РЕКОМЕНДАЦИИ КЛИЕНТАМ ООО «УК «АГАНА» по соблюдению мер информационной безопасности для защиты информации от воздействия вредоносных кодов

1. Общие положения

1.1. Термины и определения:

1.1.1. **УК** – Общество с ограниченной ответственностью «Управляющая компания «АГАНА» / ООО «УК «АГАНА»;

1.1.2. **Фишинг** – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям;

1.1.3. **ПО** - программное обеспечение;

1.1.4. **Межсетевой экран (МСЭ)** – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами;

1.1.5. **Система электронного документооборота (ЭДО)** – организационно-техническая система, представляющая собой совокупность нормативного, информационного и программно-технического обеспечения, реализующая обмен электронными документами между участниками;

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

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 УК, так и на стороне клиента.

1.3. Наиболее опасным является кража учетных 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.

1.4. Риски получения несанкционированного доступа к информации прежде всего связаны с «фишингом», а также воздействием вредоносного кода.

1.5. Цель фишинга – перехват 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.

1.6. 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 ПО, либо на перехват информации, в том числе паролей.

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

2.7. Не реже одного раза в месяц должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода.

2.8. Рекомендуется подвергать предварительному 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 внешних носителей информации должно осуществляться в автоматическом режиме.

2.9. При работе в Интернет используйте межсетевые экраны. Не устанавливайте каких-либо программы с сайтов, которые вы посещаете. Все программные средства должна устанавливать только ваша служба IT-поддержки.

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

2.11. 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.

2.12. 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.

2.13. 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. Перед просмотром входящего 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.

3.3. Внимательно читайте текст электронного письма. Если Вы видите слова на иностранном языке,

специальные символы и т. д., возможно, это - электронное письмо, отправленное мошенниками.

3.4. 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.

3.5. 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.

3.6. Не открывайте вложений, прикрепленных к письмам от неизвестных отправителей.

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. Необходимо отключать и извлекать из компьютера Ключевой носитель, если он не используются для работы в ЭДО и хранить его в сейфе, исключая возможности несанкционированного доступа. Размещение Ключевого носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключам ЭП третьими лицами;

4.5. 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.

4.6. 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.

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

4.8. 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;

4.9. 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;

4.10. Не передавайте Ключевой носитель сотрудникам службы технической поддержки для проверки работоспособности 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;

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

4.12. 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.