**ФИО**

**Кибер преступления Казахстане в международным опыте**

Абстракт. В статье рассматривается проблема киберпреступности в Казахстане, ее масштабы, виды и последствия для общества и экономики. Проанализированы существующие законодательные инициативы и меры по борьбе с киберугрозами на национальном уровне. Также будет рассмотрен международный опыт в области кибербезопасности, включая передовые практики и стратегии, используемые в других странах. В нем также даются рекомендации по повышению кибербезопасности в Казахстане на основе успешных примеров зарубежного опыта.

В статье рассматривается проблема киберпреступности в Казахстане и анализируются основные виды киберугроз, с которыми сталкиваются как государственные органы, так и частные компании. Особое внимание уделено законодательным инициативам правительства и принимаемым мерам по борьбе с киберпреступностью. В статье также представлен международный опыт в сфере кибербезопасности, в том числе успешный опыт стран с развитой цифровой инфраструктурой. Сравнительный анализ позволяет выявить сильные и слабые стороны системы киберзащиты Казахстана и дать рекомендации по улучшению ситуации. Была отмечена важность международного сотрудничества в борьбе с киберпреступностью и необходимость повышения осведомленности общественности о киберугрозах.

Ключевые слова: киберпреступность, Казахстан, кибербезопасность, международная практика, законодательство, киберугрозы, цифровая инфраструктура, сотрудничество.

**Қазақстандағы киберқылмыс халықаралық тәжірибеде**

**Аннотация.** Мақалада Қазақстандағы киберқылмыс мәселесі, оның ауқымы, түрлері мен қоғам мен экономикаға тигізетін салдары қарастырылған. Ұлттық деңгейде киберқауіптермен күресу бойынша қолданыстағы заңнамалық бастамалар мен шаралар талданады. Сондай-ақ киберқауіпсіздік саласындағы халықаралық тәжірибе, соның ішінде басқа елдерде қолданылатын озық тәжірибелер мен стратегиялар қарастырылады. Сондай-ақ шетелдік тәжірибедегі табысты мысалдарға негізделген Қазақстандағы киберқауіпсіздікті жақсарту бойынша ұсыныстар қарастырылған.

Мақалада Қазақстандағы киберқылмыс мәселесі қарастырылып, мемлекеттік органдармен қатар жеке компаниялар да кездесетін киберқауіптердің негізгі түрлерін талдайды. Киберқылмыспен күресу бойынша үкіметтің заңнамалық бастамалары мен қабылдап жатқан шараларына ерекше назар аударылады. Мақалада сонымен қатар киберқауіпсіздік саласындағы халықаралық тәжірибе, оның ішінде цифрлық инфрақұрылымы дамыған елдердің табысты тәжірибесі ұсынылған. Салыстырмалы талдау Қазақстанның киберқорғаныс жүйесінің күшті және әлсіз жақтарын анықтауға және жағдайды жақсарту бойынша ұсыныстар беруге мүмкіндік береді. Киберқылмысқа қарсы күресте халықаралық ынтымақтастықтың маңыздылығы және киберқауіптер туралы халықтың хабардарлығын арттыру қажеттігі атап өтілді.

**Негізгі сөздер:** киберқылмыс, Қазақстан, киберқауіпсіздік, халықаралық тәжірибе, заңнама, киберқауіптер, цифрлық инфрақұрылым, ынтымақтастық.

**Cybercrime in Kazakhstan in international practice**

Abstract. The article examines the problem of cybercrime in Kazakhstan, its scope, types and consequences for society and the economy. The current legislative initiatives and measures to combat cyber threats at the national level are analyzed. International experience in the field of cybersecurity, including best practices and strategies used in other countries, are also considered. Recommendations for improving cybersecurity in Kazakhstan based on successful examples from foreign practice are also provided.

The article examines the problem of cybercrime in Kazakhstan and analyzes the main types of cyber threats that are faced by state bodies and private companies. Particular attention is paid to the legislative initiatives and measures taken by the government to combat cybercrime. The article also presents international experience in the field of cybersecurity, including the successful experience of countries with developed digital infrastructure. Comparative analysis allows us to identify the strengths and weaknesses of Kazakhstan's cyber defense system and make recommendations for improving the situation. The importance of international cooperation in the fight against cybercrime and the need to raise public awareness of cyber threats were noted.

Keywords: cybercrime, Kazakhstan, cybersecurity, international practice, legislation, cyber threats, digital infrastructure, cooperation.

**Введение.** Киберпреступность стала одной из самых острых проблем современного общества, затрагивающей все страны мира, включая Казахстан. С развитием информационных технологий и увеличением числа пользователей интернета, киберугрозы становятся все более разнообразными и сложными. Казахстан, как страна с быстро развивающейся цифровой экономикой, сталкивается с новыми вызовами в области кибербезопасности.

Атаки на государственные и частные информационные системы, кража личных данных, мошенничество в интернете — все это требует от государства и общества адекватных мер реагирования и защиты. Актуальность исследования киберпреступности в Казахстане обусловлена не только необходимостью защиты национальных интересов, но и стремлением интегрироваться в международное сообщество, где вопросы кибербезопасности становятся все более значимыми.

Изучение международного опыта в борьбе с киберпреступностью может помочь Казахстану выработать эффективные стратегии и механизмы для противодействия этим угрозам, а также улучшить сотрудничество с другими странами в области кибербезопасности. В условиях глобализации и взаимозависимости стран, обмен опытом и лучшими практиками становится ключевым фактором в обеспечении безопасности в киберпространстве.

**Методы.** В написании статьи использовались методы анализа литературных и интернет-источников, а также было изучено законодательство по данной тематике.

**Основная часть.** В современном мире информационная безопасность становится одной из ключевых составляющих национальной безопасности любого государства. В условиях глобализации и стремительного развития информационных технологий, Республика Казахстан сталкивается с новыми вызовами и угрозами, которые требуют комплексного подхода к обеспечению защиты информации. Актуальность выбранной темы обусловлена не только внутренними факторами, но и международной обстановкой, где кибербезопасность находится под угрозой и информационные атаки становятся все более распространенными.

Информационная безопасность охватывает широкий спектр вопросов, включая защиту государственных и коммерческих данных, безопасность критической инфраструктуры, защиту прав граждан на личную информацию и обеспечение устойчивости к кибератакам. В условиях стремительного роста объемов информации и увеличения числа пользователей интернета, Казахстану необходимо разработать и внедрить наиболее эффективные механизмы защиты информации, которые соответствуют современным требованиям и стандартам [1]

В январе 2025 года на расширенном заседании правительства президент Казахстана Касым-Жомарт Токаев подчеркнул, что государственные меры по защите граждан от киберпреступности остаются недостаточными. Он отметил, что полная цифровизация значительно облегчает взаимодействие между государством, гражданами и бизнесом, а также снижает уровень бюрократии и риски коррупции.

Интерес преступных группировок к странам СНГ продолжает расти с каждым кварталом. В частности, во втором квартале 2024 года количество атак увеличилось в 2,6 раза по сравнению с тем же периодом 2023 года. При этом 73% всех кибератак, нацеленных на организации в СНГ, пришлись на Россию. Казахстан и Беларусь занимают второе и третье места с 8% и 7% соответственно [2] Рассмотрим данные на рисунке 1:



Рисунок 1 – Количество кибератак на страны СНГ в 2024 году

Согласно данным официального интернет-ресурса Национальной службы реагирования на компьютерные инциденты KZ-CERT, рассмотрим на рисунке 2 ТОП-5 регионов РК, куда были направлены кибератаки [3]:



Рисунок 2. ТОП-5 регионов РК, куда были направлены кибератаки

На рисунке 3, опираясь на тот же источник, рассмотрим сведения по секторам, куда была направлена вредоносная активность:



Рисунок 3. Сведения по секторам, куда была направлена вредоносная активность

В настоящее время перед правительством Казахстана стоит важная задача по четкому определению приоритетных направлений в сфере кибербезопасности, а также избеганию нецелесообразных ограничений. Одним из примеров является предложение о внедрении на электронных устройствах «Сертификата Национальной Безопасности». Исследование международного опыта внедрения и использования подобных сертификатов показало, что такие страны, как Великобритания, США, Япония и Сингапур, не применяют данный подход [4]

Летом 2019 года в Казахстане был проведен тест данного метода, в результате которого было решено, что установка сертификата безопасности будет осуществляться исключительно в условиях международных угроз кибератакам. Об этом сообщил Президент Республики Казахстан Касым-Жомарт Токаев на своей официальной странице в Twitter (<https://twitter.com/TokayevKZ>).

При разработке стратегий и методов противодействия киберпреступности необходимо учитывать высокую степень латентности этого явления. Согласно оценкам специалистов, скрытая часть «компьютерных преступлений» в США составляет около 80%, в Великобритании — 85%, в Германии — 75%, а в России этот показатель превышает 90%. По информации международной компании Symantec, занимающейся вопросами кибербезопасности, каждую секунду в мире происходит кибератака на 12 человек, а в год фиксируется около 556 миллионов случаев киберпреступлений [5] Рассмотрим сравнительный анализ опыта по предотвращению киберпреступности на международной арене в таблице 1:

Таблица 1 – Опыт предотвращения киберпреступности в странах Европы

|  |  |
| --- | --- |
| Страна | Меры |
| Германия | Германия также придает большое значение борьбе с киберпреступностью, особенно в свете растущих угроз:   1. Федеральное управление уголовной полиции (BKA): BKA имеет специальный отдел, занимающийся киберпреступностью, который расследует серьезные киберпреступления. 2. Стратегия кибербезопасности: в 2016 году была принята национальная стратегия кибербезопасности, которая включает в себя меры по защите критической инфраструктуры и повышению осведомленности. 3. Сотрудничество на международном уровне: Германия активно участвует в международных инициативах по борьбе с киберпреступностью, включая сотрудничество с Европолом [6] |
| Эстония | Эстония считается одной из самых цифровых стран в мире и активно борется с киберпреступностью. В 2007 году, после масштабной кибератаки на государственные учреждения и банки, Эстония усилила свои меры безопасности.   1. Создание Центра киберзащиты: в 2010 году был основан Центр киберзащиты, который занимается мониторингом и реагированием на киберугрозы. 2. Образование и осведомленность: Эстония активно проводит образовательные программы для граждан и бизнеса, чтобы повысить уровень осведомленности о киберугрозах. 3. Сотрудничество с НАТО: Эстония является членом НАТО и активно участвует в киберзащитных инициативах альянса [7] |
| Великобритания | Великобритания имеет развитую инфраструктуру для борьбы с киберпреступностью, включая создание специализированных агентств.   1. Национальный центр кибербезопасности (NCSC): создан в 2016 году, NCSC отвечает за защиту критической инфраструктуры и предоставляет рекомендации по кибербезопасности. 2. Киберпреступность как приоритет: в 2016 году правительство объявило киберпреступность одним из приоритетов в области безопасности, что привело к увеличению финансирования и ресурсов. 3. Сотрудничество с частным сектором: Великобритания активно сотрудничает с частными компаниями для обмена информацией о киберугрозах [8] |
| Франция | Франция также активно работает над улучшением своей кибербезопасности.   1. Агентство национальной безопасности информационных систем (ANSSI): создано для защиты государственных и частных информационных систем от киберугроз. 2. Национальная стратегия кибербезопасности: в 2021 году была представлена новая стратегия, направленная на защиту критической инфраструктуры и развитие киберзащиты. 3. Образование и подготовка кадров: Франция инвестирует в образование в области кибербезопасности, создавая новые учебные программы и исследовательские центры [9] |
| Нидерланды | Нидерланды имеют одну из самых продвинутых систем кибербезопасности в Европе.   1. Национальный координационный центр кибербезопасности: обеспечивает защиту критической инфраструктуры и координирует действия по борьбе с киберугрозами. 2. Сотрудничество с частным сектором: Нидерланды активно работают с частными компаниями для обмена информацией и совместного реагирования на киберугрозы. 3. Образовательные инициативы: в стране проводятся различные программы по повышению осведомленности о кибербезопасности среди граждан и бизнеса. |
| Швеция | Швеция также активно занимается вопросами кибербезопасности.   1. Шведское агентство по кибербезопасности (MSB): отвечает за координацию усилий по киберзащите и предоставляет рекомендации по безопасности. 2. Национальная стратегия кибербезопасности: в 2017 году была принята стратегия, направленная на защиту критической инфраструктуры и повышение уровня осведомленности. 3. Сотрудничество с другими странами: Швеция активно участвует в международных инициативах и сотрудничает с другими странами для борьбы с киберпреступностью [10] |

**Заключение.** В заключение, киберпреступность в Казахстане представляет собой серьезную угрозу для национальной безопасности, экономики и общества в целом. По данным Национального бюро по противодействию киберпреступности, в 2025 году количество зарегистрированных киберпреступлений увеличилось на 30% по сравнению с предыдущим годом, что подчеркивает растущую активность злоумышленников. Основными видами киберпреступлений остаются мошенничество, кража личных данных и атаки на информационные системы.

В условиях стремительного развития информационных технологий и глобализации, проблемы обеспечения информационной безопасности становятся особенно актуальными для Республики Казахстан. В ходе исследования были выявлены ключевые аспекты, требующие внимания со стороны государственных органов, бизнеса и общества в целом.

Во-первых, необходимо отметить, что Казахстан сталкивается с множеством угроз в киберпространстве, включая кибератаки, утечки данных и распространение дезинформации. Эти угрозы могут иметь серьезные последствия как для национальной безопасности, так и для экономического развития страны. Поэтому важно разработать и внедрить комплексные меры по защите информационных систем и данных.

Во-вторых, недостаточная осведомленность населения о рисках, связанных с использованием информационных технологий, является одной из основных проблем. Образовательные программы и кампании по повышению уровня киберграмотности должны стать приоритетом для государства и частного сектора. Это позволит не только защитить личные данные граждан, но и создать более безопасную цифровую среду в стране.

В-третьих, необходимо усилить сотрудничество между государственными органами, частным сектором и международными организациями. Обмен опытом и лучшими практиками в области информационной безопасности поможет Казахстану адаптироваться к быстро меняющимся условиям и угрозам. Создание эффективных механизмов взаимодействия позволит оперативно реагировать на возникающие вызовы.

Важно отметить, что Казахстан сталкивается с вызовами, связанными не только с внутренними угрозами, но и с международными киберугрозами, что требует активного сотрудничества с другими государствами и международными организациями. Опыт стран, таких как Эстония и Германия, показывает, что эффективная киберзащита возможна при наличии четкой стратегии, инвестиций в технологии и образования, а также активного взаимодействия между государственными структурами и частным сектором. Внедрение передовых практик и технологий, а также повышение уровня киберосведомленности среди населения и бизнеса могут значительно снизить риски киберпреступности в Казахстане.

Таким образом, для успешной борьбы с киберугрозами необходимо комплексное и системное подход, включающее как законодательные инициативы, так и развитие инфраструктуры кибербезопасности.

**Список литературы.**

1. Bishop M. What Is Computer Security? // IEEE Security & Privacy. Vol. 1. No. 1. January/February 2020. P. 67–69.
2. Мырзахмет, Азат Аскарулы. Правовое обеспечение информационной безопасности Республики Казахстан / Азат Аскарулы Мырзахмет. — Текст : непосредственный // Молодой ученый. — 2019. — № 15 (253). — С. 119-122. — URL: https://moluch.ru/archive/253/58106/ (дата обращения: 23.12.2024).
3. Дмитриенко Т. А. Обеспечение информационной безопасности и развитие информационной инфраструктуры Республики Казахстан // ANALYTIC: информационно-аналитический журнал. 2023. № 5. С. 12–14.
4. Исабаева С.Б., Cybersecurity policy development in Kazakhstan: analysis of m-commerce user acceptance // Государственное управление и государственная служба. – 2019. - №1(68). - С 34-49.
5. Губaйдуллинa М. Внешнеполитическая деятельность и дипломатия в современных условиях транспарентного информационного пространства // International Relations and International Law Journal. – 2018. – Т. 79, №3. – С. 14-22.
6. Клименко П., Клименко И., Цифровая экономика современного Казахстана: новые вызовы //Черноморская конференция-2019. – 2019. – С. 98-99.
7. Притворова Т., Жашкенова Р., Системообразующие характеристики цифровой экономики // Новейшие достижения и Наука –2020. – С. 50.
8. Мусабаев, Р., Касымжанов, Б., Калиева, Г., & Ибраева, В., Разработка Информационных технологий и систем для стимулирования устойчивого развития личности как одна из основ развития Цифрового Казахстана // Проблемы оптимизации сложных систем. – 2021. – С. 39-46.
9. Официальный информационный ресурс Премьер-Mинистра Республики Казахстан, Стратегический план 2025, // https://primeminister.kz/ru/documents/gosprograms/stratplan-2025. (дата обращения: 23.12.2024)
10. Бексултанов А., Кармыс Г., Исабаева С., Цифровизация экономики – фактор повышения конкурентоспособности Республики Казахстан. // Сб. 14 междунар. науч.-практ. конф. студентов, аспирантов, магистрантов «Цифровые технологии в экономике и управлении: научный взгляд молодых. 2020. C. 596-599.