УДК: —
МРНТИ: —

[1] Биржан Иссахан*

[1]Академии государственного управления при Президенте Республики Казахстан

**dimash_tulkibai@mail.ru*

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ МЕСТНЫХ ИСПОЛНИТЕЛЬНЫХ ОРГАНОВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В статье рассматриваются современные подходы к обеспечению информационной безопасности деятельности местных исполнительных органов в условиях цифровой трансформации государственного управления. Автором проведен анализ ключевых угроз, возникающих при внедрении цифровых технологий, включая кибератаки, утечки персональных данных и уязвимости инфраструктуры. Особое внимание уделено организационным, правовым и техническим аспектам защиты информации. Предложены практические меры по повышению устойчивости информационных систем, включая централизацию управления безопасностью, внедрение современных технологий защиты и повышение цифровой грамотности персонала.

Ключевые слова: информационная безопасность, цифровизация, местные исполнительные органы, киберугрозы, защита информации, государственное управление.

[1] Биржан Иссахан

[1]Академии государственного управления при Президенте Республики Казахстан

ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДА ЖЕРГІЛІКТІ АТҚАРУ ОРГАНДАРЫНЫҢ ҚЫЗМЕТІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ

Аңдатпа. Бұл мақалада мемлекеттік басқарудың цифрлық трансформациясы жағдайында жергілікті атқарушы органдардың ақпараттық қауіпсіздігін қамтамасыз етудің заманауи тәсілдері қарастырылған. Автор цифрлық технологияларды енгізуден туындайтын негізгі қауіптерді, соның ішінде кибершабуылдарды, жеке деректердің ағып кетуін және инфрақұрылымдық осалдықтарды талдайды. Ақпараттық қауіпсіздікті қамтамасыз етудің ұйымдастырушылық, құқықтық және техникалық аспектілеріне ерекше назар аударылады. Ақпараттық жүйелердің тұрақтылығын арттыру, оның ішінде қауіпсіздікті басқаруды орталықтандыру, қауіпсіздіктің заманауи технологияларын енгізу, персоналдың цифрлық сауаттылығын арттыру бойынша практикалық шаралар ұсынылады.

Түйінді сөздер: Ақпараттық қауіпсіздік, цифрландыру, жергілікті атқарушы органдар, киберқауіптер, ақпаратты қорғау, мемлекеттік басқару.

[1] Биржан Иссахан

[1]Академии государственного управления при Президенте Республики Казахстан

ENSURING INFORMATION SECURITY OF THE ACTIVITIES OF LOCAL EXECUTIVE BODIES IN THE CONTEXT OF DIGITALIZATION

Abstract. This article examines modern approaches to ensuring information security for local executive bodies in the context of the digital transformation of public administration. The author analyzes the key threats arising from the implementation of digital technologies, including cyberattacks, personal data leaks, and infrastructure vulnerabilities. Particular attention is paid to the organizational, legal, and technical aspects of information security. Practical measures are proposed to improve the resilience of information systems, including centralizing security management, implementing modern security technologies, and improving the digital literacy of personnel.

Keywords: information security, digitalization, local executive bodies, cyber threats, information protection, public administration.

УДК 35.077

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ МЕСТНЫХ ИСПОЛНИТЕЛЬНЫХ ОРГАНОВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Биржан Иссахан, магистрант Академии государственного управления при Президенте Республики Казахстан, Астана, Казахстан

Аннотация

В статье рассматриваются современные подходы к обеспечению информационной безопасности деятельности местных исполнительных органов в условиях цифровой трансформации государственного управления. Автором проведен анализ ключевых угроз, возникающих при внедрении цифровых технологий, включая кибератаки, утечки персональных данных и уязвимости инфраструктуры. Особое внимание уделено организационным, правовым и техническим аспектам защиты информации. Предложены практические меры по повышению устойчивости информационных систем, включая централизацию управления безопасностью, внедрение современных технологий защиты и повышение цифровой грамотности персонала.

Ключевые слова: *информационная безопасность, цифровизация, местные исполнительные органы, киберугрозы, защита информации, государственное управление.*

Keywords: *information security, digitalization, local executive bodies, cyber threats, information protection, public administration.*

Введение

Современный этап развития государственного управления характеризуется активной цифровизацией процессов оказания государственных услуг и межведомственного взаимодействия. Местные исполнительные органы (МИО) играют ключевую роль в реализации государственной политики на региональном уровне, обеспечивая взаимодействие с населением и бизнесом.

Внедрение информационных технологий, систем электронного документооборота, облачных сервисов и цифровых платформ способствует повышению эффективности работы органов власти. Однако данные процессы

сопровождаются ростом угроз информационной безопасности, что требует разработки комплексных подходов к защите данных и информационных систем.

Цель исследования — анализ современных угроз информационной безопасности МИО и разработка рекомендаций по совершенствованию системы защиты информации.

Методы исследования исследования использовались метод анализа научной и нормативной литературы; сравнительный анализ международного опыта; системный подход к оценке угроз информационной безопасности; обобщение практики функционирования МИО в условиях цифровизации.

Цифровизация государственного управления в Казахстане выступает ключевым фактором повышения эффективности, прозрачности и подотчетности государственных институтов. Внедрение цифровых технологий позволяет оптимизировать административные процессы, сократить бюрократические барьеры и повысить качество предоставления государственных услуг населению. Особое значение имеет развитие электронного правительства, обеспечивающего доступ граждан и бизнеса к услугам в онлайн-формате, что снижает временные и финансовые издержки. Кроме того, цифровизация способствует укреплению антикоррупционных механизмов за счет минимизации человеческого фактора и повышения открытости данных. В условиях глобальной цифровой трансформации Казахстан стремится интегрировать инновационные решения, включая большие данные, искусственный интеллект и облачные технологии, что формирует основу для устойчивого социально-экономического развития и повышения конкурентоспособности страны на международной арене.

Глава Государства в своем Послании народу Казахстан в сентябре 2025 года отметил важность цифровых технологий в жизнедеятельность страны [1]

Местные исполнительные органы Казахстана обладают рядом специфических характеристик, влияющих на уровень их информационной защищенности такими как м**ногофункциональность** — выполнение широкого спектра задач, включая предоставление государственных услуг, управление ресурсами и взаимодействие с населением, д**ецентрализация управления** — распределение функций между различными подразделениями, **Использование внешних подрядчиков** — повышает риски утечки информации.

Данные особенности требуют комплексного подхода к обеспечению информационной безопасности.

Информационная безопасность государственного органа представляет собой совокупность организационных, правовых и технических мер,

направленных на защиту информационных ресурсов, информационных систем и инфраструктуры от несанкционированного доступа, утечки, искажения, уничтожения или блокирования данных. Она обеспечивает сохранение конфиденциальности, целостности и доступности информации, используемой в процессе государственного управления.

Особое значение информационная безопасность приобретает в условиях цифровизации, поскольку государственные органы обрабатывают значительные объемы персональных данных граждан, служебной и стратегически важной информации. Надлежащий уровень защиты позволяет предотвратить киберугрозы, обеспечить устойчивость функционирования государственных систем и сохранить доверие общества к государственным институтам.

Таким образом, информационная безопасность является неотъемлемым элементом эффективного государственного управления, обеспечивая надежную защиту информационной среды и поддерживая стабильность работы органов власти.

В Казахстане вопросы информационной и кибербезопасности активно исследуются представителями юридических, технических и политологических наук А.Ғ. Дүйсенқұл, Г.Ж. Бегазова, Т.Т. Дюсебаев и др. [2]

В условиях цифровизации МИО сталкиваются со следующими угрозами:

1. Человеческий фактор, в часности это ошибки сотрудников, использование слабых паролей, фишинговые атаки являются одной из основных причин инцидентов.

2.Киберугрозы включают несанкционированный доступ, вредоносное программное обеспечение, атаки на информационные системы.

3. Уязвимости программного обеспечения чаще всего это использование устаревших систем и отсутствие регулярных обновлений повышают риски.

4. Угрозы цепочек поставок т.е. компрометация подрядчиков может привести к доступу к критически важной информации.

Также нужно отметить следующие проблемы обеспечения информационной безопасности в МИО

Анализ показал наличие следующих системных проблем:

- отсутствие единых стандартов защиты информации;
- дефицит квалифицированных специалистов;

- ограниченное финансирование;
- низкий уровень цифровой грамотности сотрудников;
- использование устаревшей инфраструктуры.

Заключение и рекомендации

Цифровизация деятельности местных исполнительных органов является необходимым этапом развития государственного управления. Однако данный процесс сопровождается ростом угроз информационной безопасности.

Эффективное противодействие данным угрозам возможно только при комплексном подходе, включающем организационные, правовые и технические меры. Особое значение имеет централизация управления безопасностью, повышение квалификации персонала и внедрение современных технологий защиты.

Реализация предложенных мер позволит повысить устойчивость МИО к киберугрозам и обеспечить надежную защиту информации.

Для решения указанных проблем автор предлагает т**ехнические и организационные меры защиты д**ля повышения уровня информационной безопасности предлагается внедрение следующих решений:

- сегментация сети и разграничение доступа;
- внедрение межсетевых экранов нового поколения (NGFW);
- использование систем предотвращения утечек данных (DLP);
- контроль привилегированных учетных записей (PAM);
- регулярное резервное копирование данных;
- проведение аудитов информационной безопасности.

Международный опыт

Анализ зарубежной практики показывает эффективность централизованных моделей управления информационной безопасностью. В ряде стран используется подход создания единых центров мониторинга (SOC), что позволяет повысить уровень защиты и снизить затраты.

Применение данной модели может быть эффективно адаптировано для МИО.

Практические рекомендации

На основе проведенного анализа предлагаются следующие меры:

1. Разработка единых стандартов информационной безопасности;
2. Создание региональных центров мониторинга;
3. Повышение квалификации сотрудников;
4. Внедрение современных средств защиты информации;

5. Усиление контроля за подрядными организациями;
6. Развитие цифровой культуры и кибергигиены.

Список использованной литературы

1. Послание Главы государства Касым-Жомарта Токаева народу Казахстана «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-kazahstan-v-epohu-iskusstvennogo-intellekta-aktualnye-zadachi-i-ih-resheniya-cherez-cifrovuyu-transformaciyu-885145
2. **Ғ. Дүйсенқұл, Г.Ж. Бегазова, Т.Т. Дюсебаев и др.** *«Правовое регулирование информационной безопасности в Республике Казахстан»*
Journal of Actual Problems of Jurisprudence (Вестник КазНУ, юридическая серия) https://bulletin-law.kaznu.kz/index.php/journal/article/view/3261
3. **L.F. Tatarinova** *«Соотношение понятий "информационная безопасность", "кибербезопасность" и "защита информации"» Journal of Actual Problems of Jurisprudence* https://bulletin-law.kaznu.kz/index.php/journal/article/view/1909
4. **Ш. Жандосова, О. Әуелбеков** *«Кибертерроризм — угроза информационной безопасности Республики Казахстан» Journal of Philosophy, Culture and Political Science (Вестник КазНУ)*
Ссылка: https://bulletin-philospolit.kaznu.kz/index.php/1-pol/article/view/655
5. Закон Республики Казахстан «Об информатизации». — Астана, 2015.
6. Закон Республики Казахстан «О персональных данных и их защите». — Астана, 2013.
7. Концепция цифровой трансформации Республики Казахстан. — Астана, 2021.
8. Петров А.В. Информационная безопасность органов государственной власти // Вопросы кибербезопасности. — 2023.
9. Исабеков Б.У. Управление информационной безопасностью в государственных органах. — Алматы, 2024.
10. Национальный отчет по кибербезопасности РК. — Астана, 2024.