Информационно-справочные материалы
к обзору о защите цифровых прав граждан

По линии Министерства искусственного интеллекта и цифрового развития

Законодательные изменения в сфере кибербезопасности

В рамках Года цифровизации и искусственного интеллекта в стране впервые приняты Цифровой кодекс и закон «О кибербезопасности». Принятие закона о кибербезопасности формирует единую правовую основу защиты цифровых систем государственных органов и организаций, позволяет обеспечить устойчивое развитие цифровой инфраструктуры и системно гарантировать цифровую безопасность страны. Законами предусмотрен ряд ключевых норм в сфере кибербезопасности, затрагивающих организации и граждан.

Впервые в Трудовом кодексе закреплены обязанности работодателей и работников по соблюдению требований кибербезопасности и киберкультуры. Данная норма направлена на то, чтобы каждый работник обладал базовыми знаниями и навыками для защиты своей цифровой безопасности, а также безопасно использовал информационные системы и служебные данные. Работодатели будут утверждать внутренние правила или регламенты и организовывать обучение сотрудников по вопросам кибербезопасности и повышения киберкультуры. Соответствующие рекомендации уже размещены на официальном сайте Комитета по информационной безопасности, а также на портале электронного правительства в разделе «Помощь». Кроме того, ежегодное обучение по вопросам кибербезопасности и киберкультуры должны проходить сотрудники государственных органов, акиматов и критически важных объектов.

Введена обязанность ежегодного проведения аудита кибербезопасности цифровых систем собственниками цифровых объектов. Аудит позволяет оценивать уровень защищенности цифровой инфраструктуры от внутренних и внешних угроз. При этом критически важные цифровые объекты должны ежегодно направлять отчеты о проведении аудита кибербезопасности в Комитет по информационной безопасности. Ранее такой обязанности не было.

В целях реализации Указа Президента функции государственного контроля в отношении критически важных объектов переданы Комитету национальной безопасности. То есть критически важные объекты переходят под контроль КНБ. Это позволит повысить устойчивость и безопасность критически важных цифровых объектов. В целом это соответствует мировой практике.

Законодательные изменения по защите персональных данных

Важным системным вопросом является защита персональных данных. Если ранее защита персональных данных регулировалась отраслевым законодательством, то теперь соответствующие положения впервые закреплены в новой Конституции, что подчеркивает особую значимость защиты персональных данных. В целях дальнейшей реализации конституционного положения внесены изменения в закон «О персональных данных и их защите».

Предусмотрена обязательная биометрическая аутентификация как дополнительная мера защиты при доступе к персональным данным ограниченного доступа. Это базы данных, содержащие медицинскую, коммерческую, банковскую, семейную и иные тайны. Такая мера позволит не допускать к указанным базам третьих лиц, так как потребуется биометрическая аутентификация сотрудника.

Теперь об утечке персональных данных нужно будет сообщать не только государству, но и самим гражданам. Это повысит ответственность организаций и позволит людям своевременно принимать меры для защиты своих данных.

Вводится реестр крупных операторов персональных данных с обязательным уведомлением. Это позволит уделять больше внимания организациям, которые работают с большими объемами персональных данных, и устанавливать для них дополнительные организационные и технические меры защиты.

Также введено новое понятие «идентификаторы персональных данных». К ним теперь относятся фамилия, имя, отчество (при его наличии) в совокупности; индивидуальный идентификационный номер; изображение лица субъекта; биометрический вектор лица субъекта или их производные, которые могут быть восстановлены до первоначального значения.

Представлен лишь ряд наиболее важных норм, в действительности их значительно больше. Эти изменения позволят усилить защиту персональных данных граждан и повысить уровень защищенности цифровых систем.

Подзаконные акты и государственный контроль

В рамках перечисленных законов принято около 30 подзаконных актов по вопросам кибербезопасности и защиты персональных данных. Еще около 10 по данным направлениям будут приняты до конца сентября. Наряду с совершенствованием законодательства проводится мониторинг и контроль за соблюдением требований кибербезопасности, защиты персональных данных и использования ЭЦП.

За период с 2024 года по настоящее время проведено 648 внеплановых проверок (480 по информационной безопасности и 168 по персональным данным). По итогам к нарушителям были применены штрафные санкции.

Результаты проверок показывают наличие как организационных, так и технических нарушений. К основным организационным недостаткам относятся отсутствие форм согласия на обработку персональных данных, отсутствие внутренних политик защиты данных, отсутствие базовых средств защиты информации, таких как антивирусы, межсетевые экраны и другие. Среди технических нарушений наиболее распространены известные уязвимости: отсутствие многофакторной аутентификации и криптографической защиты, несвоевременная установка обновлений безопасности, отсутствие подключения к центрам обеспечения кибербезопасности.

Эти нарушения потенциально могут привести к взломам систем или утечкам данных, поэтому всем организациям, которые хранят или собирают данные, важно соблюдать требования кибербезопасности и защиты персональных данных. Это касается не только крупных организаций, но и малых и средних предприятий: салонов красоты, образовательных центров, частных медицинских организаций, компьютерных клубов, фитнес-центров, магазинов, онлайн-платформ, турфирм и других. С учетом развития цифровизации наши данные находятся повсюду, и каждой организации, даже небольшой, важно принимать меры по их защите.

Киберкультура

Мошеннические схемы постоянно совершенствуются, поэтому одних технических и правовых мер недостаточно. Не менее важным направлением остается формирование киберкультуры населения. Практика показывает, что даже самые современные технологии не смогут обеспечить безопасность, если пользователи сами не соблюдают правила цифровой безопасности.

Для этого государством уже внедрены бесплатные цифровые сервисы и образовательные платформы, позволяющие гражданам самостоятельно повысить уровень своей защищенности. Сервис «Стопкредит» в приложении eGov Mobile позволяет установить добровольный запрет на оформление кредитов. Сервис контроля доступа к персональным данным позволяет проверить, каким организациям предоставлено согласие на их обработку, и при необходимости отозвать его. Платформа NomadGuard помогает проверить возможные утечки персональных данных и выявить фишинговые ссылки.

Для повышения уровня киберкультуры доступны бесплатные образовательные ресурсы. Это новый онлайн-курс на eGov для детей и родителей, разработанный совместно с UNICEF, по вопросам

кибербуллинга, онлайн-груминга, защиты персональных данных и безопасного поведения в интернете. Также функционирует платформа CitizenSec с курсами по основам кибергигиены для граждан и государственных служащих. Все организации в Казахстане могут воспользоваться указанными сервисами для исполнения требований Трудового кодекса.

Дополнительно каждому гражданину рекомендуется соблюдать базовые меры киберкультуры. Во-первых, никому не сообщать SMS-коды, пароли и данные банковских карт: банки и государственные органы не запрашивают такую информацию по телефону или в мессенджерах. Во-вторых, не переходить по подозрительным ссылкам и не отвечать на сообщения от неизвестных отправителей, а перед вводом персональных данных всегда проверять адрес сайта или приложения. В-третьих, использовать сложные и разные пароли для каждого сервиса и подключать двухфакторную аутентификацию. Именно сочетание современных технологий, государственных сервисов и ответственного поведения каждого гражданина позволяет существенно снизить риски кибермошенничества и повысить уровень защищенности граждан.

Дальнейшая работа

По поручению Главы государства в рамках Года цифровизации реализуется комплекс основных мероприятий, направленных на развитие технологий искусственного интеллекта, укрепление кибербезопасности, а также повышение уровня защиты цифровых систем государственных органов, бизнеса и граждан. Совместно с уполномоченными государственными органами, экспертным сообществом и Национальной палатой предпринимателей «Атамекен» продолжается разработка и реализация новых инициатив, отвечающих современным вызовам и направленных на обеспечение устойчивого цифрового развития страны.

*****

В 2024 году зарегистрировано 22 560 интернет-мошенничеств. возмещено 2,1 млрд тенге.

В 2025 году зарегистрировано 27 892 интернет-мошенничества. Возмещение - 5 млрд тенге. Доля интернет-мошенничеств в общем количестве зарегистрированных мошенничеств достигла 60,9%.

За 8 месяцев 2026 года зарегистрировано 14 414 интернет-мошенничеств - на 13% меньше, чем за аналогичный период 2025 года *(16 564).* Возмещение - 5,9 млрд тенге.

В целом за три года снижение фактов интернет-мошенничества составила 40%.

В 2024 году раскрыто 4 409 интернет-мошенничеств, к уголовной ответственности привлечено 1 564 лица *(в том числе организаторов и участников преступных групп)*.

В 2025 году раскрыто 6 016 преступлений, раскрываемость выросла до 20,6%, привлечено 1 750 лиц.

За 8 месяцев 2026 года раскрыто 3 977 преступлений. Раскрываемость повысилась до 29,9%, привлечено 1 128 лиц.

Кроме того, по статье 232-1 УК РК за дропперство зарегистрировано 1 018 уголовных правонарушений, к уголовной ответственности привлечено 364 лица *(с момента вступления в силу статьи).*

Таким образом, в 2026 году одновременно со снижением регистрации отмечается существенное повышение эффективности раскрытия интернет-мошенничеств.

Наиболее распространенными остаются телефонное мошенничество, лжеинвестиции, фишинг, мошенничество на сайтах объявлений и в социальных сетях и мессенджерах, незаконное оформление онлайн-кредитов, поддельные сайты и приложения.

В 2025-2026 годах активно развивается использование искусственного интеллекта и deepfake. Преступники подделывают изображение и голос сотрудников банков, правоохранительных органов, руководителей и родственников, создают фальшивые видеозвонки и используют ИИ для продвижения фиктивных инвестиционных платформ.

Распространяется и клонирование голоса, позволяющее имитировать знакомого человека и под предлогом чрезвычайной ситуации либо срочного поручения требовать перевод денежных средств.

Таким образом, ИИ преимущественно не создает новые виды мошенничества, а делает традиционные схемы более убедительными, персонализированными и масштабируемыми.

МВД взаимодействует с Антифрод-центром Национального Банка для оперативного выявления подозрительных транзакций и блокирования похищенных средств.

В Антифрод-системе создано 199,7 тыс. инцидентов, из которых 128,2 тыс. инициированы МВД. Заблокировано 3,4 млрд тенге на счетах отправителей и 1,7 млрд тенге на счетах дропперов. Добровольно возвращено потерпевшим порядка 1 млрд тенге.

Система развивается в направлении интеграции с данными операторов связи и IMEI, а также внедрения сессионного и транзакционного антифрода, поведенческой аналитики и искусственного интеллекта.

Основная задача – переход от реагирования на уже совершенное мошенничество к проактивному выявлению подозрительных действий, оперативной блокировке средств и предупреждению хищения.

По линии Национального банка РК

Цифровые технологии меняют саму организацию финансового рынка: появляются новые участники, инструменты инвестирования и способы проведения расчетов. Вместе с этим меняется и роль регулятора. Требуется действовать на опережение, создавать условия для инноваций и конкуренции, обеспечивая надежность финансовой системы и доверие к ней.

В настоящий момент ведется реализация стратегии Цифрового Национального Банка. Ее замысел был шире запуска отдельных проектов и систем. Задача - изменить сам подход к развитию рынка: своевременно открывать новые возможности, обеспечивать их инфраструктурой и вместе с участниками рынка переходить к практическому применению.

Практические результаты уже заметны – доля безналичных платежей продолжает устойчивый рост и превысила 90%, весь путь клиента стал «цифровым по умолчанию», а казахстанский финтех стал одним из драйверов цифровизации других отраслей – GovTech, электронной коммерции и т.д.

Основные направления этой работы.

1. Действуют все компоненты Национальной цифровой финансовой инфраструктуры, ее статус закреплен законодательно. Она объединяет безопасную биометрию, удобные межбанковские платежи, цифровой тенге и защиту граждан и бизнеса от мошенничества.

Одним из ключевых результатов этого года стал запуск Межбанковской системы мобильных платежей: переводов по номеру телефона и единого QR-кода. С момента запуска системы 19 июля т.г. обработано более 20 млн транзакций на сумму около 400 млрд тенге.

Цифровой тенге поэтапно интегрируется в цифровую экосистему государственных финансов, став одним из ключевых элементов системы эффективного госрасходования. В 2026–2027 гг. оборот цифровых тенге достигнет 2 трлн тенге.

Благодаря активной работе Национального Антифрод-центра в связке с банками предотвращены мошеннические операции более чем на 120 млрд тенге.