О внесении изменений и дополнений в некоторые нормативные правовые акты Республики Казахстан по вопросам информационной безопасности

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 20 августа 2025 года № 38. Зарегистрировано в Министерстве юстиции Республики Казахстан 28 августа 2025 года № 36711.

Примечание ИЗПИ!

Порядок введения в действие см. п. 4.

Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Утвердить Перечень нормативных правовых актов Республики Казахстан по вопросам информационной безопасности, в которые вносятся изменения и дополнения, согласно приложению к настоящему постановлению (далее - Перечень).

2. Департаменту информационной и кибербезопасности Агентства Республики Казахстан по регулированию и развитию финансового рынка 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, за исключением пункта 1 Перечня, который вводится в действие с 1 ноября 2025 года.

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

Приложение к постановлению
Правления Агентства
Республики Казахстан
по регулированию и развитию

финансового рынка
от 20 августа 2025 года № 38

Перечень нормативных правовых актов Республики Казахстан по вопросам информационной безопасности, в которые вносятся изменения и дополнения

1. Внести в постановление Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 "Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 16772) следующие изменения и дополнения:

преамбулу изложить в следующей редакции:

"В соответствии с пунктом 7 статьи 61-5 Закона Республики Казахстан "О банках и банковской деятельности в Республике Казахстан" Правление Национального Банка Республики Казахстан **ПОСТАНОВЛЯЕТ:**";

в Требованиях к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, утвержденных указанным постановлением:

подпункт 21) пункта 2 изложить в следующей редакции:

"21) центр обработки данных банка, организации – специально выделенное помещение, в котором размещены серверы, обеспечивающие работу информационных систем банка, организации;";

пункт 15 изложить в следующей редакции:

"15. Банк, организация определяют возможность возложения на подразделение по информационной безопасности функций по обеспечению технической безопасности. Подразделение по информационной безопасности не осуществляет функции, влекущие конфликт интересов с их основными функциями, в том числе предусмотренные главой 15 Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан, утвержденных постановлением Правления Национального Банка Республики Казахстан от 12 ноября 2019 года № 188, зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 19632.";

пункт 29 изложить в следующей редакции:

"29. Информация о СУИБ составляется в произвольной форме и представляется в уполномоченный орган в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых

данных, или посредством автоматизированной системы уполномоченного органа, предназначенной для обработки информации о событиях и инцидентах информационной безопасности или на бумажном носителе.";

дополнить пунктом 31-1 следующего содержания:

"31-1. Банк, организация проводят внешнюю проверку состояния системы управления информационной безопасностью банка, организации в объеме, определяемом исполнительным органом банка, организации, на соответствие национальному стандарту Республики Казахстан СТ ISO/IEC 27001-2023 " Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования" или международному стандарту ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection – Information security management systems - Requirements" (Информэйшн секьюрити, сайберсекьюрити энд прайвэси протекшн. Информэйшн секьюрити мэнэджмент системс - Реквайрментс) (Информационная безопасность, кибербезопасность и защита частной жизни - Системы менеджмента информационной безопасности - Требования) не реже одного раза в 3 (три) года.";

пункт 89 изложить в следующей редакции:

"89. С периодичностью, определяемой банком, организацией, проводится тестирование на проникновение в информационную инфраструктуру независимыми внешними экспертами в данной области. В рамках данного тестирования, кроме поиска и попыток эксплуатации уязвимостей системного и прикладного программного обеспечения, проводятся нагрузочные тесты, включая имитацию атак "отказ в обслуживании".";

подпункт 1) пункта 108 изложить в следующей редакции:

"1) методы обеспечения информационной безопасности;";

дополнить пунктом 156-1 следующего содержания:

"156-1. При аутентификации клиента в мобильном приложении на ранее не зарегистрированном за клиентом в банке, организации мобильном устройстве банк, организация проводят биометрическую идентификацию клиента с использованием биометрических данных, подтвержденных ЦОИД или полученных посредством устройств банка, организации.";

пункты 160 и 161 изложить в следующей редакции:

"160. Мобильное приложение обеспечивает:

1) однозначность идентификации принадлежности мобильного приложения банку, организации (данные в официальном магазине приложений, логотипы, корпоративные цвета);

2) блокировку функционала по оказанию дистанционных услуг банка, организации в случае обнаружения признаков нарушения целостности и (или) обхода защитных механизмов операционной системы, обнаружения процессов удаленного управления;

3) уведомление клиента о наличии обновлений мобильного приложения;

4) возможность принудительной установки обновлений мобильного приложения или блокировки функционала мобильного приложения до их установки в случаях необходимости устранения критичных уязвимостей;

5) хранение конфиденциальных данных в защищенном контейнере мобильного приложения или хранилище системных учетных данных;

6) исключение кэширования конфиденциальных данных;

7) исключение из резервных копий мобильного приложения конфиденциальных данных в открытом виде;

8) информирование клиента о методах обеспечения кибергигиены, которым рекомендуется следовать при использовании мобильного приложения;

9) информирование клиента о событиях авторизации под его учетной записью, изменения и (или) восстановления пароля, изменения, зарегистрированного банком, организацией номера мобильного телефона;

10) в ходе осуществления операций с денежными средствами - передачу в серверное ППО банка, организации геолокационных данных мобильного устройства при наличии разрешения от клиента либо передачу информации об отсутствии такого разрешения;

11) блокировку функционала по осуществлению операций с денежными средствами в случае обнаружения активного доступа к микрофону мобильного устройства в порядке, определяемом банком, организацией, при наличии разрешения от клиента либо передачу в серверное ППО банка, организации информации об отсутствии такого разрешения.

161. Банк, организация обеспечивают на своей стороне:

1) обработку ошибок и исключений безопасным способом, не допуская в ответе раскрытия конфиденциальных данных, предоставляя минимально достаточную информацию для диагностики проблемы;

2) идентификацию и аутентификацию мобильных приложений и связанных с ними устройств;

3) проверку данных на валидность для предотвращения атак с подделкой запросов и инъекций вредоносного кода;

4) хранение записей событий обнаружения процессов удаленного управления и признаков нарушения целостности и (или) обхода защитных механизмов операционной системы в мобильных приложениях клиентов на устройствах, зарегистрированных в банке, организации, а также действий по блокировке функционала мобильных приложений клиентов;

5) хранение записей о неудачных попытках аутентификации и об информировании клиентов об этих попытках.";

в Правилах и сроках предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах, утвержденных указанным постановлением:

пункт 3 изложить в следующей редакции:

"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 незамедлительно 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.".

2. Утратил силу постановлением Правления Агентства РК по регулированию и развитию финансового рынка от 03.04.2026 № 54 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

3. Внести в постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 12 сентября 2022 года № 67 "Об

утверждении Правил подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности, используемого отраслевым центром информационной безопасности финансового рынка и финансовых организаций" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 29639) следующее изменение:

Правила подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности, используемого отраслевым центром информационной безопасности финансового рынка и финансовых организаций, утвержденные указанным постановлением, изложить в редакции согласно приложению к Перечню нормативных правовых актов Республики Казахстан по вопросам информационной безопасности, в которые вносятся изменения и дополнения.

Приложение к Перечню
нормативных правовых актов
Республики Казахстан
по вопросам информационной
безопасности, в которые вносятся
изменения и дополнения

Приложение к постановлению
Правления Агентства
Республики Казахстан
по регулированию и развитию
финансового рынка
от 12 сентября 2022 года № 67

Правила подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности, используемого отраслевым центром информационной безопасности финансового рынка и финансовых организаций

Глава 1. Общие положения

1. Настоящие Правила подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности, используемого отраслевым центром информационной безопасности финансового рынка и финансовых организаций (далее – Правила) разработаны в соответствии с пунктом 4 статьи 7-5 Закона Республики Казахстан "Об информатизации" (далее – Закон об информатизации) и определяют порядок подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и

инцидентам информационной безопасности (далее – ИБ), используемого отраслевым центром информационной безопасности финансового рынка и финансовых организаций.

2. Объектом информатизации отраслевого центра информационной безопасности финансового рынка и финансовых организаций по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности является автоматизированная система обработки информации по событиям и инцидентам информационной безопасности уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций (далее - АСОИ).

3. В Правилах используются понятия, предусмотренные Законом об информатизации, а также следующие понятия:

1) ответственный работник – работник организации, в должностных обязанностях которого закреплена обработка информации в АСОИ;

2) профиль финансовой организации – структурированная информация о финансовой организации в АСОИ;

3) предупреждение об угрозе – уведомление по критичным событиям ИБ для всех финансовых организаций;

4) карта инцидента – структурированная информация об инциденте ИБ у финансовой организации, предоставляемая в уполномоченный орган в соответствии с Правилами;

5) предупреждение об уязвимости – уведомление о выявлении уязвимостей у производителей программного обеспечения и оборудования, используемого в инфраструктуре субъектов финансового рынка;

6) сигнал – структурированная информация о событии ИБ, получаемая из систем ИБ или систем, осуществляющих в реальном времени сбор и анализ информации о событиях ИБ в информационной инфраструктуре финансовой организации;

7) запрос – официальное обращение финансовых организаций друг к другу или к уполномоченному органу по регулированию, контролю и надзору финансового рынка и финансовых организаций (далее – уполномоченный орган) по вопросам обеспечения ИБ, реализованное средствами АСОИ, обеспечивающими защиту информации;

8) модуль интеграции – программное обеспечение, устанавливаемое в инфраструктуре финансовой организации для автоматизации передачи информации по событиям ИБ в инфраструктуре финансовой организации в АСОИ.

4. При использовании АСОИ соблюдаются требования Закона об информатизации, законов Республики Казахстан "О персональных данных и их защите", "О банках и банковской деятельности в Республике Казахстан" по обеспечению безопасности защищаемой информации.

Глава 2. Подключение к АСОИ

5. К АСОИ подключается подразделение информационной безопасности финансовой организации, а также оперативный центр информационной безопасности финансовой организации (далее - ОЦИБ) при его наличии. Для создания профиля финансовой организации и ОЦИБ в АСОИ ответственный работник представляет в отраслевой центр ИБ следующие учетные данные финансовой организации:

1) наименование финансовой организации и ОЦИБ;

2) бизнес-идентификационный номер юридического лица;

3) адрес электронной почты.

6. Для создания учетной записи пользователя финансовой организации и ОЦИБ в АСОИ ответственный работник представляет в отраслевой центр ИБ следующие учетные данные пользователя:

1) фамилия, имя, отчество (при наличии);

2) должность;

3) наименование организации;

4) контактные телефоны;

5) адрес электронной почты.

7. Для передачи сигналов в АСОИ банки, филиалы банков-нерезидентов Республики Казахстан (далее - банки), организации, осуществляющие отдельные виды банковских операций (далее - организации) и (или) ОЦИБ осуществляют установку модуля интеграции, предоставленного отраслевым центром ИБ, в инфраструктуре банка, организации, ОЦИБ с его подключением к системам ИБ или системам, осуществляющим в реальном времени сбор и анализ информации о событиях ИБ в информационной инфраструктуре банка, организации.

8. Сигналы передаются банками, организациями, ОЦИБ в АСОИ в случае выявления следующих событий ИБ:

1) выявление вредоносной активности IPS/IDS (система обнаружения и предотвращения вторжений);

2) выявление вредоносной активности WAF (сетевой фильтр веб-приложений);

3) выявление вредоносной активности системой защиты конечных точек;

4) получение вредоносного кода;

5) получение фишингового сообщения;

6) сетевое сканирование IP-адресов на предмет выявления активных сетевых служб;

7) перебор пароля к учетной записи (на внешнем периметре);

8) перебор учетных записей к паролю (на внешнем периметре).

9. Банк, организация обеспечивает интернет-канал для связи модуля интеграции с АСОИ.

Глава 3. Использование АСОИ

10. При обнаружении угрозы ИБ для финансового рынка Республики Казахстан ответственный работник финансовой организации или ОЦИБ по согласованию с руководством подразделения ИБ создает предупреждение об угрозе в АСОИ путем введения следующих данных:

1) источник;

2) тип угрозы;

3) степень угрозы;

4) степень конфиденциальности;

5) описание угрозы;

6) рекомендации.

11. При необходимости получения дополнительной информации для обеспечения функционирования системы управления ИБ финансовой организации ответственный работник финансовой организации или ОЦИБ по согласованию с руководством подразделения ИБ создает запрос в АСОИ уполномоченному органу или финансовым организациям.

12. Ответственный работник банка, организации или ОЦИБ по согласованию с руководством подразделения ИБ незамедлительно создает в АСОИ карту инцидента в случае выявления следующих инцидентов ИБ:

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 ИБ;

6) нарушение работы банковских систем идентификации и аутентификации клиента ;

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

13. При получении предупреждения об угрозе или уязвимости ответственный работник финансовой организации или ОЦИБ по согласованию с руководством подразделения ИБ в течение 1 (одного) рабочего дня принимает или отклоняет применение рекомендаций из предупреждения, и отражает это в АСОИ.

После завершения применения рекомендаций ответственный работник финансовой организации или ОЦИБ изменяет статус предупреждения в АСОИ на обработано.

14. При получении запроса в АСОИ ответственный работник финансовой организации или ОЦИБ по согласованию с руководством подразделения ИБ в течение 1 (одного) рабочего дня принимает его в работу или отклоняет, и отражает это в

комментариях к запросу. Не позднее 10 (десять) рабочих дней после завершения работы по запросу ответственный работник финансовой организации или ОЦИБ по согласованию с руководством подразделения ИБ формирует ответ в АСОИ.

15. Ответственный работник финансовой организации или ОЦИБ при возврате отраслевым центром ИБ в АСОИ предупреждения об угрозе, карты инцидента или ответа на запрос из-за неполноты предоставленных данных устраняет недостатки в течение 3 (трех) рабочих дней.