Приложение 1

УТВЕРЖДЕНЫ

Приказом ЗАО «Лидер»

от «10» сентября 2019г. № 72

РЕКОМЕНДАЦИИ

по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям

Москва 2019

1. Общие положения

1.1. Настоящие Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям разработаны (далее - Рекомендации) в соответствии с требованиями Положения Банка России от 17.04.2019 № 684-П «Положение 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» и включают в себя информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, и 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.

1.2. Задачи защиты информации сводятся к минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне ЗАО «Лидер», так и на стороне клиента. В целях предупреждения последствий недобросовестных действий третьих лиц, противодействия проведению незаконных финансовых операций в отношении активов, находящихся в доверительном управлении, разработаны настоящие Рекомендации.

1.3. В результате неправомерных действий третьих лиц информация, связанная с проведением финансовых операций, получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах ЗАО «Лидер», содержащаяся в электронных документах, которыми ЗАО «Лидер» обменивается с клиентами (электронные сообщения), информация, необходимая для авторизации клиента и удостоверения его прав на распоряжение активами,

информация об осуществленных финансовых операциях, а также ключевая информация применяемых средств криптографической защиты (криптографические ключи) (далее в совокупности – защищаемая информация), может быть подвергнута воздействию вредоносных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее – вредоносный код).

1.4. Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию специализированного и системного программного обеспечения (далее - ПО), либо на перехват информации, в том числе паролей.

1.5. Фишинг – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице предлагается ввести свои личные данные, при этом пользователь может полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

1.6. Средства и методы защиты информации, применяемые в ЗАО «Лидер», позволяют обеспечить необходимый уровень безопасности при осуществлении доверительного управления и предотвратить несанкционированный доступ к защищаемой информации при условии выполнения клиентами рекомендаций, изложенных в данном документе.

2. Риски получения несанкционированного доступа к защищаемой информации

2.1. Наиболее опасным риском является кража учетных данных - хищение личных данных клиента и их незаконное использование для выполнения несанкционированных операций от имени клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.

2.2. Компрометация криптографических ключей – факт доступа постороннего лица к информации, содержащей (закрытый) ключ электронной цифровой подписи, а также подозрение на компрометацию.

2.3. Риски получения несанкционированного доступа к информации прежде

всего связаны с «фишингом» (использованием ложных ресурсов сети Интернет с целью кражи идентификационных данных), а также воздействием вредоносного кода.

2.4. Утечка информации в сеть Интернет и её размещение на общедоступных доступных ресурсах, в СМИ, а также в социальных сетях.

2.5. Нарушение целостности данных (изменение структуры баз данных, связей между таблицами и т.д.), искажение данных или их потеря (удаление информации) в результате злонамеренных действий лица, получившего доступ.

3. Рекомендации по защите информации от воздействия вредоносного кода

3.1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

3.2. Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.

3.3. Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).

3.4. Не используйте права администратора без необходимости. В повседневной практике входите в систему с учетной записью пользователя, не имеющего прав администратора.

3.5. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, старайтесь периодически просматривать журнал событий и реагировать на ошибки.

3.6. Обязательно установите и своевременно обновляйте на компьютере лицензионное антивирусное программное обеспечение с функцией автоматического обновления вирусных баз. Лечение (удаление) зараженных файлов должно производиться антивирусным ПО в автоматическом режиме.

3.7. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода.

3.8. Антивирусное ПО должно запускаться автоматически, с загрузкой операционной системы.

3.9. Рекомендуется подвергать антивирусному контролю любую информацию,

получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.

3.10. При работе в сети Интернет используйте межсетевые экраны, не соглашайтесь на установку каких-либо программ с сайтов, которые вы посещаете. Все программные средства должна устанавливать только служба IT-поддержки.

3.11. Исключите возможность бесконтрольного доступа посторонних лиц (гостей, посетителей) к вашим компьютерам.

3.12. Рекомендуем ограничить информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты. Не используйте компьютер, с которого осуществляется информационный обмен по системе электронного документооборота (далее – ЭДО), для общения в социальных сетях, переписке в интернет-мессенджерах, а также для посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), так как именно через подобные ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

3.13. При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), следует полностью воздержаться от использования систем ЭДО до устранения проблемы.

3.14. Помните, что ни ЗАО «Лидер», ни оператор ЭДО не несет ответственности в случае возникновения финансовых потерь, понесенных клиентом в связи с нарушением и/или ненадлежащим исполнением им требований по защите от вредоносного кода своих автоматизированных рабочих мест (компьютера, ноутбука) для доступа к системе ЭДО.

4. Меры по предотвращению несанкционированного доступа к защищаемой информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

4.1. Мошеннический или поддельный web-сайт - это небезопасный web-сайт, на котором под каким-либо предлогом предлагается ввести конфиденциальную

информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний. Они предназначены для сбора конфиденциальной информации обманным путем. Ввод логина и пароля на таком сайте приводит к получению этих данных злоумышленниками, то есть разглашению идентификационных данных.

4.2. Во избежание использования ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс системы ЭДО, необходимо удостовериться, чтобы при подключении к системе ЭДО защищённое SSL-соединение было установлено исключительно с официальным сайтом ЭДО.

4.3. Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты, который является почти точной копией адреса настоящей компании. Подделать адрес электронной почты отправителя очень просто, поэтому будьте внимательны.

4.4. Внимательно читайте текст электронного письма. Если в тексте письма есть слова на иностранном языке, специальные символы и т. д., возможно, это - электронное письмо, отправленное мошенниками.

4.5. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. Типичное фишинговое письмо начинается с обезличенного приветствия. Не открывайте вложений, прикрепленных к подобным письмам.

4.6. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке.

5. Меры по предотвращению несанкционированного доступа к защищаемой информации третьими лицами

5.1. Рекомендуется выделить отдельный компьютер, который использовать только для работы в системе ЭДО с установленным на нем минимальным необходимым для работы набором программного обеспечения.

5.2. Не используйте на устройстве, предназначенном для доступа к системе ЭДО, средства удаленного администрирования.

5.3. Используемые в системе ЭДО логин и пароль, запрещается записывать и хранить в местах, доступных посторонним лицам. Необходимо хранить пароль в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования.

5.4. Использование ключевого носителя должно осуществляться исключительно владельцем ключа ЭЦП. Рекомендуется хранить ключевую информацию на отчуждаемом носителе (USB-накопителе) и хранить его в сейфе или запираемом шкафу исключив возможность несанкционированного доступа.

5.5. Необходимо отключать и извлекать из компьютера ключевой носитель, если он не используются для работы в ЭДО. Размещение ключевого носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключам ЭЦП третьими лицами;

5.6. Рекомендуется использовать разные уникальные пароли для различных web-сайтов и систем, на которых вводятся конфиденциальные данные.

5.7. Не пересылайте конфиденциальную информацию через электронную почту или SMS-сообщения.

5.8. Рекомендуется исключить возможность физического доступа к компьютеру, с которого осуществляется работа в системе ЭДО, для посторонних лиц и персонала, не имеющего отношения к работе с ЭДО.

5.9. Необходимо принять меры по контролю за конфигурацией компьютера, с использованием которого осуществляется информационный обмен по ЭДО, и не допускать несанкционированных программно-аппаратных изменений конфигурации.

5.10. На компьютере для работы с системой ЭДО необходимо использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить регулярную своевременную установку обновлений, выпускаемых разработчиками ЭДО, операционной системы, web-браузеров (Chrome, Edge, Firefox, Opera, IE Explorer и т.д.) и иного прикладного программного обеспечения.

5.11. На компьютере для работы с системой ЭДО необходимо исключить посещение web-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т.п. Использование нелицензионного программного обеспечения повышает риск получения несанкционированного доступа злоумышленников с целью хищения конфиденциальных данных.

5.12. В случае компрометации или подозрении на компрометацию закрытого ключа ЭЦП (утрате, потере, хищении) Ключевого носителя необходимо незамедлительно обратитесь к оператору ЭДО для блокирования скомпрометированных ключей ЭЦП.

5.13. Не передавайте ключевой носитель сотрудникам службы технической поддержки для проверки работы ЭДО. При необходимости таких проверок владелец ключа ЭП должен лично подключить ключевой носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейсе ЭДО, и ввести пароль, не допуская ознакомления с ним посторонних лиц.

5.14. В случае передачи (списания) компьютера, на котором ранее была установлена система ЭДО, необходимо гарантированно удалить с него все следы работы с системой ЭДО.

5.15. При увольнении ответственного сотрудника, имевшего доступ к ключевому носителю, уведомить оператора ЭДО об увольнении и действовать в соответствии с положениями договора на использование системы ЭДО.

5.16. Необходимо корректно завершать работу в ЭДО, используя для этого пункт меню «Выйти из системы».

Указанный выше перечень мер и рисков не является исчерпывающим в виду многообразия ситуаций, которые могут возникать при совершении финансовых операций.