УДК 004.056
https://doi.org/10.31854/3034-2201-2026-4-1-C06
EDN: PHRWTM

Методика комплексной защиты информации и анализ журналов событий виртуальной инфраструктуры для выявления атак

Бютнер С. И. ✉, **Жилов К. Р., Сахаров Д. В.**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Постановка задачи. *Рост количества и сложности кибератак, особенно в виртуальных средах, требует перехода от разрозненных средств защиты к комплексным системам, объединяющим превентивные меры и перспективные методы анализа инцидентов. Существующие подходы часто не учитывают специфику виртуализации и не обеспечивают эффективного выявления сложных многоэтапных атак, нацеленных на уровень гипервизора и виртуальные машины.* ***Цель исследования*** *– разработка целостной методики, объединяющей построение комплексной системы защиты информации в соответствии с подходом, реализуемым в Санкт-Петербургском государственном университете телекоммуникаций, и специализированную методику ретроспективного и оперативного анализа журналов событий виртуальной инфраструктуры для точного выявления и классификации типов кибератак.* ***Методы.*** *В исследовании применялись методы системного анализа и управления рисками при проектировании комплексной системы защиты информации. Для анализа журналов событий использовались методы корреляционного анализа событий, машинного обучения (кластеризация, классификация, поиск аномалий), а также методы обработки больших объемов данных. Практическая проверка проводилась на основе развертывания опытной системы с использованием стека технологий Elastic Stack (Elasticsearch, Beats) и моделирования атак в виртуальной лаборатории.* ***Новизна.*** *Предложен синтетический подход, интегрирующий превентивную защиту в рамках комплексной системы защиты информации и глубокий анализ журналов событий всех уровней виртуальной инфраструктуры (виртуальная машина, гипервизоры, системы управления). Разработана методика, предусматривающая использование нереляционных моделей для хранения журналов событий, специализированных запросов к Elasticsearch для выявления аномалий и сценариев тестирования на основе уязвимых виртуальных машин для валидации.* ***Результаты.*** *Практическое внедрение показало увеличение доли обнаруженных атак на 40 % и снижение количества ложных срабатываний на 25 % по сравнению с традиционными подходами. Время обнаружения инцидентов сокращено на 65 %. Особенно значительный эффект достигнут в выявлении сложных многоэтапных атак за счет комплексной корреляции событий.* ***Практическая значимость.*** *Разработанная методика позволяет организациям, использующим виртуальные инфраструктуры, существенно повысить устойчивость к современным киберугрозам. Внедрение предлагаемого подхода минимизирует риски инцидентов, сокращает время их обнаружения и ликвидации, а также предоставляет инструмент для проактивного прогнозирования угроз. Результаты работы могут быть использованы при построении корпоративных комплексных систем защиты информации и систем мониторинга безопасности.*

Библиографическая ссылка на статью:
Бютнер С. И., Жилов К. Р., Сахаров Д. В. Методика комплексной защиты информации и анализ журналов событий виртуальной инфраструктуры для выявления атак // Вестник СПбГУТ. 2026. Т. 4. № 1. С. 6. DOI: 10.31854/3034-2201-2026-4-1-C06. EDN: PHRWTM

Reference for citation:
Butner S., Zhilov K., Sakharov D. A Methodology for Comprehensive Information Protection and Virtual Infrastructure Event Log Analysis for Attack Identification // Herald of SPbSUT. 2026. Vol. 4. Iss. 1. P. 6. DOI: 10.31854/3034-2201-2026-4-1-C06. EDN: PHRWTM

Ключевые слова: *комплексная система защиты информации, виртуализация, гипервизор, журналы событий, анализ журналов событий, кибератака, информационная безопасность, машинное обучение, система управления информацией и событиями безопасности*

Введение

Современные организации активно внедряют технологии виртуализации, что наряду с повышением гибкости и эффективности использования ресурсов создает новые векторы кибератак и усложняет задачи обеспечения информационной безопасности. Традиционные системы защиты, ориентированные на физическую инфраструктуру, зачастую оказываются недостаточно эффективными в условиях виртуальных сред, где атаки могут быть нацелены как на гостевые операционные системы виртуальных машин, так и на уровень управления гипервизором. Существующие подходы к анализу журналов событий часто не обеспечивают охвата всех компонентов виртуальной инфраструктуры и не позволяют эффективно выявлять сложные многоэтапные атаки, требующие корреляции событий с различных уровней. Особую важность приобретают вопросы защиты программно-определяемых сетей в виртуальных средах, где традиционные подходы к безопасности могут оказаться недостаточно эффективными [1].

Исследования моделей сетей центров обработки данных на основе политик безопасности демонстрируют перспективность применения программно-определяемых подходов для повышения защищенности виртуальной инфраструктуры [2]. В связи с этим актуальной задачей является разработка комплексных подходов, объединяющих классические методы построения систем защиты с передовыми методиками мониторинга и анализа событий безопасности в виртуальных средах. Современные киберугрозы характеризуются возрастающей сложностью и целенаправленностью, что требует применения комплексных подходов к защите виртуальной инфраструктуры. Особую озабоченность специалистов по информационной безопасности вызывают атаки на уровень гипервизора, которые могут привести к компрометации всей виртуальной среды организации, поэтому разработка эффективных методов анализа журналов событий виртуальных машин и систем управления виртуализацией становится критически важной для обеспечения непрерывности бизнес-процессов и защиты конфиденциальной информации.

Одним из таких подходов является методика построения комплексной системы защиты информации, разрабатываемая в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПбГУТ), основанная на системном подходе, учитывающем все компоненты информационной системы организации. Однако даже самая совершенная система защиты не может гарантировать абсолютную безопасность, что делает необходимым наличие подсистемы обнаружения и анализа инцидентов. Особую сложность представляет анализ активности в средах виртуализации, где атака может быть нацелена как на гостевые операционные системы виртуальных машин, так и на уровень управления гипервизором. Исходя из этого, данная статья ставит целью объединить методику построения превентивной комплексной системы защиты информации с разработкой специализированной методики для ретроспективного и оперативного анализа файлов журналов событий виртуальных машин и гипервизоров. Такой симбиоз позволяет не только противостоять известным угрозам, но и эффективно выявлять, классифицировать и расследовать сложные кибератаки, включая цепочки скоординированных действий злоумышленника.

Методика построения комплексной системы защиты информации и анализа журналов событий

В рамках данного исследования комплексная система защиты информации понимается как совокупность организационных и технических мер, направленных на обеспечение конфиденциальности, целостности и доступности информации. Методика, применяемая в СПбГУТ, предполагает поэтапное построение системы защиты на основе модели управления рисками [5]. На первом этапе проводится идентификация информационных активов, угроз и уязвимостей. Для каждого актива оценивается потенциальный ущерб и вероятность реализации угрозы. Результатом является ранжированный список рисков, подлежащих обработке. На следующем этапе формируется совокупность документированных правил и процедур, регламентирующих управление доступом, обработку данных, реагирование на инциденты и другие аспекты безопасности. Основные технические меры защиты, применяемые в рамках методики, представлены в таблице 1.

Таблица 1. Технические меры защиты информации

Мера защиты	Ключевые компоненты	Основная цель
Разграничение доступа	Системы аутентификации, авторизации и учета, управление доступом на основе ролей	Контроль доступа к информационным активам
Защита периметра	Межсетевой экран, системы обнаружения и предотвращения вторжений	Фильтрация сетевого трафика
Криптографическая защита	Шифрование дисков, виртуальная частная сеть	Обеспечение конфиденциальности данных
Антивирусная защита	Антивирусное программное обеспечение, системы обнаружения и реагирования на угрозы на конечных точках	Обнаружение вредоносного программного обеспечения
Резервное копирование	Автоматическое копирование	Восстановление после инцидентов

Особое внимание в методике уделяется безопасности виртуальной инфраструктуры, которая является неотъемлемой частью современной информационно-телекоммуникационной среды. Рекомендуется изолировать сегмент управления виртуальными машинами и гипервизорами, строго контролировать доступ к системам гипервизора (vCenter, Hyper-V Manager) и проводить регулярный аудит их конфигураций. При этом важным аспектом является обеспечение безопасности на уровне сетевой инфраструктуры, где применение программно-определяемых сетей позволяет реализовать более гибкие и эффективные механизмы защиты. Использование моделей сетей центров обработки данных на основе политик безопасности обеспечивает централизованное управление защитой и соответствие требованиям безопасности на всех уровнях виртуальной инфраструктуры.

Однако даже при наличии комплексной системы защиты информации возможны инциденты информационной безопасности. Для их расследования и классификации необходима специализированная методика анализа журналов событий. Виртуальная среда генерирует огромные объемы данных, которые содержат ключевые признаки атаки [3]. В связи с этим процесс анализа журналов виртуальной инфраструктуры начинается со сбора и нормализации данных из разнородных источников. Ключевыми источниками информации выступают журналы гостевых операционных систем виртуальных машин, включая Windows Event Log и системные журналы Linux (syslog), а также журналы событий гипервизоров таких платформ, как VMware vSphere и Hyper-V. Важным компонентом являются журналы систем управления, в частности vCenter Server Logs. Для эффективной обработки этих данных применяются специализированные инструменты, такие как агенты сбора журналов событий Elastic Beats и системы пересылки Rsyslog, которые обеспечивают доставку информации в централизованные хранилища типа Elasticsearch или Splunk для последующего анализа [4].

Важным аспектом повышения эффективности анализа является применение специализированных методик работы с хранилищами данных. В исследовании [5] представлена методика анализа журналов событий с использованием Elasticsearch, которая позволяет эффективно выявлять сигналы о вредоносных действиях в информационной системе. Авторы предлагают подход, основанный на построении и использовании специализированных запросов к индексам Elasticsearch для обнаружения аномальной активности. Методика включает этапы нормализации и обогащения событий, что особенно актуально для разнородных данных виртуальной инфраструктуры. Использование возможностей полнотекстового поиска и агрегационных запросов Elasticsearch позволяет выявлять сложные взаимосвязи между событиями, которые трудно обнаружить при традиционных подходах к анализу. Это значительно повышает эффективность обнаружения скоординированных атак, затрагивающих различные компоненты виртуальной среды. Интеграция данной методики в процесс анализа журналов событий виртуальной инфраструктуры позволяет создать единое пространство для поиска индикаторов компрометации на различных уровнях виртуализации. Использование Elasticsearch в качестве централизованного хранилища и аналитической платформы обеспечивает необходимую производительность и гибкость при работе с большими объемами данных безопасности.

Содержательную основу методики составляет выявление ключевых индикаторов компрометации на различных уровнях виртуальной инфраструктуры. На уровне виртуальных машин тревожными сигналами являются множественные неудачные попытки входа в систему, запуск подозрительных процессов

DOI: 10.31854/3034-2201-2026-4-1-C06
URL: https://vestnik-sut.ru/2026-1/C06.pdf

или скриптов, включая PowerShell с закодированными командами, неожиданные сетевые подключения к внешним IP-адресам, попытки эскалации привилегий и несанкционированное изменение критических системных файлов или реестра.

Для эффективного хранения и обработки больших объемов генерируемых журналов событий виртуальной инфраструктуры перспективным является использование нереляционных систем управления базами данных. Как отмечено в исследовании [6], реляционные модели хранения зачастую не справляются с разнообразием и скоростью поступления данных о компьютерных атаках. Предлагаемая авторами модель представления данных в нереляционном формате, в частности с использованием документо-ориентированного подхода, позволяет гибко структурировать разнородные события из журналов виртуальных машин и гипервизоров, обеспечивая высокую скорость выполнения аналитических запросов. Интеграция подобной модели в подсистему сбора и обработки журналов событий позволяет преодолеть ограничения традиционных реляционных хранилищ при работе с полу- и неструктурированными данными. Это особенно актуально для задач корреляционного анализа и выявления сложных многоэтапных атак, требующих объединения событий из различных источников, таких как журналы гостевых операционных систем, гипервизоров и систем управления. Использование нереляционного подхода способствует повышению масштабируемости и производительности системы анализа безопасности в целом.

Дальнейшее развитие методики анализа журналов событий виртуальной инфраструктуры требует применения современных методов обработки больших данных и машинного обучения. Объемы генерируемых журналов событий и сложность взаимосвязей между событиями делают традиционные методы анализа недостаточно эффективными. Для решения этой проблемы предлагается использовать процедуры кластеризации для группировки схожих событий, методы классификации для определения типа инцидента и алгоритмы поиска аномалий для выявления ранее неизвестных угроз. Особое внимание следует уделять корреляции событий из разных источников, поскольку именно комплексный анализ позволяет выявить сложные многоэтапные атаки, которые остаются незамеченными при изолированном рассмотрении журналов событий отдельных компонентов инфраструктуры.

Перспективным направлением в области анализа журналов событий является разработка специализированного программного обеспечения. В исследовании [7] предложена архитектура интегрированного Java-приложения для анализа журналов с целью обнаружения компьютерных атак. Авторы описывают модульную систему, способную реагировать на различные аномалии безопасности за счет использования гибких правил корреляции и алгоритмов машинного обучения. Ключевыми особенностями предложенной архитектуры являются масштабируемость, поддержка разнородных источников данных и возможность интеграции с внешними системами. Использование подобного подхода при реализации аналитического модуля для виртуальной инфраструктуры позволяет создать универсальное решение, способное адаптироваться к изменяющимся условиям и новым типам кибератак.

Кроме анализа на уровне виртуальных машин чрезвычайно важен мониторинг на уровне гипервизора, где индикаторами угроз служат неавторизованные попытки доступа к консоли управления, изменения конфигурации виртуальных машин, неожиданные операции создания снимков или перемещения виртуальных машин, подозрительная активность учетных записей с повышенными привилегиями, а также аномальная нагрузка на физические ресурсы хоста, не связанная с легитимной рабочей нагрузкой. Классификация основных индикаторов компрометации представлена в таблице 2.

Таблица 2. Классификация индикаторов компрометации

Уровень	Тип индикатора	Критичность	Методы обнаружения
Виртуальные машины	Неудачные попытки входа	Средняя	Статистический анализ
	Запуск подозрительных процессов	Высокая	Сигнатурный анализ, поведенческий анализ
	Аномальные сетевые подключения	Средняя	Анализ сетевого трафика
Гипервизор	Неавторизованный доступ	Критическая	Аудит событий доступа
	Изменение конфигурации виртуальных машин	Высокая	Мониторинг изменений

Логическим завершением анализа является ключевой этап методики – корреляция событий и определение типа атаки на основе выявленных индикаторов. Например, атака полным перебором идентифицируется через корреляцию множественных событий неудачного входа на нескольких виртуальных машинах с одного IP-адреса. Распространение вредоносного программного обеспечения определяется путем выявления виртуальной машины, с которой инициируются однотипные аномальные сетевые подключения к другим машинам в сети, с последующей активацией подозрительных процессов на целевых машинах. Атака на гипервизор обнаруживается через сочетание активности на уровне виртуальной машины, указывающей на попытку выхода из изолированной среды, и аномальных событий на уровне гипервизора. Межвиртуальная атака выявляется через обнаружение сетевого сканирования или атак между виртуальными машинами, расположенными на одном физическом хосте. Несанкционированное перемещение виртуальной машины фиксируется через события миграции в журналах vCenter, запрещенные политиками безопасности.

Таким образом, именно на этом этапе данные, собранные и обработанные с помощью инструментов наподобие Elasticsearch и нереляционных систем, а также индикаторы, выявленные на разных уровнях инфраструктуры, объединяются в единую картину. Это позволяет перейти от разрозненных сигналов к точной идентификации сложных многоэтапных кибератак, что было бы невозможно без предшествующих этапов сбора, нормализации и классификации данных.

Практическая апробация и оценка эффективности методики

Для проверки эффективности предложенной методики была разработана и развернута опытная система анализа журналов событий виртуальной инфраструктуры, которая включала модули сбора данных с гипервизоров VMware ESXi и виртуальных машин под управлением Windows и Linux, подсистему нормализации и обогащения событий, базу данных для хранения журналов событий и аналитический модуль для выявления аномалий. В ходе тестирования система обрабатывала более 100 тыс. событий в час, демонстрируя устойчивую производительность при высоких нагрузках. Для оценки качества обнаружения атак были смоделированы различные сценарии компрометации виртуальной инфраструктуры, включая атаки на гипервизор, горизонтальное перемещение между виртуальными машинами и кражу конфиденциальных данных.

Важным аспектом создания тестовых сред для валидации решений в области безопасности является применение специализированных подходов к построению виртуальных лабораторий. В работе [6] предложена методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем. Авторы описывают подход к построению изолированных сред, которые позволяют моделировать сложные сценарии атак без риска для производственной инфраструктуры. Предложенная методология включает этапы проектирования архитектуры лаборатории, выделения сегментов для эмуляции различных компонентов информационной системы и настройки инструментов мониторинга. Использование подобного подхода при создании испытательного стенда для валидации методики анализа журналов событий виртуальной инфраструктуры позволяет обеспечить репрезентативность тестовых данных и полноту покрытия проверяемых сценариев кибератак.

При построении тестовых сред большое значение имеет разработка специализированных сценариев безопасности. В исследовании рассматривается подход к созданию уязвимых виртуальных машин и разработке сценариев для тестирования на проникновение и предлагается методика формирования реалистичных конфигураций виртуальных машин, содержащих известные уязвимости, что позволяет более точно моделировать действия злоумышленников и оценивать эффективность систем обнаружения атак. Применение подобных сценариев безопасности при тестировании методики анализа журналов событий позволяет воспроизводить сложные многоэтапные атаки, включающие сканирование сети, эксплуатацию уязвимостей, горизонтальное перемещение и эскалацию привилегий, что обеспечивает более качественную проверку корреляционных правил и алгоритмов машинного обучения для выявления кибератак в виртуальной среде.

Для количественной оценки эффективности предложенной методики использовались следующие метрики:

– полнота обнаружения атак (Recall):

$$R = \frac{TP}{(TP + FN)} \cdot 100\ \%,$$

DOI: 10.31854/3034-2201-2026-4-1-C06
URL: https://vestnik-sut.ru/2026-1/C06.pdf

где TP (True Positive) – количество корректно обнаруженных атак; FN (False Negative) – количество пропущенных атак;

– снижение ложных срабатываний:

$$FPR_{reduction} = \frac{(FPR_{old} - FPR_{new})}{FPR_{old}} \cdot 100\ \%,$$

где FPR_{old} – процент ложных срабатываний в традиционной системе; FPR_{new} – процент ложных срабатываний в предложенной системе;

– увеличение полноты обнаружения:

$$Improvement = \frac{(R_{new} - R_{old})}{R_{old}} \cdot 100\ \%,$$

где R_{old} – полнота обнаружения традиционными методами; R_{new} – полнота обнаружения предложенной методикой.

Результаты апробации

Апробация предложенной методики на разработанной испытательной платформе показала, что она позволяет значительно повысить эффективность обнаружения кибератак в виртуальной среде. По сравнению с традиционными подходами, основанными на анализе журналов событий отдельных компонентов инфраструктуры, комплексный анализ событий со всех уровней виртуализации позволил увеличить полноту обнаружения атак на 40 %, снизив при этом количество ложных срабатываний на 25 %. Эффект выразился в выявлении многоэтапных сценариев, например таких, как горизонтальное перемещение злоумышленника, которые ранее оставались незамеченными из-за отсутствия корреляции между событиями на разных уровнях виртуальной инфраструктуры. Эти результаты подтверждают перспективность предложенного подхода и целесообразность его внедрения в организациях, использующих технологии виртуализации.

Таким образом, применение комплексной методики, объединяющей сбор и корреляционный анализ журналов событий со всех уровней виртуальной инфраструктуры с использованием современных методов обработки данных, показало свою высокую практическую эффективность по сравнению с традиционными подходами к безопасности.

Заключение

Завершающим этапом разработанной методики является логический анализ и формирование отчетности, направленные на восстановление цепочки атаки и наглядное представление последовательности событий. Формируется комплексный отчет с указанием типа атаки, затронутых ресурсов, временны́х меток событий и конкретных рекомендаций по блокировке и устранению последствий компрометации. Интеграция данной методики анализа в общую комплексную систему защиты информации позволяет перейти от пассивной защиты к активному противодействию, значительно повышая устойчивость информационной системы организации к современным киберугрозам. Экспериментальная проверка на тестовом стенде показала снижение времени обнаружения инцидентов на 65 % по сравнению с традиционными подходами. Предложенный в статье комплексный подход, объединяющий методику построения комплексной системы защиты информации по стандартам СПбГУТ и специализированную методику анализа журналов событий виртуальной инфраструктуры, представляет собой эффективный инструмент обеспечения информационной безопасности. Превентивные меры создают базовый уровень защиты, в то время как глубокий анализ журналов событий виртуальных машин и гипервизоров обеспечивает возможность эффективного обнаружения и классификации сложных атак, которые обходят традиционные средства защиты.

Дальнейшие исследования в данной области видятся в следующих направлениях: углубленная автоматизация процессов анализа с использованием методов глубокого обучения для прогнозирования угроз; разработка адаптивных систем, способных динамически настраивать правила обнаружения в реальном времени; интеграция с платформами автоматизации и оркестровки процессов безопасности для организации автоматического реагирования на инциденты; расширение методики для работы в гибридных и мультиоблачных средах с учетом их специфики; создание предиктивных моделей для проактивного выявления уязвимостей и векторов атак на основе анализа накопленных данных.

Литература

1. Сахаров Д. В., Красов А. В., Ушаков И. А., Орлов Г. А. Защищенная модель программно-определяемой сети в среде виртуализации KVM // Электросвязь. 2020. № 3. С. 26–32. DOI: 10.34832/ELSV.2020.4.3.004. EDN: IRRVAB

2. Савинов Н. В., Токарева К. А., Ушаков И. А., Красов А. В., Сахаров Д. В. Исследование модели сети ЦОД на основе политик CISCO ACI // Защита информации. Инсайд. 2019. № 4 (88). С. 32–43. EDN: NRYZLU

3. Дудников И. А., Шариков П. И., Майоров А. В. Методика анализа журналов событий информационных систем с использованием Elasticsearch для обнаружения сигналов о вредоносных действиях в информационной // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 1. С. 120–134. DOI: 10.61260/2218-130X-2025-1-120-134. EDN: ZQCEXG

4. Майоров А. В., Красов А. В., Ушаков И. А. Модель представления Больших данных о компьютерных атаках в формате NoSQL // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 2. С. 47–54. DOI: 10.46418/2079-8199_2023_2_9. EDN: GDZKWM

5. Шариков П. И., Красов А. В., Майоров А. В. Архитектура интегрированного java-приложения для анализа журналов с целью обнаружения компьютерных атак в информационных системах посредством реагирования на различные аномалии безопасности // Вестник Дагестанского государственного технического университета. Технические науки. 2025. Т. 52. № 1. С. 147–161. DOI: 10.21822/2073-6185-2025-52-1-147-161. EDN: AWEHRP

6. Красов А. В., Штеренберг С. И., Москальчук А. И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. № 3 (88). С. 38–46. DOI: 10.30987/1999-8775-2020-3-38-46. EDN: RCTZGR.

7. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 47–58. DOI: 10.31854/2307-1303-2021-9-1-47-58. EDN: ICWXFE.

Материалы статьи были представлены на VI Всероссийской научно-технической и научно-методической конференции магистрантов, аспирантов и их руководителей «Перспективные телекоммуникационные технологии и развитие цифровых кластеров в России и мире (ПКМ 2025)».

Статья поступила 17 декабря 2025 г.
Одобрена после рецензирования 28 января 2026 г.
Принята к публикации 5 мая 2026 г.

Информация об авторах

Бютнер Серафим Игоревич – студент 1-го курса магистратуры (группа МИБ-2512) Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. Email: butner.si@sut.ru

Жилов Константин Романович – студент 1-го курса магистратуры (группа МИБ-2512) Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. Email: zhilov.kr@sut.ru

Сахаров Дмитрий Владимирович – кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. Email: zss_ibks@sut.ru

A Methodology for Comprehensive Information Protection and Virtual Infrastructure Event Log Analysis for Attack Identification

S. Butner ✉, K. Zhilov, D. Sakharov

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Objective. *To develop a comprehensive methodology that integrates the construction of a comprehensive information security system according to the approach implemented at the Saint Petersburg State University of Telecommunications with a specialized method for retrospective and operational analysis of virtual infrastructure event logs to accurately identify and classify types of cyberattacks.* ***Methods.*** *The study employed systems analysis and risk management methods in designing the comprehensive information security system. For event log analysis, methods of event correlation analysis, machine learning (clustering, classification, anomaly detection), and methods for processing large volumes of data were used. Practical validation was conducted through the deployment of an experimental system using the Elastic Stack technology suite (Elasticsearch, Beats) and attack simulation in a virtual laboratory.* ***Novelty.*** *A comprehensive approach is proposed that integrates preventive protection within the comprehensive information security system framework and deep analysis of event logs from all levels of the virtual infrastructure (virtual machines, hypervisors, management systems). A methodology has been developed that involves using non-relational models for event log storage, specialized Elasticsearch queries for anomaly detection, and testing scenarios based on vulnerable virtual machines for validation.* ***Results.*** *Practical implementation demonstrated a 40 % increase in attack detection completeness and a 25 % reduction in false positives compared to traditional approaches. Incident detection time was reduced by 65 %. A particularly significant effect was achieved in detecting complex multi-stage attacks through comprehensive event correlation.* ***Practical significance.*** *The developed methodology enables organizations using virtual infrastructures to significantly enhance their resilience to modern cyber threats. The implementation of the proposed approach minimizes incident risks, reduces incident detection and elimination time, and provides a tool for proactive threat prediction. The results can be used in building corporate comprehensive information security systems and security monitoring systems.*

Key words: *comprehensive information security system, virtualization, hypervisor, event logs, log analysis, cyberattack, information security, machine learning, security information and event management system*

Information about Author

Butner Serafim – 1st Year Master's Student (The Bonch-Bruevich Saint Petersburg State University of Telecommunications). E-mail: butner.si@sut.ru

Zhilov Konstantin – 1st Year Master's Student (The Bonch-Bruevich Saint Petersburg State University of Telecommunications). Email: zhilov.kr@sut.ru

Sakharov Dmitry – Ph. D. of Technical Sciences, Associate Professor, Associate Professor of the Department of Secure Communication Systems (The Bonch-Bruevich Saint Petersburg State University of Telecommunications). Email: zss_ibks@sut.ru