УТВЕРЖДЕНЫ
Приказом
Генерального директора
ООО «Системы распределенного реестра»
от «24» января 2024 г. № 240124-Пр-1

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ
при работе в информационной системе, в которой осуществляется выпуск цифровых финансовых активов

г. Москва
2024

Содержание

1. Общие положения

1.1. Настоящие Рекомендации по защите информации в информационной системе, в которой осуществляется выпуск цифровых финансовых активов (далее – Рекомендации по ЗИ), разработаны в соответствии с положениями следующих документов:

– Положения Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»;

– Правил информационной системы Общества с ограниченной ответственностью «Системы распределенного реестра», согласованных Банком России в порядке, предусмотренном законодательством Российской Федерации;

– эксплуатационной документации на средства электронной подписи, применяемые для формирования электронной подписи в ИС ЦФА.

1.2. Настоящие Рекомендации по ЗИ распространяется на всех клиентов Оператора и рекомендуемы для исполнения на средствах вычислительной техники, с использованием которых клиентами совершаются действия в ИС ЦФА.

1.3. Настоящие Рекомендации по ЗИ разработаны в целях исполнения п. 1.13 Положения Банка России от 20.04.2021 № 757-П и доведение до клиентов Оператора:

а) информации о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

б) рекомендаций по защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования СВТ (вредоносного кода), в целях противодействия незаконным финансовым операциям;

в) информации о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

1.4. Реализация клиентами на СВТ организационных и технических мер защиты информации, приведенных в настоящих Рекомендациях по ЗИ, обеспечивает минимизацию рисков несанкционированного доступа к защищаемой информации.

1.5. Настоящие Рекомендации по ЗИ не должны рассматриваться как результат каких-либо консультационных или иных услуг клиентам со стороны Оператора или оказание таких услуг. Оператор ни прямо ни косвенно не несет ответственность ни за действия или бездействия клиентов, основанных на реализации настоящих Рекомендаций по ЗИ, ни за последствия таких действий или бездействий.

2. Список терминов и определений

Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Бизнес процесс – совокупность взаимосвязанных мероприятий и работ, направленных на создание определенного продукта или услуги для потребителей.

Вредоносный код – программный код, приводящий к нарушению штатного функционирования средства вычислительной техники.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – персональные данные, ключи электронной подписи, аутентификационная информация (пароли, PIN-коды) пользователей.

Информация – сведения (сообщения, данные) независимо от формы их представления.

ИС ЦФА – информационная система, в которой осуществляется выпуск цифровых финансовых активов, на базе программы для ЭВМ «Платформа для выпуска и обмена цифровых финансовых активов».

Клиент – пользователь, присоединившийся к Правилам информационной системы Общества с ограниченной ответственностью «Системы распределенного реестра», согласованным Банком России в порядке, предусмотренном законодательством Российской Федерации.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

Компьютерная атака – целенаправленное несанкционированное воздействие на информацию, на ресурс информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Несанкционированный доступ – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Оператор – Общество с ограниченной ответственностью «Системы распределенного реестра» (ОГРН 1217700216360), включенное Банком России в реестр операторов информационных систем, осуществляющее деятельность по эксплуатации ИС ЦФА.

Операционная система – совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности системы обработки информации за счет автоматизированного управления ее работой и предоставляемого пользователю определенного набора услуг.

Пользователь – юридическое лицо, физическое лицо или физическое лицо, являющееся индивидуальным предпринимателем, включенное в Реестр пользователей.

Программное обеспечение (ПО) – совокупность программ системы обработки данных и программных документов, необходимых для эксплуатации этих программ.

Реестр пользователей – являющаяся частью ИС ЦФА совокупность информации, включающей сведения о пользователях, в том числе, сведения, необходимые для аутентификации пользователей в ИС ЦФА, сведения о том, в каком статусе или статусах пользователи аутентифицированы в ИС ЦФА.

Риск информационной безопасности – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб.

Сайт Оператора – сайт Оператора в сети общего пользования «Интернет», доступ к которому осуществляется по доменному имени «masterchain.ru».

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Средство антивирусной защиты – программное обеспечение, способное определять, удалять и защищать против всех видов вредоносного программного кода, включая вирусы, «трояны», шпионские и рекламные программы.

Средство вычислительной техники (СВТ) – совокупность технических устройств и программ, обеспечивающих их функционирование, способных функционировать самостоятельно или в составе других систем и используемых клиентами для совершения действия в ИС ЦФА.

Угроза безопасности информации (УБИ) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения

безопасности информации.

Уязвимость – недостаток (слабость) программного (программно-технического) или информационной системы в целом, который(ая) может быть использован(а) для реализации угрозы безопасности информации.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3. Информация о возможных рисках несанкционированного доступа к защищаемой информации

3.1 Возможными рисками несанкционированного доступа к защищаемой информации, которые могут наступить от реализации угроз безопасности информации, могут являться:

а) утечка или разглашение персональных данных;
б) финансовый ущерб (в т.ч. при осуществлении финансовых операций лицами, не обладающими правом их осуществления).

3.2 Основным источником рисков несанкционированного доступа к защищаемой информации являются третьи лица (группы лиц), реализующие целенаправленные компьютерные атаки, в т.ч. на СВТ клиентов, с целью личного обогащения или блокирования штатного функционирования бизнес-процессов ИС ЦФА.

3.3 Основными способами реализации рисков несанкционированного доступа к защищаемой информации являются:

а) воздействие на клиентов (телефонные звонки, рассылки в почте или мессенджерах, размещение в сети общего пользования «Интернет» поддельных сайтов и ссылок на них и др. [социальная инженерия]);
б) внедрение в СВТ вредоносного кода;
в) физическое воздействие (хищение, повреждение, уничтожение и др.) на СВТ, в т.ч. ключевые носители;
г) использование уязвимостей в программном обеспечении, в конфигурации СВТ, в обеспечении защиты сетевого взаимодействия и каналов передачи данных.

4. Рекомендации по защите информации от воздействия вредоносного кода

4.1 На СВТ необходимо применять только лицензионные средства антивирусной защиты, полученные из доверенных источников. Не используйте средства антивирусной защиты, полученные из недоверенных источников, они могут не выполнять заявленные функции или сами являться вредоносным кодом.

4.2 Необходимо обеспечить автоматический запуск средств антивирусной защиты при загрузке ОС и их функционирование в резидентном режиме (в режиме service — для операционных систем Windows, в режиме daemon — для UNIX-подобных операционных систем).

4.3 Необходимо настроить применяемые на СВТ средства антивирусной защиты на обеспечение автоматического входного контроля:

а) съемных носителей информации перед их использованием на СВТ;
б) файлов из внешних источников (съемных носителей информации, сетевых подключений, почтового трафика) при загрузке, открытии или исполнении таких файлов.

4.4 Необходимо настроить применяемые на СВТ средства антивирусной защиты на выполнение следующих видов проверок на отсутствие вредоносного кода:

а) полная проверка – не реже 1 раза в неделю;
б) проверка важных областей – ежедневно;

в) проверка файлов из внешних источников – в масштабе времени, близком к реальному.

4.5 Средствами антивирусной защиты необходимо обеспечить выполнение проверок на отсутствие вредоносного кода устанавливаемого на СВТ ПО или обновлений уже установленного ПО, а также выполнение проверок после установки или обновления ПО.

4.6 Необходимо обеспечить обновление версий программных компонентов и баз данных признаков вредоносного кода применяемых на СВТ средств антивирусной защиты по факту их выпуска вендором в масштабе времени, близком к реальному.

4.7 При подключении к СВТ съемных носителей информации не следует отключать (приостанавливать) задачу антивирусной проверки подключаемых съемных носителей информации.

4.8 При использовании электронной почты рекомендуется:

4.8.1. Проверять электронный адрес (аккаунт) отправителя. Письма, поступившие от неизвестных адресатов или от адресатов в адресах, которых присутствуют ошибки не открывать, вложения не загружать. Оператор может направлять письма с электронных адресов dfa@masterchain.ru, info@masterchain.ru, ca@masterchain.ru и других, указанных в заключенных с клиентами договорами (соглашениями).

4.8.2. Проверять расширение вложенных файлов. Если расширение вложенных файлов являются исполняемыми или неизвестными (например: *.exe, *.com, *.vbs, *.bat, *.scr, *doc.exe, *xlsx.scr и т.п.), то открывать их рекомендуется после уточнения (по другому каналу связи) у адресата о действительности направленных файлов.

4.8.3. Проверить загруженные файлы средством антивирусной защиты до запуска. Файлы, находящиеся в архиве с паролем необходимо сначала распаковать, а затем выполнять их проверку средством антивирусной защиты.

4.8.4. При открытии документа не включать макросы (встроенное в офисные приложения программное обеспечение) не убедившись перед этим (по другому каналу связи) у адресата, что он знает о них и их предназначении. По возможности не включать макросы.

4.8.5. Перед переходом на внешние ресурсы, в т.ч. в сети общего пользования «Интернет», ссылки на которые содержатся в полученном письме, убедиться, что ресурсы относятся к безопасным (по данным средства антивирусной защиты). В случае получения предупреждающих сообщений от средства антивирусной защиты прекратить доступ к внешнему ресурсу, при доступе к которому они получены.

4.9 При работе с ресурсами сети общего пользования «Интернет» рекомендуется:

4.9.1. Перед переходом на сайт убедиться, что он относится к безопасным (по данным средства антивирусной защиты). В случае получения предупреждающих сообщений от средства антивирусной защиты прекратить доступ к сайту, при посещении которого они получены.

4.9.2. Проверить загруженные файлы средством антивирусной защиты до запуска. Файлы, находящиеся в архиве с паролем необходимо сначала распаковать, а затем выполнять их проверку средством антивирусной защиты.

4.9.3. Не выполнять неконтролируемое открытие самораспаковывающихся архивов и исполняемых файлов.

5. Информации о мерах по предотвращению несанкционированного доступа к защищаемой информации

5.1. Рекомендации по противодействию воздействию на клиентов (социальной инженерии)

5.1.1. В случае поступления обращения (телефонного звонка, электронного письма и т.п.) от лица, представляющегося работником Оператора, с запросом предоставить пароль, коды для доступа к ИС ЦФА, либо предоставить другую

информацию, позволяющую получить доступ к ИС ЦФА посторонним лицам, ни в коем случае не сообщайте запрашиваемую информацию. При возникновении технических сбоев или проблем с функционированием ИС ЦФА работники Оператора не запрашивают пароли, коды или другую информацию, необходимую для доступа к ИС ЦФА.

5.1.2. Никому ни при каких обстоятельствах не сообщайте пароль или PIN-код от ключевого носителя, содержащего используемые в ИС ЦФА ключи электронной подписи.

5.1.3. При работе с электронной почтой и мессенджерами всегда проверяйте электронный адрес (аккаунт) отправителя, не открывайте письма, сообщения и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах и сообщениях ссылкам.

5.1.4. Относитесь к поступающей в звонках и сообщениях информации рационально и критически. Помните, что сильные и внезапные эмоции могут влиять отрицательно влиять на принимаемые решения, особенно в режиме спешки. В таких случаях возьмите паузу, чтобы подумать или перепроверить поступающую информацию.

5.1.5. Не предоставляйте приложениям и иному ПО доступ к данным другого установленного на СВТ ПО, в котором может содержаться защищаемая информация. Относитесь бдительно к запросам на доступ ПО к использованию микрофона и камерам.

5.1.6. При обращении к ИС ЦФА убедитесь в корректности вводимого адреса. Не рекомендуется переходить на страницы ИС ЦФА по ссылке с других ресурсов, размещенных в сети общего пользования «Интернет». Поддельные страницы фишингового сайта могут повторять дизайн ИС ЦФА и вводимые в поля логины и пароли могут в дальнейшем использоваться для получения доступа к ИС ЦФА от имени учетной записи клиента.

5.2. Рекомендации по физической защите средств вычислительной техники

5.2.1. Необходимо исключить возможность бесконтрольного доступа посторонних лиц к СВТ.

5.2.2. Необходимо располагать СВТ в помещениях так, чтобы исключить несанкционированный просмотр посторонними лицами обрабатываемой информации с экрана монитора.

5.2.3. Не допускается оставлять СВТ без контроля после ввода пароля при включенном экране монитора. При отсутствии пользователя СВТ должно быть заблокировано – на экране монитора после блокировки не должна отображаться информация сеанса пользователя (в т.ч. использование «хранителя экрана», гашение экрана или иных способов, требующих повторного ввода пароля).

5.2.4. Передача СВТ в сторонние организации для ремонта или технического обслуживания, а также в пользование третьим лицам, при необходимости, осуществляется только после удаления с него ключевой информации.

5.2.5. Необходимо исключить возможность несанкционированного не обнаруживаемого изменения аппаратной части СВТ.

5.3. Рекомендации по использованию программного обеспечения

5.3.1. На СВТ необходимо применять только лицензионное ПО (ОС, прикладное ПО) и его обновления, полученные из доверенных источников.

5.3.2. На СВТ должна быть установлена только одна ОС, не должны использоваться нестандартные, измененные или отладочные версии ОС.

5.3.3. Необходимо производить регулярную установку обновлений ОС, браузеров и иного ПО, используемого в составе СВТ. Необходимо обеспечить

установку обновлений по факту их выпуска вендором. Своевременная установка обновлений снижает вероятность эксплуатации уязвимого ПО, содержащего известные уязвимости, которые могут быть использованы для получения несанкционированного доступа к защищаемой информации.

5.3.4. На СВТ не следует использовать средства разработки или отладки ПО, а также ПО, содержащее возможности, позволяющие модифицировать содержимое произвольных областей памяти, память, выделенную для других программ, собственный код и код других программ, несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске, модифицировать настройки ОС, использовать недокументированные функции ОС.

5.4. Рекомендации по защите сетевого взаимодействия и каналов передачи данных

5.4.1. Необходимо отключить все не используемые на СВТ сервисы и сетевые протоколы.

5.4.2. Необходимо закрыть доступ ко всем не используемым на СВТ сетевым портам.

5.4.3. На СВТ необходимо использовать межсетевые экраны, в т.ч. встроенные в ОС.

5.4.4. Защита информации, передаваемой по каналу связи между СВТ и ИС ЦФА, обеспечивается по протоколу TLS.

5.5. Рекомендации по безопасной конфигурации средства вычислительной техники

5.5.1. Средствами BIOS (UEFI) необходимо исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой.

5.5.2. Необходимо настроить режимы безопасности, реализованные в ОС, на максимальный уровень.

5.5.3. Необходимо обеспечить идентификацию и аутентификацию пользователей при входе в ОС. Использование режима автоматического входа пользователя в ОС при ее загрузке должно быть исключено.

5.5.4. Необходимо ограничить количество неудачных попыток входа в ОС – не более 10. После превышения заданного количества неудачных попыток входа – ОС должна блокироваться.

5.5.5. Всем пользователям, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права. Каждый пользователь ОС, не являющийся администратором, должен иметь возможность просматривать и редактировать только свои установки в рамках прав доступа, назначенных ему администратором.

5.5.6. Для всех учетных записей, зарегистрированных в BIOS (UEFI), ОС, а также использующихся для доступа к ИС ЦФА, необходимо задать надежный пароль для входа в ОС, удовлетворяющий следующим требованиям:

а) длина пароля должна быть не менее 10 символов;

б) в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

в) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;

г) периодичность смены пароля не должна превышать 6 месяцев.

5.5.7. В качестве паролей, используемых для входа в BIOS (UEFI), ОС, а также использующихся для доступа к ИС ЦФА, не следует использовать:

а) легко вычисляемые сочетания символов (наименования, имена, фамилии, даты рождения, телефонные номера и т.п.);

б) общепринятые сокращения (USER, ADMIN, ALEX и т.п.);

в) словарные и сленговые значения паролей (P@ssw0rd, 1qaz@WSX, !QAZ2wsx,

Qwerty123, !2QwAsZx, Password111, zaq1ZAQ!, 1234QWer, Password123, Password1, 1qaz@WSX, 1qaz!QAZ, QWERasdf, 4rfv%TGB, Katy1999, xsw2#EDC, 1qazXSW@3edc, Panda1234 и т.п).

5.5.8. Не следует использовать один и тот же пароль для входа в BIOS (UEFI), ОС и для доступа к ИС ЦФА.

5.5.9. При вводе паролей обращайте внимание на окружающую обстановку и предпринимайте действия, направленные на снижение вероятности того, что вводимые символы или нажимаемые клавиши могут быть замечены посторонними лицами. Не используйте функцию отображения символов пароля, если не уверены, что значение пароля не станет в этот момент доступно посторонним лицам.

5.5.10. Не сообщайте пароли посторонним лицам, не храните их на легкодоступных носителях (бумажных, электронных), а также воздержитесь от использования функции сохранения паролей в браузере или иных онлайн-хранилищах. При необходимости сохранить пароль используйте специализированное ПО, обеспечивающее шифрование хранимой информации.

5.5.11. При подозрении на компрометацию пароля необходимо незамедлительно предпринять действия по его смене. При подозрении на компрометацию пароля, использующегося для доступа к ИС ЦФА, необходимо незамедлительно уведомить об этом Оператора по электронной почте support@masterchain.ru.

5.5.12. Необходимо обеспечить на СВТ использование системы аудита событий безопасности и регулярный анализ результатов аудита.

5.6. Рекомендации по защите от несанкционированного доступа к ключам электронной подписи

5.6.1. Перед началом работы со средством электронной подписи, используемом для формирования электронной подписи в ИС ЦФА, необходимо ознакомиться с эксплуатационной документации на соответствующее средство электронной подписи.

5.6.2. Необходимо обеспечить защиту доступа к ключевому носителю любого типа, содержащему используемые в ИС ЦФА ключи электронной подписи, паролем или PIN-кодом. Перед началом работы с ключевым носителем необходимо сменить установленное по умолчанию значение пароля или PIN-кода.

5.6.3. Необходимо задать надежный пароль/ PIN-код для доступа к ключевому носителю, удовлетворяющий следующим требованиям:

а) длина пароля/ PIN-кода должна быть не менее 6 символов;

б) в числе символов пароля/ PIN-кода обязательно должны присутствовать буквы, цифры и специальные символы (@, #, $, &, *, % и т.п.);

в) периодичность смены пароля/ PIN-кода не должна превышать 6 месяцев.

5.6.4. При работе со средствами электронной подписи и ключевыми носителями не следует:

а) оставлять без контроля СВТ после ввода ключевой информации;

б) разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения;

в) записывать на ключевые носители постороннюю информацию;

г) изменять настройки, установленные программой установки средства электронной подписи или администратором;

д) вносить какие-либо изменения в программное обеспечение средства электронной подписи;

е) оставлять ключевые носители подключенными к СВТ после завершения операций формирования электронной подписи.

5.6.5. К событиям, связанным с компрометацией ключа электронной подписи, относятся:

а) потеря, хищение ключевого носителя;
б) потеря ключевого носителя с его последующим обнаружением;
в) несанкционированный доступ постороннего лица к ключевому носителю;
г) случаи, когда невозможно достоверно установить, что произошло с ключевым носителем;
д) передача ключа электронной подписи по открытым каналам связи;
е) передача (разглашение) ключа электронной подписи постороннему лицу;
ж) потеря доверительных отношений (например, увольнение) с лицами, имевшими доступ к ключу электронной подписи;
з) нарушение правил хранения ключевой информации.

5.6.6. При компрометации ключа электронной подписи, использующегося для формирования электронной подписи в ИС ЦФА, необходимо незамедлительно прекратить его использование в ИС ЦФА и уведомить о факте компрометации ключа электронной подписи Оператора по электронной почте support@masterchain.ru.

5.6.7. При компрометации ключа электронной подписи необходимо незамедлительно сообщить в удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, о факте компрометации. По получении информации о компрометации ключа электронной подписи удостоверяющий центр досрочно прекращает действие сертификата соответствующего ключа проверки электронной подписи, в результате чего создание действительной электронной подписи с использованием скомпрометированного ключа электронной подписи становится невозможным.

Лист регистрации изменений

Версия	Дата утверждения	Дата ввода в действие	Реквизиты РД
1.0	24.01.2024	24.01.2024	Приказ от 24.01.2024 № 240124-Пр-1