002–2012	+	ISO/IEC 27002:2005	–
–	–	ISO/IEC 27002:2013	+
–	–	ISO/IEC 27002:2013/COR 1:2014	+
–	–	ISO/IEC 27002:2013/COR 2:2015	+

Из табл. 1 можно сделать вывод о том, что многие международные стандарты были уже несколько раз перевыпущены. На примере ГОСТ Р ИСО/МЭК 27002–2012 видно, что международный документ имеет несколько дополнений. Однако российская законодательная база не актуализирует российские стандарты под обновленные международные требования.

Помимо нормативных стандартов при анализе событий ИБ необходимо руководствоваться частными документами, разработанными на конкретную систему, а именно, моделью угроз и нарушителя безопасности информации и политикой информационной безопасности в РКО.

Существующие модели управления событиями ИБ

Основной моделью принятия решений, рассматриваемой в законодательной базе по управлению инцидентами, является модель PDCA (Plan-Do-Check-Act) или, как ее еще называют, модель Деминга – Шухарта.

Кратко действия, совершаемые на каждом этапе этой модели, представлены на рис. 1.

---

[1] ГОСТ Р ИСО/ МЭК 27002–2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента ИБ.

[2] ISO/IEC 27035-1-2016 Information technology – Security techniques. Information security incident management – Part 1: Principles of incident management ; ISO/IEC 27035-2-2016 Information technology – Security techniques. Information security incident management – Part 2: Guidelines to plan and prepare for incident response ; ISO/IEC 27035-3-2020 Information technology – Security techniques. Information security incident management – Part 3: Guidelines for ICT incidents response operations ; ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements ; ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security controls.

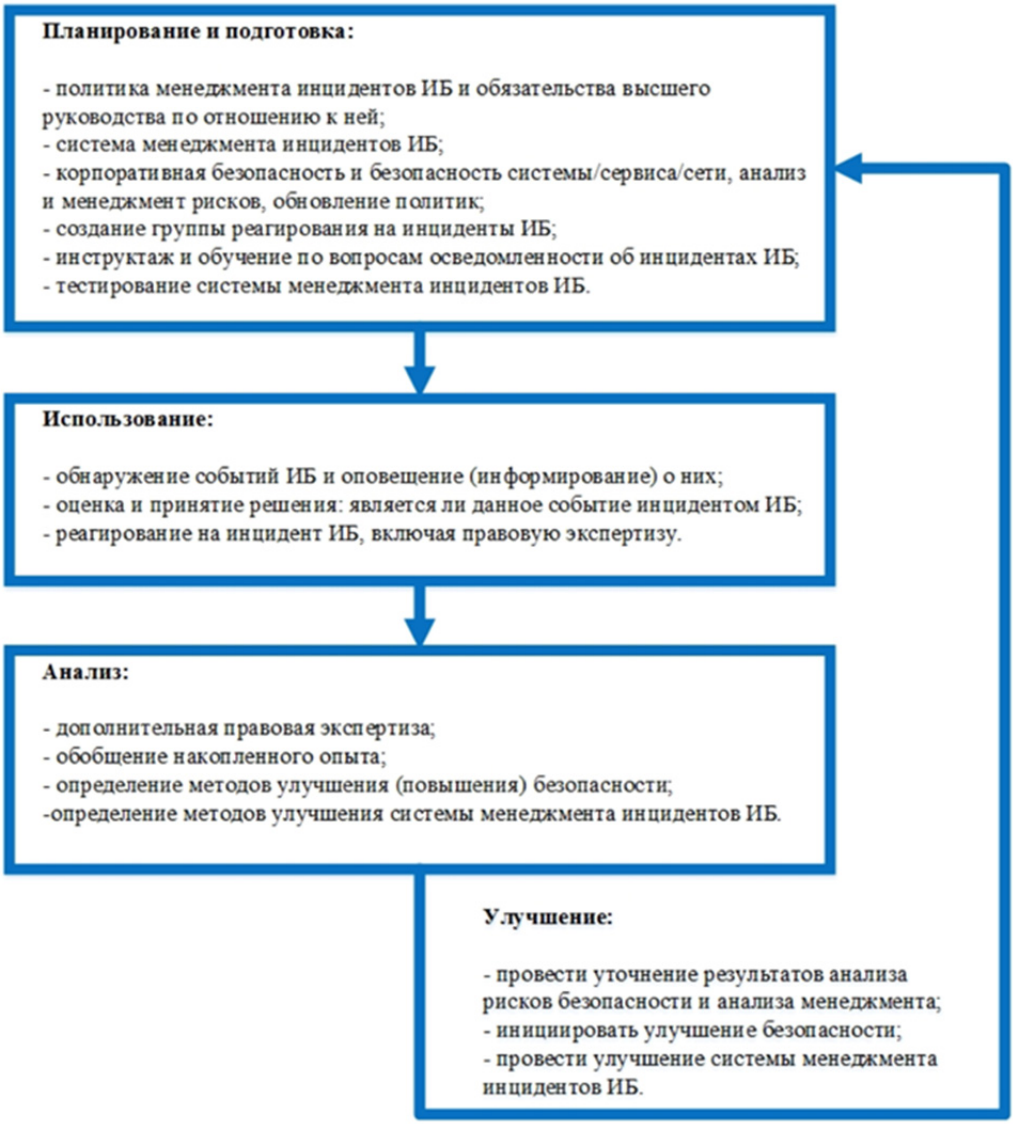

Рис. 1. Модель PDCA

Основной целью модели PDCA является обеспечение непрерывного, постоянного, цикличного процесса улучшения системы реагирования на события и инциденты.

Минусами этой модели является трудность реализации данного процесса при отсутствии большого количества персонала, решающего только задачи управления инцидентами. Данная модель будет хорошо функционировать при наличии выделенного для менеджмента инцидента подразделения, с реализованной в нем эскалацией принятия решений в зависимости от приоритета инцидента ИБ в РКО.

Моделью, описывающей процесс реагирования на инциденты, является модель PICERL (Preparation – Identidication – Eradication – Recovery – Lessons Learned).

Модель PICERL представляет собой жизненный цикл реагирования на события и инциденты ИБ. При построении процесса реагирования, основанного на приведенных в модели этапах, можно реализовать полноценный сценарий действий по управлению событиями. Минусами этой модели является то, что она ориентирована больше на построение процессов и организацию работ персонала, чем на управление техническими решениями.

Как видно из анализа, в реальных условиях при проектировании систем защиты использование только одной методики управления событиями ИБ в РКО недостаточно. Для эффективного анализа и построения системы управления событиями ИБ необходимо комбинирование существующих методик и выработка уникальных для каждой системы защиты метрик, позволяющих повысить точность обнаружения ключевых событий ИБ в РКО.

Рис. 2. Модель PICERL

Применяемые для управления событиями ИБ решения

При проектировании информационных систем в РКО невозможно применить глобальные комплексные решения, такие как например создание Security Operation Center (SOC). SOC решения включают в себя набор технических средств, автоматизированные процессы и большое количество задействованных человеческих ресурсов. Применение таких интегрированных решений невозможно вследствие отсутствия необходимости выделять такое количество ресурсов на менеджмент событий информационной безопасности в рамках одной системы, а также по большей части при проектировании систем ощущается существенная нехватка человеческих и финансовых ресурсов. Считается нецелесообразным уделять настолько большое внимание только одному аспекту защиты информации, поэтому при проектировании систем обычно считается достаточным применение только Security information and event management (SIEM) систем.

Применение SIEM-решений в первую очередь необходимо при проектировании критических информационных инфраструктур, а также при необходимости осуществления централизованного сбора событий при создании, например, государственных информационных систем.

SIEM-системы применяются для автоматизации процессов управления, для оперативной обработки данных о событиях безопасности, происходящих в системе, для осуществления централизованного сбора данных о произошедших событиях информационной безопасности.

Даже несмотря на максимальное упрощение шаблонов настроек и прозрачность функционирования применяемых решений, необходимо потратить достаточно много времени и задействовать много человеческих ресурсов для обеспечения должного уровня защищенности в РКО системы за счет применения в ней решений класса SIEM.

Для обеспечения эффективного функционирования SIEM-системы в РКО необходимо:

– провести анализ системы и определить особенности инфраструктуры, а также требования и рекомендации регулирующих организаций;

– определить список источников, которые необходимо подключить к SIEM-системе для решения поставленных задач;

– настроить автоматизированное реагирование системы в виде выполнения заданных скриптов, программ или задач при выявлении значимых отклонений показателей на этапе корреляции;

– настроить генерацию оповещений (уведомлений) о выявленных событиях ИБ;

– настроить визуализацию собираемых данных в виде диаграмм, помогающих идентифицировать аномалии или значимые отклонения, отличные от стандартного поведения систем. Так же визуализация включает в себя представление данных в виде отчетов;

– настроить хранение собранных данных в базе данных.

Методы настройки механизмов в SIEM-системах

Основными методами, применяемыми для настройки механизмов обнаружения событий безопасности, в SIEM-системах являются правила корреляции. Со стороны администратора, который производит настройки SIEM-систем, настройка правил корреляции, по большей части, выглядит как адаптация готовых шаблонов настроек под нужды конкретной системы.

Внутри шаблонных правил корреляции разработчиками используются типовые методы и алгоритмы, позволяющие обнаружить аномальное поведение системы (события и инциденты ИБ). Компании-разработчики SIEM решений полностью не раскрывают применяемые в их изделиях алгоритмы и методы. Однако базовые методы, которые являются основой для комбинации методик, применяемых в SIEM, известны.

Отличие между правилами корреляции заключается в использовании различных подходов к анализу состояния системы для формирования событий ИБ.

Существующие методы корреляции событий ИБ рассматривались во многих научных работах. В основу данной статьи легли работы [1, 2].

Ключевыми правилами корреляции, применяемыми для настройки правил реагирования системы на события, являются следующие:

– корреляция, основанная на сравнении событий безопасности;

– корреляция, основанная на базе знаний;

– статистическая корреляция.

Главными примерами корреляции, основанной на сравнении событий безопасности, являются:

– корреляция, основанная на правилах;

– корреляция, в основе которой лежит машинное обучение.

Основой корреляции на правилах является сбор (агрегация) событий из различных источников. Такими источниками могут быть: антивирус, DLP-системы, данные из мониторинга активности, IDS-системы и т.д. При появлении в системе типовых событий срабатывают правила, появление которых SIEM-система считает событием ИБ.

При использовании корреляции, в основе которой лежит машинное обучение, SIEM-система способна принимать решение об отнесении событий в системе к событиям ИБ на основе построения ветки деревьев решений.

Плюсом таких типов корреляции является простота понимания, а минусами – субъективность заданных правил, сформированных экспертом, неспособность системы автоматически обучаться на опыте применения правил и невозможность сохранять эффективность работы с правилами при появлении нестандартных ситуаций в системе.

Главными примерами корреляции, основанной на базе знаний, являются:

– корреляция, основанная на сценариях атак;

– корреляция на основе предпосылок наступления событий безопасности.

Корреляция, основанная на сценариях атак, предназначена для обнаружения многоступенчатых атак.

Корреляция на основе предпосылок наступления событий безопасности заключается в установке взаимосвязи между цепочками событий и возможными атаками на систему. Такая корреляция основывается на базе знаний, в которой содержится описание возможных предпосылок последствий наступления события ИБ.

Плюсами корреляции, основанной на базе знаний, является возможность определить первопричину возникновения события ИБ путем анализа начальных событий в цепочке. Ми-

нусами данного метода является то, что при одновременном возникновении в системе нескольких причин, повлекших за собой возникновение события ИБ, не всегда возможно будет выявить первопричину, повлекшую за собой появление такого события.

Основами статистической корреляции являются причинно-следственные связи, которые сохраняются после различных событий ИБ. Такие типы корреляции анализируют возникшие во время событий ИБ шаги атаки и обучаются с использованием статистического анализа данных.

Сравнение методов корреляции приведено в табл. 2 [1, 2].

Таблица 2

Сравнение методов корреляции

Характеристика метода	Корреляция, основанная на сравнении событий безопасности	Корреляция, основанная на базе знаний	Статистическая корреляция
Возможность сбора событий из различных источников	Да	Да	Нет
Необходимость в базе знаний	Да	Да	Нет
Обнаружение ложных событий	Да	Да	В зависимости от настроек
Обнаружение многоступенчатых атак	В зависимости от настроек	Да	В зависимости от настроек
Обнаружение новых атак	Да	Нет	Да
Вероятность ложных срабатываний	Средняя	Низкая	Высокая

При разработке правил не производится их тестирование на функционирующих в реальном времени системах. Вследствие недостаточности нагрузочных тестов частой проблемой является проблема совместимости правил с решениями, подключаемыми к SIEM.

Помимо этого, большинство правил настройки и приоритет реагирования на события ИБ все равно определяется экспертом. Нет научно обоснованной типовой методики, как выстраивать корреляцию событий и принимать решения при возникновении в системе событий ИБ в РКО таким образом, чтобы гарантированно выявлять все предпосылки по нарушениям режима безопасности и поиска первопричин произошедших событий.

Другой проблемой является недостаточная частота обновлений правил. Невозможно обеспечить оперативную доставку улучшений старых правил, добавление новых, а также их оперативную обработку в функционирующих системах.

Помимо вышесказанного разработчиками при внедрении в SIEM-системы правил не учитываются следующие нюансы РКО:

– количество подключаемых к системе средств, в том числе средств защиты информации;

– масштабы системы, в которую предполагается внедрение SIEM.

Заключение

В результате анализа существующей нормативно-методической базы по управлению инцидентами очевидно отсутствие общепринятой методики в РКО, позволяющей построить унифицированную модель управления инцидентами. Существующие модели построения процессов управления событиями ИБ в полной мере не описывают нюансы настройки технических решений, предназначенных для централизованного управления событиями ИБ в РКО. Научно-исследовательские работы и публикации в области управления инцидентами ИБ также не отвечают необходимым тенденциям и не позволяют обеспечить оперативное реагирование на возможные инциденты ИБ, их обработку и разрешение последствий таких инцидентов в информационной системе.

Это влечет за собой следующие проблемы при построении и эксплуатации систем защиты в РКО:

1. Выработка решений по большинству функций защиты производится человеком. Несмотря на интеграцию современных аппаратно-программных средств, в том числе SIEM-систем, процессы контроля инцидентов автоматизированы лишь частично. Необходимо ми-

нимизировать влияние человеческого фактора при принятии управляющих решений в части фильтрации происходящих в системе событий ИБ.

2. Отсутствие структурированного алгоритма обнаружения инцидентов может привести к несвоевременному реагированию на инциденты ИБ или, наоборот, к переизбытку поступающих в систему событий ИБ. Последствия таких настроек существенно замедляют скорость реакции на потенциальные инциденты ИБ, что негативно влияет на стойкость системы защиты к потенциальным атакам и критично сказывается на функционировании системы в целом.

3. Необходимость длительного анализа и выработки уникальных для каждой конкретной системы метрик, характеризующих ключевые показатели параметров инцидентов. Разработка унифицированных показателей и критериев оценки событий для обнаружения и идентификации инцидентов ИБ в РКО повысила бы эффективность управления событиями ИБ и ускорила бы разработку системы защиты в целом.

Исходя из всего вышесказанного, следует вывод, что необходима разработка и регламентация эффективной модели управления инцидентами, позволяющей систематизировать и скоординировать действия при анализе событий, расследовании, предотвращении и устранении причин и последствий инцидентов ИБ в системе РКО.

Список литературы

1. Москвичев А. Д., Долгачев М. В. Алгоритмы корреляции событий информационной безопасности // Автоматизация процессов управления. 2020. № 3. С. 50–59.
2. Новикова Е. С., Бекенева Я. А., Шоров А. В., Федотов Е. С. Обзор алгоритмов корреляции событий безопасности для обеспечения безопасности облачных вычислительных сред // Информационно-управляющие системы. 2017. № 5. С. 95–104.

References

1. Moskvichev A.D., Dolgachev M.V. Algorithms of correlation of information security events. *Avtomatizatsiya protsessov upravleniya = Automation of management processes*. 2020;(3):50–59. (In Russ.)
2. Novikova E.S., Bekeneva Ya.A., Shorov A.V., Fedotov E.S. Review of algorithms for correlation of security events to ensure the security of cloud computing environments. *Informatsionno-upravlyayushchie sistemy = Information management systems*. 2017;(5):95–104. (In Russ.)

Информация об авторах / Information about the authors

Владимир Алексеевич Селифанов
кандидат технических наук,
начальник сектора создания систем
передачи данных,
АО «Российские космические системы»
(Россия, г. Москва, ул. Авиамоторная, 53)
E-mail: selifanov.va@spacecorp.ru

Vladimir A. Selifanov
Candidate of technical sciences,
head of the sector for the creation
of data transmission systems,
Joint Stock Company "Russian Space Systems"
(53 Aviamotornaya, Moscow, Russia)

Антон Валерьевич Ляшенко
заместитель начальника отдела создания
систем обеспечения безопасности информации
и передачи данных НАКУ КА и ИКК,
АО «Российские космические системы»
(Россия, г. Москва, ул. Авиамоторная, 53)
E-mail: lyashenko.av@spacecorp.ru

Anton V. Lyashenko
Deputy head of the department for creating
information security systems and data transmission,
Joint Stock Company "Russian Space Systems"
(53 Aviamotornaya, Moscow, Russia)

Валентин Валентинович Мартыненко
начальник отдела создания систем
обеспечения безопасности информации
и передачи данных НАКУ КА и ИКК,
АО «Российские космические системы»
(Россия, г. Москва, ул. Авиамоторная, 53)
E-mail: martynenko.vv@spacecorp.ru

Valentin V. Martynenko
Head of the department for creating
information security systems and data transmission,
Joint Stock Company "Russian Space Systems"
(53 Aviamotornaya, Moscow, Russia)

Михаил Алексеевич Фролов
начальник центра создания наземных средств,
систем и комплексов НАКУ КА и ИКК,
АО «Российские космические системы»
(Россия, г. Москва, ул. Авиамоторная, 53)
E-mail: frolov.ma@spacecorp.ru

Michail A. Frolov
Head of the center for the creation
of ground facilities and complexes
Joint Stock Company "Russian Space Systems"
(53 Aviamotornaya, Moscow, Russia)

Авторы заявляют об отсутствии конфликта интересов /
The authors declare no conflicts of interests.

Поступила в редакцию/Received 17.06.2021
Поступила после рецензирования/Revised 24.06.2021
Принята к публикации/Accepted 29.09.2021