Об утверждении минимальных требований по обеспечению информационной безопасности на финансовом рынке

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 20 апреля 2026 года № 81. Зарегистрировано в Министерстве юстиции Республики Казахстан 22 апреля 2026 года № 38505

Примечание ИЗПИ!

Вводится в действие с 12.07.2026

В соответствии с подпунктом 1-1) статьи 13-6 Закона Республики Казахстан "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций" и подпунктом 86–1) пункта 14 Положения об Агентстве Республики Казахстан по регулированию и развитию финансового рынка, утвержденного Указом Президента Республики Казахстан от 11 ноября 2019 года № 203, Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые минимальные требования по обеспечению информационной безопасности на финансовом рынке.

2. Департаменту информационной и кибербезопасности в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) размещение настоящего постановления на официальном интернет-ресурсе Агентства Республики Казахстан по регулированию и развитию финансового рынка после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего постановления представление в Юридический департамент сведений об исполнении мероприятия, предусмотренного подпунктом 2) настоящего пункта.

3. Контроль за исполнением настоящего постановления возложить на курирующего заместителя Председателя Агентства Республики Казахстан по регулированию и развитию финансового рынка.

4. Настоящее постановление вводится в действие с 12 июля 2026 года и подлежит официальному опубликованию.

Председатель Агентства
Республики Казахстан
по регулированию и развитию
финансового рынка *М. Абылкасымова*

Утверждены постановлением
Правления Агентства

Республики Казахстан
по регулированию и развитию
финансового рынка
от 20 апреля 2026 года № 81

Минимальные требования по обеспечению информационной безопасности на финансовом рынке

Глава 1. Общие положения

1. Настоящие минимальные требования по обеспечению информационной безопасности на финансовом рынке (далее – Требования) разработаны в соответствии с подпунктом 1-1) статьи 13-6 Закона Республики Казахстан "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций" и подпунктом 86–1) пункта 14 Положения об Агентстве Республики Казахстан по регулированию и развитию финансового рынка, утвержденного Указом Президента Республики Казахстан от 11 ноября 2019 года № 203.

Целью Требований является регламентация основных процессов обеспечения информационной безопасности финансовых организаций, использующих в своей работе цифровые системы и (или) цифровую инфраструктуру.

2. В Требованиях используются следующие термины и определения:

1) информационная безопасность (далее – информационная безопасность) – состояние защищенности информации, от внешних и внутренних угроз, при котором обеспечены ее конфиденциальность, целостность и доступность";

2) обеспечение информационной безопасности – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информации в финансовой организации;

3) средства обработки информации – средства обработки, хранения и резервного копирования цифровых ресурсов;

4) государственная база данных изображений – база данных, принадлежащая государству, содержащая идентификационные данные физических лиц, а также соответствующие им эталонные изображения лица;

5) цифровая инфраструктура – совокупность объектов цифровой инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования цифровых ресурсов и предоставления доступа к ним;

6) периметр защиты цифровой инфраструктуры (далее – периметр защиты) – совокупность программно-аппаратных средств, отделяющих цифровую инфраструктуру финансовой организации от внешних сетей телекоммуникаций и реализующих их защиту от угроз информационной безопасности.

Глава 2. Организационные требования к обеспечению информационной безопасности

3. Руководство финансовой организации утверждает политику информационной безопасности, которая устанавливает подходы к обеспечению информационной безопасности в финансовой организации.

4. Первый руководитель финансовой организации несет персональную ответственность за обеспечение информационной безопасности финансовой организации.

5. Финансовая организация обеспечивает ознакомление нового работника с основными внутренними документами и требованиями к обеспечению информационной безопасности под подпись не позднее 5 (пяти) рабочих дней с момента приема на работу. Результат ознакомления фиксируется в соответствующем журнале инструктажа или отдельном документе, подтверждающем прохождение инструктажа, который приобщается к личному делу работника.

6. Финансовая организация обеспечивает информационную безопасность при доступе к своей цифровой инфраструктуре работников, клиентов финансовой организации, а также лиц, не являющихся работниками или клиентами финансовой организации (далее – третьи лица).

7. В заключаемых с третьими лицами соглашениях, договорах, в соответствии с которыми третьи лица получают доступ к информации и(или) цифровой инфраструктуре финансовой организации, включаются положения о соблюдении третьими лицами требований к обеспечению информационной безопасности финансовой организации.

8. Финансовая организация предоставляет в уполномоченный орган информацию о следующих выявленных инцидентах информационной безопасности:

1) эксплуатация уязвимостей в прикладном и системном программном обеспечении ;

2) несанкционированный доступ в цифровую систему;

3) атака "отказ в обслуживании" на цифровую систему или сеть передачи данных;

4) заражение сервера вредоносной программой или кодом;

5) совершение несанкционированного перевода денежных средств вследствие нарушения контролей информационной безопасности;

6) нарушение работы систем идентификации и аутентификации клиента;

7) иных инцидентах информационной безопасности, повлекших простои цифровых систем более одного часа.

Информация об инцидентах информационной безопасности, указанных в настоящем пункте, предоставляется финансовой организацией незамедлительно посредством автоматизированной системы уполномоченного органа, предназначенной для обработки информации о событиях и инцидентах информационной безопасности (

далее – АСОИ) или в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных.

В случае недоступности вышеуказанных систем передача информации об инциденте осуществляется с телефонного номера финансовой организации, указанного при регистрации финансовой организации в АСОИ, на телефонный номер уполномоченного органа, указанный для связи на интернет-ресурсе уполномоченного органа в разделе "Информационная безопасность" с дублированием на бумажном носителе официальным письмом финансовой организации.

При отсутствии подключения финансовой организации к АСОИ информация об инцидентах информационной безопасности передается на адрес электронной почты Агентства, указанный на интернет-ресурсе уполномоченного органа в разделе " Информационная безопасность".

Для юридических лиц, пятьдесят и более процентов голосующих акций которых принадлежат Национальному Банку Республики Казахстан или находятся в его доверительном управлении, допускается передача сведений об инцидентах информационной безопасности посредством объектов цифровой инфраструктуры Национального Банка Республики Казахстан, интегрированных с АСОИ.

9. Финансовая организация реализует меры физической безопасности в помещениях , в том числе организует пропускной и внутриобъектовый режим.

Глава 3. Технические требования к обеспечению информационной безопасности

10. Финансовая организация обеспечивает функционирование периметра защиты финансовой организации.

11. Телекоммуникационные соединения, выходящие за пределы периметра защиты финансовой организации, подлежат шифрованию.

12. Почтовые сервисы финансовых организаций, используемые в том числе для взаимодействия с государственными органами и гражданами Республики Казахстан, функционируют только на цифровой инфраструктуре, физически размещенной на территории Республики Казахстан (далее – казахстанские адреса электронной почты).

13. Финансовая организация публикует в общедоступных источниках информацию о своих казахстанских адресах электронной почты с пояснением, что они должны использоваться гражданами Республики Казахстан для взаимодействия с финансовой организацией.

14. Финансовая организация использует почтовые сервисы, обеспечивающие при отправке и получении электронных почтовых сообщений применение следующих защитных механизмов электронной почты: Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication Reporting & Conformance (DMARC).

15. Финансовая организация обеспечивает контроль изменения настроек и целостности конфигурационных файлов программно-аппаратных средств периметра защиты.

16. Работникам финансовой организации не предоставляются права доступа локального администратора или аналогичные права доступа, за исключением случаев, когда права доступа локального администратора или права, аналогичные правам доступа локального администратора, требуются для функционирования программного обеспечения, используемого работником для исполнения своих функциональных обязанностей.

17. Финансовая организация использует антивирусные системы или системы, контролирующие целостность и неизменность программной среды, как на серверах, так и на рабочих станциях, ноутбуках, мобильных устройствах (при наличии технической возможности) финансовой организации. При этом обеспечивается:

1) наличие лицензий, обновлений и технической поддержки;

2) обеспечение невозможности для конечного пользователя прерывания функционирования данной системы.

18. В случаях размещения финансовой организацией серверных мощностей в сторонних центрах обработки данных, использования внешних сервисов обработки и (или) хранения данных исключается возможность доступа третьих лиц к информации, передача которой третьим лицам не допускается в соответствии с гражданским, банковским законодательством Республики Казахстан, законодательством Республики Казахстан о персональных данных и их защите.

19. Резервное копирование цифровых систем и обрабатываемых в них данных обеспечивается финансовой организацией исходя из потребностей в восстановлении после сбоев в работе цифровых систем. Порядок и периодичность резервного копирования, хранения, восстановления данных, периодичность тестирования восстановления работоспособности цифровых систем из резервных копий определяется финансовой организацией во внутренних документах на основе проведенного анализа воздействия на бизнес.

Глава 4. Обеспечение безопасности при организации доступа к цифровым системам

20. Требования настоящей главы применяются к цифровым системам, используемым финансовой организацией для обработки, хранения или передачи информации, подлежащей защите в соответствии с законодательством Республики Казахстан, либо отнесенным к критичным по результатам оценки рисков информационной безопасности, проведенной в соответствии с требованиями уполномоченного органа.

Финансовая организация составляет перечень цифровых систем, отнесенных к сфере применения требований настоящей главы (далее - Перечень).

21. Доступ работников финансовой организации, третьих лиц, с которыми у финансовой организации заключены договорные отношения, (далее – пользователь) или клиентов финансовой организации (далее – клиент) к цифровым системам финансовой организации осуществляется по результатам процедуры идентификации и аутентификации, за исключением цифровых систем, по которым внутренним документом финансовой организации утвержден иной порядок доступа с обоснованием его целесообразности и безопасности.

22. В цифровых системах финансовой организации используется функция ведения аудиторского следа, которая отражает как минимум:

1) события установления соединений, идентификации, аутентификации и авторизации (успешные и неуспешные), включая IP-адрес источника соединения;

2) события модификации настроек безопасности;

3) события модификации групп пользователей и их полномочий;

4) события модификации учетных записей пользователей и их полномочий;

5) события, отражающие установку обновлений и (или) изменений;

6) события изменения параметров ведения аудиторского следа.

23. При хранении аудиторского следа обеспечивается контроль его неизменности. Срок хранения аудиторского следа составляет не менее 3 (трех) месяцев в оперативном доступе и не менее 1 (одного) года в архивном доступе, либо не менее 1 (одного) года в оперативном доступе.

24. В целях обеспечения контроля деятельности пользователей и клиентов ведется аудиторский след действий их учетных записей в цифровых системах финансовой организации.

25. Идентификация и аутентификация пользователя или клиента осуществляется при помощи одного или нескольких факторов, включая знание, владение или неотъемлемость. Фактор знания основывается на информации, которую должен знать пользователь или клиент. Фактор владения основывается на владении пользователя или клиента определенным физическим устройством или криптографическим ключом. Фактор неотъемлемости основывается на уникальных биометрических особенностях пользователя или клиента.

26. Доступ пользователей и клиентов извне периметра защиты финансовой организации к цифровым системам осуществляется с применением как минимум двух различных факторов аутентификации.

27. Доступ работника финансовой организации к цифровым системам осуществляется в соответствии с внутренними документами финансовой организации при наличии утвержденных документов финансовой организации, подтверждающих необходимость такого доступа для исполнения обязанностей работника.

28. Доступ третьих лиц к цифровым системам осуществляется в соответствии с внутренними документами финансовой организации при наличии действующего

договора, предусматривающего необходимость такого доступа третьим лицам к цифровым системам финансовой организации.

29. Идентификация и аутентификация клиента финансовой организации осуществляется в соответствии с внутренними документами финансовой организации на основании данных, полученных при регистрации клиента финансовой организации.

30. Регистрация клиента в цифровых системах финансовой организации осуществляется в соответствии с внутренними документами финансовой организации после подтверждения личности клиента. Для дистанционного подтверждения личности при регистрации применяется комбинация как минимум из следующих проверок:

1) биометрическая проверка клиента по изображению лица с использованием государственной базы данных изображений или по биометрическим данным, полученным при личном присутствии клиента посредством специально предназначенных для этого устройств финансовой организации;

2) проверка владения телефонным номером, зарегистрированным в государственной базе номеров мобильных телефонов граждан, либо проверка владения закрытым ключом сертификата электронной цифровой подписи, выпущенного аккредитованным удостоверяющим центром.

31. В целях последующей идентификации и аутентификации клиента в ходе регистрации допускается сбор следующих данных:

1) пароль, задаваемый клиентом;

2) вектор инициализации, серийный номер или иная информация, необходимая для подключения аппаратного или программного генератора одноразовых паролей (OTP-генератора);

3) уникальный идентификатор установки мобильного приложения на мобильное устройство, а также индивидуальные характеристики мобильного устройства;

4) сертификат электронной цифровой подписи, соответствующий закрытому ключу, хранимому на устройстве клиента;

5) дополнительный номер мобильного телефона, владение клиента которым подтверждено;

6) биометрические данные клиента, проверенные посредством государственной базы данных изображений или полученные посредством устройств финансовой организации;

7) открытый криптографический ключ, соответствующий закрытому криптографическому ключу, хранимому на устройстве клиента.

32. Проверка владения мобильным телефонным номером осуществляется путем отправки на проверяемый мобильный телефонный номер сгенерированного непредсказуемого кода с последующим получением данного кода от владельца мобильного телефонного номера аутентифицирующей системой.

33. Проверка владения закрытым ключом сертификата электронной цифровой подписи осуществляется в соответствии с правилами аккредитованного удостоверяющего центра, выпустившего данный сертификат электронной цифровой подписи.