Рекомендации по информационной безопасности

Уважаемый клиент!

Система электронных платежей CyberPlat® ("КиберПлат") считает своим долгом заботу о Вашей безопасности и безопасности Вашего бизнеса. В настоящей рекомендации мы информируем Вас о событиях, способных, на наш взгляд, оказывать неблагоприятное влияние на Ваш бизнес и наше с Вами сотрудничество.

В настоящее время мошенничество в системах электронных платежей - это действия не хакера-одиночки, который ради любопытства или славы пишет вирусы и получает пароли доступа, а **действия организованных преступных сообществ**. В них четко прописаны роли каждого члена группы: одни создают вредоносное ПО, другие его распространяют, третьи регистрируют номера телефонов/кредитные карты/электронные кошельки, четвертые обналичивают деньги. Целью этих преступников является завладение денежными средствами клиентов систем электронных платежей.

Мошенники хитры и изобретательны в достижении своих целей и готовы на многое. Наше с Вами сотрудничество может являться объектом мошенничества.

Используемые нами технологии, в первую очередь, направлены на **безопасность и удобство** нашей с Вами совместной работы. Не имея прямой возможности влияния на нашу Систему, мошенники фокусируют все свои усилия на наших клиентах. В первую очередь, их интересуют **ключи и пароли** для доступа в кабинет платежного агента и к точкам приема платежей, которые, как правило, добываются путем кражи (в том числе, с помощью вредоносного программного обеспечения).

Поэтому мы разработали несколько простых рекомендаций для того, чтобы уберечь Вас. Следуя им, Вы в значительной мере **снизите вероятность мошеннических действий**, направленных на Ваш бизнес и наше с Вами сотрудничество. Постарайтесь выполнить **все рекомендации**, так как только применение комплекса мер позволит эффективно противостоять злоумышленникам.

Меры противодействия кражам ключей

Поскольку хищение денежных средств со счета агента невозможно без знания его закрытого ключа, ключа главного администратора (ГА) или ключей точек приема платежей (ТПП), мы рассматриваем следующие меры противодействия кражам ключей, которые делим на три категории:

1. Параметры безопасности системы CyberPlat® ("КиберПлат") **.**
2. Предотвращение несанкционированного доступа (НСД) к ключам.
3. **Безопасная среда (окружение).**

1. Параметры безопасности системы CyberPlat® ("КиберПлат")

Для предотвращения мошеннических операций в системе CyberPlat® ("КиберПлат") реализованы следующие механизмы безопасности:

1.1. **Использование смарткарт/USB-токенов** для генерации и хранения закрытых ключей платежного агента (здесь и далее по тексту «ключи платежного агента» – любые ключи платежного агента, например, ключи главного администратора, администратора, ключи ТПП и т.д.).

1.2. Использование встроенной функции **привязки ключа к оборудованию АРМ**[1], где пункт 1.1 неприменим.

1.3. Использование встроенной функции **привязки ключа главного администратора к статическому IP-адресу.**

1.4. Использование технологии **одноразовых паролей для подтверждения критичных операций**.

1.5. Использование встроенной функции **привязки точки приема платежей к статическому IP-адресу**.

1.6. Использование системы «**Мониторинг платежей**».

1.7. Установка **лимита:**

- на максимальную допустимую сумму **платежа** по заданной точке.
- на максимально допустимый дневной **оборот** платежей по заданной точке (суточный лимит).
- на максимальное количество платежей на **одни реквизиты** в сутки независимо от точки приема платежей (ТПП).
- на максимальную сумму **списания** за день **по типам провайдеров** для каждой ТПП.
- на максимальную сумму **платежа** по типам провайдеров для каждой ТПП.

1.8. Установка **времени работы** ТПП.

Использование технологии одноразовых паролей дает возможность использовать два канала (Интернет и мобильный телефон) для авторизации критичных операций. Для каждого ГА агента назначается номер мобильного телефона, на который приходят одноразовые пароли для выполнения критичных операций: активация точки приема, активация ключа точки и др. Без ввода одноразового пароля выполнение операции невозможно. Одноразовый пароль действителен в течение 30 минут для выполнения одной критичной операции.

[1] АРМ- автоматизированное рабочее место (компьютер или любое другое средство вычислительной техники)

Назначение номеров телефонов и IP-адресов для оперативного оповещения должно производиться таким способом, чтобы эти номера и адреса невозможно было сменить, воспользовавшись закрытым ключом ГА.

Операция установки лимитов и времени работы ТПП доступна только для главных администраторов агента/субагента. При этом ГА агента/субагента имеет возможность установки указанных ограничений на точках всех субагентов, находящихся ниже по иерархии. Расписание работы точки позволяет принимать платежи только в рамках установленного времени работы точки.

В случае если ключ главного администратора агента/субагента не привязан к IP-адресу, для установки лимита потребуется дополнительная авторизация операции при помощи **одноразового пароля**, который отправляется в SMS-сообщении.

Данные лимиты устанавливают ограничение на любые платежи, кроме денежных переводов. Для денежных переводов устанавливается отдельный лимит на максимально допустимый дневной оборот переводов по заданной точке.

2. Предотвращение несанкционированного доступа к ключам

Для предотвращения несанкционированного доступа к ключам платежного агента рекомендуется соблюдать следующие правила:

2.1. Использование **смарт-карт/USB-токенов** для генерации и хранения закрытых ключей.

2.2. **Минимизация времени** использования смарт-карты/USB-токена с закрытым ключом.

2.3. Контроль и **ограничение физического доступа** к смарт-карте/USB-токену с закрытым ключом.

2.4. **Оперативное блокирование открытого ключа** платежного агента, зарегистрированного в системе электронных платежей, в случае утери смарткарты/USB-токена с соответствующим закрытым ключом.

Использование смарт-карт/USB-токенов для генерации и хранения закрытого ключа имеет следующие преимущества:

- закрытый ключ не может быть извлечен из памяти этих устройств, поскольку это не предусмотрено конструкцией устройств;
- закрытый ключ не может быть скопирован из резервной копии, потому что генерация ключа происходит непосредственно в защищенной памяти смарт-карт/USB-токенов, что делает создание резервной копии закрытого ключа невозможным.

(Смарткарты и USB-токены находятся в свободной продаже, стоимость от 700 руб.).

Использование смарт-карт/USB-токенов является наиболее надежным способом предотвращения несанкционированного копирования ключа. Если по каким-либо причинам использовать USB-токен нельзя, можно использовать для хранения ключей шифрованные диски (TrueCrypt, PGP Disk, Aladdin SecretDisk).

Минимизация времени использования смарт-карты/USB-токена с закрытым ключом означает, что данное устройство должно подключаться к компьютеру только на время работы. Все остальное время устройство должно быть отключено от АРМ.

Контроль и ограничение физического доступа к смарт-карте/USB-токену с закрытым ключом означает, что данное устройство должно быть физически доступно только ограниченному кругу лиц, уполномоченных работать с данным закрытым ключом. В случае ключей ГА агента, ГА должен быть единственным лицом, отвечающим за сохранность смарт-карты/ USB-токена со своим ключом, и предпринимать меры по ограничению физического доступа к нему других лиц, например, хранить его в сейфе. Кроме того, ГА должен регулярно контролировать наличие устройства и оперативно оповещать администрацию агента о его утере.
Администрация агента, со своей стороны, будучи проинформирована об утере смарт-карты/USB-токена с закрытым ключом, должна немедленно инициировать процедуру блокирования и замены открытого ключа, зарегистрированного в системе электронных платежей.

3. Безопасная среда (окружение)

Противодействие внедрению вредоносного программного обеспечения (ПО) в конфигурацию АРМ платежного агента включает в себя **организационные** и **технические меры** информационной безопасности.

Здесь и далее по тексту «АРМ/АРМ платежного агента» – любое АРМ (например, терминал или персональный компьютер) платежного агента, используемое для приема платежей и/или организации/контроля работы агентской сети (АРМ Главного администратора).

3.1. Организационные меры

3.1.1. **Использование только лицензионного программного обеспечения (ПО)** для организации АРМ платежного агента. Использование пиратских версий ПО и различных активаторов для него является недопустимым.

Используемое ПО должно удовлетворять следующим критериям:

- ПО должно быть лицензионным;
- ПО, поставляемое на дистрибутивном носителе (retail, box), - заводская упаковка ПО и средства контроля вскрытия (ленты, печати, пломбы), используемые производителем, не должны быть повреждены;
- предустановленное ПО (OEM) - заводская упаковка АРМ с предустановленным ПО и средства контроля вскрытия (ленты, печати, пломбы), используемые производителем, не должны быть повреждены. В комплекте с АРМ должен поставляться дистрибутивный носитель ПО;
- фирменное ПО производителя оборудования (драйвера, утилиты) должно быть загружено непосредственно на АРМ платежного агента с сайта производителя оборудования;
- фирменное ПО системы электронных платежей должно быть загружено непосредственно на АРМ с сайта системы электронных платежей по адресу https:\\www.cyberplat.ru.

3.1.2. Для корректной работы с АРМ платежного агента на предприятии агента следует разработать и ввести в действие **правила пользования АРМ платежного агента** и ознакомить с ними сотрудников под подпись.

Правилами пользования АРМ платежного агента должно быть явно запрещено следующее:

- установка ПО от имени платежного агента;
- использование для работы электронной почты;
- использование для доступа к ресурсам сети Интернет (интернет-серфинг);
- использование для общения программ обмена мгновенными сообщениями (MSN Messenger, ICQ, Skype, Jabber и т.д.);
- организация удаленного доступа к АРМ платежного агента и удаленное управление им;
- организация папок общего доступа;
- подключение (установка) съемных носителей информации (дискет, USB flash, картридеров и и.д.);
- использование АРМ без установленного/включенного антивирусного ПО;
- следование провокациям мошенников, рассылающих электронные письма якобы от имени ЗАО «КиберПлат» (По всем сомнительным операциям, вопросам или призывам немедленно обращаться к своему менеджеру в ЗАО «КиберПлат». Необходимо немедленно удалять спам-письма, не открывая их и ничего не запуская).

3.1.3. **Размещение АРМ платежного агента в помещении с контролируемым доступом**. В случае отсутствия такого помещения - развертывание АРМ на базе нетбука (субноутбука), размеры которого позволяют хранить его в сейфе. Последний вариант организации АРМ наиболее предпочтителен.

3.1.4. **Ограничение времени работы АРМ платежного агента**.
Компьютер, на базе которого развернуто АРМ, должен включаться только на время работы. В остальное время АРМ должно быть выключено.

3.1.5. **Контроль и ограничение физического доступа к АРМ платежного агента.**
Помещение, в котором оборудовано АРМ, должно опечатываться и сдаваться под охрану в нерабочее время. Нетбук/субноутбук, на базе которого развернуто АРМ, в нерабочее время должен храниться в сейфе. Сейф должен опечатываться, целостность печати должна контролироваться уполномоченным сотрудником при вскрытии сейфа.

3.1.6. **Круглосуточное видеонаблюдение помещения**, в котором оборудовано АРМ **платежного агента**.

3.2. Технические меры

3.2.1. Обязательное использование **антивирусного ПО** с актуальными антивирусными базами.

3.2.2. **Использование АРМ Главного администратора** ТОЛЬКО для работы в кабинете платежного агента.

3.2.3. **Учетную запись и ключи Главного администратора** использовать ТОЛЬКО для управления сетью точек приема платежей.

Эта запись должна иметь полномочия обычного пользователя операционной системы.

3.2.4. Завести специальную учетную запись с правами **администратора агента** и использовать ее ТОЛЬКО для **просмотра статистики**.

Эта запись должна иметь полномочия обычного пользователя операционной системы.

3.2.5. **Организация отдельной учетной записи администратора АРМ платежного агента**: запись должна иметь административные полномочия и использоваться только для обслуживания АРМ платежного агента, например, для установки и настройки программного обеспечения (ПО).

Эта единственная учетная запись, которая имеет административные полномочия в операционной системе.

3.2.6. **Организация отдельной учетной записи оператора приема платежей** для проведения платежей.

Эта запись должна иметь полномочия обычного пользователя операционной системы.

3.2.7. Удаление из конфигурации АРМ всех почтовых клиентов и программ обмена мгновенными сообщениями.

3.2.8. Удаление из конфигурации АРМ компонента операционной системы (ОС) "Удаленный доступ к рабочему столу".

3.2.9. Удаление из конфигурации всех сетевых подключений операционной системы всех компонентов, за исключением компонента "Протокол Интернета (TCP/IP)".

3.2.10. Запрет всех без исключений входящих подключений к АРМ с помощью встроенного межсетевого экрана ОС или специального ПО.

3.2.11. Физическое исключение из состава АРМ всех накопителей на съемных носителях.

3.2.12. Отключение в менеджере устройств накопителей на съемных носителях, которых невозможно исключить из состава АРМ. В случае невозможности отключения физическая блокировка доступа к накопителям.

3.2.13. Блокирование использования накопителей с интерфейсом USB путем запрета запуска драйвера класса устройств "Usb Storage", либо с помощью групповой политики, либо путем установки специализированного ПО, предназначенного для решения этой задачи.

3.2.14. Настройка политики электропитания с тем, чтобы АРМ переходил в режим гибернации после 5-10 минут простоя.

3.2.15. Включение запроса пароля по выходу из спящего режима.

Таким образом, применив все вышеперечисленные меры, Вы значительно **снизите вероятность мошеннических действий**, направленных на Ваш бизнес и наше с Вами сотрудничество.