О внесении изменений в некоторые нормативные правовые акты Республики Казахстан по вопросам регулирования информационной безопасности на рынке ценных бумаг

Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 15 ноября 2021 года № 102. Зарегистрировано в Министерстве юстиции Республики Казахстан 25 ноября 2021 года № 25385

В соответствии с подпунктом 2) пункта 1 статьи 48 и статьей 49-1 Закона Республики Казахстан "О рынке ценных бумаг" Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка ПОСТАНОВЛЯЕТ:

1. Внести в постановление Правления Национального Банка Республики Казахстан от 28 апреля 2012 года № 165 "Об утверждении Требований к программно-техническим средствам и иному оборудованию, необходимым для осуществления деятельности на рынке ценных бумаг" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов Республики Казахстан под № 7734) следующее изменение:

Требования к программно-техническим средствам и иному оборудованию, необходимым для осуществления деятельности на рынке ценных бумаг, утвержденные указанным постановлением, изложить в новой редакции согласно приложению к настоящему постановлению.

2. 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 приложении 5:

подпункт 11) пункта 1 изложить в следующей редакции:

"11) документация по обеспечению информационной безопасности;";

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 сведения , составляющие 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 антивирусной защиты 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 использования Интернета и электронной почты;

17) порядок управления обновлениями информационных систем.";

подпункт 4) пункта 18 изложить в следующей редакции:

"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.".

3. 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.

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 по истечении десяти календарных дней после дня его первого официального опубликования.

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

Приложение к постановлению
Правления Агентства
Республики Казахстан
по регулированию и развитию

финансового рынка
от 15 ноября 2021 года № 102
Утверждены
постановлением Правления
Национального Банка
Республики Казахстан
от 28 апреля 2012 года № 165

Требования к программно-техническим средствам и иному оборудованию, необходимым для осуществления деятельности на рынке ценных бумаг

Глава 1. Общие положения

1. Настоящие Требования к программно-техническим средствам и иному оборудованию, необходимым для осуществления деятельности на рынке ценных бумаг (далее - Требования), определяют минимально необходимый функционал программно-технических средств и иного оборудования (далее – информационная система), а также набор требований к обеспечению информационной безопасности при обработке информации, содержащей коммерческую тайну, на программно-технических средствах и ином оборудовании организаций, осуществляющих деятельность на рынке ценных бумаг (далее – организации).

2. Действие Требований не распространяется на:

1) отношения, возникающие при использовании информационных ресурсов Национального Банка Республики Казахстан и (или) уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций (далее – уполномоченный орган) на основании соответствующего соглашения, заключенного между профессиональным участником рынка ценных бумаг и Национальным Банком Республики Казахстан и (или) уполномоченным органом;

2) страховые (перестраховочные) организации, осуществляющие деятельность в отрасли "страхование жизни", имеющие лицензию уполномоченного органа на осуществление деятельности по управлению инвестиционным портфелем на рынке ценных бумаг.

3. В Требованиях используются следующие понятия:

1) обеспечение информационной безопасности – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информации организации;

2) привилегированная учетная запись – учетная запись в информационной системе, обладающая привилегиями создания, удаления и изменения прав доступа других учетных записей;

3) журнал аудита - специализированное средство, разработанное с целью отражения штатных и критических действий в процессе функционирования программного обеспечения;

4) администратор – работник или подразделение (работники или подразделения) организации, наделенный (наделенные) правами конфигурирования информационной системы или группы информационных систем;

5) рабочая станция – стационарный персональный компьютер пользователя информационной системы организации;

6) доступ – возможность использования информационных систем;

7) мобильное устройство – электронное устройство индивидуального пользования, функционирующее на основе мобильной версии операционной системы;

8) ноутбук – персональный компьютер, исполненный в форме, удобной для переноски и использования в том числе, за пределами периметра защиты;

9) резервная копия – копия данных на носителе информации, предназначенная для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения;

10) технологическая учетная запись – учетная запись в информационной системе, предназначенная для аутентификации при взаимодействии информационных систем.

Глава 2. Требования к функционалу информационных систем

4. Информационные системы обеспечивают:

1) контроль полноты вводимых данных полей обязательных к заполнению, необходимых для проведения и регистрации операций (в случае выполнения функций или операций без полного заполнения всех полей информационная система обеспечивает выдачу соответствующего уведомления);

2) поиск информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по любым параметрам (определенным для данной информационной системы) и возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в информационной системе;

3) обработку информации и ее хранение по дате и времени;

4) автоматизированное формирование форм отчетов, представляемых профессиональными участниками рынка ценных бумаг в Национальный Банк Республики Казахстан, а также выписок с лицевого счета, отчетов о проведенных операциях;

5) ведение и автоматизированное формирование журналов системы внутреннего учета профессиональных участников рынка ценных бумаг, предусмотренных Законом Республики Казахстан "О рынке ценных бумаг" (далее – Закон о рынке ценных бумаг). Информационная система формирует журнал полностью, а также частично (на указанный диапазон дат, определенную дату, для конкретного зарегистрированного лица, для конкретного статуса входящего документа);

6) возможность вывода выходных документов на экран, принтер или в файл;

7) применение системы двойного ввода приказов разными пользователями ("первый ввод" и "второй ввод") или системы подтверждения ввода приказов разными пользователями (валидация или верификация) в целях исключения ошибок при вводе данной информации (за исключением ввода заявок на покупку и продажу финансовых инструментов в торговую систему фондовой биржи и ввода приказов клиентами центрального депозитария посредством информационной системы центрального депозитария).

При введении информации пользователи "второго ввода" не имеют доступа к информации, введенной пользователями "первого ввода". В случае несоответствия данных "второго ввода" данным "первого ввода" информационная система выдает соответствующее уведомление.

При использовании системы подтверждения ввода приказов разными пользователями (валидация или верификация) информация, введенная первым пользователем, подтверждается вторым пользователем.

Используемый способ (двойной ввод, валидация или верификация) и перечень приказов, подлежащих вводу с применением указанных способов, определяются внутренними документами профессионального участника рынка ценных бумаг;

8) возможность обмена электронными документами.

5. Для организаций, осуществляющих на основании соответствующей лицензии уполномоченного органа либо в соответствии с Законом о рынке ценных бумаг брокерскую и (или) дилерскую деятельность с правом ведения счетов клиентов в качестве номинального держателя, деятельность по ведению системы реестров держателей ценных бумаг, кастодиальную деятельность, информационная система в дополнение к требованиям, предусмотренным пунктом 4 Требований, обеспечивает:

1) проведение следующих операций:

открытие лицевого счета;

изменение сведений о зарегистрированном лице, паевом инвестиционном фонде или об управляющей компании паевого инвестиционного фонда;

внесение записей об аннулировании выпуска эмиссионных ценных бумаг;

списание (зачисление) ценных бумаг со (на) счетов (счета) зарегистрированных лиц ;

внесение записей об увеличении количества акций на лицевом счете зарегистрированного лица в связи с увеличением количества размещенных акций эмитента (за вычетом акций, выкупленных эмитентом);

внесение записей о конвертировании ценных бумаг и иных денежных обязательств эмитента в простые акции эмитента;

внесение записей об обмене размещенных акций эмитента одного вида на акции данного эмитента другого вида;

обременение ценных бумаг и снятие обременения;

блокирование ценных бумаг и снятие блокирования ценных бумаг;

внесение записи о доверительном управляющем и удаление записи о доверительном управляющем;

закрытие лицевого счета;

составление и выдачу выписок с лицевого счета (субсчета) на определенную дату и время, отчетов о проведенных операциях и отчетов по запросам держателей ценных бумаг, центрального депозитария, эмитентов и уполномоченного органа;

2) сохранность изменяемых данных при изменении фамилии, имени, отчества (при его наличии) или полного наименования зарегистрированного лица и поиск зарегистрированного лица по прежним данным;

3) сохранность информации по всем операциям, проведенным по лицевому счету за весь период;

4) взаимодействие с информационной системой центрального депозитария в процессе регистрации операций с эмиссионными ценными бумагами.

6. В соответствии с Законом о рынке ценных бумаг для организаций, осуществляющих брокерскую и (или) дилерскую деятельность с правом ведения счетов клиентов в качестве номинального держателя, имеющих субсчет депонента, открытый в системе учета центрального депозитария, для агрегированного учета финансовых инструментов, принадлежащих его клиентам, информационная система в дополнение к требованиям, предусмотренным пунктами 4 и 5 Требований, обеспечивает:

1) ведение журнала аудита в процессе функционирования программного обеспечения;

2) автоматизированную передачу в центральный депозитарий по вышеуказанному субсчету депонента электронных данных об остатках финансовых инструментов и операциях с финансовыми инструментами, требуемых в соответствии со сводом правил центрального депозитария.

7. Информационная система организаций, обладающих лицензиями на осуществление брокерской и (или) дилерской деятельности с правом ведения счетов клиентов в качестве номинального держателя, кастодиальной деятельности, в дополнение к требованиям, предусмотренным пунктами 4 и 5 Требований, обеспечивает:

1) возможность учета активов клиентов, переданных в номинальное держание и (или) на кастодиальное обслуживание;

2) ведение персонального учета активов клиента, всех операций по его счетам, возможность анализа истории операций по счетам, в том числе автоматизированное формирование сведений об остатках денег по состоянию на любую дату и время в течение операционного дня, а также о движении денег в разрезе каждого клиента и организации, которая осуществляет учет и хранение денег клиента, включая, но не ограничиваясь следующей информацией:

дата и время проведения операции с деньгами;

наименование операции;

реквизиты и наименование подтверждающего документа;

фамилия, имя, отчество (при его наличии) или наименование клиента;

наименование расчетно-депозитарной системы, через которую осуществляются расчеты по сделкам с финансовыми инструментами;

наименование организации, которой осуществляется учет и хранение денег брокера и (или) дилера и его клиентов;

сумма каждой операции по деньгам по счету клиента;

сумма вознаграждения брокера и (или) дилера, кастодиана, фондовой биржи и иных организаций с указанием услуги и (или) сделки (операции), за оказание (проведение) которой данное вознаграждение было начислено и (или) списано со счета;

назначение платежа;

наименование контрагента по операции с деньгами и реквизиты его счета;

наименование банка второго уровня, филиала банка-нерезидента Республики Казахстан или организации, осуществляющей отдельные виды банковских операций, выступающей со стороны контрагента по операции с деньгами, и реквизиты его (ее) счета;

3) взаимодействие с информационной системой фондовой биржи и (или) клиринговой организации в процессе регистрации сделок с эмиссионными ценными бумагами.

8. Информационная система организаций, обладающих лицензией на осуществление брокерской и (или) дилерской деятельности с правом ведения счетов клиентов в качестве номинального держателя, в дополнение к требованиям, предусмотренным пунктами 4, 5, 6 и 7 Требований, обеспечивает:

автоматизированный расчет значений рисков на одного клиента, установленных Правилами формирования системы управления рисками и внутреннего контроля для организаций, осуществляющих брокерскую и дилерскую деятельность на рынке ценных бумаг, деятельность по управлению инвестиционным портфелем, утвержденными постановлением Правления Национального Банка Республики Казахстан от 27 августа 2013 года № 214, зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 8796. Данный расчет осуществляется в случае исполнения клиентских заказов при отсутствии достаточного количества денег и (или) ценных бумаг у клиента на банковском и (или) лицевом счете данного брокера и (или) дилера или организации, осуществляющей управление инвестиционным портфелем, являющейся брокером и (или) дилером, для исполнения данного заказа;

автоматизированный расчет значений пруденциальных нормативов для брокера и (или) дилера в соответствии с Правилами расчета значений пруденциальных

нормативов, обязательных к соблюдению организациями, осуществляющими брокерскую и (или) дилерскую деятельность на рынке ценных бумаг, утвержденными постановлением Правления Национального Банка Республики Казахстан от 27 апреля 2018 года № 80, зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 17005;

осуществление отдельного учета финансовых инструментов и денег, принадлежащих брокеру и (или) дилеру первой категории, от финансовых инструментов и денег его клиентов.

Информационная система организаций, осуществляющих управление инвестиционным портфелем, в дополнение к требованиям, предусмотренным пунктом 4 Требований, обеспечивает:

автоматизированный расчет значений пруденциальных нормативов для организации, осуществляющей управление инвестиционным портфелем, в соответствии с Правилами расчета значений пруденциальных нормативов, обязательных к соблюдению организациями, осуществляющими деятельность по управлению инвестиционным портфелем, утвержденными постановлением Правления Национального Банка Республики Казахстан от 27 апреля 2018 года № 79, зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 17008;

осуществление отдельного учета финансовых инструментов и денег, принадлежащих организации, осуществляющей управление инвестиционным портфелем, от финансовых инструментов и денег его клиентов.

9. Типовые формы электронных документов, которыми обмениваются организации, осуществляющие на основании соответствующей лицензии уполномоченного органа либо в соответствии с Законом о рынке ценных бумаг брокерскую и (или) дилерскую деятельность с правом ведения счетов клиентов в качестве номинального держателя, деятельность по ведению системы реестров держателей ценных бумаг, кастодиальную деятельность, определяются внутренним документом центрального депозитария и соответствуют требованиям, определенным сводом правил центрального депозитария.

10. Информационная система фондовой биржи в дополнение к требованиям, предусмотренным пунктом 4 Требований, обеспечивает:

1) идентификацию физических лиц, уполномоченных на заключение сделок от имени члена фондовой биржи и выполнение действий от имени члена фондовой биржи с использованием торговой системы данной фондовой биржи (трейдер), при каждом использовании торговой системы фондовой биржи;

2) ведение реестра трейдеров фондовой биржи, допущенных к торгам, отстраненных от участия в торгах (с указанием причины отстранения);

3) ограничение возможности заключения сделок с использованием торговой системы фондовой биржи лицами, не обладающими таким правом в соответствии с внутренними документами фондовой биржи;

4) мониторинг параметров сделок, заключаемых в торговой системе фондовой биржи, на предмет выявления сделок с ценными бумагами, соответствующих условиям , определенным пунктами 5 и 6 статьи 56 Закона о рынке ценных бумаг, а также случаям, установленным главой 9 Правил осуществления деятельности организации торговли с ценными бумагами и иными финансовыми инструментами, утвержденных постановлением Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 29 октября 2008 года № 170, зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 5406;

5) предоставление уполномоченному органу доступа к программному обеспечению фондовой биржи (без возможности внесения корректировок), обеспечивающему осуществление функций, предусмотренных подпунктом 4) настоящего пункта;

6) возможность мониторинга сделок, заключенных в торговой системе фондовой биржи, на предмет соответствия требованиям Закона о рынке ценных бумаг и правил фондовой биржи;

7) автоматизированный сбор, обработку и хранение финансовой отчетности и иной информации, предоставляемой членами фондовой биржи и эмитентами, чьи ценные бумаги предполагаются к включению или включены в список фондовой биржи, в том числе в целях мониторинга их финансового состояния;

8) возможность мониторинга раскрытия эмитентами ценных бумаг, включенных в список фондовой биржи, информации в объеме, определенном Законом о рынке ценных бумаг, Законом Республики Казахстан "Об акционерных обществах" и внутренними документами фондовой биржи.

11. Информационная система центрального депозитария в дополнение к требованиям, предусмотренным пунктом 4, подпунктами 1), 2) и 3) пункта 5 и пунктом 7 Требований, обеспечивает:

1) до совершения операции по лицевому счету (субсчету) зарегистрированного лица проверку:

возможности совершения такой операции с учетом требований Закона о рынке ценных бумаг, Правил осуществления деятельности центрального депозитария, утвержденных постановлением Правления Национального Банка Республики Казахстан от 29 ноября 2018 года № 307, зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 17920 (далее – Правила № 307) и свода правил центрального депозитария;

реквизитов документов, на основании которых совершается операция по лицевому счету (субсчету) зарегистрированного лица, на предмет наличия и соответствия требованиям свода правил центрального депозитария;

2) идентификацию документов, подтверждающих полномочия лиц, передающих документы, на основании которых совершается операция по лицевому счету (субсчету) зарегистрированного лица, совершать данные действия, а также полномочия лиц, подписавших приказы, на основании которых регистрируется операция по лицевому счету (субсчету) или проводится информационная операция;

3) отказ в совершении операции по лицевому счету (субсчету) зарегистрированного лица, если по итогам проверки, произведенной в соответствии с подпунктом 1) настоящего пункта:

установлено несоответствие предполагаемой к совершению операции требованиям Закона о рынке ценных бумаг, Правил № 307 и свода правил центрального депозитария ;

установлено отсутствие или несоответствие реквизитов в документах, на основании которых совершается операция по лицевому счету (субсчету) зарегистрированного лица, требованиям свода правил центрального депозитария;

не подтверждены полномочия лиц, передающих документы, на основании которых совершается операция по лицевому счету (субсчету) зарегистрированного лица, совершать данные действия;

4) ограничение возможности для проведения операций по лицевым счетам (субсчетам) зарегистрированных лиц, после закрытия операционного дня, если следующий операционный день не открыт;

5) ведение журнала аудита в процессе функционирования информационной системы;

6) ведение реестра сделок с производными финансовыми инструментами, заключенными на организованном и неорганизованном рынках.

12. Информационная система клиринговой организации в дополнение к требованиям, предусмотренным пунктом 4 Требований, обеспечивает:

1) автоматизированный сбор, обработку и хранение информации по сделкам, по которым данная клиринговая организация осуществляет клиринговое обслуживание, ее сверку и корректировку;

2) учет параметров всех заключенных сделок в торговой системе организатора торгов и (или) на товарной бирже, принятых на клиринговое обслуживание;

3) возможность осуществления расчета требований и (или) обязательств клиринговых участников торгов, в том числе определения чистых позиций клиринговых участников торгов;

4) автоматизированную передачу информации, указанной в подпункте 3) настоящего пункта, в центральный депозитарий и (или) иную организацию,

осуществляющую организацию расчетов (платежей) по сделкам с финансовыми инструментами;

5) формирование отчета по результатам клиринговой деятельности для клиринговых участников торгов.

13. Обеспечивается резервное хранение данных информационных систем, их файлов и настроек, которое обеспечивает восстановление работоспособной копии информационной системы. Порядок и периодичность резервного копирования, хранения, восстановления информации, периодичность тестирования восстановления работоспособности информационных систем из резервных копий определяются внутренними документами организации.

14. При выполнении операций информационная система выдает уведомление, при наступлении следующих условий:

1) количество ценных бумаг (денег), подлежащих списанию с лицевого счета, превышает количество ценных бумаг (денег) на счету;

2) ценные бумаги, подлежащие списанию, обременены или блокированы. Уведомление содержит ссылку на лицевой счет и раздел залогодержателя;

3) списываемые ценные бумаги, учитываемые на лицевом счету, находятся в общей собственности нескольких лиц;

4) лицевой счет, с которого списываются ценные бумаги, блокирован.

15. При исправлении ошибки в поле "комментарий" ошибочной записи регистрационного журнала в информационной системе записывается текст "ошибка" (в случае, если возможно исправление записи об ошибочной операции) и указывается номер записи регистрационного журнала об операции, предназначенной для исправления ошибки.

Глава 3. Требования к обеспечению информационной безопасности при обработке в информационных системах информации, содержащей коммерческую тайну

16. Доступ к информации в информационных системах предоставляется работникам организации в объеме, необходимом для исполнения их функциональных обязанностей
.

17. Предоставление доступа к информационным системам организации производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей информационных систем их функциональным обязанностям. Совокупность таких ролей представляет собой матрицу доступа к информационной системе, которая формируется в электронной форме или на бумажном носителе.

18. Доступ к информационным системам осуществляется путем идентификации и аутентификации пользователей информационных систем.

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

19. В информационных системах используются только персонализированные пользовательские учетные записи.

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

21. В информационных системах применяются функции по управлению учетными записями и паролями, а также блокировке учетных записей пользователей, определяемые внутренним документом организации.

22. В информационных системах применяются следующие параметры функции по управлению паролями и блокировками учетных записей пользователей:

1) минимальная длина пароля – значение данного параметра составляет не менее 8 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 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 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 информационную систему и смене пароля. По истечении максимального срока действия пароля информационная система блокирует доступ и требует обязательную смену пароля;

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

7) в случае отсутствия активности пользователя в 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 информационная система автоматически завершает сеанс работы пользователя либо блокирует рабочую

станцию или ноутбук с возможностью разблокировки только при вводе аутентификационных данных пользователя.

23. 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.

24. Обеспечивается синхронизация системного времени информационной системы с централизованным источником эталонного времени.

25. Разработка и доработка информационных систем не осуществляется в среде промышленной эксплуатации.

26. Работники, осуществляющие разработку информационных систем, не имеют полномочий на перенос изменений информационной системы в промышленную среду, а также административный доступ к информационным системам в промышленной среде.

27. Перед вводом в промышленную эксплуатацию 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.

28. Контроль использования привилегированных учетных записей обеспечивается путем:

1) составления и утверждения перечня администраторов информационных систем (операционная система, система управления базами данных, приложение);

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

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

30. Информационные системы обеспечиваются технической поддержкой, в состав которой входят услуги по предоставлению обновлений соответствующей информационной системы, в том числе обновлений безопасности.

31. Обеспечивается ведение и неизменность аудиторского следа информационной системы, как на организационном, так и на техническом уровне.

32. В информационных системах используется функция ведения аудиторского следа, которая отражает следующее:

1) события установления соединений, идентификации, аутентификации и авторизации в 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 информационной системе;

6) события изменения параметров аудита;

7) события изменений системных параметров.

33. 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).

34. Срок хранения аудиторского следа составляет не менее 3 (трех) месяцев в оперативном доступе и не менее 5 (пяти) лет в архивном доступе. Агрегированное хранение аудиторского следа нескольких информационных систем осуществляется в специализированной информационной системе хранения аудиторского следа.

35. Для защиты информационных систем используется лицензионное антивирусное программное обеспечение или системы, обеспечивающие целостность и неизменность программной среды на рабочих станциях, ноутбуках и мобильных устройствах.

36. 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 организацией;

8) для мобильных устройств и иных устройств, используемых вне периметра защиты организации, использование антивирусного программного обеспечения со встроенной функцией межсетевого экранирования.

37. 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.

38. Антивирусное программное обеспечение максимально исключает прерывание пользователем всех служебных процессов (сканирование по расписанию, обновление и другие процессы). Обновление антивирусного программного обеспечения производится не реже одного раза в сутки, полное сканирование устройства – не реже одного раза в неделю.

39. Обеспечивается своевременная установка обновлений безопасности информационных систем.

40. Обновления безопасности информационных систем, устраняющие критичные уязвимости, устанавливаются не позднее одного месяца со дня их публикации и распространения производителем.

41. Обновления информационных систем до установки в промышленную среду проходят испытания в тестовой среде.

42. В целях обеспечения непрерывности функционирования информационных систем во внутренних документах определяются:

1) допустимые сроки простоя информационных систем;

2) перечень информационных систем, подлежащих восстановлению и подходы к их восстановлению;

3) критерии и порядок принятия решений о восстановлении информационных систем;

4) планы восстановления информационных систем.

43. При наличии резервного центра во внутренних документах отражается:

1) местонахождение резервного центра;

2) перечень бизнес–процессов, технических, программных или других средств, обеспечивающих работу информационных систем, восстановление которых планируется в резервном центре;

3) порядок восстановления работы информационных систем 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.

44. В целях проверки готовности процессов восстановления деятельности информационных систем не менее одного раза в год проводится тестирование восстановления информационных систем в соответствии с планами восстановления (далее – тестирование планов восстановления).

Тестирование планов восстановления проводится по разработанной и утвержденной программе, предусматривающей описание сценария возникновения нештатной ситуации, восстанавливаемых рабочих процессов и информационных систем, действий команды восстановления, требований по срокам и месту проведения работ.

45. По итогам тестирования планов восстановления подготавливается документ о результатах тестирования (протокол) с указанием:

1) перечня информационных систем, по которым проведено тестирование;

2) времени, затраченного на восстановление работы информационных систем;

3) выявленных недостатков планов восстановления и предложений по их устранению.