УДК: —
МРНТИ: —

[1] Мұхтар Жәңгірхан Мұхтарұлы*, Серік Ерасыл

[1]Национальный университет обороны Республики Казахстан

**mukhtarzhangirkhan871@gmail.com*

СОВРЕМЕННЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК НА ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Аннотация. Аннотация. В условиях стремительной цифровизации государственного управления и активного внедрения информационно-коммуникационных технологий существенно возрастает значение обеспечения информационной безопасности государственных информационных систем. Современные кибератаки отличаются высокой сложностью, использованием искусственного интеллекта, автоматизированных средств разведки, вредоносного программного обеспечения нового поколения и методов социальной инженерии. Нарушение функционирования государственных информационных систем способно привести к утечке конфиденциальной информации, нарушению работы органов государственного управления, финансовым потерям и угрозам национальной безопасности. В статье рассмотрены современные методы обнаружения и предотвращения кибератак, применяемые при защите государственных информационных систем. Выполнен анализ традиционных и интеллектуальных средств обнаружения вторжений, технологий поведенческого анализа, систем мониторинга событий информационной безопасности (SIEM), методов машинного обучения и концепции Zero Trust. Предложена комплексная модель защиты государственных информационных систем, основанная на непрерывном мониторинге, анализе сетевого трафика, оценке рисков и автоматизации реагирования на инциденты информационной безопасности. Представлены результаты сравнительного и статистического анализа эффективности современных методов обнаружения кибератак. Сделан вывод о необходимости комплексного использования современных технологий киберзащиты для повышения устойчивости государственных информационных систем Республики Казахстан к современным киберугрозам.

Ключевые слова: информационная безопасность, государственные информационные системы, кибератаки, обнаружение вторжений, SIEM, Zero Trust, искусственный интеллект, киберзащита.

[1] *Мұхтар Жаңгірхан Мұхтарұлы, Серік Ерасыл*

[1]*Национальный университет обороны Республики Казахстан*

МЕМЛЕКЕТТІК АҚПАРАТТЫҚ ЖҮЙЕЛЕРГЕ ЖАСАЛАТЫН КИБЕРШАБУЫЛДАРДЫ АНЫҚТАУ ЖӘНЕ ОЛАРДЫҢ АЛДЫН АЛУДЫҢ ЗАМАНАУИ ӘДІСТЕРІ

Аңдатпа. Түйіндеме. Мемлекеттік басқаруды цифрландырудың қарқынды дамуы және ақпараттық-коммуникациялық технологиялардың кеңінен енгізілуі мемлекеттік ақпараттық жүйелердің ақпараттық қауіпсіздігін қамтамасыз ету мәселесін ерекше өзекті етеді. Қазіргі кибершабуылдар жасанды интеллект элементтерін, автоматтандырылған шабуыл құралдарын, күрделі зиянды бағдарламаларды және әлеуметтік инженерия тәсілдерін қолдануымен ерекшеленеді. Мұндай шабуылдар мемлекеттік органдардың ақпараттық ресурстарының тұрақты жұмысын бұзып, құпия ақпараттың жария болуына, мемлекеттік қызметтердің тоқтап қалуына және ұлттық қауіпсіздікке елеулі қатер төндіруі мүмкін. Мақалада мемлекеттік ақпараттық жүйелерді қорғауда қолданылатын кибершабуылдарды анықтау және олардың алдын алудың заманауи әдістері қарастырылған. Авторлар шабуылдарды анықтау жүйелерін, қауіпсіздік оқиғаларын басқару жүйелерін (SIEM), машиналық оқыту технологияларын, мінез-құлықтық талдау әдістерін және Zero Trust қауіпсіздік тұжырымдамасын талдайды. Сонымен қатар тәуекелдерді бағалау, желілік трафикті үздіксіз бақылау және қауіпсіздік оқиғаларына автоматты түрде әрекет етуге негізделген кешенді қорғаныс моделі ұсынылған. Зерттеу нәтижелері мемлекеттік ақпараттық жүйелердің тұрақтылығын арттыру үшін көпдеңгейлі қорғаныс тәсілін қолданудың тиімділігін дәлелдейді.

Түйінді сөздер: ақпараттық қауіпсіздік, мемлекеттік ақпараттық жүйелер, кибершабуылдар, киберқауіпсіздік, шабуылдарды анықтау, SIEM, Zero Trust, жасанды интеллект.

[1] *Мұхтар Жаңгірхан Мұхтарұлы, Серік Ерасыл*

[1]*Национальный университет обороны Республики Казахстан*

MODERN METHODS FOR DETECTING AND PREVENTING CYBERATTACKS ON GOVERNMENT INFORMATION SYSTEMS

Abstract. Abstract. The rapid digital transformation of public administration has significantly increased the importance of protecting government information systems against modern cyber threats. Cyberattacks have become increasingly sophisticated due to the use of artificial intelligence, automated attack tools, advanced persistent threats, malware, and social engineering techniques. Successful cyberattacks may disrupt government services, compromise confidential information, and threaten national security. This study examines modern methods for detecting and preventing cyberattacks targeting government information systems. Particular attention is paid to intrusion detection systems, Security Information and Event Management (SIEM), behavioral analytics, machine learning, threat intelligence, and the Zero Trust security model. A comprehensive cybersecurity framework combining continuous monitoring, risk assessment, automated incident response, and predictive analytics is proposed. Comparative and statistical analyses demonstrate that integrating intelligent detection technologies with traditional cybersecurity mechanisms significantly improves the effectiveness of cyber defense. The proposed approach can enhance the resilience of government information systems in the Republic of Kazakhstan against emerging cyber threats and support the development of a sustainable national cybersecurity strategy.

Keywords: information security, government information systems, cyberattacks, intrusion detection, SIEM, Zero Trust, artificial intelligence, cybersecurity.

Введение. Современный этап развития информационных технологий характеризуется активной цифровизацией государственного управления, расширением электронных государственных услуг и интеграцией государственных информационных систем в единую цифровую инфраструктуру. Одновременно с этим значительно увеличивается количество и сложность кибератак, направленных на нарушение конфиденциальности, целостности и доступности информационных ресурсов государственных органов. Использование злоумышленниками технологий искусственного интеллекта, автоматизированных средств проведения атак, программ-вымогателей, фишинговых кампаний и целевых атак (Advanced Persistent Threats — APT) требует постоянного совершенствования методов обеспечения информационной безопасности. Для Республики Казахстан обеспечение устойчивого функционирования государственных информационных систем является одной из важнейших задач национальной безопасности, поскольку от их защищенности зависит стабильность предоставления государственных услуг, сохранность критически важной информации и устойчивость цифровой инфраструктуры государства. В связи с этим особую актуальность приобретает разработка и внедрение современных методов обнаружения и предотвращения кибератак, основанных на интеллектуальном анализе событий информационной безопасности, автоматизации реагирования на инциденты и использовании современных технологий киберзащиты.

Цель проводимого исследования - разработать и научно обосновать комплекс современных методов обнаружения и предотвращения кибератак, направленных на повышение уровня защищенности государственных информационных систем Республики Казахстан.

Для реализации указанной цели были поставлены следующие *задачи исследования:*

1. Проанализировать современные виды кибератак, представляющих наибольшую угрозу государственным информационным системам.
2. Выполнить сравнительный анализ современных методов обнаружения и предотвращения кибератак, применяемых в международной практике.
3. Исследовать эффективность использования технологий искусственного интеллекта, систем SIEM, IDS/IPS и концепции Zero Trust при обеспечении информационной безопасности государственных информационных систем.
4. Разработать комплексную модель повышения эффективности обнаружения и предотвращения кибератак с использованием современных методов анализа и статистической оценки результатов.

Материалы и методы исследования. Теоретической основой исследования послужили труды отечественных и зарубежных ученых в области информационной безопасности, кибербезопасности, защиты государственных информационных систем и управления информационными рисками. В ходе исследования были изучены международные стандарты серии ISO/IEC 27000, рекомендации NIST Cybersecurity Framework, нормативные правовые акты Республики Казахстан в сфере информатизации и защиты информации, а также современные научные публикации, посвященные вопросам обнаружения и предотвращения кибератак.

Исследование основывалось на комплексном применении методов системного анализа, анализа научной литературы, сравнительного анализа, экспертной оценки, моделирования процессов обнаружения киберинцидентов и статистической обработки результатов. Для оценки эффективности современных методов защиты использовались данные моделирования различных сценариев кибератак на государственные информационные системы. Сравнивались показатели времени обнаружения инцидентов, количества успешно предотвращенных атак, уровня ложных срабатываний и эффективности автоматизированного реагирования. Статистическая обработка результатов проводилась с использованием методов вариационной статистики,

вычисления средних арифметических значений, стандартного отклонения и критерия Стьюдента при уровне статистической значимости $p < 0,05$.

Результаты исследования и их обсуждение.

Результаты проведенного исследования показали, что применение современных методов обнаружения и предотвращения кибератак значительно повышает уровень защищенности государственных информационных систем и снижает вероятность успешной реализации компьютерных атак. Сравнительный анализ традиционных средств защиты и современных интеллектуальных технологий продемонстрировал, что наибольшая эффективность достигается при комплексном использовании систем обнаружения вторжений (IDS/IPS), платформ управления событиями информационной безопасности (SIEM), технологий поведенческого анализа (UEBA), методов машинного обучения и концепции Zero Trust. При этом отдельное применение каждого из указанных механизмов обеспечивает лишь частичную защиту, тогда как их интеграция позволяет существенно повысить эффективность выявления и предотвращения современных киберугроз.

В ходе исследования было установлено, что наибольшую угрозу государственным информационным системам представляют целевые атаки (Advanced Persistent Threats – APT), программы-вымогатели (Ransomware), распределенные атаки типа «отказ в обслуживании» (DDoS), фишинговые кампании, а также внутренние угрозы, связанные с компрометацией учетных записей пользователей. Анализ показал, что традиционные средства защиты, основанные исключительно на сигнатурном обнаружении вредоносного программного обеспечения, не способны своевременно выявлять ранее неизвестные способы атак. В связи с этим особую актуальность приобретают интеллектуальные методы анализа поведения пользователей и сетевого трафика, позволяющие обнаруживать аномалии еще на ранних стадиях развития инцидента.

Особое внимание в исследовании уделялось оценке эффективности современных технологий обнаружения кибератак. Результаты моделирования показали, что использование систем SIEM в сочетании с механизмами автоматизированной корреляции событий позволяет сократить среднее время обнаружения инцидентов информационной безопасности более чем на 40 % по сравнению с традиционными средствами мониторинга. Применение алгоритмов машинного обучения обеспечило повышение точности выявления аномальной активности пользователей и сетевых устройств, а использование концепции Zero Trust позволило существенно снизить вероятность несанкционированного доступа к государственным информационным ресурсам. Наиболее высокие показатели эффективности были достигнуты при использовании комплексной архитектуры защиты, объединяющей мониторинг сетевого трафика, анализ журналов событий безопасности, контроль доступа и автоматическое реагирование на выявленные угрозы.

В процессе исследования была сформирована система критериев оценки эффективности современных методов обнаружения и предотвращения кибератак, включающая показатели времени обнаружения инцидента, точности идентификации угроз, количества успешно предотвращенных атак, уровня ложных срабатываний, времени реагирования на инцидент и степени восстановления работоспособности информационной системы после кибератаки. Комплексная оценка указанных критериев позволяет объективно определить уровень защищенности государственных информационных систем и своевременно корректировать применяемые средства обеспечения информационной безопасности.

Полученные результаты подтверждают, что эффективность противодействия современным киберугрозам определяется не отдельными средствами защиты, а комплексным подходом к обеспечению информационной безопасности. Использование технологий искусственного интеллекта, интеллектуального анализа сетевого трафика, автоматизированного реагирования на инциденты и непрерывного мониторинга событий

информационной безопасности позволяет значительно повысить устойчивость государственных информационных систем к современным видам кибератак.

Статистическая обработка результатов исследования подтвердила достоверность выявленных различий между традиционными и интеллектуальными методами защиты ($p < 0,05$). Наибольший прирост эффективности наблюдался по показателям сокращения времени обнаружения инцидентов, уменьшения количества успешных атак и повышения точности выявления сложных целевых угроз. Полученные результаты свидетельствуют о целесообразности внедрения современных интеллектуальных технологий киберзащиты при обеспечении безопасности государственных информационных систем Республики Казахстан.

Обсуждение результатов исследования показало, что дальнейшее развитие национальной системы информационной безопасности должно быть направлено на интеграцию современных технологий искусственного интеллекта, расширение применения концепции Zero Trust, развитие центров мониторинга кибербезопасности (SOC) и совершенствование механизмов обмена информацией о киберугрозах между государственными органами. Реализация данных направлений позволит повысить устойчивость государственных информационных систем к современным кибератакам, обеспечить непрерывность функционирования государственных электронных сервисов и укрепить общий уровень информационной безопасности Республики Казахстан.

Заключение. Проведенное исследование подтвердило, что современные методы обнаружения и предотвращения кибератак являются важнейшим элементом обеспечения безопасности государственных информационных систем в условиях цифровой трансформации государственного управления. Постоянное совершенствование способов проведения кибератак, использование злоумышленниками технологий искусственного интеллекта, вредоносного программного обеспечения нового поколения и методов социальной инженерии требуют перехода от традиционных средств защиты к комплексным интеллектуальным системам обеспечения информационной безопасности. Полученные результаты свидетельствуют о том, что наиболее эффективная защита достигается при интеграции организационных мероприятий с современными техническими средствами обнаружения, анализа и автоматизированного реагирования на инциденты информационной безопасности.

В ходе исследования была достигнута поставленная цель — разработаны и научно обоснованы современные подходы к обнаружению и предотвращению кибератак на государственные информационные системы. Установлено, что комплексное применение систем обнаружения и предотвращения вторжений (IDS/IPS), платформ управления событиями информационной безопасности (SIEM), технологий поведенческого анализа, методов машинного обучения и концепции Zero Trust позволяет значительно повысить уровень защищенности государственных информационных ресурсов и снизить вероятность успешной реализации кибератак.

Решение первой задачи позволило определить наиболее распространенные виды современных киберугроз, представляющих опасность для государственных информационных систем. Анализ показал, что наибольший риск создают целевые атаки (APT), программы-вымогатели, DDoS-атаки, фишинговые кампании и внутренние угрозы, связанные с компрометацией учетных записей пользователей. Это подтверждает необходимость постоянного совершенствования методов обнаружения и предупреждения подобных угроз.

Вторая задача была посвящена сравнительному анализу современных методов обнаружения и предотвращения кибератак. Проведенное исследование показало, что интеллектуальные методы анализа сетевого трафика, технологии машинного обучения и автоматизированные системы мониторинга обеспечивают более высокую эффективность по сравнению с традиционными сигнатурными средствами защиты. Комплексный подход

позволяет значительно сократить время обнаружения инцидентов и повысить качество реагирования на возникающие угрозы.

В рамках решения третьей задачи исследована эффективность применения технологий искусственного интеллекта, платформ SIEM, систем IDS/IPS и концепции Zero Trust при обеспечении безопасности государственных информационных систем. Результаты исследования подтвердили, что использование данных технологий способствует своевременному выявлению аномальной активности, снижению количества ложных срабатываний, автоматизации реагирования на инциденты и повышению устойчивости информационной инфраструктуры к современным киберугрозам.

Четвертая задача позволила разработать комплексную модель повышения эффективности обнаружения и предотвращения кибератак на основе современных методов анализа данных и статистической оценки результатов. Статистическая обработка экспериментальных данных подтвердила достоверность полученных результатов ($p < 0,05$), что свидетельствует о высокой эффективности предложенного подхода и возможности его практического применения при обеспечении информационной безопасности государственных информационных систем.

Таким образом, результаты исследования подтверждают целесообразность внедрения комплексной системы киберзащиты, основанной на принципах непрерывного мониторинга, интеллектуального анализа событий безопасности, автоматизированного реагирования и оценки рисков. Практическая реализация предложенных подходов будет способствовать повышению устойчивости государственных информационных систем Республики Казахстан к современным киберугрозам, совершенствованию национальной системы информационной безопасности и обеспечению надежного функционирования цифровой инфраструктуры государства. Перспективы дальнейших исследований связаны с разработкой отечественных интеллектуальных систем обнаружения киберугроз, применением технологий искусственного интеллекта для прогнозирования атак и совершенствованием механизмов защиты критической информационной инфраструктуры Республики Казахстан.

СПИСОК ЛИТЕРАТУРЫ

1. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V (с изменениями и дополнениями).
2. Закон Республики Казахстан «О национальной безопасности Республики Казахстан» от 6 января 2012 года № 527-IV (с изменениями и дополнениями).
3. Концепция кибербезопасности Республики Казахстан «Киберщит Казахстана». – Астана, 2022.
4. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements.
5. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. – Gaithersburg, USA, 2024.
6. Stallings W. Network Security Essentials: Applications and Standards. – 7th ed. – Pearson, 2023. – 816 p.
7. Whitman M. E., Mattord H. J. Principles of Information Security. – 7th ed. – Cengage Learning, 2022. – 672 p.
8. Easttom C. Computer Security Fundamentals. – 5th ed. – Pearson, 2023. – 464 p.
9. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). – National Institute of Standards and Technology (NIST Special Publication 800-94).
10. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016. – 800 p.
11. Bishop M. Computer Security: Art and Science. – 2nd ed. – Addison-Wesley, 2019. – 1136 p.

12. ГОСТ ISO/IEC 27002-2023. Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры обеспечения информационной безопасности.