О внесении изменений и дополнений в постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 "Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности"

Постановление Правительства Республики Казахстан от 25 февраля 2026 года № 119

Правительство Республики Казахстан ПОСТАНОВЛЯЕТ:

1. Внести в постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 "Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности" следующие изменения и дополнения:

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 3) статьи 6 Закона Республики Казахстан "Об информатизации" Правительство Республики Казахстан **ПОСТАНОВЛЯЕТ**:";

в единых требованиях в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденных указанным постановлением:

пункт 2 изложить в следующей редакции:

"2. Положения ЕТ, относящиеся к сфере обеспечения информационной безопасности, обязательны для применения государственными органами, местными исполнительными органами, государственными юридическими лицами, субъектами квазигосударственного сектора, собственниками и владельцами негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, собственниками и владельцами критически важных объектов информационно-коммуникационной инфраструктуры, а также оперативными центрами информационной безопасности.";

пункт 5 дополнить подпунктом 7) следующего содержания:

"7) определение единых принципов обеспечения и управления информационной безопасностью автоматизированных систем управления технологическими процессами.
";

пункт 6 дополнить подпунктами 41), 42), 43), 44) и 45) следующего содержания:

"41) пользователь – субъект информатизации, использующий объекты информатизации для выполнения конкретной функции и (или) задачи;

42) автоматизированная система управления технологическими процессами (далее – АСУ ТП) – объект цифровой инфраструктуры, предназначенный для автоматизации,

управления, контроля и мониторинга производственных процессов в режиме реального времени;

43) искусственный интеллект (далее – ИИ) – функциональная способность к имитации когнитивных функций, характерных для человека, обеспечивающая результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их;

44) система искусственного интеллекта – объект информатизации, функционирующий на основе одной или нескольких моделей искусственного интеллекта;

45) национальная платформа искусственного интеллекта –технологическая платформа, предназначенная для сбора, обработки, хранения и распространения библиотек данных и предоставления услуг в сфере искусственного интеллекта.";

пункт 7-1 изложить в следующей редакции:

"7-1. Платформенность основывается на выполнении следующих требований:

1) осуществление создания и развитие решений на базе технологических платформ информационно-коммуникационной инфраструктуры "электронного правительства", национальной платформы искусственного интеллекта и (или) использование функциональных возможностей технологических платформ информационно-коммуникационной инфраструктуры "электронного правительства" и национальной платформы искусственного интеллекта;

2) исключение компонентов, дублирующих функциональные возможности технологических платформ информационно-коммуникационной инфраструктуры " электронного правительства" и национальной платформы искусственного интеллекта;

3) обеспечение автоматизации процессов выполнения государственных функций и вытекающих из них услуг с использованием технологических платформ информационно-коммуникационной инфраструктуры "электронного правительства" и национальной платформы искусственного интеллекта.";

пункт 8-2 изложить в следующей редакции:

"8-2. Универсальность решений основывается на выполнении следующих требований:

1) использование готового программного обеспечения и сервисных программных продуктов, платформенных программных продуктов для автоматизации процессов выполнения типовых прикладных задач, обеспечивающих государственные функции;

2) адаптация особенностей выполнения государственных функций государственного органа к процессам, реализованным в готовом программном обеспечении и сервисных программных продуктах, платформенных программных продуктах, без необходимости настройки и доработки программного обеспечения в процессе внедрения;

3) отсутствие дополнительных затрат государственных органов на внедрение, обучение пользователей, приобретение программного обеспечения и компонентов информационно-коммуникационной инфраструктуры при использовании сервисных программных продуктов, платформенных программных продуктов.";

пункт 29 изложить в следующей редакции:

"29. При организации, обеспечении и управлении ИБ в ГО, МИО или организации необходимо руководствоваться положениями национального стандарта Республики Казахстан СТ РК ISO/IEC 27002-2023 "Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью".";

в пункте 37:

подпункт 1) изложить в следующей редакции:

"1) выбор методики оценки рисков в соответствии с рекомендациями национального стандарта Республики Казахстан СТ РК 31010-2020 "Менеджмент риска . Методы оценки риска" и разработка процедуры анализа рисков;";

подпункт 4) изложить в следующей редакции:

"4) формирование каталога угроз (рисков) ИБ, включающего оценку (переоценку) идентифицированных рисков в соответствии с требованиями национального стандарта Республики Казахстан СТ РК ISO/IEC 27005-2022 "Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности ";";

дополнить пунктом 37-1 следующего содержания:

"37-1. С целью управления рисками в сфере ИИ в ГО или МИО осуществляется управление рисками систем искусственного интеллекта в соответствии с национальным стандартом Республики Казахстан СТ РК 23894-2025 "Руководство по управлению рисками.";

пункт 44 изложить в следующей редакции:

"44. Кадровая служба организует и ведет учет прохождения служащими ГО, МИО или работниками организаций обучения в сфере информатизации и области обеспечения ИБ с выдачей электронного сертификата, обеспечением хранения в материалах личного дела.";

пункт 45 изложить в следующей редакции:

"45. При инициировании создания или развития объектов информатизации первого и второго классов в соответствии с классификатором объектов информатизации, утвержденным уполномоченным органом в сфере информатизации в соответствии с подпунктом 11) статьи 7 Закона (далее – классификатор), а также конфиденциальных ИС разрабатываются профили защиты для составных компонентов и задание по безопасности в соответствии с требованиями национального стандарта Республики Казахстан СТ РК ISO/IEC 15408-2017 "Информационные технологии. Методы и

средства обеспечения безопасности. Критерии оценки безопасности информационных технологий".";

пункт 48 изложить в следующей редакции:

"48. С целью защиты служебной информации ограниченного распространения, конфиденциальных ИС, конфиденциальных ЭИР и ЭИР, содержащих персональные данные ограниченного доступа, применяются СКЗИ (программные или аппаратные) с параметрами, соответствующими требованиям к СКЗИ в соответствии с национальным стандартом Республики Казахстан СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования" для объектов информатизации:

первого класса в соответствии с классификатором – третьего уровня безопасности;

второго класса в соответствии с классификатором – второго уровня безопасности;

третьего класса в соответствии с классификатором – первого уровня безопасности.";

пункт 50-1 изложить в следующей редакции:

"50-1. Собственники или владельцы негосударственных информационных систем, предназначенных для формирования государственных электронных информационных ресурсов, осуществления государственных функций и оказания государственных услуг, до интеграции с информационными системами государственных органов создают собственный оперативный центр информационной безопасности и обеспечивают его функционирование или приобретают услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским кодексом Республики Казахстан, а также обеспечивают взаимодействие его с Национальным координационным центром информационной безопасности.

Владельцы критически важных объектов информационно-коммуникационной инфраструктуры создают собственный оперативный центр информационной безопасности и обеспечивают его функционирование или приобретают услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским кодексом Республики Казахстан.

Собственники или владельцы критически важных объектов информационно-коммуникационной инфраструктуры, за исключением государственных органов, органов местного самоуправления, государственных юридических лиц, субъектов квазигосударственного сектора, в течение шести месяцев со дня включения в перечень критически важных объектов информационно-коммуникационной инфраструктуры создают собственный оперативный центр информационной безопасности и обеспечивают его функционирование или приобретают услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским кодексом Республики Казахстан, а также обеспечивают взаимодействие его с Национальным координационным центром информационной безопасности.";

пункт 54 изложить в следующей редакции:

"54. На этапе опытной и промышленной эксплуатации объектов информатизации используются средства защиты информации, обеспечивающие возможность:

обнаружения и предотвращения вредоносного кода;

мониторинга и управления инцидентами и событиями ИБ;

обнаружения и предотвращения вторжений;

мониторинга и управления информационной инфраструктурой.";

пункт 55 изложить в следующей редакции:

"55. Для подписания электронных документов информационная система использует регистрационные свидетельства, выданные аккредитованными удостоверяющими центрами.";

пункт 60 изложить в следующей редакции:

"60. Создание или развитие ИР осуществляются с учетом требований национальных стандартов Республики Казахстан СТ РК 2190-2012 "Информационные технологии. Интернет-ресурсы государственных органов и организаций. Требования", СТ РК 2191-2023 "Информационные технологии. Доступность веб-контента для лиц с инвалидностью", СТ РК 2192-2012 "Информационные технологии. Интернет-ресурс, интернет-портал, интранет-портал. Общие описания", СТ РК 2193-2012 " Информационные технологии. Рекомендуемая практика разработки мобильных веб-приложений", СТ РК 2199-2012 "Информационные технологии. Требования к безопасности веб-приложений в государственных органах".";

пункт 68 изложить в следующей редакции:

"68. Требования к создаваемому или развиваемому прикладному ПО ИС определяются в техническом задании, создаваемом в соответствии с требованиями национального стандарта Республики Казахстан СТ РК 34.015-2002 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы", настоящими ЕТ и правилами составления и рассмотрения технических заданий на создание и развитие объектов информатизации "электронного правительства", утверждаемыми уполномоченным органом в сфере обеспечения информационной безопасности в соответствии с пунктом 3 статьи 39 Закона.";

подпункт 1) пункта 78 изложить в следующей редакции:

"1) на этапе разработки ПО учитываются рекомендации национального стандарта Республики Казахстан СТ РК ГОСТ Р 50739-2006 "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования";";

пункт 98-1 изложить в следующей редакции:

"98-1. На информационную систему критически важных объектов ИКИ также распространяются требования национального стандарта Республики Казахстан СТ РК IEC/PAS 62443-3-2017 "Сети коммуникационные промышленные. Защищенность (

кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления.";

пункт 130 изложить в следующей редакции:

"130. В ГО или МИО допускается организация пунктов общественного доступа к Интернету для посетителей.

Организация пунктов общественного доступа допускается при условии использования отдельных каналов связи, не подключЎнных к ЕШДИ и исключающих соединения с ЕТС ГО и локальными сетями ГО или МИО.

Владелец пунктов общественного доступа обеспечивает безопасность подключения посетителей с применением технических средств защиты информации от сетевых атак, в соответствии с Правилами оказания услуг связи, утвержденными приказом исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 24 февраля 2015 года № 171 (зарегистрирован в реестре государственной регистрации нормативных правовых актов за № 10999).";

в пункте 139:

подпункт 4) изложить в следующей редакции:

"4) применяются средства:

идентификации, аутентификации и управления доступом пользователей;

идентификации оборудования;

защиты диагностических и конфигурационных портов;

физического сегментирования локальной сети;

логического сегментирования локальной сети;

управления сетевыми соединениями;

межсетевого экранирования;

сокрытия внутреннего адресного пространства локальной сети;

контроля целостности данных, сообщений и конфигураций;

криптографической защиты информации в соответствии с пунктом 48 настоящих ЕТ;

физической защиты каналов передачи данных и сетевого оборудования;

регистрации событий ИБ;

мониторинга и анализа сетевого трафика;

управления сетью;";

подпункт 10-1) изложить в следующей редакции:

"10-1) при использовании в ЛС внутреннего контура объектов информатизации, размещенных в Интернете, или ЛС внешнего контура ГО, МИО или организации, которые не подключены посредством ВШЭП, используют экранированную подсеть, соответствующую следующим требованиям:

подсеть ограничена со стороны ЛС внутреннего контура и ЛС внешнего контура отдельными межсетевыми экранами с функциями обнаружения и предотвращения

вторжений, а также преобразования внешних сетевых адресов для сокрытия адресного пространства сетей внутреннего и внешнего контура;

все подключения из ЛС внешнего контура в ЛС внутреннего контура, а также из ЛС внутреннего контура в ЛС внешнего контура осуществляются исключительно на сервер или маршрутизатор с функцией перенаправления запросов, находящийся внутри экранированной подсети, без возможности перенаправления сетевого трафика по иному маршруту, отличающемуся от изначального;

не допускаются сохранение запросов и ответов, а также свободное использование на рабочих станциях доступов к общедоступным ресурсам Интернета или ЕТС через экранированную подсеть;";

подпункт 1) пункта 148 изложить в следующей редакции:

"1) обеспечивается исполнение Правил технической эксплуатации электроустановок потребителей, утвержденных приказом Министра энергетики Республики Казахстан от 30 марта 2015 года № 246 (зарегистрирован в реестре государственной регистрации нормативных правовых актов под № 10949);";

дополнить главой 4 следующего содержания:

"Глава 4. Требования к автоматизированным системам управления технологическими процессами

Параграф 1. Требования к организации автоматизированных систем управления технологическими процессами

164. Собственники и владельцы КВОИКИ, которыми обеспечивается функционирование АСУ ТП, разрабатывают и поддерживают в актуальном состоянии перечень документов по информационной безопасности:

1. Политику информационной безопасности АСУ ТП, определяющую цели, принципы и распределение ответственности, согласованную с отраслевым центром информационной безопасности.

2. Паспорт технологической сети АСУ ТП, содержащий ее архитектурное и техническое описание.

3. Документ по анализу и оценке рисков информационной безопасности для активов АСУ ТП.

4. Карту (модель) сети АСУ ТП, классифицирующую активы (оборудование, данные, каналы связи) по уровням критичности с учетом их роли в обеспечении непрерывности технологических процессов. Карта актуализируется при изменении конфигурации сети или профиля угроз.

5. Регламенты и инструкции по информационной безопасности, включающие (но не ограничиваясь):

регламент управления доступом пользователей и учетными записями;

инструкции по обнаружению, реагированию и расследованию инцидентов информационной безопасности;

6. План обеспечения непрерывности и восстановления АСУ ТП после сбоев и аварий, который должен содержать:

установленные целевые показатели восстановления: допустимое время простоя и допустимый объем утраченных данных для критических технологических процессов и систем управления;

процедуры резервного копирования, восстановления данных и конфигураций;

порядок регулярных проверок работоспособности резервных систем и процедур восстановления;

описание взаимодействия и порядка интеграции с иными связанными информационными системами в процессе восстановления.

Указанные документы должны:

быть детализированы с учетом конкретных выявленных рисков АСУ ТП;

обеспечивать возможность их оперативного практического применения персоналом в аварийных ситуациях;

предусматривать ведение журналов аудита и мониторинга событий информационной безопасности для контроля их эффективности.

165. В целях обеспечения защиты от несанкционированного доступа собственниками или владельцами АСУ ТП реализуются:

1) идентификация и аутентификация всех пользователей и устройств;

2) использование многофакторной аутентификации (MFA) для критических систем (определяется собственником и владельцем КВОИКИ самостоятельно);

3) применение ролевой модели доступа (RBAC) с минимальными привилегиями;

4) ограничение использования в АСУ ТП учетных записей по умолчанию и общих паролей;

5) использование систем кибербезопасности для защиты промышленных сетей и систем управления;

6) ограничение доступа в серверные помещения и зоны размещения оборудования АСУ ТП.".

2. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Премьер-Министр
Республики Казахстан *О. Бектенов*