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

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 12 сентября 2022 года № 67. Зарегистрировано в Министерстве юстиции Республики Казахстан 16 сентября 2022 года № 29639.

В соответствии с пунктом 4 статьи 7-5 Закона Республики Казахстан "Об информатизации" Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые 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.

2. Управлению 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*

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

Сноска. Правила - в редакции приказа Правления Агентства РК регулированию и развитию финансового рынка от 20.08.2025 № 38 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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.