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

Утративший силу

Постановление Правления Национального Банка Республики Казахстан от 27 августа 2013 года № 218. Зарегистрирован в Министерстве юстиции Республики Казахстан 10 октября 2013 года № 8801. Утратило силу постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 26 июня 2023 года № 60.

Сноска. Утратило силу постановлением Правления Агентства РК по регулированию и развитию финансового рынка от 26.06.2023 № 60 (вводится в действие с 01.07.2023).

Примечание РЦПИ!

Порядок введения в действие приказа см. п.2

В соответствии с Законом Республики Казахстан от 21 июня 2013 года "О пенсионном обеспечении в Республике Казахстан" Правление Национального Банка Республики Казахстан **ПОСТАНОВЛЯЕТ:**

1. Утвердить прилагаемые Требования к автоматизированным информационным системам для учета пенсионных активов и накоплений (далее - Требования).

2. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования, за исключением подпунктов 1), 2), 3) и 4) пункта 5, подпункта 1) и абзацев второго и четвертого подпункта 6) пункта 6 и пункта 7 Требований, в части норм, определяющих требования к автоматизированным информационным системам для учета пенсионных активов и накоплений, сформированных за счет обязательных профессиональных пенсионных взносов, которые действуют с 1 января 2014 года.

Председатель

Национального Банка Г. Марченко

Утверждены
постановлением
Правления Национального
Банка Республики Казахстан
от 27 августа 2013 года № 218

Требования к автоматизированным информационным системам для учета пенсионных активов и накоплений

1. Общие положения

1. Настоящие Требования к автоматизированным информационным системам для учета пенсионных активов и накоплений (далее - Требования) разработаны в соответствии с Законом Республики Казахстан от 21 июня 2013 года "О пенсионном обеспечении в Республике Казахстан" (далее - Закон) и устанавливают требования к автоматизированным информационным системам единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда для учета пенсионных активов и накоплений в целях обеспечения надежного и устойчивого функционирования действующих электронных информационных ресурсов и формирования системы информационной безопасности.

2. В Требованиях используются следующие понятия:

1) 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;

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) информационная безопасность – защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, утечки, хищения, утраты, уничтожения, искажения, копирования, подделки, блокирования и других угроз, возникающих в результате несанкционированного доступа;

4) защита информации – комплекс мероприятий, обеспечивающих информационную безопасность;

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

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

7) автоматизированные информационные системы – организационная упорядоченная совокупность документов, систем технических средств и способов обработки информации;

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

9) модуль – составляющая автоматизированной информационной системы, предназначенная для выполнения определенных функций;

10) 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;

11) идентификатор – уникальные персональный код или имя, присвоенные субъекту и (или) объекту системы и предназначенные для регламентированного доступа в систему и (или) к ресурсам системы;

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

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

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

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

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 (в случае выполнения 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. Автоматизированные информационные системы единого накопительного пенсионного фонда включают следующие функциональные модули:

1) модуль "Персонифицированный учет пенсионных накоплений и условных пенсионных обязательств";

2) модуль "Отчетность";

3) модуль "Взаимодействие с внешними пользователями";

4) модуль "Внутренний аудит".

Сноска. Пункт 4 с изменением, внесенным постановлением Правления Национального Банка РК от 28.11.2015 № 209 (вводится в действие с 01.01.2023).

4-1. Автоматизированные информационные системы добровольного накопительного пенсионного фонда включают следующие функциональные модули:

1) модуль "Персонифицированный учет пенсионных накоплений";

2) модуль "Отчетность";

3) модуль "Взаимодействие с внешними пользователями";

4) модуль "Внутренний аудит".

Сноска. Требования дополнены пунктом 4-1 в соответствии с постановлением Правления Национального Банка РК от 28.11.2015 № 209 (вводится в действие с 01.01.2023).

5. Модуль "Персонифицированный учет пенсионных накоплений и условных пенсионных обязательств" единого накопительного пенсионного фонда предназначен для ведения персонального учета:

1) договоров о пенсионном обеспечении за счет обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов, добровольных пенсионных взносов;

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

3) инвестиционного дохода на индивидуальных пенсионных счетах вкладчиков (получателей) обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов, добровольных пенсионных взносов;

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

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

6) переводов пенсионных накоплений за счет обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов в страховую организацию.

Сноска. Пункт 5 - в редакции постановления Правления Национального Банка РК от 28.11.2015 № 209 (вводится в действие с 01.01.2023).

5-1. Модуль "Персонифицированный учет пенсионных накоплений" добровольного накопительного пенсионного фонда предназначен для ведения персонального учета:

1) договоров о пенсионном обеспечении за счет добровольных пенсионных взносов;

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

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

4) пенсионных выплат за счет добровольных пенсионных взносов;

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

Сноска. Требования дополнены пунктом 5-1 в соответствии с постановлением Правления Национального Банка РК от 28.11.2015 № 209 (вводится в действие с 01.01.2023).

6. Модуль "Персонифицированный учет пенсионных накоплений и условных пенсионных обязательств" единого накопительного пенсионного фонда обеспечивает:

1) ведение аналитического и синтетического бухгалтерского учета операций с :

индивидуальными пенсионными счетами вкладчиков (получателей) обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов, добровольных пенсионных взносов;

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

2) объединение индивидуальных пенсионных счетов за счет обязательных пенсионных взносов вкладчиков (получателей) в едином накопительном пенсионном фонде с сохранением истории по произведенным единым накопительным пенсионным фондом объединением индивидуальных пенсионных счетов вкладчиков (получателей) за счет обязательных пенсионных взносов;

3) формирование платежных документов;

4) осуществление проверки правильности формирования платежных документов;

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

6) взаимодействие с автоматизированной информационной системой Государственной корпорации "Правительство для граждан" (далее – Государственная корпорация) по:

обмену информацией об открытых и закрытых индивидуальных пенсионных счетах по учету обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов;

обмену информацией по физическим лицам, на имя которых открыты условные пенсионные счета по учету обязательных пенсионных взносов работодателя;

движению на индивидуальных пенсионных счетах, условных пенсионных счетах на основании договора, заключенного между Государственной корпорацией и единым накопительным пенсионным фондом;

обмену платежными документами;

внесению изменений в реквизиты вкладчика (получателя) обязательных пенсионных взносов, обязательных профессиональных пенсионных взносов, физического лица, на имя которого открыт условный пенсионный счет в едином накопительном пенсионном фонде, на основании информации, поступившей от Государственной корпорации.

Сноска. Пункт 6 с изменениями, внесенными постановлениями Правления Национального Банка РК от 28.11.2015 № 209 (вводится в действие с 01.01.2023); от 28.06.2019 № 103 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

6-1. Модуль "Персонифицированный учет пенсионных накоплений" добровольного накопительного пенсионного фонда обеспечивает:

1) ведение аналитического и синтетического бухгалтерского учета операций с индивидуальными пенсионными счетами вкладчиков (получателей) добровольных пенсионных взносов;

2) формирование платежных документов;

3) осуществление проверки правильности формирования платежных документов;

4) идентификацию вкладчиков (получателей) по уникальным реквизитам (по номеру договора, индивидуальному идентификационному номеру, фамилии, имени, отчеству при его наличии и другим параметрам).

Сноска. Требования дополнены пунктом 6-1 в соответствии с постановлением Правления Национального Банка РК от 28.11.2015 № 209 (вводится в действие с 01.01.2023).

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 Законом;

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.

Сноска. Пункт 7 - в редакции постановления Правления Национального Банка РК от 28.11.2015 № 209 (вводится в действие с 01.01.2023).

8. Модуль "Отчетность" предназначен для формирования отчетности в виде электронных форм, электронных файлов и для обеспечения выполнения следующих функций:

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

2) межформенный и внутриформенный контроль в отчетности.

9. Модуль "Взаимодействие с внешними пользователями" предназначен для обеспечения электронного информационного обмена с:

1) филиалами и представительствами;

2) банком–кастодианом;

3) управляющим инвестиционным портфелем (при наличии);

4) актуариями;

5) государственными органами путем интеграции посредством шлюза электронного правительства.

10. Модуль "Внутренний аудит" предназначен для регистрации и идентификации происходящих системных событий в модулях, указанных в подпунктах 1), 2) и 3) пункта 4 Требований, 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.

11. Модуль "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.

Для администратора в модуле "Внутренний аудит" реализуется возможность отслеживания событий, происходящих в модулях, указанных в подпунктах 1), 2) и 3) пункта 4 Требований, по каждому пользователю и (или) по автоматизированной информационной системе в целом.

12. Допускается реализация в автоматизированных информационных системах дополнительных функций и задач (модулей), улучшающих функциональные характеристики системы в целом.

13. 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 существующие модули, разработка новых модулей, внедрение и ввод в эксплуатацию системы осуществляются согласно плану мероприятий по реализации корпоративной стратегии развития единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда, утвержденной решением совета директоров единого накопительного пенсионного фонда и совета директоров добровольного накопительного пенсионного фонда.

Сноска. Пункт 13 с изменением, внесенным постановлением Правления Национального Банка РК от 28.11.2015 № 209 (вводится в действие с 01.01.2016).

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

14. 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.

15. 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 газопожаротушения;

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.

16. 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.

17. Средства связи единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда по обмену данными с филиалами и представительствами, 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.

18. Рабочие места пользователей автоматизированной информационной системы фонда соответствуют следующим требованиям:

1) средства технической защиты помещения организации 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 организации;

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.

Сноска. Пункт 18 с изменением, внесенным постановлением Правления Национального Банка РК от 22.12.2017 № 254 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

19. 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 в обязательном порядке 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 оформляется согласно внутренних документов единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда и хранится у администратора безопасности.

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

20. Основной целью системы информационной безопасности является обеспечение устойчивого функционирования единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда и предотвращение реализации угроз безопасности, защита интересов единого накопительного пенсионного фонда и добровольного накопительного

пенсионного фонда от противоправных действий любых физических и юридических лиц, недопущение хищения его имущества, разглашения, утраты, утечки, искажения и уничтожения информации.

21. Ключевым документом по обеспечению информационной безопасности автоматизированной информационной системы для учета пенсионных активов и накоплений является политика информационной безопасности, которая включает комплекс предупредительных мер по обеспечению информационной безопасности, правила, процедуры и принципы в области безопасности, которыми руководствуется единый накопительный пенсионный фонд и добровольный накопительный пенсионный фонд в своей деятельности, и охватывает автоматизированные, телекоммуникационные системы, автоматизированные рабочие места.

22. Политика информационной безопасности определяет:

1) общие направления работы в области информационной безопасности;

2) цель защиты информационной системы;

3) общие требования к защите информационной системы в целом и отдельным ее частям;

4) основные принципы и способы достижения необходимого уровня безопасности;

5) перечень должностных лиц, ответственных за разработку необходимых требований, определяющих политику информационной безопасности;

6) перечень подразделений, ответственных за создание и поддержание работоспособности защиты информационных систем;

7) закрепление администратора безопасности, ответственного за разработку и контроль необходимых требований, определяющих политику безопасности;

8) меры, предотвращающие нарушения режима безопасности информационных систем в случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, отключение электроэнергии, повреждение линий связи, массовые беспорядки, забастовки, военные действия.

23. Политика информационной безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы, и содержит:

1) описание состава информационной системы;

2) список пользователей автоматизированной информационной системы единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда, их права и приоритеты (в зависимости от их служебного положения и характера выполняемых функций) на доступ к информации, программным и техническим средствам;

3) план мероприятий по защите информации, который включает организационные и программно–технические меры.

24. Для построения надежной и эффективной системы защиты информационной системы используются следующие принципы и подходы:

1) подготовка персонала обеспечивает обязательное периодическое обучение всех работников, участвующих в управлении, использовании или функционировании системы защиты информации;

2) привлечение для разработки и установки средств и систем защиты информационных систем на договорной основе организаций, предоставляющих данные услуги.

25. Организационные меры обеспечивают соблюдение нормативных правовых актов Республики Казахстан и внутренних требований единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда, отслеживание состояния безопасности внутри единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда, реагирование на случаи нарушений, развитие защитных мер с учетом изменений в едином накопительном пенсионном фонде и добровольном накопительном пенсионном фонде.

26. К организационным мерам обеспечения безопасности относятся следующие мероприятия:

1) физическая защита информационных систем;

2) поддержание работоспособности информационных систем, имеющих отношение к информационной безопасности;

3) установление каждому пользователю соответствующего права доступа, необходимого для выполнения им возложенных должностных обязанностей и обеспечения взаимозаменяемости;

4) реагирование ответственных лиц на нарушения режима информационной безопасности;

5) планирование восстановительных работ.

27. Физическая защита подразделяется на:

1) физическое управление доступом;

2) меры противопожарной безопасности;

3) защита поддерживающей инфраструктуры;

4) защита от перехвата данных, защита мобильных систем.

28. Мероприятия по поддержанию работоспособности информационных систем:

1) поддержка пользователей – организация консультаций по вопросам информационной безопасности, выявление их типичных ошибок и обеспечение памятками с рекомендациями для распространенных ситуаций;

2) поддержка программного обеспечения – контроль лицензионной (сертифицированной) чистоты программного обеспечения;

3) конфигурационное управление – контроль и фиксирование изменений, вносимых в программную и техническую конфигурацию;

4) резервное копирование для восстановления информационной системы и данных в случае аварии и других обстоятельств непреодолимой силы;

5) управление носителями данных – правила учета, обращения и хранения;

6) документирование – актуальное отражение текущего состояния дел.

29. В случае нарушения режима безопасности информационных систем администратор безопасности осуществляет:

1) выполнение оперативных мероприятий с целью уменьшения наносимого вреда – выявление лица, совершившего несанкционированный доступ и его блокирование;

2) обзор накопленной статистики нарушений – анализ инцидентов, выявление повторных нарушений, разработку мер по усовершенствованию системы защиты

.

30. Программно–технические меры по обеспечению информационной безопасности включают в себя системы:

1) управления доступом;

2) протоколирования и проверки технического состояния.

31. Система управления доступом обеспечивает выполнение следующих мероприятий:

1) определение перечня групп данных, задач и установления им уровня секретности;

2) установление способов и процедур защиты каждой группы данных;

3) определение групп пользователей информационных систем, разбивка их на категории по выполняемым функциям и установление им уровней доступа к информации.

32. К числу событий, затрагивающих безопасность информационной системы и требующих проверки, относятся:

1) вход в систему (успешный или неуспешный);

2) выход из системы;

3) обращение к удаленной системе.

33. Политика работы в локальной сети включает в себя:

1) общие положения;

2) права пользователей (в зависимости от их служебного положения и характера выполняемых функций) на доступ к информации, к программным и техническим средствам;

3) обязанности пользователя при работе в локальной сети;

4) обязанности персонала;

5) список программного обеспечения, устанавливаемого на компьютеры и используемого в локальной сети.

34. Политика резервного копирования включает в себя:

1) общие положения;

2) порядок резервного копирования;

3) контроль результатов резервного копирования;

4) восстановление информации с резервных копий;

5) хранение резервных копий;

6) наличие резервного сервера информационной системы, расположенного в не сейсмоопасной зоне, с обеспечением ежедневного резервного копирования информации.

35. Ответственность за соблюдение информационной безопасности в соответствии с должностными обязанностями несут:

1) первый руководитель единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда;

2) администратор автоматизированной информационной системы;

3) администратор безопасности;

4) лицо, определенное приказом первого руководителя единого накопительного пенсионного фонда и добровольного накопительного пенсионного фонда.

36. Администратор безопасности:

1) осуществляет анализ рисков, выявление объектов, требующих защиты, и уязвимых мест информационных систем, оценивая размер возможного ущерба от нарушения режима безопасности и выбирая эффективные средства защиты;

2) обеспечивает проведение обучения персонала мерам безопасности и правилам поведения в чрезвычайных (экстренных) ситуациях путем обращения особого внимания на вопросы, связанные с антивирусным контролем и правильным вхождением в систему (с указанием при регистрации только своего идентификатора);

3) обеспечивает обязательность процедуры идентификации и аутентификации для доступа к ресурсам информационных систем;

4) не допускает получения права доступа к информационным ресурсам неавторизованными пользователями, предоставляет пользователям входные имена и начальные пароли только после заполнения регистрационных форм;

5) контролирует регулярность выполнения резервного копирования информации, обрабатываемой информационной системой;

6) проводит плановую и внеплановую проверку надежности защиты ресурсов системы;

7) информирует специально назначенных ответственных исполнителей об эффективности существующей политики безопасности и вносит на их рассмотрение предложения об улучшении системы защиты;

8) обеспечивает защиту оборудования корпоративной сети, в том числе специальных межсетевых программных средств;

9) оперативно и эффективно реагирует на события, содержащие угрозу, принимает меры по отражению угрозы и выявлению нарушителей, фиксирует и информирует специально назначенных ответственных исполнителей о попытках нарушения защиты;

10) использует проверенные программно-технические средства отслеживания процесса функционирования информационной системы с целью обнаружения подозрительных ситуаций, наличия зловредного программного обеспечения и его влияния на работу информационной системы и ее компонентов;

11) ежедневно анализирует регистрационную информацию, относящуюся к информационной системе в целом и к файловым серверам в особенности;

12) проводит обзор новинок в области информационной безопасности, информирует о них пользователей и специально назначенных ответственных исполнителей.

37. Пользователи системы:

1) соблюдают и применяют внутренние требования, обеспечивающие безопасность информационных систем;

2) используют доступные зарегистрированные защитные механизмы для обеспечения конфиденциальности и целостности своей информации;

3) выбирают личные пароли длиной не менее восьми буквенно-цифровых символов;

4) обеспечивают недоступность личных паролей другим лицам;

5) информируют администраторов безопасности информационных систем и (или) специально назначенных ответственных исполнителей о нарушениях безопасности и иных подозрительных ситуациях;

6) в случае обнаружения слабых мест в защите ресурсов информационных систем незамедлительно сообщают об этом администраторам безопасности информационных систем и (или) специально назначенным ответственным исполнителям;

7) обеспечивают представление корректной идентификационной и аутентификационной информации;

8) выполняют процедуры для предупреждения проникновения опасного кода, его обнаружения и уничтожения;

9) выполняют нормы поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий и иных обстоятельств непреодолимой силы.

38. Для обеспечения информационной безопасности автоматизированной информационной системы фонда выполняются следующие требования:

1) защита каналов передачи данных с шифрованием трафика с помощью аппаратных и программных средств;

2) использование программно-технических средств отслеживания процесса функционирования автоматизированной информационной системы с целью обнаружения подозрительных ситуаций, наличия зловредного программного обеспечения и его влияния на работу автоматизированной информационной системы и ее компонентов;

3) использование системы обнаружения (предотвращения) атак из сети интернет в компьютерную сеть единого накопительного пенсионного фонда или добровольного накопительного пенсионного фонда;

4) наличие минимум одного программно-аппаратного межсетевого экрана;

5) анализ и оценка уязвимостей на постоянной основе;

6) доступ к входным данным, функциям, операциям, отчетам обеспечивается посредством ввода соответствующего пароля, который меняется не реже одного раза в тридцать календарных дней;

7) в случае неправильного ввода пароля более трех раз подряд, учетная запись пользователя автоматизированной информационной системы блокируется . Последующая разблокировка производится администратором на основании заявки пользователя автоматизированной информационной системы;

8) при смене пароля автоматизированная информационная система отслеживает использование предыдущих паролей (не менее трех предыдущих паролей);

9) автоматизированная информационная система единого накопительного пенсионного фонда или добровольного накопительного пенсионного фонда обеспечивает сохранение сведений относительно времени совершения операции или внесения изменений в автоматизированную информационную систему и идентификацию пользователя, осуществившего данную операцию или запись;

10) автоматическое завершение операций пользователя или администратора, прерванных в результате отключения электропитания, аварии сетей, телекоммуникаций, разрыва соединений, попытки несанкционированного доступа.

39. Защита информации обеспечивается следующими функциями уровня доступа "администратор":

1) определение групп пользователей, разделение их на категории по выполняемым функциям и установление им уровней доступа к информации, смена паролей;

2) блокирование доступа пользователей к данным и функциям автоматизированных информационных систем;

3) настройка параметров функционирования автоматизированных информационных систем;

4) просмотр подключенных к автоматизированным информационным системам пользователей;

5) исключен постановлением Правления Национального Банка РК от 28.06.2019 № 103 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования);

6) отключение пользователей от автоматизированных информационных систем в случае необходимости.

Сноска. Пункт 39 с изменением, внесенным постановлением Правления Национального Банка РК от 28.06.2019 № 103 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).