Об утверждении Требований к автоматизированным информационным системам для учета пенсионных активов и накоплений

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 26 июня 2023 года № 60. Зарегистрировано в Министерстве юстиции Республики Казахстан 1 июля 2023 года № 33017

Примечание ИЗПИ!

Вводится в действие с 01.07.2023

В соответствии с пунктом 5 статьи 57 Социального кодекса Республики Казахстан Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Утвердить Требования к автоматизированным информационным системам для учета пенсионных активов и накоплений согласно приложению 1 к настоящему постановлению.

2. Признать утратившими силу нормативный правовой акт Республики Казахстан, а также отдельные структурные элементы некоторых нормативных правовых актов Республики Казахстан по перечню согласно приложению 2 к настоящему постановлению.

3. Департаменту рынка ценных бумаг 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.

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

5. Настоящее постановление вводится в действие с 1 июля 2023 года и подлежит официальному опубликованию.

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

Приложение 1 к постановлению
Правления Агентства
Республики Казахстан
по регулированию и развитию
финансового рынка
от 26 июня 2023 года № 60

Требования к автоматизированным информационным системам для учета пенсионных активов и накоплений

Глава 1. Общие положения

1. Настоящие Требования к автоматизированным информационным системам для учета пенсионных активов и накоплений (далее - Требования) разработаны в соответствии с пунктом 5 статьи 57 Социального кодекса Республики Казахстан (далее – Социальный кодекс) и устанавливают требования к автоматизированным информационным системам единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда для учета пенсионных активов и накоплений.

2. В Требованиях используются следующие понятия:

1) автоматизированные информационные системы – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

2) администратор автоматизированной информационной системы (далее - администратор) – сотрудник единого накопительного пенсионного фонда или добровольного накопительного пенсионного фонда, обеспечивающий функционирование, настройку, поддержку и сопровождение технических средств автоматизированной информационной системы и участвующий в информационном процессе с помощью аппаратно-программных средств;

3) раскрытие информации (данных, программного обеспечения, информационных сообщений) – действие, происходящее в результате получения несанкционированного доступа к информации и возможного раскрытия полученных сведений;

4) защита информации – комплекс мероприятий, обеспечивающих информационную безопасность в сфере информатизации (далее – информационная безопасность);

5) аутентификация – подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа имеющимся в системе;

6) вредоносное программное обеспечение – программное обеспечение, создаваемое с целью причинения вреда информационным системам и информационным ресурсам;

7) идентификатор – уникальный персональный код или имя, присвоенный(-ое) субъекту и (или) объекту системы и предназначенный(-ое) для регламентированного доступа в систему и (или) к ресурсам системы;

8) идентификация – присвоение или определение соответствия предъявленного для получения доступа в систему и (или) к ресурсу системы идентификатора перечню идентификаторов, имеющихся в системе;

9) администратор безопасности – сотрудник единого накопительного пенсионного фонда или добровольного накопительного пенсионного фонда, обеспечивающий реализацию мер по защите информационных систем, технических средств, а также поддержание системы в рамках политики безопасности;

10) система безопасности – комплекс организационных мер и программно-технических средств защиты информации;

11) политика безопасности – нормы и практические приемы, регулирующие управление, защиту и распределение информации ограниченного распространения, которые определяют общие направления работы в области информационной безопасности и требования к защите автоматизированной информационной системы;

12) специализированная организация – организация, предоставляющая телекоммуникационные услуги и услуги хранения и обработки данных;

13) серверное помещение – помещение, предназначенное для размещения серверного, активного и пассивного сетевого (телекоммуникационного) оборудования (телекоммуникационного) и оборудования структурированных кабельных систем.

Глава 2. Требования к автоматизированным информационным системам для учета пенсионных активов и накоплений

3. Автоматизированные информационные системы единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда для учета пенсионных активов и накоплений обеспечивают:

1) надежное хранение информации, защиту от несанкционированного доступа, целостность программного обеспечения и полную сохранность информации в электронных архивах и базах данных при:

полном или частичном отключении электропитания в любое время;

аварии сетей, телекоммуникаций, разрыве установленных физических и виртуальных соединений на любом этапе выполнения операции;

полном или частичном отказе любых вычислительных средств программного обеспечения в процессе выполнения любой функции программного обеспечения;

попытке несанкционированного доступа к информации, хранящейся в автоматизированных информационных системах;

2) многоуровневый доступ к данным, функциям, операциям, отчетам, реализованным в автоматизированных информационных системах, с обеспечением, как минимум, двух уровней доступа: администратор и пользователь;

3) контроль полноты вводимых данных (при выполнении функций или операций без полного заполнения всех полей автоматизированная информационная система обеспечивает выдачу соответствующего уведомления);

4) поиск информации по индивидуальному запросу и по любым критериям с сохранением запроса, а также сортировку информации по любым параметрам и возможность просмотра информации за предыдущие даты;

5) обработку и хранение информации по датам без сокращений;

6) возможность архивации (восстановление данных из архива);

7) возможность вывода входных и выходных документов на экран, принтер или в файл.

4. Автоматизированная информационная система единого накопительного пенсионного фонда включает следующий перечень функционала:

1) персонифицированный учет пенсионных накоплений и условных пенсионных обязательств;

2) формирование отчетности;

3) взаимодействие с внешними пользователями;

4) внутренний аудит;

5) администрирование;

6) ведение справочной информации (в том числе с выгрузкой в Excel).

Персонифицированный учет пенсионных накоплений и условных пенсионных обязательств обеспечивает:

1) ведение бухгалтерского учета операций с:

индивидуальными пенсионными счетами вкладчиков (получателей) обязательных пенсионных взносов, физических лиц, за которых перечислены обязательные профессиональные пенсионные взносы, добровольные пенсионные взносы, (получателей обязательных профессиональных пенсионных взносов, добровольных пенсионных взносов) (далее – вкладчики (получатели);

условными пенсионными счетами физических лиц, за которых перечислены обязательные пенсионные взносы работодателя;

2) учет пенсионных взносов, накоплений, пени, поступающих на индивидуальные пенсионные счета вкладчиков (получателей) и условные пенсионные счета физических лиц;

3) учет инвестиционного дохода на:

индивидуальных пенсионных счетах вкладчиков (получателей) в разрезе управляющих инвестиционным портфелем;

условных пенсионных счетах физических лиц, за которых перечислены обязательные пенсионные взносы работодателя;

4) учет пенсионных выплат за счет обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов, добровольных пенсионных взносов, обязательных пенсионных взносов работодателя;

5) учет переводов пенсионных накоплений:

за счет добровольных пенсионных взносов в другой добровольный накопительный пенсионный фонд;

в страховую организацию;

6) объединение индивидуальных пенсионных счетов за счет обязательных пенсионных взносов вкладчиков с сохранением истории по произведенным единым накопительным пенсионным фондом объединением индивидуальных пенсионных счетов вкладчиков (получателей) за счет обязательных пенсионных взносов;

7) идентификацию вкладчиков (получателей) по уникальным реквизитам (индивидуальному идентификационному номеру, фамилии, имени, отчеству (при наличии) и другим параметрам);

8) формирование платежных документов;

9) осуществление проверки правильности формирования платежных документов;

10) обмен данными с Государственной корпорацией "Правительство для граждан" (далее – Корпорация), состав и объем которых определены соответствующим соглашением, заключенным между единым накопительным пенсионным фондом и Корпорацией.

Формирование отчетности осуществляется в виде электронных форм, электронных файлов и обеспечивает:

1) формирование отчетов в соответствии с установленными требованиями Национального Банка Республики Казахстан;

2) межформенный и внутриформенный контроль в отчетности;

3) просмотр и печать (в том числе конвертация в Excel) отчетов.

Взаимодействие с внешними пользователями предназначено для осуществления электронного информационного обмена с:

1) банком-кастодианом;

2) управляющим инвестиционным портфелем (при наличии);

3) страховыми организациями;

4) государственными органами путем интеграции посредством шлюза " электронного правительства" или внешнего шлюза "электронного правительства".

Внутренний аудит предназначен для регистрации и идентификации происходящих системных событий в функционалах, указанных в подпунктах 1), 2) и 3) части первой настоящего пункта, с сохранением следующих атрибутов:

1) аутентификации пользователя автоматизированной информационной системы с указанием даты и времени входа и выхода пользователя автоматизированной информационной системы;

2) идентификации бизнес-процесса, результата выполнения бизнес-процесса.

Внутренний аудит обеспечивает:

1) просмотр и сохранение в файл электронного журнала аудита системных событий;

2) перенос записей аудита автоматизированной информационной системы в архив с возможностью восстановления архивных записей;

3) возможность аудита следующих событий:

добавление, изменение, удаление записи;

ведение справочников;

формирование выходных форм пользователями;

4) возможность отслеживания администратором событий, происходящих в функционалах, указанных в подпунктах 1), 2) и 3) части первой настоящего пункта, по каждому пользователю и (или) по автоматизированной информационной системе в целом;

5) фиксацию событий в регистрационных журналах, содержащую следующие сведения:

наименование аудируемого события;

имя пользователя, инициировавшего аудируемое событие;

местоположение;

время события.

Администрирование обеспечивает:

1) регистрацию, изменение и блокировку пользователей в системе;

2) администрирование системы;

3) управление правами доступа пользователей к функциям системы;

4) автоматизацию контроля над сложностью пароля;

5) контроль активных подключений пользователей к базе данных системы;

6) настройку параметров функционирования системы.

5. Автоматизированная информационная система добровольного накопительного пенсионного фонда включает следующий перечень функционала:

1) персонифицированный учет пенсионных накоплений добровольного накопительного пенсионного фонда;

2) формирование отчетности;

3) взаимодействие с внешними пользователями;

4) внутренний аудит;

5) администрирование;

6) ведение справочной информации (с выгрузкой в Excel).

Персонифицированный учет пенсионных накоплений добровольного накопительного пенсионного фонда обеспечивает:

1) ведение персонального учета:

договоров о пенсионном обеспечении за счет добровольных пенсионных взносов;

пенсионных взносов, накоплений, пени, поступающих на индивидуальные пенсионные счета вкладчиков (получателей) добровольных пенсионных взносов;

инвестиционного дохода на индивидуальных пенсионных счетах вкладчиков (получателей) добровольных пенсионных взносов;

пенсионных выплат за счет добровольных пенсионных взносов;

переводов пенсионных накоплений за счет добровольных пенсионных взносов в единый накопительный пенсионный фонд, другой добровольный накопительный пенсионный фонд или страховую организацию;

2) ведение бухгалтерского учета операций с индивидуальными пенсионными счетами вкладчиков (получателей) добровольных пенсионных взносов;

3) формирование платежных документов;

4) осуществление проверки правильности формирования платежных документов;

5) идентификацию вкладчиков (получателей) добровольных пенсионных взносов по уникальным реквизитам (по номеру договора, индивидуальному идентификационному номеру, фамилии, имени, отчеству (при наличии) и другим параметрам).

Формирование отчетности осуществляется в виде электронных форм, электронных файлов и обеспечивает:

1) формирование отчетов в соответствии с установленными требованиями Национального Банка Республики Казахстан;

2) межформенный и внутриформенный контроль в отчетности;

3) просмотр и печать (в том числе конвертация в Excel) отчетов.

Взаимодействие с внешними пользователями предназначено для осуществления электронного информационного обмена с:

1) банком-кастодианом;

2) управляющим инвестиционным портфелем (при наличии);

3) страховыми организациями;

4) государственными органами путем интеграции посредством шлюза " электронного правительства" или внешнего шлюза "электронного правительства".

Внутренний аудит предназначен для регистрации и идентификации происходящих системных событий в функционалах, указанных в подпунктах 1), 2) и 3) части первой настоящего пункта, с сохранением следующих атрибутов:

1) аутентификации пользователя автоматизированной информационной системы с указанием даты и времени входа и выхода пользователя автоматизированной информационной системы;

2) идентификации бизнес-процесса, результата выполнения бизнес-процесса.

Внутренний аудит обеспечивает:

1) просмотр и сохранение в файл электронного журнала аудита системных событий;

2) перенос записей аудита автоматизированной информационной системы в архив с возможностью восстановления архивных записей;

3) возможность аудита следующих событий:

добавление, изменение, удаление записи;

ведение справочников;

формирование выходных форм пользователями;

4) возможность отслеживания администратором событий, происходящих в функционалах, указанных в подпунктах 1), 2) и 3) части первой настоящего пункта, по каждому пользователю и (или) по автоматизированной информационной системе в целом.

5) фиксацию событий в регистрационных журналах, содержащую следующие сведения:

наименование аудируемого события;

имя пользователя, инициировавшего аудируемое событие;

местоположение;

время события.

Администрирование обеспечивает:

1) регистрацию, изменение и блокировку пользователей в системе;

2) администрирование системы;

3) управление правами доступа пользователей к функциям системы;

4) автоматизацию контроля над сложностью пароля;

5) контроль активных подключений пользователей к базе данных системы;

6) настройку параметров функционирования системы.

6. Предоставление доступа к автоматизированной информационной системе единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда определяется внутренними документами единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда.

7. При осуществлении пенсионных выплат за счет обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов, добровольных пенсионных взносов, обязательных пенсионных взносов работодателя обеспечивается выполнение следующих функций:

1) расчет сумм пенсионных выплат за счет обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов, добровольных пенсионных взносов, обязательных пенсионных взносов работодателя по каждому получателю пенсионных выплат за счет обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов, добровольных пенсионных взносов, обязательных пенсионных взносов работодателя;

2) удержание подоходного налога с причитающейся суммы пенсионных выплат за счет обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов, добровольных пенсионных взносов в соответствии с Кодексом Республики Казахстан "О налогах и других обязательных платежах в бюджет (Налоговый кодекс)";

3) прогнозирование пенсионных выплат за счет обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов, добровольных пенсионных взносов, обязательных пенсионных взносов работодателя на заданную дату и (или) на заданный промежуток времени.

8. Допускается реализация в автоматизированных информационных системах дополнительных функций и задач, улучшающих функциональные характеристики системы в целом.

9. Процесс разработки, внедрения и сопровождения автоматизированной информационной системы единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда обеспечивает выполнение этапов разработки, порядка внесения изменений, приема, тестирования, ввода в эксплуатацию и сопровождение программного обеспечения системы, требований к документированию всех этапов работ.

В целях исключения несанкционированного изменения программного обеспечения и (или) информации в автоматизированной информационной системе внесение изменений в существующий функционал, разработка нового функционала, внедрение и ввод в эксплуатацию системы осуществляются согласно корпоративной стратегии развития единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда, утвержденной решением совета директоров единого накопительного пенсионного фонда, добровольного накопительного пенсионного фонда.

Глава 3. Требования к организации информационного процесса единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда

10. Для создания информационно-коммуникационных технологий инфраструктуры и обеспечения информационной безопасности единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда обеспечивается выполнение соответствующих требований к:

1) серверному помещению;

2) техническим средствам;

3) средствам связи;

4) рабочим местам пользователей;

5) программным средствам.

11. Серверное помещение единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда соответствует следующим требованиям:

1) при расположении помещения на первых и последних этажах зданий окна помещения оборудуются металлическими решетками или аналогичными средствами защиты, предназначенными для предотвращения физического проникновения в помещение;

2) наличие специально выделенного помещения ограниченного доступа;

3) наличие системы контроля доступа (индивидуальный электронный пропуск) для осуществления мониторинга событий доступа в помещение в режиме реального времени и записи событий доступа в помещение в электронном журнале с возможностью получения отчета о событиях доступа в помещение. Записи событий в электронном журнале хранятся не менее 6 (шести) месяцев;

4) наличие системы видеоконтроля (в режиме реального времени с возможностью записи видеосигналов);

5) наличие системы охранной сигнализации;

6) наличие системы автоматического поддержания заданной температуры и влажности, достаточной для охлаждения всего оборудования до температуры, указанной производителем, в любое время года в период максимальной загрузки;

7) наличие пожарной сигнализации и оборудования автоматического газового пожаротушения;

8) наличие системы гарантированного питания – щита автоматического включения резерва, дизельного генерирующего устройства, работающих от сигнала с двух источников бесперебойного питания и непрерывно поддерживающих электричество в сети чистого питания.

При аренде помещения центра обработки данных специализированных организаций , а также необходимых технических средств необходимо соответствие требованиям, предъявляемым к собственным серверным помещениям и техническим средствам единого накопительного пенсионного фонда или добровольного накопительного пенсионного фонда.

12. Технические средства единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда соответствуют следующим требованиям:

1) наличие собственного аппаратного обеспечения (компьютерное оборудование, серверы, аппаратные средства защиты, комплектующие и другое оборудование), наличие документов, подтверждающих принадлежность аппаратного обеспечения единому накопительному пенсионному фонду или добровольному накопительному пенсионному фонду или аренду аппаратного обеспечения у специализированной организации;

2) наличие сертификата соответствия, выдаваемого производителем или поставщиком на используемое оборудование.

13. Средства связи единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда по обмену данными с банком-кастодианом, управляющим инвестиционным портфелем (при наличии), государственными органами соответствуют следующим требованиям:

1) наличие основного канала, обеспечивающего полноценный объем передаваемой и получаемой информации;

2) наличие резервного канала, обеспечивающего полноценный объем передаваемой и получаемой информации;

3) наличие физически разделенных каналов от разных провайдеров.

14. Рабочие места пользователей автоматизированной информационной системы единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда соответствуют следующим требованиям:

1) средства технической защиты помещения единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда исключают возможность неконтролируемого проникновения в это помещение лиц, не допущенных к рабочему месту. Допуск в помещение и к рабочему месту осуществляется в соответствии с регламентом и должностными обязанностями сотрудников единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда;

2) все аппаратные средства имеют гарантийный срок (гарантийный талон) и (или) находятся на техническом сопровождении специализированной организации и (или) имеется возможность оперативной замены аппаратных средств в случае выхода их из строя;

3) порядок доступа к рабочему месту пользователя посредством сети и иных технических каналов передачи данных исключает возможность несанкционированного доступа;

4) порядок доступа к ресурсам (сетевое (серверное) оборудование, дисковое пространство, директории, сетевые ресурсы, базы данных), выделенным для накопления в них информации для передачи в рамках обмена информации, хранения, архивирования либо другой обработки информации, исключает возможность доступа к этим ресурсам лиц, не допущенных к работе с ними;

5) рабочее место пользователя размещается в локальной сети (LAN);

6) доступ к портам считывания (записи или копирования) информации компьютера пользователя отключен, в том числе и в настройках базовой системы ввода-вывода;

7) системный блок персонального компьютера пользователя опечатывается или опломбировывается администратором безопасности;

8) права по установлению и изменению настроек средств защиты от несанкционированного доступа рабочего места пользователя предоставляются только пользователям, выполняющим функции администратора;

9) одно системное имя пользователя, по которому идентифицируется пользователь, соответствует одному физическому лицу;

10) порядок хранения и использования технических средств, паролей или другой информации, обеспечивающих доступ к рабочему месту пользователя, исключает возможность их несанкционированного использования;

11) доступ к сетевым ресурсам для рабочего места пользователя ограничивается в пределах защищенной подсети автоматизированной информационной системы;

12) при наличии у пользователя резервного рабочего места условия и требования, установленные Требованиями, также распространяются и на такое рабочее место.

15. Программные средства, используемые на рабочих местах пользователей, соответствуют следующим требованиям:

1) используется только лицензионное программное обеспечение;

2) на рабочем месте пользователя не допускается установка программных средств, которые не требуются для исполнения его должностных обязанностей;

3) наличие на рабочем месте пользователя программных средств, позволяющих обеспечить идентификацию и аутентификацию пользователей;

4) на рабочем месте пользователя устанавливается лицензионное антивирусное программное обеспечение с регулярно обновляемой антивирусной базой;

5) возможность ведения электронных журналов в течение срока хранения электронных документов с целью контроля событий, связанных с доступом к компьютеру и действиями пользователей;

6) программное обеспечение устанавливается на персональном компьютере, имеющем паспорт (описание рабочего места с подробными данными о его конфигурации, а также установленные на данном рабочем месте аппаратные и программные средства);

7) паспорт, указанный в подпункте 6) настоящего пункта, оформляется согласно внутренним документам единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда и хранится у администратора безопасности.

Глава 4. Требования к обеспечению информационной безопасности автоматизированной информационной системы единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда

16. В целях обеспечения информационной безопасности автоматизированной информационной системы единого накопительного пенсионного фонда и

добровольного накопительного пенсионного фонда единый накопительный пенсионный фонд и добровольный накопительный пенсионный фонд обеспечивают создание системы управления информационной безопасностью.

17. Система управления информационной безопасностью обеспечивает защиту информационных активов единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда, предусматривающую минимальный уровень потенциального ущерба для бизнес-процессов.

18. Единый накопительный пенсионный фонд и добровольный накопительный пенсионный фонд обеспечивают надлежащий уровень системы управления информационной безопасностью, ее развитие и улучшение.

19. Документация по обеспечению информационной безопасности единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда включает:

1) политику информационной безопасности;

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

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

7) порядок обеспечения антивирусной защиты информационной инфраструктуры единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда;

8) перечень разрешенного к использованию в едином накопительном пенсионном фонде и добровольном накопительном пенсионном фонде программного обеспечения;

9) 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 имеет отношение к информационной безопасности (далее - события информационной безопасности);

10) перечень событий информационной безопасности, подлежащих мониторингу;

11) перечень источников событий информационной безопасности;

12) 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);

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

14) порядок доступа лиц, не являющихся работниками единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда, к информационным системам, обрабатывающим защищаемую информацию;

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

16) порядок управления обновлениями информационных систем.

20. Политика информационной безопасности определяет:

1) цели, задачи и основные принципы построения системы управления информационной безопасностью;

2) область действия системы управления информационной безопасностью;

3) требования к управлению доступом к создаваемой, хранимой и обрабатываемой информации в информационных активах единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда;

4) требования к осуществлению мониторинга деятельности по обеспечению информационной безопасности;

5) ответственность работников единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей.

21. Доступ к информации в автоматизированной информационной системе предоставляется работникам единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда в объеме, необходимом для исполнения их функциональных обязанностей.

22. Предоставление доступа к автоматизированной информационной системе единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей автоматизированной информационной системы их функциональным обязанностям. Совокупность таких ролей представляет собой матрицу доступа к автоматизированной информационной системе, которая формируется в электронной форме или на бумажном носителе.

23. Доступ к автоматизированной информационной системе осуществляется путем идентификации и аутентификации пользователей автоматизированной информационной системы.

Идентификация и аутентификация пользователей автоматизированной информационной системы производится посредством ввода пары "учетная запись (идентификатор) – пароль" и (или) биометрической и (или) криптографической и (или) аппаратной аутентификации.

24. В автоматизированной информационной системе используются только персонализированные пользовательские учетные записи.

25. Использование технологических учетных записей осуществляется в соответствии с перечнем таких учетных записей для автоматизированной информационной системы с указанием лиц, персонально ответственных за их использование и актуальность.

26. В автоматизированной информационной системе применяются функции по управлению учетными записями и паролями, а также блокировке учетных записей пользователей, определяемые внутренним документом единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда.

27. В автоматизированной информационной системе применяются следующие параметры функции по управлению паролями и блокировками учетных записей пользователей:

1) минимальная длина пароля – значение данного параметра составляет не менее 8 (восьми) символов. Проверка пароля на соответствие данному параметру производится при каждой смене пароля, в случае несоответствия – выдается уведомление пользователю;

2) сложность пароля – возможность проверки наличия в пароле как минимум 3 (трех) групп символов: строчных букв, заглавных букв, цифровых значений, специальных символов. Проверка пароля на соответствие данному параметру производится при каждой смене пароля, в случае несоответствия – выдается уведомление пользователю;

3) история пароля – новый пароль не повторяет как минимум 7 (семь) предыдущих паролей. Проверка пароля на соответствие данному параметру производится при каждой смене пароля, в случае несоответствия выдается уведомление пользователю;

4) минимальный срок действия пароля – 1 (один) рабочий день;

5) максимальный срок действия пароля – не более 60 (шестидесяти) календарных дней. Проверка пароля на соответствие данному параметру производится при каждом входе в автоматизированную информационную систему и смене пароля. По истечении максимального срока действия пароля автоматизированная информационная система блокирует доступ и требует обязательную смену пароля;

6) при первом входе в автоматизированную информационную систему либо после смены пароля администратором, автоматизированная информационная система запрашивает у пользователя смену пароля с невозможностью отклонить данную процедуру. Данное правило превалирует над правилом о сроке действия пароля;

7) при отсутствии активности пользователя в автоматизированной информационной системе более 30 (тридцати) календарных дней его учетная запись автоматически блокируется;

8) при последовательном пятикратном вводе неправильного пароля учетная запись пользователя временно блокируется;

9) при неактивности пользователя более 30 (тридцати) минут автоматизированная информационная система автоматически завершает сеанс работы пользователя либо блокирует рабочую станцию или ноутбук с возможностью разблокировки только при вводе аутентификационных данных пользователя.

28. Уничтожение защищаемой информации производится методами, исключающими ее восстановление, с использованием любого из следующих методов уничтожения информации в зависимости от типа носителя:

1) физическое уничтожение носителя информации;

2) электромагнитное воздействие на носитель информации (для магнитных носителей);

3) программное уничтожение электронной информации специализированными программными средствами.

29. В едином накопительном пенсионном фонде и добровольном накопительном пенсионном фонде обеспечивается синхронизация системного времени автоматизированной информационной системы с централизованным источником эталонного времени.

30. Разработка и доработка автоматизированной информационной системы не осуществляется в среде промышленной эксплуатации.

31. Работники, осуществляющие разработку автоматизированной информационной системы, не имеют полномочий на перенос изменений автоматизированной информационной системы в промышленную среду, а также административный доступ к автоматизированной информационной системе в промышленной среде.

32. Перед вводом в промышленную эксплуатацию автоматизированной информационной системы в ней изменяются настройки безопасности, установленные по умолчанию, на настройки, соответствующие требованиям к информационной безопасности. Указанные настройки включают замену паролей, используемых при тестировании, а также удаление всех тестовых учетных записей.

33. Контроль использования привилегированных учетных записей обеспечивается путем:

1) составления и утверждения перечня администраторов автоматизированной информационной системы (операционная система, система управления базами данных, приложение);

2) введения двойного контроля при исполнении функций администрирования автоматизированной информационной системы и (или) внедрения специальных комплексов контроля использования привилегированных учетных записей.

34. Защищенный депозитарий программного обеспечения, в котором хранятся эталонные исходные коды (при наличии) и исполняемые модули автоматизированных информационных систем, ведется в виде, обеспечивающем возможность своевременного восстановления работоспособности исполняемых модулей, автоматизированных информационных систем.

35. Автоматизированная информационная система обеспечивается технической поддержкой, в состав которой входят услуги по предоставлению обновлений автоматизированной информационной системы, в том числе обновлений безопасности.

36. В едином накопительном пенсионном фонде и добровольном накопительном пенсионном фонде обеспечивается ведение и неизменность аудиторского следа автоматизированной информационной системы, как на организационном, так и на техническом уровне.

37. В автоматизированной информационной системе используется функция ведения аудиторского следа, которая отражает следующее:

1) события установления соединений, идентификации, аутентификации и авторизации в автоматизированной информационной системе (успешные и неуспешные);

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 в автоматизированной информационной системе;

6) события изменения параметров аудита;

7) события изменений системных параметров.

38. Формат аудиторского следа включает следующую информацию:

1) идентификатор (логин) пользователя, совершившего действие;

2) дата и время совершения действия;

3) наименование рабочей станции пользователя и (или) IP (АЙПИ) адрес, с которого совершено действие;

4) название объектов, с которыми проводилось действие;

5) тип или название совершенного действия;

6) результат действия (успешно или не успешно).

39. Срок хранения аудиторского следа составляет не менее 3 (трех) месяцев в оперативном доступе и не менее 5 (пяти) лет в архивном доступе.

40. Для защиты автоматизированной информационной системы используется лицензионное антивирусное программное обеспечение или системы, обеспечивающие

целостность и неизменность программной среды на рабочих станциях, ноутбуках и мобильных устройствах.

41. Используемое антивирусное программное обеспечение соответствует следующим требованиям:

1) обнаружение вирусов на основе известных сигнатур;

2) обнаружение вирусов на основе эвристического анализа (поиска характерных для вирусов команд и поведенческого анализа);

3) сканирование сменных носителей при подключении;

4) запуск сканирования и обновления антивирусной базы по расписанию;

5) наличие централизованной консоли администрирования и мониторинга;

6) блокирование для пользователя возможности прерывания функционирования антивирусного программного обеспечения, а также процессов обновления антивирусного программного обеспечения и плановой проверки на отсутствие вирусов;

7) для виртуальных сред – использование антивирусным программным обеспечением встроенных функций безопасности виртуальных сред (балансировка нагрузки, централизованная установка и проверка на уровне гипервизора и другие функции), при отсутствии таких возможностей – подтверждение производителя о тестировании антивирусного программного обеспечения в виртуальных средах, используемых в едином накопительном пенсионном фонде и добровольном накопительном пенсионном фонде;

8) для мобильных устройств и иных устройств, используемых вне периметра защиты единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда, использование антивирусного программного обеспечения со встроенной функцией межсетевого экранирования.

42. При использовании систем, обеспечивающих целостность и неизменность программной среды, минимальными требованиями являются:

1) наличие лицензионного программного обеспечения, предусматривающего обновление и техническую поддержку;

2) наличие централизованной консоли администрирования и мониторинга;

3) наличие возможности блокирования для конечного пользователя возможности прерывания функционирования данной системы;

4) наличие возможности проверки образа программной среды антивирусным программным обеспечением перед установкой на конечные устройства;

5) наличие межсетевого экрана для мобильных устройств и иных устройств, используемых вне периметра защиты.

43. Антивирусное программное обеспечение максимально исключает прерывание пользователем всех служебных процессов (сканирование по расписанию, обновление и

другие процессы). Обновление антивирусного программного обеспечения производится не реже 1 (одного) раза в сутки, полное сканирование устройства – не реже 1 (одного) раза в неделю.

44. В едином накопительном пенсионном фонде и добровольном накопительном пенсионном фонде обеспечивается своевременная установка обновлений безопасности автоматизированной информационной системы.

45. Обновления безопасности автоматизированной информационной системы, устраняющие критичные уязвимости, устанавливаются не позднее 1 (одного месяца) со дня их публикации и распространения производителем.

46. Обновления автоматизированной информационной системы до установки в промышленную среду проходят испытания в тестовой среде.

47. В целях обеспечения непрерывности функционирования автоматизированной информационной системы во внутренних документах определяются:

1) допустимые сроки простоя автоматизированной информационной системы;

2) план восстановления автоматизированной информационной системы.

48. При наличии резервного центра во внутренних документах единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда отражается:

1) местонахождение резервного центра;

2) перечень бизнес-процессов, технических, программных или других средств, обеспечивающих работу автоматизированной информационной системы;

3) порядок восстановления работы автоматизированной информационной системы в резервном центре;

4) критерии, позволяющие принять решение о завершении работы в резервном центре, порядок принятия такого решения, а также порядок возврата в штатный режим функционирования в основном центре;

5) порядок проведения, периодичность и сценарии тестирования функционирования резервного центра.

49. В целях проверки готовности процессов восстановления деятельности автоматизированной информационной системы не менее 1 (одного) раза в год проводится тестирование восстановления автоматизированной информационной системы в соответствии с планом восстановления (далее – тестирование планов восстановления).

Тестирование плана восстановления проводится по разработанной и утвержденной единым накопительным пенсионным фондом и добровольным накопительным пенсионным фондом программе, предусматривающей описание сценария возникновения нештатной ситуации, восстанавливаемых рабочих процессов, действий команды восстановления, требований по срокам и месту проведения работ.

50. По итогам тестирования плана восстановления подготавливается документ о результатах тестирования (протокол) с указанием:

1) перечня функционала автоматизированной информационной системы, по которому проведено тестирование;

2) времени, затраченного на восстановление работы автоматизированной информационной системы;

3) выявленных недостатков плана восстановления и предложений по их устранению

.

Приложение 2 к постановлению
Правления Агентства
Республики Казахстан
по регулированию и развитию
финансового рынка
от 26 июня 2023 года № 60

Перечень нормативного правового акта Республики Казахстан, а также отдельных структурных элементов некоторых нормативных правовых актов Республики Казахстан, которые признаются утратившими силу

1. Постановление Правления Национального Банка Республики Казахстан от 27 августа 2013 года № 218 "Об утверждении Требований к автоматизированным информационным системам для учета пенсионных активов и накоплений" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 8801).

2. Пункт 2 Перечня нормативных правовых актов Республики Казахстан по вопросам пенсионного обеспечения, в которые вносятся изменения и дополнения, утвержденного постановлением Правления Национального Банка Республики Казахстан от 28 ноября 2015 года № 209 "О внесении изменений и дополнений в некоторые нормативные правовые акты Республики Казахстан по вопросам пенсионного обеспечения" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 12529).

3. Пункт 2 Перечня нормативных правовых актов Республики Казахстан по вопросам пенсионного обеспечения, в которые вносятся изменения и дополнение, утвержденного постановлением Правления Национального Банка Республики Казахстан от 22 декабря 2017 года № 254 "О внесении изменений и дополнения в некоторые нормативные правовые акты Республики Казахстан по вопросам пенсионного обеспечения" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 16246).

4. Пункт 3 Перечня нормативных правовых актов Республики Казахстан по вопросам пенсионного обеспечения, в которые вносятся изменения, утвержденного постановлением Правления Национального Банка Республики Казахстан от 28 июня

2019 года № 103 "О внесении изменений в некоторые нормативные правовые акты Республики Казахстан по вопросам пенсионного обеспечения" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 18995).