НАСТРОЙКИ ПО MARATL В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ СТАНДАРТА БЕЗОПАСНОСТИ PA-DSS

вер. 5.7.0

МОСКВА
8-495-783-5959

РОССИЯ
8-800-200-0059

ФАКС
8-495-926-4619

WEB
WWW.QIWI.RU

СОДЕРЖАНИЕ

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Расшифровка/определение
ПО Maratl	Программное обеспечение, разработанное АО «QIWI». По тексту данного документа – Приложение
АО «QIWI»	Акционерное общество «QIWI»
ОС	Операционная система
АСО	Автомат самообслуживания. В контексте данного документа – терминал, на котором установлено ПО Maratl
PA-DSS	Payment Application Data Security Standard, Стандарт безопасности данных платёжных приложений. Версия Стандарта доступна на сайте: https://ru.pcisecuritystandarts.org
PCI DSS	Payment Card Industry Data Security Standard, Стандарт безопасности данных индустрии платёжных карт.
Агент	Юридическое лицо или индивидуальный предприниматель, подписавшее Договор о приеме Платежей Платежным субагентом

ВВЕДЕНИЕ

Целью документа является информирование Агентов о применении средств защиты данных платежных карт в Приложении Maratl в соответствии с требованиями стандартов безопасности в индустрии платежных карт PCI DSS и PA-DSS.

Документ содержит руководство по настройке программного обеспечения Maratl в соответствии с требованиями стандарта PCI DSS.

Название программного обеспечения – Maratl.

Версия программного обеспечения – 5.7.x

Все терминалы самообслуживания, использующие Приложение, должны быть настроены в соответствии с этим руководством.

Актуальная версия документа и дистрибутив ПО Maratl с файлом release notes, в котором указывается номер новой версии приложения и список основных изменений, опубликованы на официальном сайте Компании.

Положения документа пересматривается в следующих случаях:

- не реже 1 раза в год;
- обновления ПО (при необходимости);
- изменений стандартов PCI DSS и PA-DSS.

Отметки о доработках PA-DSS Implementation Guide вносятся в историю изменений документа согласно Табл. 1.

Табл. 1. История изменений документа

Автор	Дата изменений	Номер	Описание изменений
	03/04/2015	01	Исходная редакция документа, разработанная с учетом требований PCI DSS версия 3.0 и PA-DSS версия 3.0.
	07/20/2016	02	Доработан с учетом требований PCI DSS v3.1 и PA-DSS v3.1
	03/22/2021	03	Обновлен в связи с выходом новой версии Maratl

1. ЗАЩИТА ДАННЫХ ПЛАТЕЖНЫХ КАРТ

Требования стандартов PCI DSS и PA-DSS запрещают хранить критичные данные авторизации (после проведения авторизации). Так же запрещено хранить полный номер платежной карты (PAN) в открытом виде.

К данным держателя платежной карты относятся:

- Номер платежной карты (держателя карты) (PAN);
- Имя держателя карты (Cardholder Name);
- Срок действия карты (Expiration Date);
- Сервисный код (Service Code).

К критичным данным авторизации относятся:

- Полное содержание носителей данных карты (данные, хранящиеся на магнитной полосе или на чипе);
- CAV2/CVC2/CVV2/CID;
- ПИН/ПИН-блок.

Maratl не обрабатывает, не хранит, и не передает критичные авторизационные данные во время проведения операций. Предыдущие версии Приложения также не обрабатывали критичные данные авторизации.

В приложении Maratl в случае выполнения авторизации данные держателя платежной карты обрабатываются в оперативной памяти, а также сохраняются до момента завершения авторизации в файле `%working_dir%\import.xml` и в реестре Windows `HKLM\SOFTWARE\OSMP\tr`.

Для защиты хранимых данных платежных карт применяется стойкое шифрование.

Для защиты данных в реестре применяется шифрование с помощью CryptProtectData, расшифровка производится с помощью CryptUnprotectData. CryptProtectData использует алгоритм шифрования 3-DES и ключ сессии, который генерируется на основе Мастер-ключа, который в свою очередь генерируется на основе пользовательского пароля.

Для шифрования файла `import.xml` используется алгоритм AES с длиной ключа 256 бит.
Для шифрования ключа используется алгоритм RSA-2048.

После завершения авторизации данные держателя платежной карты автоматически удаляются. Если данные не были удалены автоматически после завершения транзакции, (например, при отсутствии связи с процессинговым центром) следует убедиться, что данные удалены, в противном случае удалить их вручную, используя методы безопасного и гарантированного удаления, например, с помощью программы «SDelete»[1]. Для этого необходимо удалить данные в директории: `%working_dir%\import.xml`. В соответствии с требованиями PCI DSS и PA-DSS, данные держателя карты должны быть удалены по истечению срока их хранения: когда эти данные перестают быть необходимыми по регуляторным, юридическим или бизнес-причинам.

Для отображения номера карты на экране АСО и чеках используется маскированный вид номера карты (отображаются только первые 4 и последние 4 цифры). Данная функциональность реализована на уровне кода приложения. Стоит отметить, что отображение полного номера карты осуществляется только во время ввода номера карты пользователем. Дополнительных действий по настройке отображения номера карты агенту производить не требуется.

В случае необходимости осуществления сбора и передачи данных разработчику, данные должны предоставляться в объеме, минимально необходимом. Для передачи и хранения таких данных Агентам необходимо использовать стойкое шифрование. Место хранения log-файлов за текущую дату: `%working_dir%\logs\current_date.log`

[1] https://technet.microsoft.com/en-us/sysinternals/sdelete.aspx

Для исключения неконтролируемого хранения данных держателей карт (например, в случае отказа операционной системы) рекомендуется отключить файл подкачки, либо перенести его на предварительно подготовленный шифрованный раздел (инструкция по настройке приведена в Приложении А).

По истечению срока хранения данных держателей карт Агенту необходимо использовать методы безопасного удаления данных, например, с помощью программы «SDelete».

2. ДОСТУП К ДАННЫМ ПЛАТЕЖНЫХ КАРТ

В ПО Maratl существует один тип учетных записей пользователей – агент. Данная учетная запись не имеет доступа к данным платежных карт и административных привилегий, влияющих на выполнение требований стандарта PA-DSS. При входе в АСО с установленным приложением Maratl используется механизм аутентификации ОС Windows.

Управление учетными записями для доступа к АСО осуществляется администратором ОС. Для учетных записей, заведенных на уровне ОС Windows, Агенту необходимо настроить следующие атрибуты парольной политики:

- пользователь должен использовать только персональную учетную запись и пароль доступа;
- пароль должен меняться пользователем каждые 90 дней;
- длина пароля должна составлять не менее 7 символов;
- пароль должен содержать цифры и буквы разного регистра;
- уникальность паролей должна быть обеспечена в течение 4 периодов их действия;
- учетная запись должна блокироваться после 6 неуспешных попыток введения пароля. Срок блокировки должен составлять как минимум 30 минут, или до момента ручной разблокировки этой учетной записи администратором ОС.

Приложение не поддерживает доступ с правами администратора вне консоли. Для удаленного доступа к операционной системе АСО должна использоваться многофакторная аутентификация. Методы аутентификации, также известные как факторы, включают в себя:

- что-то известное пользователю, напр. пароль;
- что-то, что есть в наличии у пользователя, напр. смарт-карта или eToken;
- сам пользователь, т.е. биометрические данные.

Чтобы включить многофакторную аутентификацию, в дополнение к паролю необходимо использовать один или более дополнительный метод аутентификации: eToken, смарт-карта, PIN и т.д.

Инструкция по настройке парольной политики в ОС приведена в Приложении Б.

3. РЕГИСТРАЦИЯ СОБЫТИЙ

Журнал протоколирования событий в приложении Maratl включен по умолчанию. Агенты не имеют функциональной возможности отключить или изменить параметры протоколирования ПО Maratl.

В журнале протоколирования могут содержаться только маскированные данные платежной карты (только первые 4 и последние 4 цифры). Данная функциональность реализована на уровне кода Приложения. Дополнительных действий по настройке журналов протоколирования Агенту производить не требуется.

Запись событий вида «Создание и удаление объектов системного уровня» реализована на уровне кода Приложения. Запись журналов осуществляется в файле `%working_dir%\logs\curent_date.log`.

Для облегчения централизованного протоколирования, журналы Maratl записываются в формате «текст с разделителями». Решения по агрегированию журналов такие как технологии SIEM могут быть использованы для сбора и передачи журналов на центральный сервер и для их автоматического анализа.

4. КОММУНИКАЦИИ

Для передачи данных между АСО и процессинговым центром, в качестве каналов связи могут использоваться следующие типы соединений:

- GPRS;
- 3G;
- LAN.

Рекомендуется использовать типы соединения, которые позволяют производить обмен данными с более высокой скоростью. Использование Wi-Fi в терминалах самообслуживания не рекомендовано.

Программное обеспечение Maratl поддерживает форматы передачи данных согласно Табл. 2.

Табл. 2. Форматы передачи данных Maratl

Протокол	Передача данных между клиентским и серверным ПО построена на основе протокола HTTP (RFC 2616: HTTP/1.1)
Метод передачи данных	Передаются только зашифрованные AES 256 + RSA-2048 данные. В качестве шифрования канала связи используется TLS версии 1.2. Для передачи данных используется метод RAW POST – поток данных передается в теле запроса, отправляемого клиентом на сервер
Формат данных	Данные передаются в формате XML (Extensible Markup Language (XML) 1.0)
Порт	Программное обеспечение Maratl использует порты UDP 53 (DNS), TCP 80 (HTTP), 123 (NTP), 443 (HTTPS)

Maratl не позволяет передавать номера карт с помощью технологий обмена сообщениями между конечными пользователями.

Средствами Приложения не предоставляется возможность удаленного доступа к Maratl. В случае необходимости удаленного доступа к ОС Windows на которой установлено ПО Maratl, удаленный доступ должен быть реализован безопасными методами и аутентифицирован с помощью механизма двухфакторной аутентификации. Для реализации двухфакторной аутентификации возможно использовать токен, смарт-карту, PIN к аппаратному устройству аутентификации и т.д.

АСО не должны иметь прямой доступ (прямая маршрутизация) в интернет. Для этой цели необходимо применять межсетевые экраны, поддерживающие динамическую фильтрацию пакетов с учетом состояния соединений (stateful inspection). Пример настройки встроенного в ОС Windows межсетевого экрана приведен в Приложении В.

Если на терминале самообслуживания с установленным Maratl используется подключение через Wi-Fi, необходимо настроить беспроводное соединение в соответствии с требованиями PCI DSS:

- сменить ключи шифрования, установленные по умолчанию, в момент настройки;
- сменить настройки сообщества SNMP, установленные по умолчанию (напр., public, private);
- сменить пароли по умолчанию на всех точках доступа;
- менять все перечисленные выше параметры каждый раз, когда сотрудник, обладающий этими знаниями, покидает организацию или меняет должность;
- включить технологию IEEE 802.11.i (WPA2) для шифрования и аутентификации. Использование WEP для контроля безопасности запрещено.

5. НЕОБХОДИМЫЙ ПЕРЕЧЕНЬ ПО

Для того, чтобы использовать сертифицированную версию Приложения Maratl, необходимо использовать следующее программное обеспечение на АСО:

1. Операционная система:

- Windows POSReady 7.

2. Программное обеспечение:

- Браузер MS Internet Explorer (начиная с 6 версии);
- Процессинговое ПО QIWI.

6. ПОЛИТИКА ВЕРСИОННОСТИ ПО

Присвоение номера версии ПО Maratl производится согласно Табл. 3.

Каждое изменение версии (релиз) сопровождается уведомлением в адрес всех пользователей Приложения (агентов), которое содержит новый номер версии Приложения и список основных изменений.

Табл. 3. Присвоение номера версии ПО Maratl

Изменения версии ПО	Тип изменений	Примеры	Тип изменений по стандарту PA-DSS (согласно 3.2)
Нумерация версии не меняется Третья цифра может нумероваться по шаблону "*" (например, 5.7.*)	Изменение параметров запуска приложения; Изменение названия приложения	Изменение наименования приложения или правообладателя приложения, исправление некритичных ошибок	Administrative
Изменяется третья цифра. Например, с 5.7.1 на 5.7.2. Во всех версиях с такими изменениями третья цифра может нумероваться по шаблону "*" (например, 5.7.*)	Изменения в пользовательском интерфейсе приложения; Изменение вида платежных отчетных документов (чеков и квитанций); Добавление команд в интерфейсы взаимодействия с устройствами или с процессингом; Изменения конфигурации локального хранилища данных (СУБД) приложения или стороннего ПО (например, Flash Player), используемого приложением; Изменение / добавление платежных шлюзов	Реализация бизнес-задач, улучшение бизнес-логики, новые плановые изменения, исправление критичных для функциональности приложения ошибок, не влияющих на безопасность	No Impact
Изменяется вторая цифра. Например, с 5.7.* на 5.8.*	Изменения, влияющие на операции с карточными данными; Изменения, влияющие на безопасность приложения; Изменения, влияющие на безопасность передачи данных по беспроводным сетям; Изменения в шифровании трафика и протоколах передачи данных	Изменения в ПО, влияющие на механизмы работы с данными платежных карт, устранение выявленных уязвимостей приложения, завершение годичного цикла разработки (при наличии других изменений)	Low Impact
Изменяется первая цифра. Например, с 5.7.* на 6.0.*	Изменение архитектуры приложения; Переработка более 50% исходного кода;	Крупные изменения в архитектуре ПО, глобальные переделки кода, новые стандарты	High Impact

Изменения версии ПО	Тип изменений	Примеры	Тип изменений по стандарту PA-DSS (согласно 3.2)
	Изменение принципов взаимодействия с устройствами; Изменение принципов взаимодействия с процессингом; Поддержка новых ОС / платформ	передачи сообщений между приложением и процессингом	

7. ОБНОВЛЕНИЯ

Приложение Maratl и его обновления необходимо загружать с официального сайта компании (https://corp.qiwi.com/business/activeagents). На сайте также размещен список изменений для каждого обновления. Список изменений содержит:

- новую версию приложений;
- описание каждого изменения и его влияния.

Информация об обновлениях также направляется агентам в рассылке.

После установки и подключения к процессинговому центру Maratl загружает обновления автоматически. Агенты не могут отключить автоматические обновления.

Обновления Приложения всегда загружаются в безопасном режиме. При загрузке Приложения с сайта Компании и при автоматических обновлениях используется HTTPS, TLS 1.2.

Для всех обновлений публикуется контрольная сумма (SHA256). Агенты должны использовать это значение, чтобы подтвердить целостность обновления.

ПРИЛОЖЕНИЕ А: Отключение/перенос файла подкачки

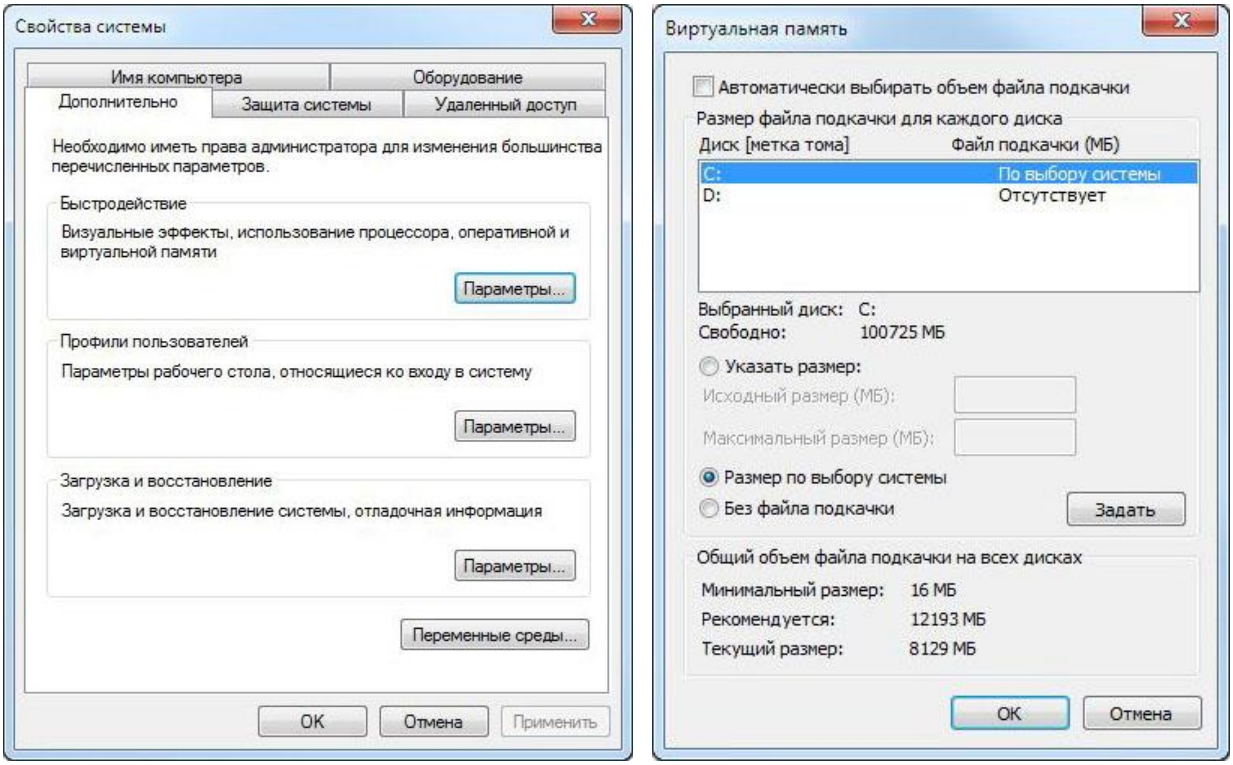
ОС Windows использует физическую память, а когда ее становится недостаточно, обращается к своп-файлу, где хранятся данные, не поместившиеся на физической памяти. Файл подкачки имеет строго заданное название `pagefile.sys`.

Чтобы изменить стандартное расположение `pagefile.sys`, необходимо выполнить:

«Мой компьютер» → «Свойства» → «Дополнительные параметры системы» → «Дополнительно» → «Параметры» (во вкладке «Быстродействие») → «Дополнительно» → «Изменить» (в отсеке «Виртуальная память») («Computer» → «Properties» → «Advanced system settings» → «Advanced» «Performance» → «Advanced» → «Virtual memory» → «Change…»).

Появится диалоговое окно «Виртуальная память» (см. Рис. 1).

Рис. 1. Окно «Виртуальная память»



Далее необходимо выбрать «Без файла подкачки» («No paging file») или «Задать» («Set»), где указать шифрованный раздел.

Так же необходимо настроить очищение файла подкачки при завершении работы. Для этого выполните:

«Пуск» → «Выполнить» → secpol.msc («Start» → «Run» → secpol.msc)

В параметрах безопасности необходимо включить параметр: «Завершение работы: очистка своп-файла виртуальной памяти» («Shutdown: Clear virtual memory pagefile»).

ПРИЛОЖЕНИЕ Б: Настройка парольной политики

Для настройки атрибутов парольной политики необходимо выполнить действия согласно Табл. 4.

Табл. 4. Атрибуты парольной политики

Значение	Детали конфигурации
Максимальный срок действия пароля не более 90 дней	Control Panel → Administrative Tools → Local Security Settings (Вкладка «Account Policies» → «Password Policy») (Панель управления → Администрирование → Локальные параметры безопасности (Вкладка «Политики учетных записей» → «Политика паролей») Maximum Password Age (Максимальный срок действия пароля) 90
Сложность пароля (должен содержать цифры и буквы)	Control Panel → Administrative Tools → Local Security Settings (Вкладка «Account Policies» → «Password Policy») (Панель управления → Администрирование → Локальные параметры безопасности (Вкладка «Политики учетных записей» → «Политика паролей») Password Complexity Requirements (Пароль должен отвечать требованиям сложности) Enabled (включить)
Минимальная длина пароля не менее 7 символов	Control Panel → Administrative Tools → Local Security Settings (Вкладка «Account Policies» → «Password Policy») (Панель управления → Администрирование → Локальные параметры безопасности (Вкладка «Политики учетных записей» → «Политика паролей») Minimum Password Length (Минимальная длина пароля) 8
Уникальность паролей должна быть обеспечена в течение 4 периодов их действия	Control Panel → Administrative Tools → Local Security Settings (Вкладка «Account Policies» → «Password Policy») (Панель управления → Администрирование → Локальные параметры безопасности (Вкладка «Политики учетных записей» → «Политика паролей») Enforce password history (Вести журнал паролей) 4
Не хранить пароли, используя обратимое шифрование	Control Panel → Administrative Tools → Local Security Settings (Вкладка «Account Policies» → «Password Policy») (Панель управления → Администрирование → Локальные параметры безопасности (Вкладка «Политики учетных записей» → «Политика паролей») Reversible Encryption for Passwords (Хранить пароли, используя обратимое шифрование) Disabled (отключить)
Максимальное кол-во неудачных попыток входа должно быть не более 6	Control Panel → Administrative Tools → Local Security Settings (Вкладка «Account Policies» → «Account Lockout Policy») (Панель управления → Администрирование → Локальные параметры безопасности (Вкладка «Политики учетных записей» → «Политика блокировки учетной записи») Account lockout threshold (Пороговое значение блокировки) 6
Время блокировки учетной записи должно быть не менее 30 минут, либо не выставлять ничего, тогда	Control Panel → Administrative Tools → Local Security Settings (Вкладка «Account Policies» → «Account Lockout Policy»)

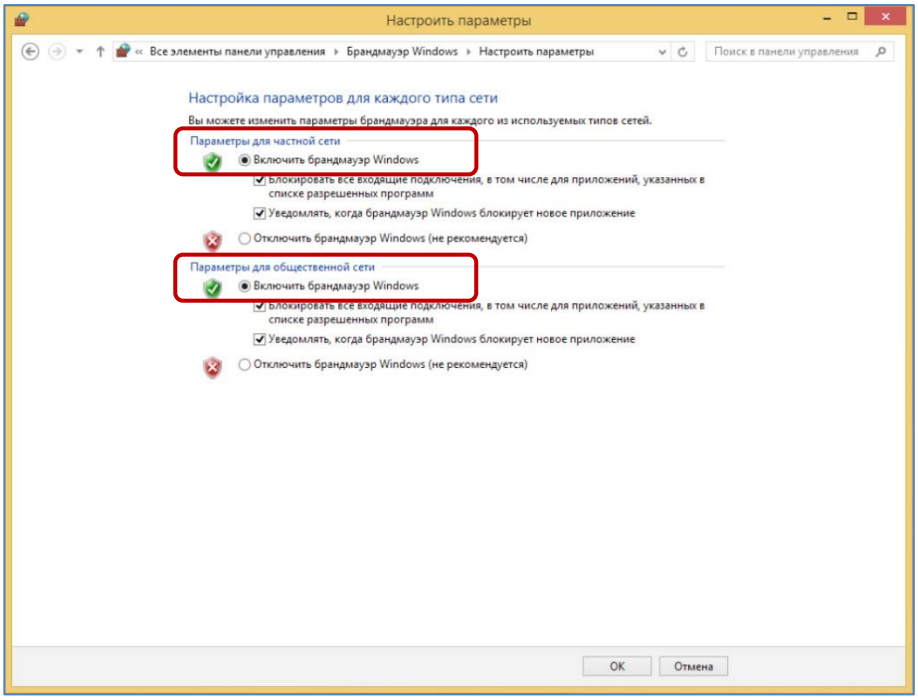
Значение	Детали конфигурации
разблокировать сможет только администратор	(Панель управления → Администрирование → Локальные параметры безопасности (Вкладка «Политики учетных записей» → «Политика блокировки учетной записи») Account lockout duration (Блокировка учетной записи на) 30

ПРИЛОЖЕНИЕ B: Настройка Windows Firewall

Для того, чтобы включить межсетевой экран Windows, необходимо выполнить:

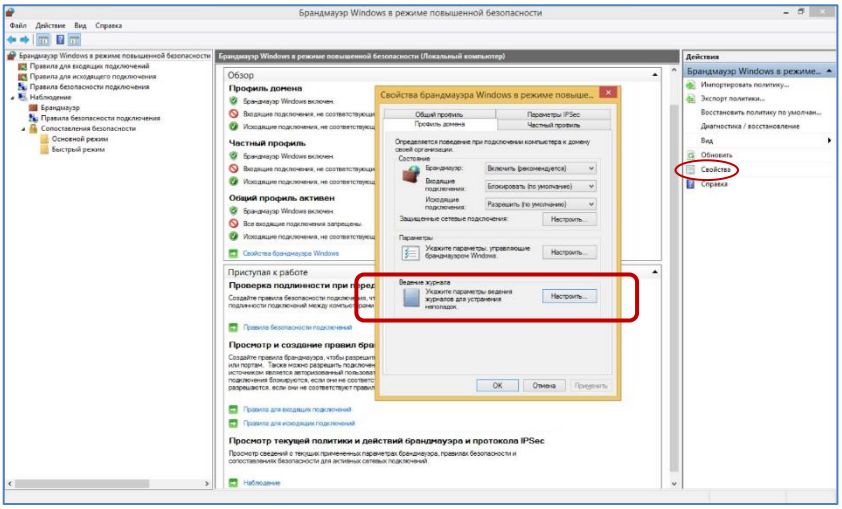
«Пуск» → «Панель управления» → «Система и безопасность» → «Брандмауэр Windows» → «Включение и отключение брандмауэра Windows» («Start» → «Control Panel» → «System and Security» → «Windows Firewall» → «Turn Windows Firewall on or off») на вкладке «Настройка параметров» («Customize Settings») включите «Включение брандмауэра Windows» («Turn on Windows Firewall») для «Параметры размещения в домашней или рабочей (частной) сети» и «Параметры размещений в общедоступной сети» («Home or work (private) network location settings» и «Public network location settings») (см. Рис. 2).

Рис. 2. Окно «Настройка параметров» («Customize Settings»)



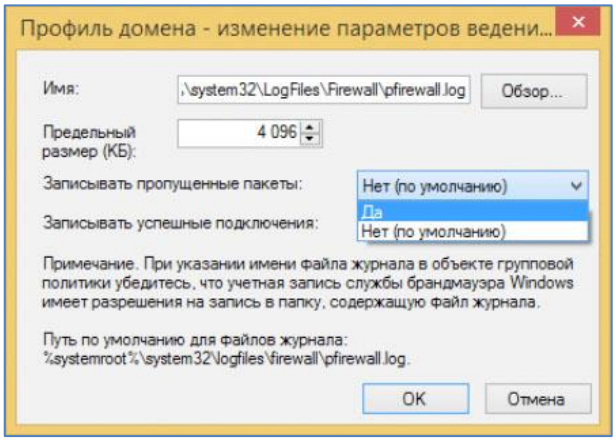
Включите ведение журналов (по умолчанию ведение журналов отключено). Для этого необходимо перейти на закладку «Дополнительные параметры» («Advanced») и справа в группе «Действия» («Actions») нажать кнопку «Свойства» («Properties»).

Рис. 3. Дополнительные настройки брандмауэра



В появившемся окне в блоке «Ведение журнала» («Security Logging») нажмите кнопку «Настроить» («Settings») и включите переключатели «Записывать пропущенные пакеты» («Log dropped packets») и «Записывать успешные подключения» («Log successful connections»). Нажмите кнопку «OK».

Рис. 4. Ведение журналов



СПИСОК РИСУНКОВ

СПИСОК ТАБЛИЦ