Об утверждении Правил и сроков предоставления банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, информации об уязвимостях в информационно-коммуникационной инфраструктуре, полученной в том числе от третьих сторон, а также о событиях и инцидентах информационной безопасности, включая сведения о нарушениях и сбоях в информационных системах

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 31 марта 2026 года № 37. Зарегистрировано в Министерстве юстиции Республики Казахстан 3 апреля 2026 года № 38302

В соответствии с пунктами 5 и 10 статьи 55 Закона Республики Казахстан "О банках и банковской деятельности в Республике Казахстан" Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые Правила и сроки предоставления банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, информации об уязвимостях в информационно-коммуникационной инфраструктуре, полученной в том числе от третьих сторон, а также о событиях и инцидентах информационной безопасности, включая сведения о нарушениях и сбоях в информационных системах.

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 по истечении десяти календарных дней после дня его первого официального опубликования.

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 31 марта 2026 года
№ 37

Правила и сроки предоставления банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, информации об уязвимостях в информационно-коммуникационной инфраструктуре, полученной в том числе от третьих сторон, а также о событиях и инцидентах информационной безопасности, включая сведения о нарушениях и сбоях в информационных системах

1. Настоящие Правила и сроки предоставления банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, информации об уязвимостях в информационно-коммуникационной инфраструктуре, полученной в том числе от третьих сторон, а также о событиях и инцидентах информационной безопасности, включая сведения о нарушениях и сбоях в информационных системах (далее – Правила) разработаны в соответствии с пунктами 5 и 10 статьи 55 Закона Республики Казахстан "О банках и банковской деятельности в Республике Казахстан" и определяют порядок и сроки предоставления банками, филиалами банков-нерезидентов Республики Казахстан (далее – банк) и организациями, осуществляющими отдельные виды банковских операций (далее – организация), информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах.

2. В Правилах используются понятия, предусмотренные Законом Республики Казахстан "Об информатизации", а также следующие понятия:

1) информационная безопасность в сфере информатизации (далее – информационная безопасность) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

2) информационно-коммуникационная инфраструктура (далее – информационная инфраструктура) – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

3) угроза информационной безопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

4) инцидент информационной безопасности – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее

объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов банка, организации;

5) периметр защиты информационно-коммуникационной инфраструктуры – совокупность программно-аппаратных средств, отделяющих информационно-коммуникационную инфраструктуру банка, организации от внешних информационных сетей и реализующих защиту от угроз информационной безопасности;

6) доступ – возможность использования информационных активов;

7) атака типа "отказ в обслуживании" – атака на информационную систему с целью нарушения штатного режима ее работы или создание условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым ресурсам, либо этот доступ затруднен;

8) уязвимость – недостаток объекта информатизации, использование которого может привести к нарушению целостности и (или) конфиденциальности, и (или) доступности объекта информатизации;

9) уполномоченный орган – уполномоченный орган по регулированию, контролю и надзору финансового рынка и финансовых организаций.

3. Банк, организация предоставляют в уполномоченный орган информацию о следующих выявленных инцидентах информационной безопасности:

1) эксплуатация уязвимостей в прикладном и системном программном обеспечении ;

2) несанкционированный доступ в информационную систему;

3) атака "отказ в обслуживании" на информационную 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 банковских систем идентификации и аутентификации клиента ;

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

Информация об инцидентах информационной безопасности, указанных в настоящем пункте, предоставляется банком или организацией в течение двадцати четырех часов с момента выявления инцидента, посредством автоматизированной системы уполномоченного органа, предназначенной для обработки информации о событиях и инцидентах информационной безопасности (далее – АСОИ) и интегрированной с системами информационной безопасности или системами банка, организации, осуществляющими в реальном времени сбор и анализ информации о

событиях в информационной инфраструктуре 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 банка, организации, указанного при регистрации банка, 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 банка, организации.

4. Банк, организация обеспечивают передачу сведений об отдельно или серийно возникающих событиях в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, включая системы информационной безопасности, свидетельствующих о нарушении принятых мер обеспечения информационной безопасности либо о ситуации, потенциально имеющей отношение к информационной безопасности (далее – сведения о нарушениях, сбоях в информационных системах) посредством АСОИ. Сведения о нарушениях, сбоях в информационных системах предоставляются в автоматизированном режиме путем передачи из систем информационной безопасности или систем банка, организации, осуществляющих в реальном времени сбор и анализ информации о событиях в информационной инфраструктуре банка, организации.

Для организаций, входящих в структуру Национального Банка Республики Казахстан, и юридических лиц, пятьдесят и более процентов голосующих акций которых принадлежат Национальному Банку Республики Казахстан, допускается передача сведений о нарушениях, сбоях в информационных системах посредством объектов информатизации Национального Банка Республики Казахстан, интегрированных с АСОИ.

5. Банк, организация обеспечивает передачу сведений посредством АСОИ о полученных в том числе от третьих сторон уязвимостях в информационно-коммуникационной инфраструктуре банка, организации, доступных извне периметра защиты, в течение двадцати четырех часов с момента их выявления. Для организаций, входящих в структуру Национального Банка Республики Казахстан, и юридических лиц, пятьдесят и более процентов голосующих акций которых принадлежат Национальному Банку Республики Казахстан, допускается передача сведений об уязвимостях посредством цифровых систем Национального Банка Республики Казахстан, интегрированных с АСОИ.