Рекомендации клиентам АО УК «Прогрессивные инвестиционные идеи» по соблюдению мер информационной безопасности при использовании системы обмена электронными документами

1. Общие положения

1.1. 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 управляющей компании (УК), так и на стороне клиента.

1.2. Наиболее опасным является кража учетных данных - хищение личных данных клиента УК 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.

1.3. 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.

1.4. 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 Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

1.5. 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.

1.6. Средства и методы защиты информации, применяемые в УК, позволяют обеспечить необходимый уровень безопасности при осуществлении переводов денежных средств и предотвратить мошеннический вывод денежных средств со счетов клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе.

2. Рекомендации по защите информации от воздействия вредоносного кода.

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

2.2. Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.

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

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

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

2.6. 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.

2.7. 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.

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

2.9. 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.

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

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

2.12. Рекомендуем ограничить информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты. Не используйте компьютер, с которого Вы осуществляете информационный обмен по системе 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.

2.13. 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.

2.14. Помните, что ни УК, 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.

3. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

3.1. Мошеннический или поддельный web-сайт - это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете. Они предназначены для сбора конфиденциальной информации обманным путем. Ввод логина и пароля на таком сайте приводит к получению этих данных злоумышленниками, т.е. разглашению идентификационных данных.

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

3.3. 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.

3.4. Внимательно читайте текст электронного письма. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это - электронное письмо, отправленное мошенниками.

3.5. 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.

3.6. 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.

4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

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

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

4.3. Используемые в 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.

4.4. Генерация рабочих ключей электронной подписи (ЭП) осуществляется владельцем ключа ЭП самостоятельно;

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

4.6. 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 ЭП третьими лицами;

4.7. Рекомендуется использовать разные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные.

4.8. В том случае, если Вы обнаружили, что Ваш пароль от системы ЭДО скомпрометирован или в процессе работы Вы столкнулись с тем, что ранее действовавший пароль не срабатывает и не позволяет Вам войти в систему, рекомендуем незамедлительно принять меры по смене пароля и можно быстрее обратиться к оператору ЭДО для получения инструкций по смене пароля.

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

4.10. Рекомендуем исключить возможность физического доступа к компьютеру, с которого Вы осуществляете работу в системе ЭДО, для посторонних лиц и персонала, не имеющего отношения к работе с ЭДО.

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

4.12. 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;

4.13. Применять на компьютере для работы с ЭДО лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновление компонентов антивирусной защиты;

4.14. 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;

4.15. Рекомендуется осуществлять работу с системой ЭДО только под учетной записью с ограниченными правами и не допускать штатную работу в системе ЭДО под учетной записью с правами администратора;

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

4.17. 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;

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

4.19. 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.

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