**Сүлеймен Ерсұлтан Раматиллаұлы**

*Студент 2-го курса образовательной программы «****6B06152-Системы информационной безопасности» Кызылординского университета имени Коркыт Ата***

**Государственная стратегия информационной безопасности Казахстана: проблемы реализации и пути совершенствования**

Информационная безопасность (ИБ) является одним из ключевых направлений государственной политики Республики Казахстан в условиях цифровизации экономики и общества. С развитием цифровых технологий возросла зависимость критически важных инфраструктур от устойчивого и безопасного функционирования информационных систем. В 2017 году была утверждена Концепция «Кибершит Казахстана», направленная на формирование устойчивой системы защиты национального киберпространства. Несмотря на реализацию ряда государственных программ и создание нормативно-правовой базы, в Казахстане сохраняются актуальные проблемы в области обеспечения ИБ, что требует комплексного анализа и выработки рекомендаций по их решению.

В основе государственной политики ИБ лежат следующие документы (таблица 1):

* Концепция кибербезопасности «Кибершит Казахстана» (2017 г., актуализирована в 2021 г.);
* Закон РК «Об информатизации» (с изменениями от 2023 г.);
* Государственная программа «Цифровой Казахстан» (2020–2025 гг.);
* Стратегия национальной безопасности РК (обновлена в 2021 г.).

Однако в практике применения этих норм выявляются определенные сложности: ряд положений носит рамочный характер и требует конкретизации под современные угрозы. Например, в условиях быстрого развития технологий искусственного интеллекта, Интернета вещей и облачных сервисов возникают новые векторы атак, которые часто не охватываются действующими нормативами.

Таблица 1 — Основные нормативные акты в области ИБ

|  |  |  |  |
| --- | --- | --- | --- |
| № | Документ | Год | Цель |
| 1 | Концепция «Кибершит Казахстана» | 2017/2021 | Формирование системы киберзащиты |
| 2 | Закон «Об информатизации» | 2015/2023 | Регулирование информатизации и ИБ |
| 3 | «Цифровой Казахстан» | 2020–2025 | Цифровая трансформация и ИБ |
| 4 | Стратегия нац. безопасности | 2021 | Комплексная национальная безопасность |

Источник: Министерство цифрового развития, инноваций и аэрокосмической промышленности РК [https://www.gov.kz/memleket/entities/mdai?lang=ru]

Несмотря на развитие нормативной базы и запуск национальных программ, остаются следующие проблемы:

**1) Недостаточная координация между госорганами и частным сектором.** Многие объекты критической инфраструктуры находятся в ведении частных компаний, однако обмен информацией о киберинцидентах и совместная работа по их предотвращению зачастую недостаточно развиты;

**2) Дефицит квалифицированных кадров.** Как показывают данные исследований, на казахстанском рынке наблюдается острая нехватка специалистов в области кибербезопасности. Существующие образовательные программы нередко отстают от быстро меняющихся практик;

**3) Низкая киберграмотность населения.** Ряд киберинцидентов (фишинг, социальная инженерия) становится возможным из-за недостаточного уровня осведомленности пользователей о базовых принципах цифровой безопасности;

**4) Ограниченность технической базы и инфраструктуры.** Ряд государственных и региональных органов использует устаревшее программное и аппаратное обеспечение, что увеличивает уязвимость к кибератакам.

В таблице 2 приведена общая структура киберугроз в РК за 2022-2023 годы.

Таблица 2 — Структура инцидентов киберугроз в РК (2022–2023)

|  |  |  |
| --- | --- | --- |
| Тип инцидента | 2022 | 2023 |
| Фишинг | 35% | 37% |
| Вредоносное ПО | 25% | 23% |
| DDoS-атаки | 20% | 21% |
| Утечки данных | 15% | 14% |
| Прочие | 5% | 5% |

Источник: CERT-KZ, Отчёт о киберугрозах 2023 [<https://www.cert.gov.kz>].

Анализ данных национальной службы реагирования на компьютерные инциденты (CERT) КИИ включает энергетический сектор, транспорт, телекоммуникации и финансовую систему. Наиболее уязвимыми остаются энергетические объекты и транспорт (рис. 1).

Рисунок 1 — Доля инцидентов по секторам КИИ

Источник: Анализ CERT-KZ (2023).

Для повышения эффективности реализации государственной стратегии ИБ целесообразно учитывать успешный опыт ведущих стран. Мировая практика показывает высокую эффективность моделей киберрезервов (Канада, Великобритания), государственно-частного партнёрства (Сингапур, Израиль) и многоуровневого контроля (ЕС).

Таблица 3 — Сравнение стратегий ИБ

|  |  |  |
| --- | --- | --- |
| Страна | Ключевая особенность | Результат |
| Сингапур | Национальный центр кибербезопасности | Снижение инцидентов на 15% |
| Израиль | Программа резервистов | Быстрая реакция на угрозы |
| ЕС | Закон GDPR и NIS2 | Усиленный контроль КИИ |

Для Казахстана важным может быть расширение международного сотрудничества с целью обмена информацией об угрозах и лучших практиках реагирования. В этом направлении уже действует ряд соглашений с ОЭСР и странами ЕАЭС, однако требуется более широкое практическое наполнение таких договоренностей.

С учетом выявленных проблем можно выделить ряд приоритетных направлений совершенствования государственной стратегии информационной безопасности в Казахстане:

**1) Совершенствование законодательства.** Необходимо адаптировать нормативно-правовую базу с учетом новых технологий, в том числе IoT, Big Data и искусственного интеллекта. Следует закрепить требования к защите инфраструктуры умных городов и облачных сервисов;

**2) Развитие кадрового потенциала.** Актуальным является расширение профильных образовательных программ в вузах, внедрение краткосрочных курсов переподготовки, создание региональных центров компетенций по кибербезопасности;

**3) Повышение уровня киберграмотности населения.** Следует развивать массовые просветительские кампании, обучающие программы для школьников и студентов, а также мероприятия для сотрудников госорганов;

**4) Модернизация технической базы.** Важной задачей остается обновление оборудования и программного обеспечения на объектах государственной инфраструктуры. Также необходимо развивать отечественные решения в сфере криптографии и кибермониторинга;

**5) Развитие государственно-частного партнерства.** Эффективная защита киберпространства невозможна без тесного взаимодействия государства и бизнеса. Требуется создание платформ для обмена информацией о киберинцидентах и совместного реагирования.

Таким образом, информационная безопасность является одной из ключевых составляющих национальной безопасности Казахстана. Несмотря на достигнутые успехи, перед страной стоят серьезные вызовы, связанные как с техническими аспектами, так и с правовым регулированием и кадровым обеспечением. Реализация государственной стратегии ИБ требует системного подхода, активного взаимодействия всех заинтересованных сторон и учета мирового опыта. Только при условии комплексного подхода можно выстроить надежную и устойчивую систему защиты казахстанского киберпространства.

 **СПИСОК ЛИТЕРАТУРЫ**

1. Концепция кибербезопасности «Киберщит Казахстана». Послание Президента Республики Казахстан "Третья модернизация Казахстана: Глобальная конкурентоспособность" с учетом подходов Стратегии "Казахстан-2050" по вхождению Казахстана в число 30-ти самых развитых государств мира. [Электронный ресурс]. URL: <https://www.gov.kz/memleket/entities/knb/activities/250>

2. Ахметов, Б., & Лахно, В. (2022). ЗАЩИТА ИНФОРМАЦИИ И КИБЕРБЕЗОПАСНОСТЬ ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ УНИВЕРСИТЕТА. *Вестник КазАТК*, *120*(1), 134–141. <https://doi.org/10.52167/1609-1817-2022-120-1-134-141>

3. Майлыбаев, Е., & Мади, Р. (2024). ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ IoT. *Вестник КазАТК*, *134*(5), 168–175. <https://doi.org/10.52167/1609-1817-2024-134-5-168-175>

4. Исабаева С.Б. Обеспечение кибербезопасности Казахстана в условиях глобальной цифровизации. Диссертация на соискание степени доктора по профилю. УДК 451.86:004(574). Нур-Султан, 2020

5. Верещагина Е.А., Проблемы безопасностей интернета вещей. -Москва, 2021. –с. 26.

6. АверкиевА.А., Кибербезопасность виды и методы, Научно-образовательный журнал для студентов и преподавателей «StudNet» No1/2022, Ростов на Дону,2022.-с. 567.

7. Колисниченко Д.Н.,Секреты безопасности и анонимности в интернете. -Санкт-Петербург,2020. –с.33.

8. Интернет вещей: обзор проблем безопасности [Электрондық ресурс]. ‒ URL:https://business-online.su/blog/internet-veshchey-problemy-bezopasnosti