О внесении изменений в постановление Правления Национального Банка Республики Казахстан от 28 декабря 2018 года № 318 "Об утверждении Правил формирования системы управления рисками и внутреннего контроля для центрального депозитария"

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 30 мая 2022 года № 40. Зарегистрировано в Министерстве юстиции Республики Казахстан 7 июня 2022 года № 28402

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

1. Внести в постановление Правления Национального Банка Республики Казахстан от 28 декабря 2018 года № 318 "Об утверждении Правил формирования системы управления рисками и внутреннего контроля для центрального депозитария" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов Республики Казахстан под № 18180) следующие изменения:

в Правилах формирования системы управления рисками и внутреннего контроля для центрального депозитария, утвержденных указанным постановлением:

в Требованиях к внутренним документам системы управления рисками и внутреннего контроля согласно приложению 5:

пункт 1 изложить в следующей редакции:

"1. Система управления рисками центрального депозитария предусматривает, но не ограничивается наличием следующих внутренних документов:

1) политика центрального депозитария по управлению рисками;

2) порядок инвестирования собственных активов центрального депозитария;

3) процедуры осуществления внутреннего контроля и внутреннего аудита;

4) процедуры, направленные на противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

5) процедуры управления существующими и потенциальными конфликтами интересов в центральном депозитарии;

6) процедуры обеспечения сохранности сведений, составляющих коммерческую и (или) иную охраняемую законами Республики Казахстан тайну (далее - конфиденциальная информация), направленные на предотвращение их использования в собственных интересах центрального депозитария, его работников или третьих лиц;

7) процедуры осуществления клиринга по сделкам с финансовыми инструментами;

8) процедуры мониторинга и контроля эмитентов и держателей ценных бумаг на предмет соответствия требованиям законодательства Республики Казахстан о рынке

ценных бумаг, регламентирующего порядок их деятельности по выпуску, размещению и обращению ценных бумаг, и внутренним документам центрального депозитария;

9) информационная политика центрального депозитария;

10) инструкция по технике безопасности;

11) документация по обеспечению информационной безопасности;

12) процедуры, направленные на предотвращение несвоевременности исполнения и (или) неисполнения приказов клиентов, эмитентов и (или) держателей ценных бумаг, а также ошибочного ввода данных в систему учета центрального депозитария, систему реестров сделок с производными финансовыми инструментами, заключенных на организованном и неорганизованном рынках ценных бумаг;

13) процедуры по оптимизации эффективности существующего контроля операционных процессов центрального депозитария;

14) процедуры составления и раскрытия информации в процессе осуществления деятельности центрального депозитария;

15) требования к резервному техническому центру;

16) требования к помещению для хранения архивных документов центрального депозитария, составляющих систему реестров держателей ценных бумаг;

17) порядок функционирования системы управленческой информации;

18) иные документы, установленные советом директоров центрального депозитария .";

пункт 16 изложить в следующей редакции:

"16. Документация по обеспечению информационной безопасности определяет:

1) политику информационной безопасности центрального депозитария;

2) перечень информации, подлежащей защите и включающий, в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну (далее – защищаемая информация);

3) порядок работы с защищаемой информацией;

4) перечень информационных систем, обрабатывающих защищаемую информацию;

5) требования к обеспечению информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем, обрабатывающих защищаемую информацию;

6) порядок управления доступом к информационным системам, обрабатывающим защищаемую информацию;

7) порядок резервного копирования, хранения, восстановления, тестирования работоспособности резервных копий информационных систем, обрабатывающих защищаемую информацию;

8) порядок обеспечения антивирусной защиты информационной инфраструктуры центрального депозитария;

9) перечень разрешенного к использованию в центральном депозитарии программного обеспечения;

10) периодичность и правила мониторинга отдельно или серийно возникающих событий в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, включая системы информационной безопасности, свидетельствующих о нарушении принятых мер обеспечения информационной безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к информационной безопасности (далее - события информационной безопасности);

11) перечень событий информационной безопасности, подлежащих мониторингу;

12) перечень источников событий информационной безопасности;

13) порядок обработки отдельно или серийно возникающих сбоев в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающих угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования защищаемой информации (далее - инциденты информационной безопасности);

14) порядок отнесения событий информационной безопасности к инцидентам информационной безопасности;

15) порядок доступа лиц, не являющихся работниками центрального депозитария, к информационным системам, обрабатывающим защищаемую информацию;

16) порядок защиты информации при использовании Интернета и электронной почты;

17) порядок управления обновлениями информационных систем.";

пункт 18 изложить в следующей редакции:

"18. Процедуры по оптимизации эффективности существующего контроля операционных процессов центрального депозитария определяют:

1) риски, связанные с осуществлением действий на основе первичных документов:

представление первичных документов неуполномоченным лицом;

кража, подмена или утеря первичных документов;

ввод несуществующего приказа в информационную систему, системы учета и реестров;

двойной ввод данных одного и того же приказа разными работниками в информационную систему, системы учета и реестров;

некорректный ввод данных приказа в информационную систему, системы учета и реестров;

невыполнение ввода приказа в информационную систему, системы учета и реестров
;

несвоевременный ввод приказа в информационную систему, системы учета и реестров;

выбор некорректного статуса приказа в информационной системе, системе учета центрального депозитария;

невнесение изменения в статус приказа в информационной системе, системах учета и реестров;

изменение статуса приказа в информационной системе, системах учета и реестров, не подлежавшего изменению;

изменение данных справочников в информационной системе, системах учета и реестров, не подлежавших изменению;

некорректное изменение данных справочников в информационной системе, системах учета и реестров;

невнесение изменения в данные справочников в информационной системе, системах учета и реестров;

изменение данных справочников в информационной системе, системах учета и реестров без соответствующего документа;

несвоевременное изменение данных справочников в информационной системе, системах учета и реестров;

2) риски, связанные с выдачей отчетных и иных документов на основе первичных документов:

невыполнение формирования отчетного документа;

несвоевременное формирование отчетного документа;

некорректные данные в отчетном документе;

формирование отчета об исполнении с указанием неправильного статуса приказа;

выдача отчетного документа неуполномоченному лицу;

кража, подмена и утеря отчетных документов;

3) риски, связанные с использование информационных систем:

невыполнение процедур открытия (закрытия) операционного дня;

невыполнение включения терминала фондовой биржи;

некорректный формат входящего файла;

некорректное содержание входящего файла;

двойной ввод данных разными работниками для формирования записи в базе данных;

невыполнение формирования записи в базе данных;

некорректное формирование записи в базе данных;

повтор документов от отправителя в информационной системе (в течение операционного дня);

постановка приказа в очередь с отложенной датой расчетов;

ошибки при проведении транзакций в информационной системе;

исполнение приказа без встречного приказа (по сделкам, которые регистрируются на основании двух встречных приказов);

исполнение приказа по ценным бумагам, не находящимся в обращении;
исполнение приказа во время, не входящее в регламент;
прием приказа во время, не входящее в регламент;
исполнение приказа в момент не открытого операционного дня;
исполнение приказа в момент приостановления операций с ценными бумагами;
исполнение приказа на неразрешенные операции;
4) риски, связанные с эксплуатацией информационных систем:
заражение компьютерными вирусами;
использование нелицензионных программ;
неавторизованный доступ к информационным системам;
ошибка при техническом обслуживании серверного оборудования;
сбой в системе электропитания;
сбой систем кондиционирования серверов;
технический сбой серверного оборудования;
технический сбой сетевого оборудования;
кража, преднамеренная порча носителей данных (жестких дисков и иных носителей);
неавторизованный доступ к носителям данных (жестким дискам и иным носителям) ;
чрезвычайная ситуация природного характера;
пожар в серверной комнате;
затопление серверной комнаты;
программный сбой в информационной системе;
отсутствие формализованного требования заказчика по разработке программного обеспечения;
некорректное составление технического задания для кодировщиков программного обеспечения;
ошибка при написании кода программного обеспечения;
ошибка при внедрении разработанного программного обеспечения;
ошибка при разработке и (или) внедрении программного обеспечения.".
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*