

Нормативная правовая база в области образования и информационных технологий в РК

В Республике Казахстан нормативная правовая база в области информационных технологий развивается в рамках общегосударственной политики цифровизации. Основные нормативные документы регулируют использование и развитие ИТ, защиту информации и персональных данных, а также обеспечение информационной безопасности.

Список ключевых законов и нормативных актов в данной сфере:

- Закон «Об информатизации» - определяющий правовые, организационные и экономические основы формирования, обработки и защиты информации.
- Закон «О связи» - регулирующий отношения в области электросвязи и почтовой связи.
- Закон «О персональных данных и их защите» - устанавливающий правила обработки персональных данных, требования к защите таких данных, а также права и обязанности субъектов, занимающихся обработкой персональных данных.
- Закон «Об электронном документообороте и электронной цифровой подписи» - регулирующий отношения, связанные с созданием, обращением, хранением и признанием электронного документа, подписанного электронной цифровой подписью.
- Закон «О государственных услугах» - включающий положения о предоставлении государственных услуг через электронные каналы взаимодействия, что также затрагивает использование информационных технологий.
- Закон «О государственных закупках» - регулирует процесс приобретения товаров, работ и услуг для нужд государства, государственных организациях.
- Закон «О защите прав потребителей» - включающий в себя положения, касающиеся информационных технологий в контексте защиты прав потребителей.
- Постановление «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», утвержденный Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.
- Приказ «Об утверждении правил организации и функционирования объектов информатизации в области дошкольного, среднего, технического и профессионального, послесреднего образования, дополнительного образования», утвержденный приказом и.о. Министра образования и науки Республики Казахстан от 1 декабря 2011 года № 503. регламентирует использование информационно-коммуникационных технологий (ИКТ) и обеспечение информационной безопасности в организациях образования.
- Приказ «Об утверждении правил организации и функционирования объектов информатизации в области дошкольного, среднего, технического и профессионального, послесреднего образования, дополнительного образования», утвержденный Приказ Министра просвещения Республики Казахстан от от 1 декабря 2011 года № 503.
- Приказ «Об определении минимальных требований к программно-аппаратному комплексу и прикладному программному обеспечению, используемых в организациях образования», утвержденный Приказ Министра просвещения Республики Казахстан от 02 марта 2020 года № 79.
- Приказ «Об утверждении минимальных требований к объектам информатизации в области образования», утвержденный Приказ Министра просвещения Республики Казахстан от 14 ноября 2022 года № 456.
- Приказ «Об утверждении требований к организациям образования по предоставлению дистанционного обучения и правил организации учебного процесса по дистанционному обучению по образовательным программам начального, основного среднего, общего среднего, технического и профессионального, послесреднего образования и в форме онлайн-обучения по образовательным программам технического и профессионального, послесреднего образования», утвержденный Приказ Министра просвещения Республики Казахстан от 27 ноября 2023 года № 349.

- Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы,
- Концепции развития искусственного интеллекта на 2024 – 2029 годы.

Основные нормативные документы и стандарты

1. Закон Республики Казахстан «Об информатизации»:

- Определяет общие принципы и требования к использованию ИКТ в различных сферах, включая образование.
- Описывает права и обязанности участников информационных процессов и их ответственность за нарушение законодательства в области информатизации.

2. Закон Республики Казахстан «О защите персональных данных»:

- Регламентирует порядок сбора, обработки и защиты персональных данных, включая данные учащихся и работников образовательных учреждений.
- Устанавливает требования к обеспечению конфиденциальности и безопасности персональных данных.

3. Государственные образовательные стандарты:

- Включают требования к использованию ИКТ в образовательном процессе на разных уровнях образования.
- Определяют минимальные технические и программные средства, необходимые для обеспечения качественного образовательного процесса.

4. Национальные стандарты по информационной безопасности (ГОСТ):

- Устанавливают требования к защите информации и систем управления в организациях образования.
- Регламентируют методы и средства защиты информации, включая шифрование, контроль доступа и мониторинг безопасности.

Основные аспекты правил организации и функционирования объектов информатизации:

1. Техническая инфраструктура:

- Оснащение организаций образования необходимыми техническими средствами, включая компьютеры, серверы, сетевое оборудование и программное обеспечение.
- Обеспечение доступности и надежности ИКТ-инфраструктуры для всех участников образовательного процесса.

2. Образовательные ресурсы и контент:

- Создание и поддержка электронных образовательных ресурсов (ЭОР), таких как электронные учебники, онлайн-курсы и базы данных.
- Обеспечение доступности и актуальности образовательного контента.

3. Обучение и повышение квалификации:

- Регулярное обучение педагогических работников и сотрудников организации образования по вопросам использования ИКТ и обеспечения информационной безопасности.
- Повышение квалификации специалистов по ИКТ и информационной безопасности.

4. Информационная безопасность:

- Внедрение и поддержка системы информационной безопасности, включая защиту данных, контроль доступа и мониторинг безопасности.
- Проведение регулярных аудитов и тестов на проникновение для выявления и устранения уязвимостей.

5. Контроль и мониторинг:

- Постоянный мониторинг работы ИКТ-инфраструктуры и информационных систем для обеспечения их бесперебойного функционирования.
- Введение системы отчетности и контроля за использованием ИКТ в образовательных учреждениях.

6. Соответствие нормативным требованиям:

- Соблюдение требований законодательства и нормативных актов в области информатизации и защиты персональных данных.
- Регулярное обновление и корректировка внутренних нормативных документов в соответствии с изменениями законодательства.

Организация и функционирование объектов информатизации в области образования осуществляется с учетом требований Закона Республики Казахстан "Об информатизации", а также Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденных постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.

Единые требования в области информационно-коммуникационных технологий (ИКТ) и обеспечения информационной безопасности для организаций образования регулируются несколькими ключевыми нормативными актами и стандартами. Основные аспекты таких требований включают защиту информационных систем и данных, управление доступом, а также обеспечение соответствия законодательным и нормативным требованиям. Вот основные элементы, которые включаются в такие требования в РК:

1. Информационная безопасность

- **Политики и процедуры:** Разработка и внедрение политик информационной безопасности, которые охватывают все аспекты защиты информации в организациях образования.
- **Обучение и осведомленность:** Проведение регулярных обучающих программ для сотрудников и студентов по вопросам информационной безопасности, включая меры по защите от фишинговых атак и других киберугроз.
- **Контроль доступа:** Введение ограничений на доступ к информационным системам и данным для уполномоченных лиц. Использование средств аутентификации, включая многофакторную аутентификацию.
- **Защита данных:** Шифрование данных в состоянии покоя и при передаче. Регулярное создание и тестирование резервных копий данных для обеспечения их целостности.
- **Мониторинг и аудит:** Постоянный мониторинг систем на предмет безопасности, проведение регулярных аудитов и тестов на проникновение для выявления и устранения уязвимостей.

2. Информационно-коммуникационные технологии

- **Инфраструктура:** Использование надежных и современных аппаратных и программных решений для создания устойчивой ИКТ-инфраструктуры.
- **Сетевые технологии:** Защита сетевых коммуникаций с использованием межсетевых экранов (firewalls), систем предотвращения вторжений (IDS/IPS) и виртуальных частных сетей (VPN).
- **Программное обеспечение:** Применение лицензированного и обновленного программного обеспечения. Регулярное обновление программных продуктов для устранения выявленных уязвимостей.
- **Интернет-безопасность:** Фильтрация интернет-контента для предотвращения доступа к вредоносным сайтам и защита от интернет-угроз.

3. Соответствие нормативным требованиям

- **Законодательство:** Соответствие национальным законам как Закон «Об информатизации» и Закон «О защите персональных данных».
- **Стандарты:** Применение международных стандартов информационной безопасности, таких как ISO/IEC 27001, а также национальных стандартов, принятых в Казахстане.

4. Управление инцидентами

- **План реагирования:** Разработка и внедрение плана реагирования на инциденты информационной безопасности, включающего процедуры обнаружения, оценки, управления и восстановления после инцидентов.

- **Команда реагирования:** Создание команды реагирования на инциденты (IRT), состоящей из квалифицированных специалистов, готовых оперативно реагировать на угрозы и инциденты.

5. Физическая безопасность

- **Защита оборудования:** Обеспечение физической безопасности серверов, компьютеров и другого оборудования, включая контроль доступа к помещениям, где оно находится.

- **Электронные системы безопасности:** Установка систем видеонаблюдения, сигнализации и других электронных средств защиты.

6. Обеспечение непрерывности бизнеса (BCP) и планирование восстановления после катастроф (DRP)

- **BCP и DRP:** Разработка и тестирование планов обеспечения непрерывности бизнеса и восстановления после катастроф, чтобы минимизировать простои и потери данных в случае инцидентов.

Эти правила и требования направлены на создание эффективной, безопасной и надежной ИКТ-среды в организациях образования, способствующей повышению качества образования и защите данных всех участников образовательного процесса. Важно отметить, что конкретные детали и нормативные акты могут обновляться, поэтому организации образования должны следить за актуальными требованиями и рекомендациями от государственных органов и специализированных организаций.