МРНТИ 81.93.29
УДК 004:728 **DOI 10.70239/arsu.2026.t84.n2.10**

ТРАНСФОРМАЦИЯ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ РЕСПУБЛИКИ КАЗАХСТАН

УРАЗБАЕВ Н.А.[1*], ЖЕКСЕНБАЙ Ж.Н.[2]

[*]**Уразбаев Назар Александрович[1]** - Магистрант, Академия государственного управления при Президенте Республики Казахстан, г. Астана, Казахстан.
E-mail: nazar-urazbaev@mail.ru, https://orcid.org/ 0009-0000-6012-6295
Жексенбай Жулдыз Нургалиевна[2] – Кандидат физико-математических наук, Управляющий директор, АО «Отбасы банк», г. Астана, Казахстан.
E-mail: Zhexenbay@gmail.com, https://orcid.org/0009-0006-0034-3582

Аннотация. В статье рассматриваются вопросы трансформации сетевой инфраструктуры государственных органов Республики Казахстан в условиях цифровизации государственного управления.

Актуальность исследования обусловлена возрастающими требованиями к информационной безопасности, эффективности обработки данных, устойчивости сетевых систем и необходимости интеграции государственных информационных ресурсов в рамках единой цифровой среды.

Целью работы является разработка архитектурного решения, обеспечивающего оптимальное сочетание безопасности, управляемости и эффективности функционирования сетевой инфраструктуры государственных органов. В исследовании использованы методы сравнительного анализа, системного подхода и моделирования сетевых архитектур. Эмпирическую базу исследования составили данные, полученные в ходе анкетирования непосредственных пользователей сетевой инфраструктуры.

Проведен анализ существующей модели, основанной на физическом разделении сетей, выявлены её недостатки, включая высокие затраты, сложность администрирования и снижение производительности пользователей. Предложена архитектура, основанная на логической сегментации, использовании технологий VPN, DMZ и принципов Zero Trust.

Показано, что внедрение предложенного решения позволяет существенно снизить затраты на инфраструктуру, повысить эффективность работы пользователей и обеспечить высокий уровень защиты информации.

Научная новизна заключается в разработке интегрированной модели сетевой инфраструктуры, адаптированной к условиям государственных органов Республики Казахстан.

Ключевые слова: цифровизация, государственное управление, ЕТС ГО, VPN, DMZ, информационная безопасность, Zero Trust, логическая сегментация.

Введение

В условиях стремительного развития цифровых технологий государственные органы Республики Казахстан сталкиваются с необходимостью модернизации информационно-коммуникационной инфраструктуры. Современные требования к скорости обработки информации, безопасности данных и повышения эффективности работы сотрудников требуют внедрения новых подходов к организации сетевых решений.

В Республике Казахстан процессы цифровизации реализуются в рамках государственных программ, направленных на повышение доступности государственных услуг и эффективности государственного управления [1]. Одним из ключевых факторов успешной цифровой трансформации является обеспечение защищённого взаимодействия государственных информационных систем [2].

Традиционно в государственных органах применяется модель физического разделения сетей, при которой доступ к различным ресурсам осуществляется с использованием отдельных рабочих станций. Данный подход соответствует требованиям информационной безопасности [3], однако приводит к увеличению затрат и снижению удобства работы пользователей.

В современных условиях наблюдается рост нагрузки на сетевую инфраструктуру, обусловленный необходимостью интеграции различных информационных систем и обеспечения их защищённого взаимодействия [4]. Это требует перехода к более гибким и

эффективным архитектурным решениям.

Научная новизна заключается в разработке архитектурной модели, интегрирующей механизмы логической сегментации, VPN-доступа и хоста-бастиона в единую систему защищённого доступа к ресурсам ЕТС ГО с учётом требований нормативной базы Республики Казахстан.

Материалы и методы исследования

Исследование проводилось в три этапа: анализ существующей архитектуры; сравнительный анализ международных подходов; разработка и моделирование предлагаемого решения.

Методологической основой исследования являются методы системного анализа, сравнительного анализа и моделирования сетевых архитектур. В рамках исследования проведено сопоставление традиционных и современных подходов к организации сетевой инфраструктуры.

Анализ международного опыта показал, что в развитых странах наблюдается переход от моделей физической изоляции к архитектурам, основанным на логической сегментации и контролируемом доступе. Концепция Zero Trust предполагает отказ от доверия к сетевому периметру и внедрение принципа постоянной проверки пользователей и устройств [5, 10].

Дополнительно были рассмотрены стандарты информационной безопасности, включая ISO/IEC 27001, определяющие требования к системам управления информационной безопасностью [6, 12].

В исследовании также использованы нормативные акты Республики Казахстан: Закон «Об информатизации» [2], Закон «О персональных данных и их защите» [4], Постановление Правительства № 832 [3].

Метод моделирования позволил разработать архитектурную модель, учитывающую требования безопасности, масштабируемости и эффективности.

В целях получения эмпирических данных в рамках исследования было проведено анкетирование пользователей государственных информационных систем. Опрос был направлен на выявление основных проблем, связанных с использованием существующей сетевой инфраструктуры, включая вопросы удобства работы, производительности и доступности ресурсов.

Результаты и их обсуждение

Анализ существующей модели показал, что в государственных органах применяется архитектура, основанная на физическом разделении сетей. Основными сегментами являются сеть с доступом в Интернет и сеть доступа к Единой транспортной среде государственных органов (ЕТС ГО).

Текущая схема

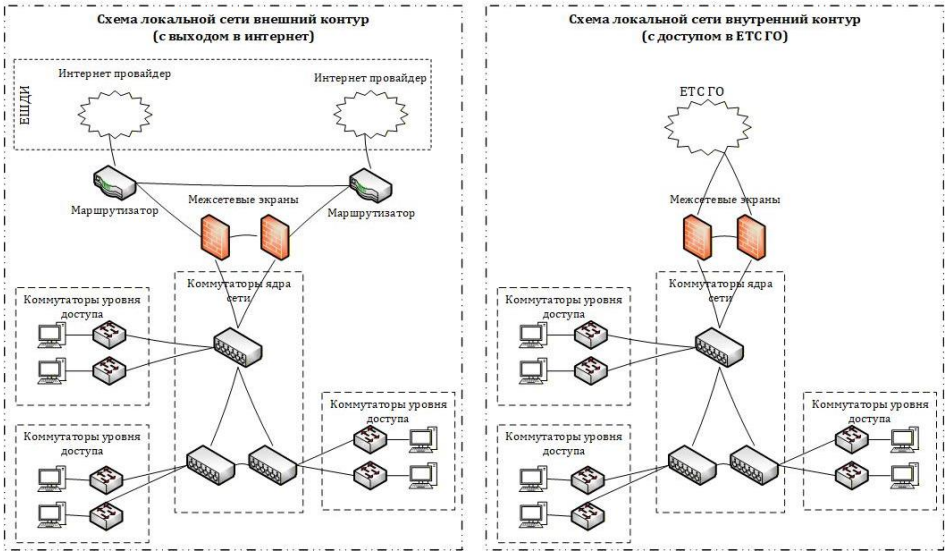

Рисунок 1. Существующая модель архитектуры сетевой инфраструктуры

Данная архитектура формировалась с учётом требований информационной безопасности, в частности положений Постановления Правительства Республики Казахстан № 832, которые ограничивают возможность подключения внутреннего контура к внешним сетям (рисунок 1).

Практическая реализация данной модели предполагает использование двух рабочих станций на одного пользователя, что обеспечивает высокий уровень безопасности, но приводит к существенным недостаткам: увеличению затрат, усложнению администрирования и снижению производительности труда [3].

Однако проведённый анализ показывает, что данный подход обладает рядом существенных недостатков:

- дублирование сетевой инфраструктуры;
- увеличение затрат на закупку и обслуживание оборудования;
- усложнение администрирования;
- снижение удобства работы пользователей;
- необходимость использования переносных носителей информации.

Таким образом, несмотря на высокий уровень защищённости, существующая модель не отвечает современным требованиям эффективности и гибкости.

В качестве альтернативы предлагается архитектура логической сегментации сети. Данная модель предусматривает использование единой рабочей станции с организацией защищённого доступа через VPN. Взаимодействие осуществляется через многоуровневую систему защиты, включающую межсетевые экраны, DMZ-зону и хост-бастион.

Применение VPN обеспечивает шифрование данных, а DMZ позволяет изолировать критические компоненты инфраструктуры [7, 25]. Предлагаемая архитектура соответствует принципам Zero Trust и международным стандартам безопасности [5, 14; 6, 18].

Результаты анкетирования пользователей показали наличие существенных проблем при использовании существующей модели сетевой инфраструктуры. Наиболее значимыми факторами являются неудобство работы с несколькими рабочими станциями, снижение производительности и ограниченность доступа к информационным ресурсам.

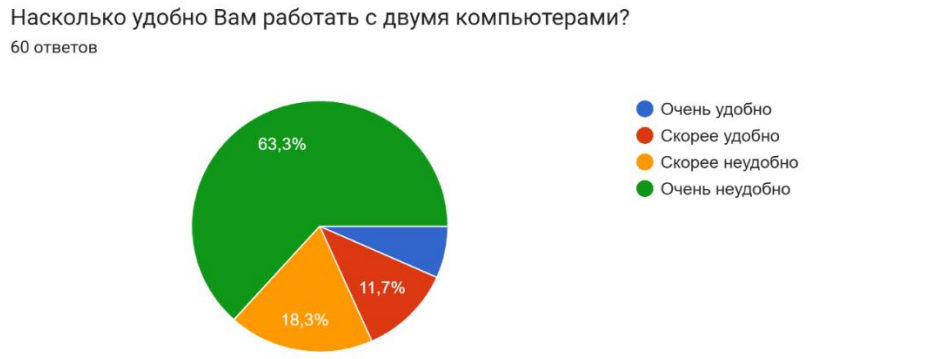

Рисунок 2. Результаты анкетирования пользователей

Большинство пользователей отмечают снижение эффективности работы, обусловленное необходимостью использования нескольких рабочих станций. Это подтверждает необходимость перехода к более гибким архитектурным решениям (рисунок 2).

Предлагаемая архитектура сетевой инфраструктуры

В целях повышения эффективности функционирования сетевой инфраструктуры предлагается переход от модели физического разделения к модели логической сегментации с использованием современных технологий защиты информации.

Предлагаемая архитектура основана на следующих принципах:

- использование единой пользовательской рабочей станции;
- организация защищённого доступа к государственным информационным системам через VPN;
- применение экранированной подсети (DMZ);
- использование хоста-бастиона в качестве контролируемой точки доступа;
- централизованное управление доступом и мониторинг.

Доступ пользователей к ресурсам ЕТС ГО осуществляется через инфраструктуру АО «Национальные информационные технологии», где реализуется многоуровневая система защиты.

Архитектура доступа включает:

1. VPN-клиент на стороне пользователя;
2. межсетевой экран;
3. DMZ-зону;
4. хост-бастион;
5. внутренний сегмент с доступом к государственным системам.

Такой подход исключает прямое подключение внутреннего контура к сети Интернет и соответствует требованиям нормативной базы.

Предлагаемая схема по подключению к ЕТС ГО

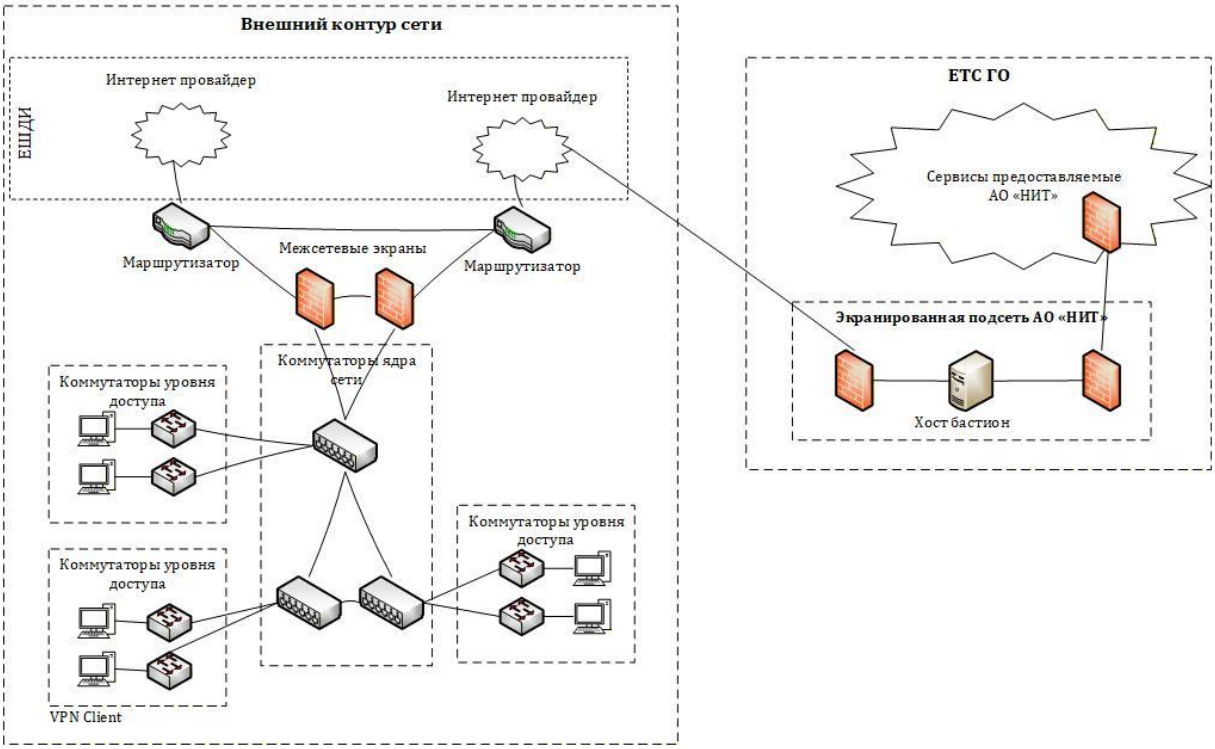

Рисунок 3. Предлагаемая архитектура сетевой инфраструктуры

Предлагаемая архитектура предусматривает многоуровневую модель взаимодействия, включающую несколько уровней защиты (рисунок 3).

На уровне пользователя осуществляется предварительная проверка состояния устройства, включая наличие антивирусного программного обеспечения и актуальных обновлений безопасности.

На уровне сетевого взаимодействия используется защищённый VPN-канал, обеспечивающий шифрование передаваемых данных.

В экранированной подсети реализуются механизмы фильтрации и контроля трафика, а также размещается хост-бастион, выполняющий функции посредника при доступе к информационным системам.

Маршрутизация между сегментами осуществляется через межсетевые экраны с применением политик безопасности.

Предлагаемая архитектура реализует современные подходы к обеспечению информационной безопасности, основанные на принципах многоуровневой защиты и концепции Zero Trust Architecture.

Основные механизмы защиты включают:

- аутентификацию и авторизацию пользователей;
- многофакторную аутентификацию;
- контроль состояния пользовательских устройств;
- фильтрацию сетевого трафика;
- мониторинг и аудит действий пользователей.

Использование хоста-бастиона позволяет исключить прямой доступ пользователей к критическим ресурсам и обеспечить полный контроль над действиями в системе.

Таким образом, безопасность обеспечивается не за счёт физической изоляции, а за счёт контролируемого доступа и постоянного мониторинга.

Несмотря на преимущества предлагаемого решения, его внедрение связано с рядом потенциальных рисков.

К основным рискам относятся:

- компрометация пользовательских устройств;
- ошибки конфигурации сетевого оборудования;
- зависимость от инфраструктуры оператора;
- необходимость адаптации нормативной базы.

Однако при использовании современных средств защиты информации, включая многофакторную аутентификацию, контроль состояния устройств и централизованное управление доступом, указанные риски могут быть минимизированы.

Оценка экономической эффективности

Одним из ключевых преимуществ предлагаемой архитектуры является снижение затрат на содержание сетевой инфраструктуры.

Проведённая оценка показывает, что внедрение решения позволяет:

- сократить количество рабочих станций на 50 %;
- исключить дублирующую сетевую инфраструктуру;
- снизить затраты на обслуживание оборудования;
- уменьшить энергопотребление.

Кроме того, сокращается необходимость модернизации устаревшего оборудования, что дополнительно снижает капитальные расходы.

Кроме прямых затрат, следует учитывать косвенные экономические эффекты, включая повышение производительности труда сотрудников, снижение времени выполнения задач и уменьшение количества простоев.

Экономическая оценка показывает, что внедрение модели позволяет сократить капитальные и эксплуатационные затраты. Оценочно экономический эффект составляет порядка 200 тыс. долларов США за счёт сокращения оборудования и до 60 тыс. долларов ежегодно за счёт снижения эксплуатационных затрат (оценочно).

Заключение

Проведённое исследование показало, что традиционная модель сетевой инфраструктуры, основанная на физическом разделении, является неэффективной в современных условиях [3].

Предложенная архитектура обеспечивает высокий уровень безопасности и эффективности за счёт логической сегментации, VPN и принципов Zero Trust [5; 6]. Внедрение решения позволяет снизить затраты, повысить удобство работы и упростить администрирование.

Практическая значимость заключается в возможности применения модели при модернизации государственных информационных систем Республики Казахстан.

Әдебиеттер тізімі

1. «Цифрлық Қазақстан» мемлекеттік бағдарламасы https://adilet.zan.kz/kaz/docs/P1700000827

2. 2015 жылғы 24 қарашадағы № 418-V ҚРЗ «Ақпараттандыру туралы» Қазақстан Республикасының Заңы. https://adilet.zan.kz/kaz/docs/Z1500000418

3. № 832 Қазақстан Республикасы Үкіметінің Қаулысы. https://adilet.zan.kz/kaz/docs/P1600000832

4. 2013 жылғы 21 мамырдағы № 94-V ҚРЗ «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының Заңы. https://adilet.zan.kz/kaz/docs/Z1300000094.

5. NIST SP 800-207 Zero Trust Architecture https://www.isms.online/nist.

6. ISO / IEC 27001:2013 Ақпараттық қауіпсіздікті басқару жүйесі https://www.iso-cert.kz.

7. Cisco Systems. Enterprise Network Architecture Guide https://www.cisco.com/site/us/en/learn/topics/networking/what-is-an-enterprise-network.html

References

1. «Sifrlyq Qazaqstan» memlekettık bağdarlamasy https://adilet.zan.kz/kaz/docs/P1700000827

2. 2015 jylğy 24 qaraşadağy № 418-V QRZ «Aqparattandyru turaly» Qazaqstan

Respublikasynyñ Zañy. https://adilet.zan.kz/kaz/docs/Z1500000418
3. № 832 Qazaqstan Respublikasy Ükımetınıñ Qaulysy. https://adilet.zan.kz/kaz/docs/P1600000832
4. 2013 jylğy 21 mamyrdağy № 94-V QRZ «Derbes derekter jäne olardy qorğau turaly» Qazaqstan Respublikasynyñ Zañy. https://adilet.zan.kz/kaz/docs/Z1300000094
5. NIST SP 800-207 Zero Trust Architecture https://www.isms.online/nist.
6. ISO / IEC 27001:2013 Aqparattyq qauıpsızdıktı basqaru jüiesı https://www.iso-cert.kz.
7. Cisco Systems. Enterprise Network Architecture Guide https://www.cisco.com/site/us/en/learn/topics/networking/what-is-an-enterprise-network.html

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ МЕМЛЕКЕТТІК ОРГАНДАРЫНЫҢ ЖЕЛІЛІК ИНФРАҚҰРЫЛЫМЫН ТРАНСФОРМАЦИЯЛАУ

УРАЗБАЕВ Н.А.[1*], ЖЕКСЕНБАЙ Ж.Н.[2]

[*]**Уразбаев Назар Александрович[1]** - Магистрант, Қазақстан Республикасы Президентінің жанындағы мемлекеттік басқару академиясы, Астана қ., Қазақстан.
E-mail: nazar-urazbaev@mail.ru, https://orcid.org/0009-0000-6012-6295
Жексенбай Жүлдыз Нұрғалиқызы[2] – Физика-математика ғылымдарының кандидаты, басқарушы директор, «Отбасыбанк» АҚ, Астана қ., Қазақстан
E-mail: Zhexenbay@gmail.com, https://orcid.org/0009-0006-0034-3582

Аңдатпа. Мақалада мемлекеттік басқаруды цифрландыру жағдайында Қазақстан Республикасы мемлекеттік органдарының желілік инфрақұрылымын трансформациялау мәселелері қарастырылды.

Зерттеудің өзектілігі ақпараттық қауіпсіздікке, деректерді өңдеудің тиімділігіне, желілік жүйелердің тұрақтылығына және бірыңғай цифрлық орта шеңберінде мемлекеттік ақпараттық ресурстарды интеграциялау қажеттілігіне қойылатын талаптардың артуына байланысты.

Жұмыстың мақсаты мемлекеттік органдардың желілік инфрақұрылымының қауіпсіздігін, басқарылуын және жұмыс істеу тиімділігін оңтайлы үйлестіруді қамтамасыз ететін архитектуралық шешімді әзірлеу болып табылады. Зерттеуде салыстырмалы талдау, жүйелік тәсіл және желілік архитектураны модельдеу әдістері қолданылды. Зерттеудің эмпирикалық базасы желілік инфрақұрылымды тікелей пайдаланушылардың сауалнамасы барысында алынған мәліметтер болды.

Желілердің физикалық бөлінуіне негізделген қолданыстағы модельге талдау жүргізілді, оның жоғары шығындары, басқарудың күрделілігі және пайдаланушылардың өнімділігінің төмендеуі сияқты кемшіліктері анықталды. Логикалық сегментацияға, vpn, DMZ технологияларын және Zero Trust принциптерін қолдануға негізделген архитектура ұсынылды.

Ұсынылған шешімді енгізу инфрақұрылым шығындарын едәуір төмендетуге, пайдаланушылардың тиімділігін арттыруға және ақпаратты қорғаудың жоғары деңгейін қамтамасыз етуге мүмкіндік беретіні көрсетілген.

Ғылыми жаңалық Қазақстан Республикасы мемлекеттік органдарының жағдайларына бейімделген желілік инфрақұрылымның интеграцияланған моделін әзірлеуден тұрады.

Түйін сөздер: цифрландыру, мемлекеттік басқару, МО БКО, VPN, DMZ, ақпараттық қауіпсіздік, Zero Trust, логикалық сегментация.

TRANSFORMATION OF THE NETWORK INFRASTRUCTURE OF THE STATE BODIES OF THE REPUBLIC OF KAZAKHSTAN

URAZBAYEV N.A.[1*], ZHEXENBAY ZH.N.[2]

[*]**Urazbayev Nazar Aleksandrovich[1]** - Master's student, Academy of public administration under the President of the Republic of Kazakhstan, Astana, Kazakhstan.
E-mail: nazar-urazbaev@mail.ru, https://orcid.org/ 0009-0000-6012-6295
Zhexenbay Zhuldyz Nurgalikyzy[2] - Candidate of mathematics and physics sciences, managing director, «Otbasybank» JSC Astana, Kazakhstan.
E-mail: Zhexenbay@gmail.com, https://orcid.org/0009-0006-0034-3582

Abstract. The article discusses the issues of transformation of the network infrastructure of the state bodies of the Republic of Kazakhstan in the context of digitalization of public administration.

The relevance of the research is due to the increasing requirements for information security, data processing efficiency, network system stability and the need to integrate government information resources within a single digital environment.

The aim of the work is to develop an architectural solution that provides an optimal combination of security, manageability and efficiency of the functioning of the network infrastructure of government agencies. The research uses methods of comparative analysis, system approach and modeling of network architectures.

An analysis of the existing model based on the physical separation of networks has been carried out, and its disadvantages have been identified, including high costs, administrative complexity, and reduced user productivity. An architecture based on logical segmentation, the use of VPN technologies, DMZ, and Zero Trust principles is proposed.

It is shown that the implementation of the proposed solution can significantly reduce infrastructure costs, increase user efficiency and ensure a high level of information protection.

The scientific novelty lies in the development of an integrated network infrastructure model adapted to the conditions of the state bodies of the Republic of Kazakhstan.

Key words: digitalization, public administration, Government Intranet, VPN, DMZ, information security, Zero Trust, logical segmentation.