НАСТРОЙКИ ПО QIWI КАССИР В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ СТАНДАРТА БЕЗОПАСНОСТИ PA-DSS

вер. 1.1

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 QIWI Кассир	Программное обеспечение, разработанное АО «КИВИ». По тексту данного документа – ПО, Приложение
АО «КИВИ»	Акционерное общество «КИВИ»
ОС	Операционная система
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 QIWI Кассир в соответствии с требованиями стандартов безопасности в индустрии платежных карт PCI DSS и PA-DSS. Для использования сертифицированной версии программного обеспечения QIWI Кассир требованиям стандарта PA-DSS, Агенту необходимо настроить Приложение согласно настоящему документу PA-DSS Implementation Guide.

Название программного обеспечения – QIWI Кассир.

Версия программного обеспечения – 3.1.x

Актуальная версия документа и дистрибутив ПО QIWI Кассир 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 таблице 1

1 История изменений документа

Автор	Дата изменений	Номер	Описание изменений
	09/12/2016	01	·Исходная редакция документа, разработанная с учетом требований PCI DSS и PA DSS версия 3.2.

1. ЗАЩИТА ДАННЫХ ПЛАТЕЖНЫХ КАРТ

Требования стандартов PCI DSS и PA-DSS запрещают хранить критичные аутентификационные данные (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);
- Срок действия карты (Expiration Date);
- Имя держателя карты (Cardholder Name);
- Сервисный код (Service Code).

К критичным аутентификационным данным относятся:

- Полное содержание магнитной полосы карты (Track1, Track2);
- CAV2/CVC2/CVV2/CID;
- ПИН/ПИН-блок.

Для функционирования программного обеспечения QIWI Кассир не требуется обработка критичных аутентификационных данных. Предыдущие версии программного обеспечения QIWI Кассир также не обрабатывали критичные аутентификационные данные.

В приложении QIWI Кассир в рамках выполнения авторизации данные держателя платежной карты обрабатываются в оперативной памяти, а также сохраняются до момента завершения авторизации в файле `%working_dir%\payments.db`. Для защиты хранимых данных платежных карт в файле `payments.db` применяется стойкое шифрование. Используется алгоритм AES с длиной ключа 256 бит.

Если данные не были удалены автоматически после завершения транзакции, (например, в случае отсутствия связи с процессинговым центром) следует удалить их вручную, используя методы безопасного и гарантированного удаления, например, с помощью программы «SDelete». Для этого необходимо удалить данные:

- файл `%working_dir%\payments.db`;
- файл `%working_dir%\archive.db`.

После завершения авторизации маскированный номер карты (первые 4 и последние 4 цифры) хранится в файле `%working_dir%\payments.db` и `%working_dir%\archive.db`. Оба файла зашифрованы. Используется алгоритм AES с длиной ключа 256 бит.

Для отображения номера карты на экране и чеках используется маскированный вид номера карты (отображаются только первые 4 и последние 4 цифры). Данный функционал реализован на уровне кода приложения. Стоит отметить, что отображение полного номера карты осуществляется только во время ввода номера карты Агентом. Дополнительных действий по настройке отображения номера карты Агенту производить не требуется.

В случае необходимости осуществления сбора и передачи данных платежных карт, данные должны предоставляться в объеме, минимально необходимом. Для передачи и хранения таких данных Агентам необходимо использовать стойкое шифрование. 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).

2. ДОСТУП К ДАННЫМ ПЛАТЕЖНЫХ КАРТ

В ПО QIWI Кассир отсутствуют учетные записи. Доступ к данным платежных карт или административным привилегиям, влияющим на выполнение требований стандарта PA DSS, невозможен. Для запуска QIWI Кассир необходимо ввести пароль от сертификата, который расположен на токене или в системном хранилище.

При входе в операционную систему с установленным приложением QIWI Кассир используется механизм аутентификации ОС Windows. Управление учетными записями 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;
- длина пароля должна составлять не менее 8 символов;
- пароль должен содержать цифры и буквы разного регистра;
- пароль должен меняться пользователем каждые 90 дней;
- уникальность паролей должна быть обеспечена в течение 5 периодов их действия;
- запрет хранения паролей, используя обратимое шифрование.

Настройками системы должно обеспечиваться принудительное блокирование учетной записи после пятикратного введения неверного пароля. Разблокирование учетной записи должно происходить автоматически не менее чем на 30 минут или администратором.

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

3. РЕГИСТРАЦИЯ СОБЫТИЙ

Журнал протоколирования событий типа «Creation and deletion of system-level objects» в приложении QIWI Кассир включен по умолчанию. Агенты не имеют функциональной возможности отключить или изменить параметры протоколирования.

Номера карт в журнале протоколирования содержатся только в маскированном виде (отображаются только первые 4 и последние 4 цифры). Данный функционал реализован на уровне кода приложения. Дополнительных действий по настройке журналов протоколирования Агенту производить не требуется.

Запись журналов на уровне ПО осуществляется в файле
c:\Users\%user_login%\AppData\Roaming\osmp\qiwicashier\logs\current_date.log.

4. КОММУНИКАЦИИ

Для передачи данных между ПО QIWI Кассир и процессинговым центром АО «КИВИ» в качестве каналов связи могут использоваться следующие типы соединений:

- GPRS;
- LAN;
- Wi-Fi.

Рекомендуется использовать типы соединения, которые позволяют производить обмен данными с более высокой скоростью.

Программное обеспечение QIWI Кассир поддерживает форматы передачи данных согласно Таблице 2.

2 Форматы передачи данных

Протокол	Передача данных между клиентским и серверным ПО построена на основе протокола **HTTPS**
Метод передачи данных	Передаются только зашифрованные данные. В качестве шифрования канала связи используется TLS не ниже версии 1.1. 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 QIWI Кассир использует порты UDP 53 (DNS), TCP 80 (HTTP), 123 (NTP), 443 (HTTPS)

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

Средствами Приложения не предоставляется возможность удаленного доступа к QIWI Кассир. В случае необходимости удаленного доступа к ОС Windows, на которой установлено ПО QIWI Кассир, 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.

Компьютер с установленным на нем ПО QIWI Кассир не должен иметь прямого доступа (прямой маршрутизации) к 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.

5. НЕОБХОДИМЫЙ ПЕРЕЧЕНЬ ПО

Для того, чтобы использовать сертифицированную версию Приложения QIWI Кассир, необходимо использовать следующее программное обеспечение:

1. Операционная система:

Windows 7, Windows 8.1

3 Информация о поддержке операционных систем

Тип операционной системы	Дата завершения срока поддержки	Действия после завершения срока поддержки
Windows 7	4/9/2013	Отслеживание уязвимостей (включая: базы данный уязвимостей, информацию от производителя операционной системы, информацию от разработчика ПО, информацию из других источников) Реализация мер по снижению угроз безопасности Переход на новую версию операционной системы
Windows 8.1	1/10/2023	
Public vulnerabilities database: – http://nvd.nist.gov/ – http://cwe.mitre.org – http://www.securityfocus.com – http://cwe.mitre.org/ – http://cwe.mitre.org/top25/index.html – http://owasp.org/ – http://bdu.fstec.ru/threat OS vendors information: – https://support.microsoft.com/en-us/lifecycle/search		

2. Программное обеспечение:

- СУБД SQLite версия 3.15 и выше.

6. ПОЛИТИКА ВЕРСИОННОСТИ ПО

Присвоение номера версии ПО QIWI Кассир производится согласно Таблице 4.

4 Присвоение номера версии ПО

Изменения версии	Тип изменений	Примеры	Тип изменений по стандарту PA-DSS
Нумерация версии не меняется **Четвертая цифра может нумероваться по шаблону "*" (например, 5.1.1.*).**	– Изменение параметров запуска приложения – Изменение названия приложения	Изменение наименования приложения или правообладателя приложения, исправление некритичных ошибок	Administrative
Изменяется четвертая цифра. **Четвертая цифра может нумероваться по шаблону "*" (например, 5.1.1.*).**	– Изменения и рефакторинг, не затрагивающие платежную логику – Изменение параметров запуска приложения – Изменение названия приложения	Дополнительный дебаг, исправление мелких багов, изменение отчетов агентов, добавление нестандартного провайдера, изменения на прикладном сетевом уровне	No Impact
Изменяется третья цифра. Например, с 5.1.1 на 5.1.2. **Во всех версиях с такими изменениями третья цифра может нумероваться по шаблону "*" (например, 5.1.*).**	– Изменения в пользовательском интерфейсе приложения – Изменение вида платежных отчетных документов – Изменение взаимодействия с контрольно-кассовой техникой – Изменения конфигурации локального хранилища данных (СУБД) приложения или стороннего ПО, используемого приложением	Реализация бизнес-задач, улучшение бизнес-логики, новые плановые изменения, исправление критичных для функциональности приложения ошибок, не влияющих на безопасность , переход на новую версию Framework	No Impact
Изменяется вторая цифра. Например, с 5.1.* на 5.2.*	– 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 – Изменение логики шифрования локальной БД	Изменения в ПО, влияющие на механизмы работы с данными платежных карт, устранение выявленных уязвимостей приложения, завершение годичного цикла разработки (при наличии других изменений), смена процедуры шифрования локальной БД	Low Impact

Изменения версии	Тип изменений	Примеры	Тип изменений по стандарту PA-DSS
Изменяется первая цифра. Например, с 5.3.* на 6.0.*	– Изменение архитектуры приложения – Переработка более 50% исходного кода – Изменение принципов взаимодействия с устройствами – Изменение принципов взаимодействия с процессингом – Поддержка новых ОС / платформ	Крупные изменения в архитектуре ПО, глобальные переделки кода, новые стандарты передачи сообщений между приложением и процессингом, смена парка контрольно-кассовой техники	High Impact

Выпуск каждой версии (релиз) сопровождается отправкой оповещения всем пользователям приложения (агентам), в котором указывается номер новой версии приложения и список основных изменений в версии.

ПРИЛОЖЕНИЕ А: Отключение/перенос файла подкачки

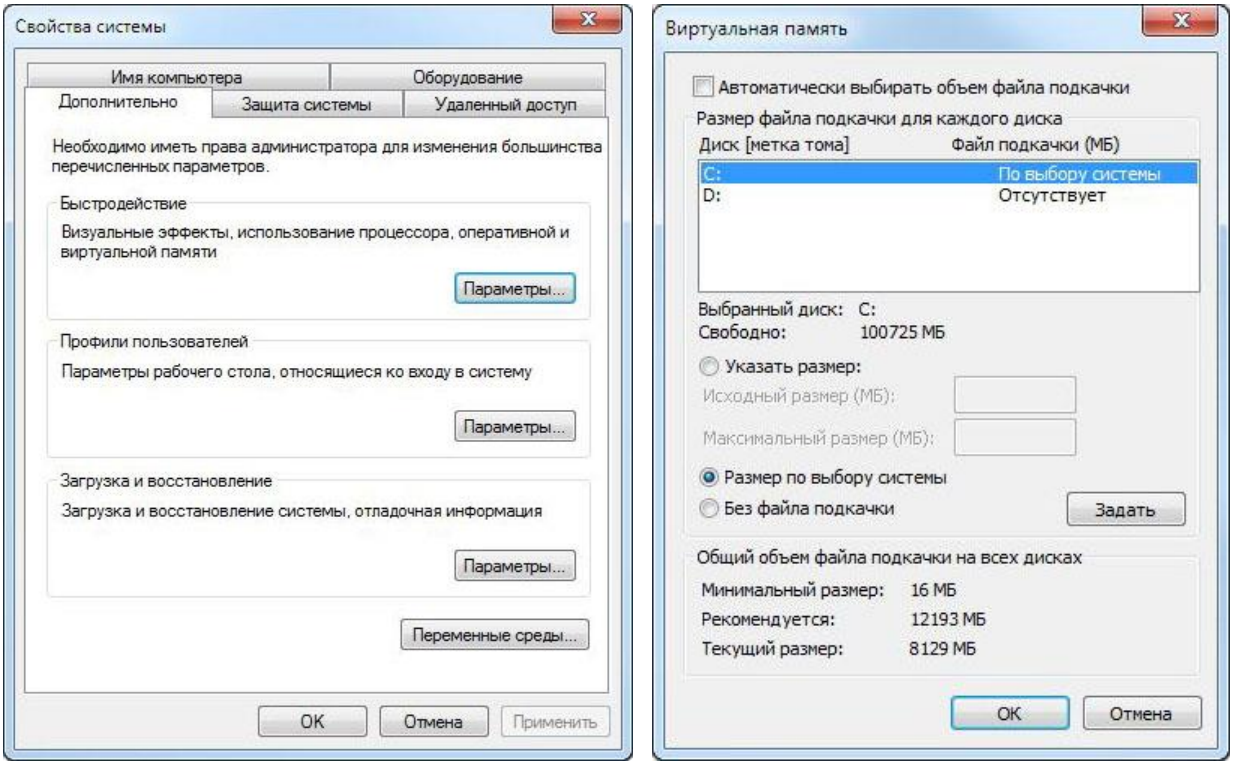
ОС Windows 7 использует физическую память, а когда ее становится недостаточно, обращается к своп-файлу, где хранятся данные, не поместившиеся на физической памяти. Файл подкачки имеет строго заданное название `pagefile.sys`.

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 таблице 5.

5 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	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 8 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 5 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) 5
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 5-ти	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) 5
Время блокировки учетной записи должно быть не менее 30 минут либо не	Control Panel → Administrative Tools → Local Security Settings (Вкладка «Account Policies» → «Account Lockout Policy»)

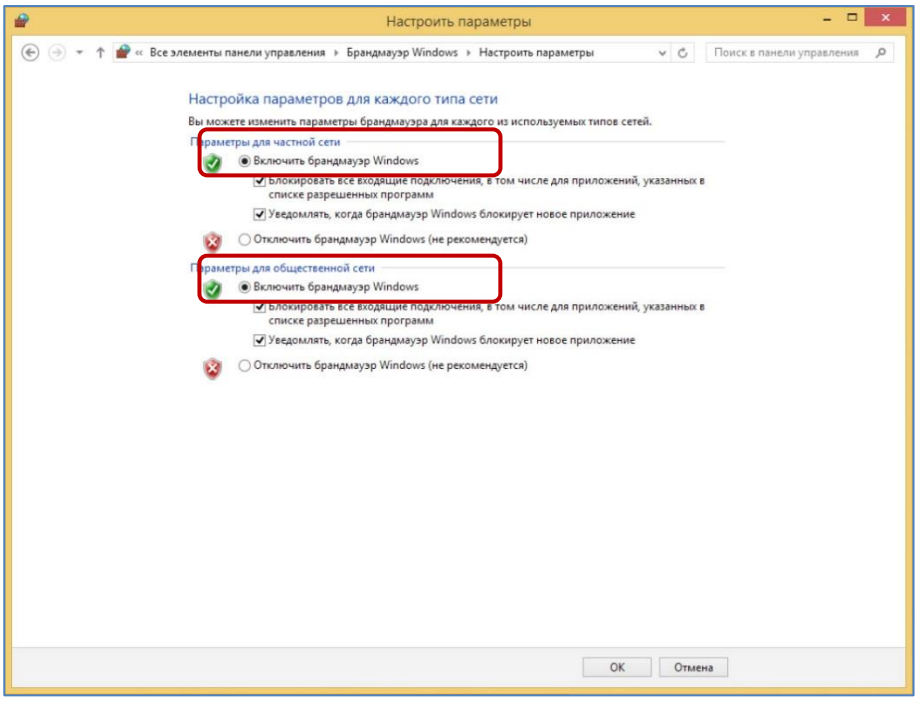
Значение	Детали конфигурации
выставлять ничего, тогда разблокировать сможет только администратор	(Панель управления → Администрирование → Локальные параметры безопасности (Вкладка «Политики учетных записей» → «Политика блокировки учетной записи») Account lockout duration (Блокировка учетной записи на)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

ПРИЛОЖЕНИЕ В: Настройка Windows Firewall

Для того, чтобы включить межсетевой экран Windows необходимо выполнить:

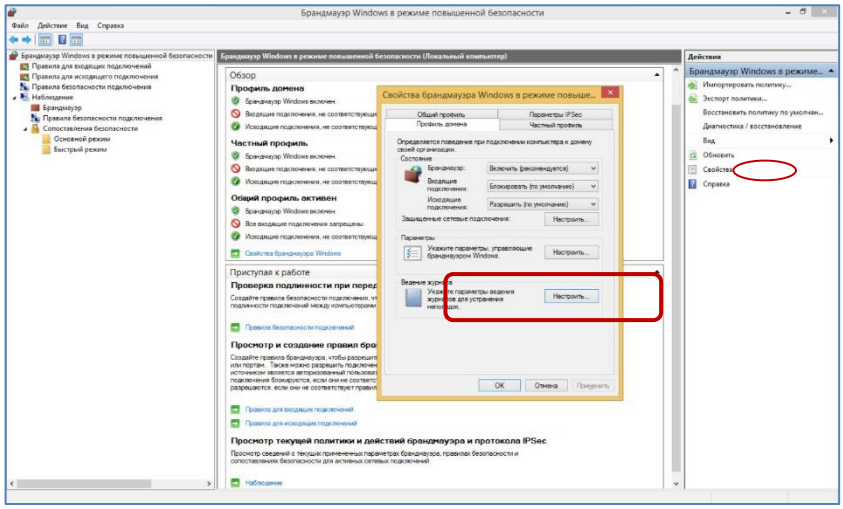
«Пуск» → «Панель управления» → «Система и безопасность» → «Брандмауэр Windows» → «Включение и отключение брандмауэра Windows» («Start» → «Control Panel» → «System and Security» → «Windows Firewall» → «Turn Windows Firewall on or off») на вкладке «Настройка параметров» («Customize Settings») включите «Windows Firewall» «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

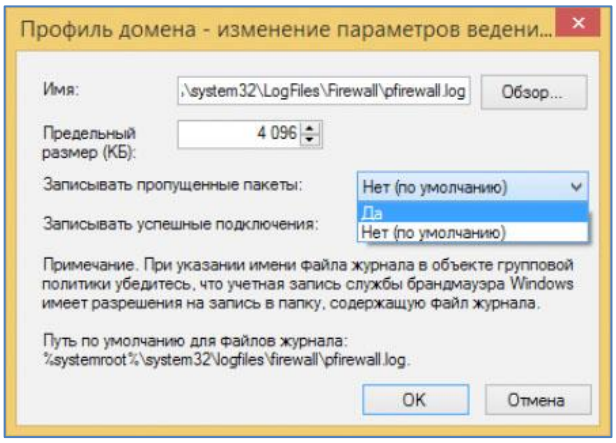


В появившемся окне в блоке «Ведение журнала» («Security Logging») нажмите кнопку «Настроить» («Settings») и включите переключатели:

- «Записывать пропущенные пакеты» («Log dropped packets») – в положение «Да»;
- «Записывать успешные подключения» («Log successful connections») – в положение «Да».

Нажмите кнопку «ОК».

Рис. 4. Ведение журналов



СПИСОК РИСУНКОВ

СПИСОК ТАБЛИЦ