**Ссылка для цитирования этой статьи:**

Солодовников Д.В., Соколов А.К., Шорохов К.Д., Кучук М.И. Компьютерная безопасность в облачных информационных системах: риски и способы их минимизации // Human Progress. 2024. Том 10, Вып. 5. URL: http://progress-human.com/images/2024/Tom10_5/Solodovnikov.pdf DOI 10.46320/2073-4506-2024-5a-3.

# Информационные системы и технологии для мониторинга и управления компьютерной безопасностью в реальном времени

**Солодовников Дмитрий Викторович**
студент Дальневосточного федерального университета
г. Владивосток, Российская Федерация

**Соколов Александр Кириллович**
студент Дальневосточного федерального университета
г. Владивосток, Российская Федерация

**Шорохов Константин Дмитриевич**
студент Дальневосточного федерального университета
г. Владивосток, Российская Федерация

**Кучук Максим Игоревич**
студент Дальневосточного федерального университета
г. Владивосток, Российская Федерация

**Аннотация.** В статье рассматриваются современные информационные системы и технологии, применяемые для мониторинга и управления компьютерной безопасностью в реальном времени. Основное внимание уделяется системам обнаружения и предотвращения вторжений (IDS/IPS), системам управления событиями и информацией безопасности (SIEM), а также применению искусственного интеллекта и машинного обучения для улучшения процессов анализа и реагирования на инциденты. Обсуждаются основные проблемы и вызовы, с которыми сталкиваются организации в области кибербезопасности, такие как нехватка квалифицированных специалистов, сложность обработки больших объемов данных и быстрое развитие технологий. Также рассматриваются перспективные подходы и инновации, включая автоматизацию процессов безопасности, использование облачных решений и блокчейн-технологий. Статья подчеркивает важность комплексного подхода к мониторингу безопасности и необходимости повышения осведомленности сотрудников о киберугрозах.

©Солодовников Д.В., Соколов А.К.,
Шорохов К.Д., Кучук М.И.

DOI 10.46320/2073-4506-2024-5a-3

**Ключевые слова:** информационные системы, мониторинг безопасности, компьютерная безопасность, системы обнаружения вторжений, системы управления событиями, искусственный интеллект, машинное обучение, автоматизация безопасности, облачные решения, блокчейн.

**Введение**

Информационные системы для мониторинга безопасности представляют собой сложные структуры, объединяющие технологии, методы и процессы, направленные на защиту данных и систем от потенциальных угроз. Основные компоненты таких систем включают системы обнаружения и предотвращения вторжений (IDS/IPS), системы управления событиями и информацией о безопасности (SIEM), а также различные инструменты для анализа и обработки данных. В условиях растущих киберугроз и усложнения атак важность применения информационных технологий для обеспечения безопасности становится неоспоримой.

**Основная часть**

Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) являются основными элементами мониторинга безопасности. IDS анализирует сетевой трафик и выявляет подозрительную активность, информируя администраторов о возможных атаках. Согласно исследованию Gartner, внедрение IDS в организациях позволяет сократить время реагирования на инциденты в среднем на 30%. В свою очередь, IPS не только обнаруживает, но и автоматически блокирует вредоносные действия. Например, организация, внедрившая IPS, смогла сократить количество инцидентов кибербезопасности на 40% за первый год.

Системы управления событиями и информацией о безопасности (SIEM) собирают, обрабатывают и анализируют данные из различных источников, таких как журналы событий, сетевые устройства и системы мониторинга. SIEM позволяет интегрировать информацию о событиях и инцидентах безопасности в единую платформу, что значительно улучшает возможности анализа и обнаружения угроз. Согласно Forrester Research, компании, использующие SIEM, сообщают о сокращении времени расследования инцидентов на 50%. Это позволяет не только быстрее реагировать на угрозы, но и повышает общую безопасность системы. В частности, одна из финансовых организаций, внедрившая SIEM, отметила, что удалось выявить 70% атак, которые ранее оставались незамеченными.

Анализ больших данных и применение методов машинного обучения также играют важную роль в мониторинге безопасности. Инструменты, использующие алгоритмы машинного обучения, способны выявлять аномалии в поведении пользователей и систем, что

©Солодовников Д.В., Соколов А.К.,
Шорохов К.Д., Кучук М.И.

DOI 10.46320/2073-4506-2024-5a-3

позволяет обнаруживать ранее неизвестные угрозы. Например, система, основанная на машинном обучении, смогла обнаружить кибератаку на 60% быстрее по сравнению с традиционными методами. Это достигается за счет автоматического обучения на исторических данных и способности адаптироваться к новым угрозам.

Мониторинг безопасности в реальном времени требует применения комплексных подходов. Ключевыми аспектами являются не только технологии, но и организационные меры, такие как обучение сотрудников, разработка политик безопасности и проведение регулярных аудитов. Согласно отчету Ponemon Institute, более 50% организаций, проводящих регулярные аудиты безопасности, отмечают снижение количества инцидентов на 25%. Эффективное управление безопасностью информации также включает в себя создание инцидентных команд, которые могут оперативно реагировать на угрозы и инциденты.

Важным направлением для повышения эффективности мониторинга безопасности является интеграция различных систем и технологий. Использование единой платформы для управления событиями безопасности, обнаружения вторжений и анализа данных значительно улучшает взаимодействие между командами и позволяет оперативно реагировать на инциденты. Например, организация, внедрившая такую интеграцию, сообщила о сокращении времени на реагирование на инциденты на 40%, что свидетельствует о высокой эффективности подобного подхода.

Кроме того, применение технологий блокчейн в мониторинге безопасности открывает новые возможности для защиты данных. Блокчейн обеспечивает прозрачность и неизменность записей, что затрудняет несанкционированные изменения данных. Применение блокчейн-технологий в мониторинге безопасности позволяет создать более надежные системы учета и контроля, что повышает уровень доверия к защищаемой информации.

Современные технологии мониторинга безопасности играют ключевую роль в защите информационных систем от киберугроз. Эти технологии позволяют оперативно выявлять, анализировать и реагировать на инциденты, связанные с безопасностью, минимизируя потенциальные риски. В рамках этого направления выделяется несколько основных технологий и методов, которые активно используются в различных отраслях.

Системы обнаружения и предотвращения вторжений (IDS/IPS) являются основными компонентами мониторинга безопасности. IDS анализируют сетевой трафик и события, фиксируя подозрительную активность. Важно отметить, что современные IDS используют продвинутые алгоритмы, включая машинное обучение, для повышения точности обнаружения. Например, системы, применяющие методы анализа поведения, способны выявлять аномалии, которые могут указывать на кибератаку, и сообщать о них

©Солодовников Д.В., Соколов А.К.,
Шорохов К.Д., Кучук М.И.

DOI 10.46320/2073-4506-2024-5a-3

администраторам. Согласно отчету Gartner, более 60% организаций, внедривших IDS, отмечают значительное улучшение в выявлении вторжений, что снижает вероятность утечек данных.

IPS, в отличие от IDS, не только обнаруживают, но и блокируют подозрительную активность в реальном времени. Использование IPS позволяет предотвратить атаки до того, как они смогут нанести ущерб системе. Организации, использующие IPS, как правило, сообщают о сокращении инцидентов безопасности на 40% в течение первого года после внедрения. Например, в одной из крупных финансовых организаций внедрение IPS привело к снижению случаев мошенничества на 50%.

Системы управления событиями и информацией о безопасности (SIEM) играют важную роль в интеграции данных о событиях безопасности из различных источников. SIEM собирает, обрабатывает и анализирует данные, позволяя организациям получать полную картину событий безопасности в режиме реального времени. Применение SIEM позволяет выявлять сложные атаки, которые могут быть пропущены отдельными системами. Согласно исследованию Forrester Research, компании, использующие SIEM, сокращают время реагирования на инциденты в среднем на 50%. Например, одна крупная медицинская организация, внедрившая SIEM, смогла сократить время реагирования на инциденты с 48 до 12 часов.

Анализ больших данных и применение технологий машинного обучения являются важными аспектами современных систем мониторинга безопасности. Алгоритмы машинного обучения могут анализировать большие объемы данных, выявляя закономерности и аномалии. Это позволяет организациям не только реагировать на известные угрозы, но и выявлять новые, ранее неизвестные уязвимости. Например, система на основе машинного обучения смогла обнаружить кибератаку на 70% быстрее, чем традиционные методы. Это позволяет не только предотвратить ущерб, но и снизить затраты на реагирование на инциденты.

Также стоит упомянуть о роли облачных технологий в мониторинге безопасности. Облачные решения предоставляют гибкость и масштабируемость, позволяя организациям быстро адаптироваться к изменяющимся условиям. Современные облачные платформы предлагают встроенные средства безопасности, включая мониторинг и управление доступом, что облегчает соблюдение стандартов безопасности. По данным McKinsey, более 80% компаний, использующих облачные технологии, сообщают о повышении уровня безопасности благодаря встроенным решениям.

Технологии блокчейн также начинают находить применение в мониторинге безопасности. Блокчейн обеспечивает надежную и прозрачную систему учета, что затрудняет

©Солодовников Д.В., Соколов А.К.,
Шорохов К.Д., Кучук М.И.

DOI 10.46320/2073-4506-2024-5a-3

несанкционированные изменения данных. Внедрение блокчейн-технологий позволяет создавать децентрализованные решения для защиты информации, что усиливает уровень доверия к защищаемым данным. Например, некоторые компании начали использовать блокчейн для обеспечения безопасности транзакций и контроля доступа к чувствительным данным.

Проблемы и вызовы в сфере мониторинга безопасности остаются актуальными для организаций любого размера и отрасли. Несмотря на развитие технологий и внедрение современных решений, множество факторов продолжают угрожать эффективности мониторинга и управления кибербезопасностью.

Одной из основных проблем является сложность и объём данных, которые необходимо обрабатывать. Современные системы генерируют огромные объёмы информации, что затрудняет её анализ и может привести к перегрузке специалистов по безопасности. Например, исследования показывают, что 70% событий, зафиксированных системами мониторинга, являются ложными срабатываниями, что приводит к значительным затратам времени и ресурсов на их анализ. Это затрудняет выявление реальных угроз и может снизить общий уровень безопасности.

Другим важным вызовом является недостаток квалифицированных специалистов в области кибербезопасности. На фоне растущего числа кибератак многие организации сталкиваются с нехваткой кадров, способных эффективно управлять системами мониторинга и реагирования на инциденты. По данным Cybersecurity Workforce Study, глобальная нехватка специалистов в области кибербезопасности составляет более 3,1 миллиона человек. Это приводит к увеличению нагрузки на существующих сотрудников и снижению качества мониторинга.

Кроме того, быстрое развитие технологий и изменение методов атак создают постоянные вызовы для мониторинга безопасности. Киберпреступники используют все более сложные и изощренные методы, что требует от организаций постоянного обновления и адаптации своих систем безопасности. Например, атаки на основе искусственного интеллекта становятся все более распространенными, что делает традиционные методы обнаружения угроз менее эффективными. Это ставит перед организациями задачу не только внедрения новых технологий, но и постоянного обучения сотрудников.

Безопасность облачных технологий также вызывает обеспокоенность. Переход организаций на облачные решения создает новые уязвимости и требует пересмотра подходов к мониторингу безопасности. Например, многие компании сталкиваются с проблемами управления доступом и защиты данных в облачной среде, что может привести к утечке

©Солодовников Д.В., Соколов А.К.,
Шорохов К.Д., Кучук М.И.

DOI 10.46320/2073-4506-2024-5a-3

информации. Исследования показывают, что более 30% инцидентов, связанных с безопасностью в облаке, вызваны ошибками конфигурации, что подчеркивает необходимость строгого контроля и мониторинга.

**Заключение**

Взаимодействие между различными системами безопасности также представляет собой проблему. Многие организации используют несколько решений для мониторинга и управления безопасностью, что может привести к несоответствиям и трудностям в интеграции данных. Недостаточная совместимость систем затрудняет получение целостной картины событий, связанных с безопасностью, и может снижать скорость реагирования на инциденты. По данным Ponemon Institute, 65% организаций испытывают трудности с интеграцией данных из разных источников, что приводит к задержкам в реагировании на угрозы.

Наконец, недостаточная осведомленность сотрудников о киберугрозах и методах защиты также является серьезной проблемой. Человеческий фактор часто становится самой уязвимой частью системы безопасности. Исследования показывают, что более 90% инцидентов безопасности связаны с человеческой ошибкой, что подчеркивает важность обучения и повышения осведомленности сотрудников. Неэффективные процедуры обучения могут привести к тому, что сотрудники не смогут распознать фишинг-атаки или другие угрозы, что увеличивает риски для всей организации.

.

**Список литературы**

1. Мелл П., Грэнс Т. Определение облачных вычислений в NIST. Специальное издание Национального института стандартов и технологий. Гейтерсбург, Мэриленд: NIST. 2011.
2. Кучеренко, И. А. Кибербезопасность в информационных системах: современные вызовы и решения / И. А. Кучеренко. — Москва: Инфра-М, 2020. — 256 с.
3. Баранов, С. В. Безопасность информации: теория и практика / С. В. Баранов. — Санкт-Петербург: БХВ-Петербург, 2019. — 300 с.
4. Соловьев, В. А. Информационные технологии и безопасность: учебное пособие / В. А. Соловьев. — Казань: Казанский университет, 2021. — 198 с.
5. Столлингс У. Основы сетевой безопасности: приложения и стандарты. — 5-е изд. — Бостон: Пирсон, 2016. — 400 с.

©Солодовников Д.В., Соколов А.К.,
Шорохов К.Д., Кучук М.И.

DOI 10.46320/2073-4506-2024-5a-3