Рекомендации для членов СПОК «Киквидзенский» при использовании на ПК систем дистанционного банковского обслуживания (Интернет-Банк, Клиент-Банк), а также при использовании мобильных приложений, по мерам снижения риска возникновения несанкционированного доступа к защищаемой информации, с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, а также рекомендации по защите информации от воздействий вредоносного кода

Сельскохозяйственный потребительский обслуживающий кооператив «Киквидзенский» не использует в своей деятельности систем дистанционного обслуживания своих членов. Тем не менее, не редки ситуации, когда наши члены пользуются системами дистанционного банковского обслуживания (ДБО), а также мобильными приложениями для осуществления платежей по займам, внесения членских, паевых, вступительных взносов, других финансовых операций, чтобы не ехать лишний раз в офис СПОК.

Поэтому, исполнительная дирекция кооператива доводит до сведения своих членов информацию о существующих рисках возникновения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, а также приводит **список рекомендаций** по защите информации от воздействия вредоносного кода (компьютерные вирусы, «трояны», «руткиты» и т.п.), о **мерах соблюдения информационной безопасности и способах пресечения хищения.**

Банк России отмечает участившиеся случаи несанкционированного доступа (далее —НСД) вследствие которых осуществляются операции перевода денежных средств с использованием **устройств мобильной связи** — смартфоны, планшеты и т.п. (далее — **УМС**) без согласия лиц, обладающими правом распоряжения этими денежными средствами. Не рекомендуется сообщать посторонним лицам свою персональную информацию (ФИО, логин, пароль, номер карты, счета, паспорта и т.д.). Сотрудник Банка имеет право уточнять у Клиента подобную информацию только в случае, если Клиент самостоятельно обратился в Банк.

Банк не направляет своим Клиентам электронные письма, за исключением деловой переписки, инициированной обращением Клиента, по вопросам, связанным с функционированием системы дистанционного банковского обслуживания физических лиц, «Мобильные платежи» (далее — Система), и SMS- сообщения с просьбой уточнить их персональную информацию.

Число преступлений, связанных с системами ДБО, за последние несколько лет выросло многократно. При этом используемые банками меры защиты не являются непреодолимым препятствием для злоумышленников. Практика показывает, что кибермошенники могут вмешаться в процесс обработки платежных операций на любом этапе.

1. С кем боремся?

За истекший год специалистами и разработчиками программ-антивирусов было выявлено множество вредоносных программ, предназначенных для кражи пользовательской информации, в том числе данных для доступа к системам «Банк-

Клиент» и электронным кошелькам.

Наиболее распространены и опасны Trojan.Winspy, Trojan.Carberp, Trojan.PWS.lbank, Trojan.PWS.Panda, которые передают злоумышленникам данные, необходимые для доступа к банковским сервисам, умеет красть ключи и пароли от различных программ, отслеживать нажатия клавиш, делать снимки экрана, объединяться в сети, обрабатывать поступающие от удаленного командного центра команды и выполнять на зараженном компьютере.

Кроме того, банковские троянцы могут перенаправлять пользователя на поддельные (фишинговые) сайты для кражи пользовательских паролей и ключей.

В настоящее время банковские троянцы существуют для ВСЕХ операционных систем. Заражение компьютера может происходить различными способами:

- • Посещение зараженного сайта;
- • Перенос вирусов на внешнем носителе (флешка, внешний диск, плеер, телефон и т.д.);
- • Заражение по локальной сети;
- • Скачивание и запуск зараженных файлов из сети Интернет;
- • Заражение через систему автообновления популярных программ.

Кроме троянов для получения доступа к системам ДБО активно используются средства социальной инженерии. Например, рассылка от имени банков писем по электронной почте с требованием (под разными предлогами) перейти по предлагаемой ссылке, где требуется ввести логин и пароль от системы ДБО. Ссылка ведет на поддельный сайт со схожим дизайном, а логин и пароль оказываются в руках злоумышленников. Зафиксированы и адресные атаки мошенников на конкретные предприятия.

2. Как это происходит?

После заражения компьютера и получения доступа к нему производится поиск следов использования ДБО и сбор информации. Собранные данные передаются на управляющий сервер, где проверяются на полноту и достаточность для совершения мошеннической операции.

Если фальшивое платежное поручение не может быть отправлено с другого компьютера, то используются средства удаленного администрирования, что позволяет отправлять платежные поручения непосредственно с компьютера пользователя. Троянами может производиться подмена легитимных платежных поручений на мошеннические при отправке их на подпись, при этом пользователь видит на экране и подписывает свое платежное поручение,

Как только мошенническая операция проведена, и платежное поручение отправлено, главная задача злоумышленников — ограничить доступ пользователя к системе ДБО. Для этого компьютер пользователя приводят в неработоспособное состояние путем удаления компонентов Windows или форматированием жесткого диска. Для дополнительного отвлечения внимания часто удаляются данные бухгалтерских программ.

3. На что следует обращать внимание?

- • необычно медленная работа компьютера, зависания во время сеансов ДБО или при попытке входа, произвольная перезагрузка;

- • перебои с доступом в систему ДБО;
- • невозможность авторизации в системе ДБО;
- • несоответствие порядковых номеров платежных поручений;
- • попытки авторизации в ДБО с других IP-адресов или в нерабочее время;
- • неоднократное удаление антивирусным монитором одного и того же вируса;
- • выход из строя ПК, на котором установлена система ДБО;
- • DDoS-атака на вашу ИТ-инфраструктуру.

В случае обнаружении вирусов или сбоев в работе компьютера или УМС следует немедленно приостановить работу с ДБО и провести полную проверку компьютера или УМС антивирусным сканером. Повторяющееся заражение одним и тем же или схожими вирусами может свидетельствовать о том, что вирус уничтожается не полностью, какая-то его часть продолжает функционировать и загружает из Интернета обновленные вредоносные программные модули. В такой ситуации следует провести более детальный анализ вирусной активности. Если самостоятельно не удается установить источник заражения, необходимо обратиться в Службу поддержки пользователей разработчика антивирусной программы.

При работе с системой ДБО следует исходить из соображений, что данный сервис должен функционировать абсолютно бесперебойно, поэтому всякое отклонение от нормальной работы следует воспринимать как сигнал тревоги. К примеру, если Вы не можете войти в систему ДБО в течение 5 - 10 минут, обязательно свяжитесь с банком и установите источник проблемы (в банке или в вашей сети). Если проблема в вашем оборудовании или программах, и Вы не можете её быстро разрешить или локализовать, обязательно свяжитесь с банком, проверьте последние отправленные поручения и сообщите сотрудникам банка об имеющихся проблемах.

К несанкционированным операциям по переводу денежных средств относятся (включая, но не ограничиваясь ими):

- ✓ • операции по оплате товаров и услуг при осуществлении доступа к сети Интернет через УМС Клиента, в том числе по реквизитам платёжных карт;
- ✓ • операции по переводу денежных средств, предоставленных оператору связи в качестве оплаты услуг связи, в том числе перечисление денежных средств на «короткие номера»;
- ✓ • операции, осуществляемые с использованием приложения Системы, предоставляемого Банком и установленного Клиентом на УМС;
- ✓ • операции по оплате товаров и услуг с использованием иных приложений, установленных на УМС Клиента.

4. Как с этим бороться?

Анализ происшедших инцидентов с ДБО позволяет сделать однозначный вывод о том, что успеху злоумышленников способствует пренебрежение пользователями (а иногда и сотрудниками банка) элементарных правил безопасной работы с системами ДБО. Типичный пример такого поведения — хранение ключей ЭЦП на жестком диске или постоянно подключенных к компьютеру флешках, токенах, отказ от дополнительных мер безопасности, предлагаемых банком.

Основные правила безопасной работы с ДБО как на ПК, так и с использованием УМС:

- ♣ На УМС для работы с Системой следует использовать безопасный способ подключения с помощью специального приложения, а не браузера. Загружать и устанавливать специальное приложение следует только с официальных сайтов - Google P1ay или App1e Apporе. Ссылки для загрузки размещены на официальном сайте Банка. Эти приложения для разных платформ соответствуют требованиям безопасности и периодически обновляются;
- ♣ В случае утери УМС, с установленным специальным приложением, используемым для работы с Системой, необходимо незамедлительно заблокировать SIM-карту у оператора сотовой связи и обратиться в Банк для блокировки доступа в Систему;
- ♣ В случае изменения номера телефона УМС для работы в Системе, обратитесь в Банк для изменения доступа со старого номера на новый номер телефона. Необходимо помнить, что старый номер сотовый оператор может передать другому абоненту в случае, если он неактивен некоторое время;
- ♣ Если у Вас неожиданно перестала работать iM-карты — незамедлительно обратитесь к оператору сотовой связи для выяснения причин, так как в отношении Вас третьими лицами возможно проведение мошеннических действии;
- ♣ Для работы с Системой используйте защищенные УМС — не пытайтесь обходить установленные производителем защитные механизмы (например, через джейлбрейк (Jailbreak) или рутинг (Rooting)). Не перепрошивайте свое УМС прошивками сторонних лиц, не являющихся производителями устройства, т.к. это может сделать Ваше устройство уязвимым к заражению вредоносным кодом.
- ♣ При создании паролей придерживайтесь следующих правил. Не допускается использовать в качестве пароля простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в другие системы. Пароль должен соответствовать следующим требованиям — длина пароля должна быть не менее 8 символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, , °/о и т.п.), пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, год рождения, номер телефона и т.п.);
- ♣ Необходимо хранить код доступа в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования. Не рекомендуется записывать код доступа к Системе там, где доступ к нему могут получить посторонние лица (включая УМС);
- ♣ Не сообщайте код доступа, SMS-коды, необходимые для проведения операций, ПИН - код платежной карты и контрольный код, указанный на оборотной стороне платёжной карте (CVV / CVC-код) посторонним лицам, сотрудникам Банка по телефону, электронной почте или иным способом. Использование SMS-кодов допускается только при работе непосредственно с Системой, без участия сотрудников Банка. При наличии подозрения, что такие данные стали известны третьему лицу, необходимо сообщить об этом по контактным телефонам, указанным на официальном сайте Банка;
- ♣ Не оставляйте УМС без присмотра. Необходимо установить пароль на доступ к УМС и/или на доступ к SMS-сообщениям. Это затруднит доступ

злоумышленникам к УМС в случае его утраты;

- ♣ Не допускается работать в Системе через публичные беспроводные сети (Wi-Fi), незащищенные беспроводные сети. Специальные приложения применяют механизмы защиты своих данных при передаче, а так как публичные беспроводные сети сравнительно труднее контролировать, то у злоумышленников появляется больше возможностей для попыток обхода защитных механизмов. Для работы необходимо использовать подключение к сети Интернет через мобильного оператора или через доверенную защищенную беспроводную сеть;
- ♣ Необходимо корректно завершать работу в Системе, используя для этого пункт меню «Выход»;
- ♣ На компьютере с системами ДБО ограничить работу в сети Интернет минимальным необходимым количеством сайтов;
- ♣ Хранить ключи ЭЦП на съемных носителях и извлекать их по окончании сеанса;
- ♣ Не оставлять включенным сеанс ДБО сверх необходимого времени;
- ♣ Не использовать на компьютере с ДБО средств удаленного доступа и администрирования;
- ♣ Доступ к ресурсам компьютера с системами ДБО из локальной сети должен быть закрыт, папок общего доступа быть не должно;
- ♣ Не устанавливать без особой необходимости системы ДБО на мобильные устройства, которые могут покидать офис и подключаться к другим сетям;
- ♣ На компьютере с системами ДБО желательно не использовать сеть Wi-Fi. В случае необходимости — устанавливать максимально возможный уровень защиты сети;
- ♣ Поддерживать систему антивирусной защиты в работоспособном и актуальном состоянии;
- ♣ Не пользоваться ДБО в случае возникновения проблем с антивирусной защитой;
- ♣ Не пользоваться ДБО при повторяющихся сбоях в работе компьютера.

Технические аспекты защиты

- ♣ На ПК должны быть установлены все актуальные обновления безопасности Windows;
- ♣ Антивирусная защита должна включать, кроме обычных функций, модули проверки почты, входящего http-трафика, Брандмауер, СПАМ фильтр и обновляться не реже одного раза в час. Пользователь ДБО должен быть лишен возможности управления антивирусной защитой и возможности её отключения;
- ♣ Необходимо применять на УМС, с которых ведётся работа с Системой, лицензионные средства антивирусной защиты, работающие в автоматическом режиме. В обязательном порядке обеспечить на постоянной основе автоматическое обновление антивирусных баз;
- ♣ Необходимо осуществлять проверку УМС на наличие вредоносного кода перед началом работы с Системой, а также после доступа к Вашему УМС сотрудников технической поддержки различных организаций или любых других частных мастеров, выполнивших работу по установке, обновлению и поддержке

различных программ;

- ♣ Не рекомендуется передавать УМС для использования третьим лицам, в том числе родственникам, т.к. на оставленном без присмотра УМС может быть совершён ряд действий, направленных на получение доступа к Системе. Например, злоумышленник может установить программное обеспечение с вредоносным кодом, настроить переадресацию SMS-сообщений на другой телефонный аппарат и т.п.;
- ♣ На компьютере с ДБО не должно быть установлено программ, не являющихся необходимыми на данном рабочем месте;
- ♣ Обновление программ (Adobe Reader, браузеры и т.д) должно проводиться только вручную с официальных сайтов. Автообновление необходимо отключить;
- ♣ Пользователь не должен работать с правами Администратора;
- ♣ Исключить прямой доступ в Интернет без использования межсетевого экрана Пользовательские пароли должны быть сложными и периодически изменяться;
- ♣ Доступ к ресурсам сети Интернет должен быть ограничен фиксированным списком доверенных сайтов, не допускать использование месседжеров типа ICQ, Skype и др.;
- ♣ Не допускать использования социальных сетей;
- ♣ Использовать только корпоративную почту через почтового клиента. Использовать СПАМ фильтр с жестким ограничением;
- ♣ Отключить службы сервера, удаленного доступа и др. связанные с удаленным администрированием;
- ♣ Применение внешних устройств должно быть ограничен набором флешек (Токенов) с ключами ЭЦП.
- ♣ Не рекомендуется переходить по ссылкам, приходящим в почтовых сообщениях, SMS и MMS-сообщениях из недостоверных источников, в том числе на известные сайты;
- ♣ Не рекомендуется загружать и устанавливать на ПК и УМС программное обеспечение, полученное из недостоверных источников: интернет-сайты, ссылки в и MMS-сообщениях и открытках.

В случае если требования безопасности не могут быть выполнены в полном объеме на компьютере пользователя, необходимо взвесить риски и, возможно, принять решение о выделении отдельного компьютера для работы с ДБО. Именно такой вариант рекомендуется многими банками.

Учитывая тот факт, что работники бухгалтерий не являются специалистами в области информационной безопасности, они бывают недостаточно информированы о рисках и могут недооценивать необходимость дополнительных мероприятий по защите систем ДБО. Поэтому разъяснение правил безопасной работы является одним из важнейших составляющих общей системы безопасности.

Для повышения уровня ответственности и дисциплины, общие правила безопасной работы с ДБО следует оформить соответствующим приказом руководителя предприятия.

5. Если произошел инцидент

В случае обнаружения факта (или попытки) мошенничества необходимо максимально быстро сообщить о происшествии в банк с целью остановки платежа и блокирования доступа к системе ДБО.

Компьютер с системой ДБО необходимо выключить. Если в компании имеется межсетевой экран или прокси-сервер, на котором ведутся логи, то необходимо сохранить их на внешнем устройстве. В случае проведения самостоятельного расследования или привлечения для этих целей консультантов, следует иметь в виду, что работа с оригиналами носителей информации может повредить целостности доказательств, хранящихся на них.

Даже если мошенничество не было завершено, и вы успели остановить его, инцидент остается уголовным преступлением, которое попадает под ряд статей, начиная с создания и распространения вредоносного программного обеспечения и заканчивая попыткой хищения в особо крупном размере. Поэтому следует обязательно написать заявление в правоохранительные органы с требованием возбудить уголовное дело.

6. Заключение.

На сегодняшний день не существует ни одной системы ДБО со стопроцентной надежностью, но само осознание этого факта и применение даже самых простых мер по повышению уровня безопасности может существенно снизить риски финансовых потерь. Необходимо понимать, что ежедневно появляются сотни новых вирусов и их модификаций и, несмотря на то, что, например, обновление вирусных баз Dr.Web, а также Лабораторий Касперского выходят каждые тридцать минут - час, всегда есть риск заражения новым вирусом. Поэтому при выборе системы антивирусной защиты следует принимать во внимание не только стоимость, но и устойчивость антивируса к заражению неизвестными вирусами, а также наличие эффективной службы поддержки пользователей.

Учитывая, что сумма ущерба может оказаться равной сумме остатка на банковском счете, необходимые затраты на повышение безопасности вероятно следует отнести к не самым плохим инвестициям.