УТВЕРЖДЕН

RU.83128364.501540-XS-7.8.24-ЛУ

Сетевой сканер безопасности XSpider 7.8.24

Описание применения

RU.83128364.501540-XS-7.8.24 31 01

Листов 22

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

АННОТАЦИЯ

Настоящий документ является составной частью документации на сетевой сканер безопасности XSpider 7.8.24 (далее Программа).

В разделе «Назначение Программы» приведено описание назначения, функциональные возможности Программы, основные характеристики и ограничения, накладываемые на область применения.

В разделе «Условия применения» указаны условия, необходимые для функционирования Программы (требования к необходимым для Программы техническим средствам, общие характеристики входной и выходной информации, а также требования и условия организационного, технического и технологического характера).

В разделе «Описание задачи» указаны задачи, решаемые Программой, и методы их решения.

В разделе «Входные и выходные данные» указаны сведения о входных и выходных данных Программы.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

СОДЕРЖАНИЕ

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа предназначена для выявления и контроля уязвимостей в контролируемых узлах информационной инфраструктуры.

Программа позволяет решать следующие классы задач:

– Идентификацию узлов и сетевых служб;
– Выявление уязвимостей и ошибок конфигурирования;
– Планирование и автоматизация сканирования;
– Формирование отчетов;
– Разграничение доступа к функциям программы.

Программа обеспечивать идентификацию операционных систем (ОС), перечисленных в Таб. 1

Таб. 1 - Перечень наименований и версий ОС

Наименование	**Версии**
Операционные системы семейства Microsoft Windows	
Microsoft Windows 2000 Server[1]	sp4
Microsoft Windows XP	sp3
Microsoft Windows 7 Professional	sp1
Microsoft Windows 2003 R2 Server Enterprise Edition	sp2
Microsoft Windows 2008 Server Enterprise Edition	sp2
Microsoft Windows 2008 R2 Server Standard Edition	sp1
Операционные системы семейства Unix и GNU/Linux	
Sun Solaris	10.0
Debian	6.0
FreeBSD	7.1

[1] Обнаружение уязвимостей в браузерах, входящих в состав Microsoft Windows 2000, осуществляется начиная с версии в Internet Explorer 6.0.

Наименование	Версии
Операционные системы телекоммуникационного оборудования	
Cisco IOS	12.1

Программа обеспечивать сканирование и идентификацию узлов сети, реализующих сетевые сервисы, доступные по протоколам UDP:

- Echo;
- Date;
- Quota;
- Chargen;
- DNS;
- TFTP;
- PortMapper;
- NTP;
- Microsoft RPC;
- NetBIOS Name;
- SNMP;
- MsSQL;
- Internet Key Exchange (IKE);
- SIP;
- mDNS.

Программа обеспечивает идентификацию уязвимостей и ошибок конфигурирования для следующего ПО, функционирующего в среде Windows:

- Microsoft Windows;
- Microsoft SQL Server;
- Microsoft Internet Explorer (версия 6 и старше);
- Microsoft Windows MDAC;
- Microsoft Internet Information Services;
- Microsoft WINS Server;
- Microsoft DNS Server;
- Microsoft Windows Media;
- Microsoft Exchange.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Программа обеспечивает выявление уязвимостей прикладных систем, построенных с использованием веб-технологий.

Программа обеспечивает автоматический запуск задач на сканирование в соответствии с задаваемым пользователем расписанием.

По результатам сканирования Программа может формировать отчеты следующих типов:

– информационный;
– дифференциальный.

В Программе реализованы возможности по управлению доступом к собственным ресурсам. Программа обеспечивает:

– Аутентификацию пользователя по паролю при входе в Программу;
– Возможность смены пароля пользователя;
– Регистрацию событий.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Общие требования

Программа устанавливается на аппаратную платформу с характеристиками не ниже, чем приведенные в Таб. 2.

Таб. 2 – Минимальные аппаратные требования для установки Программы

Компонента	**Процессор**	**Оперативная память**	**Жесткий диск**
XSpider	P4 1,6 ГГц	2 Гб	5 Гб

Разрешение монитора для установки и работы с системой должно составлять не менее 1280 x 1024 пикс.

Выполнения данных требований достаточно для установки программных компонентов, однако для полнофункциональной работы могут потребоваться дополнительные аппаратные ресурсы.

Программа функционирует под управлением операционных систем (ОС), приведенных в Таб. 3.

Таб. 3 – Перечень совместимых ОС

Наименование программного обеспечения	**Версии**
Microsoft Windows XP Professional	SP 3 (x86)
Microsoft Windows 2008 R2 Standard Edition	SP1 (x64)
Microsoft Windows 7 Professional	SP1 (x86,x64)

Программа в процессе функционирования использует внешнюю (по отношению к программе, но не по отношению к аппаратной платформе) базу данных (версия Express):

– Microsoft SQL Server 2008 R2.

На аппаратную платформу с Программой дополнительно должны быть установлены:

– Microsoft Internet Explorer одной из следующих версий 7, 8, 9, 10;

– Microsoft .NET Framework Version 4.0.

Информационное взаимодействие между Программой и сканируемыми объектами осуществляться с использованием стека (набора) протоколов TCP/IP.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Программа имеет возможность использования в виртуальной среде. В качестве средств виртуализации поддерживается:

– VMware ESXI 4.1.

2.2. Требования к сетевой инфраструктуре

При использовании Программы, следует учитывать возможное влияние на него сетевой архитектуры и средств защиты информации контролируемых ЛВС.

2.2.1 Сетевые транспорты

Все параметры сетевой архитектуры тесно связаны с понятием транспорта. Система XSpider реализует концепцию сканирования узлов без применения заранее установленных агентов.

Транспорт – это набор сетевых протоколов, используемых сканером XSpider для проведения сканирования.

В системе XSpider используется транспорт RPC. Номера портов RPC присваиваются автоматически, в диапазоне 1024 – 65535 обычно используются для ОС Windows 2000\XP\2003, а для ОС Windows Vista\2008 используется диапазон 49152 – 65535.

2.2.2 Межсетевые экраны

Межсетевые экраны (МЭ) осуществляют фильтрацию трафика и могут блокировать доступ к сетевым портам, на которых работают протоколы удаленного управления, используемые Программой при проведении сканирования. Для решения этой проблемы можно использовать два подхода: открытие сетевых портов, используемых программой на МЭ, или размещение Программы за межсетевым экраном в непосредственной близости от объекта сканирования.

Оптимальным с точки зрения достоверности и скорости сканирования является отсутствие межсетевого экрана между объектом сканирования и сканером XSpider.

2.2.3 Системы обнаружения и предотвращения атак

Системы обнаружения/предотвращения атак в большинстве случаев реагируют на процесс сканирования как на потенциальную атаку. В связи с этим рекомендуется внести изменения в список исключений системы обнаружения атак.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

2.2.4 Средства защиты прикладного уровня

Большинство современных сетевых средств обеспечения безопасности содержат модули анализа прикладных протоколов (Stateful Inspection, Application Firewall). Данные механизмы могут вмешиваться в работу сканера, снижая достоверность полученных результатов. Так, например, сканирование веб-приложения через МЭ, поддерживающий функции защиты веб-приложений (Web Application Firewall), не будет достоверным, поскольку МЭ заблокирует ряд потенциально опасных запросов, используемых сканером.

В некоторых средствах защиты не существует возможности отключить фильтрацию прикладных протоколов только для отдельных узлов. При возникновении таких ситуаций рекомендуется выносить сканер за МЭ.

2.2.5 Средства защиты уровня узла

В случае использования персональных МЭ и других средств защиты уровня узла на сканируемых АРМ необходимо обеспечить доступ по используемым программой протоколам.

2.3. Требования и условия организационного и технологического характера

При эксплуатации Программы, должно быть обеспечено выполнение следующих требований:

– наличие администратора информационной безопасности Программы, отвечающего за необходимые настройки политик безопасности;

– сохранение в секрете пароля администратора (пользователя) Программы;

– обеспечение физической охраны технических средств, на которых развернута Программа, предусматривающей наличие надежных препятствий для несанкционированного проникновения в помещение с Программой;

– реализация мероприятий по антивирусной защите Программы;

– периодическое тестирование функций защиты Программы администратором информационной безопасности не реже одного раза в год;

– использование средств периодического контроля за целостностью программной и информационной части Программы, а также обеспечить неизменность ее программной среды;

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

– осуществлять регистрацию результатов тестирования и проверок Программы в Формуляре.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

3. ОПИСАНИЕ ЗАДАЧ

Программа позволяет решать следующие классы задач:

– Идентификацию узлов и сетевых служб;
– Выявление уязвимостей и ошибок конфигурирования;
– Планирование и автоматизация сканирования;
– Формирование отчетов;
– Разграничение доступа к функциям программы.

3.1 Сканирование узлов сети

Для решения задач идентификации узлов и сетевых служб, выявления уязвимостей и ошибок конфигурирования проводится сканирование контролируемых узлов сети.

Для проведения сканирования необходимо создать задачу, указать сканируемые узлы, настроить профиль сканирования и запустить сканирование.

Все основные операции по управлению сканированием осуществляются из вкладки «Сканирование» (см. Рис. 1).

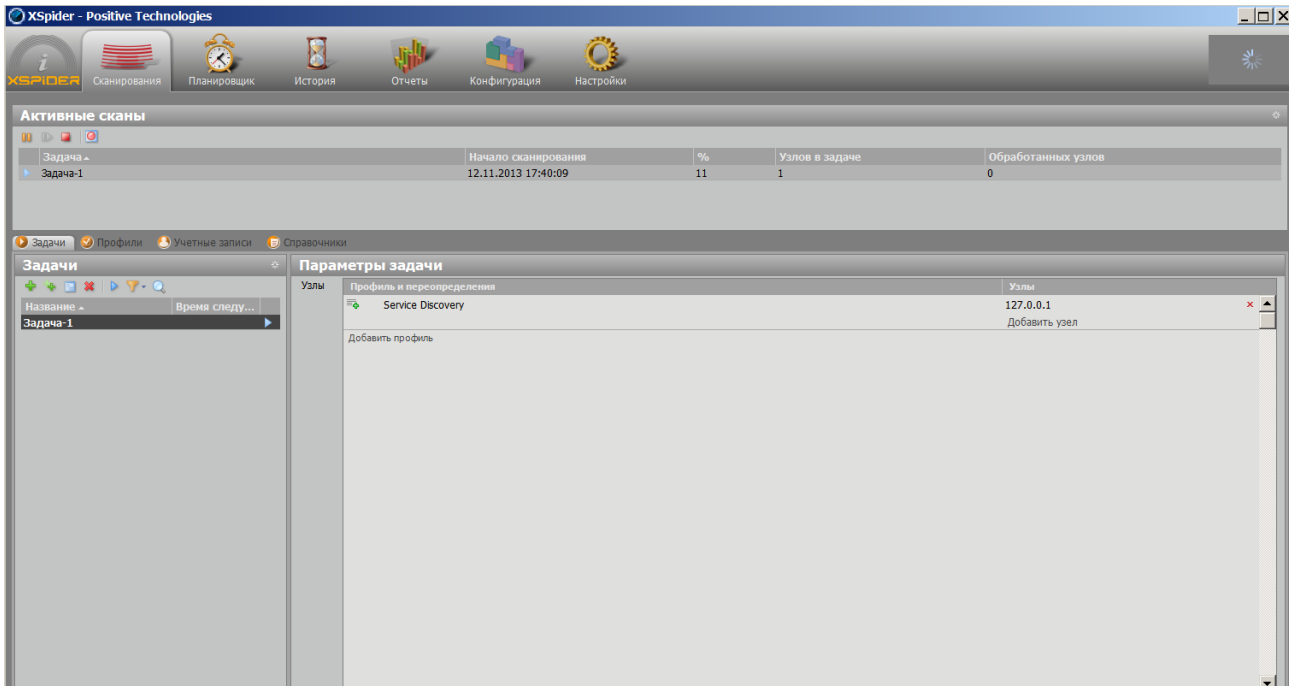

Рис. 1 – Вкладка «Сканирование»

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Вкладка Сканирования предназначена для отображения информации об активных сканах и управления ими, а также для управления профилями сканирования, которые задают настройки, используемые при сканировании

В Программе существует несколько режимов запуска задач на выполнение:

– Собственно запуск задачи;
– Сканирование выбранных узлов;
– Режим Host discovery

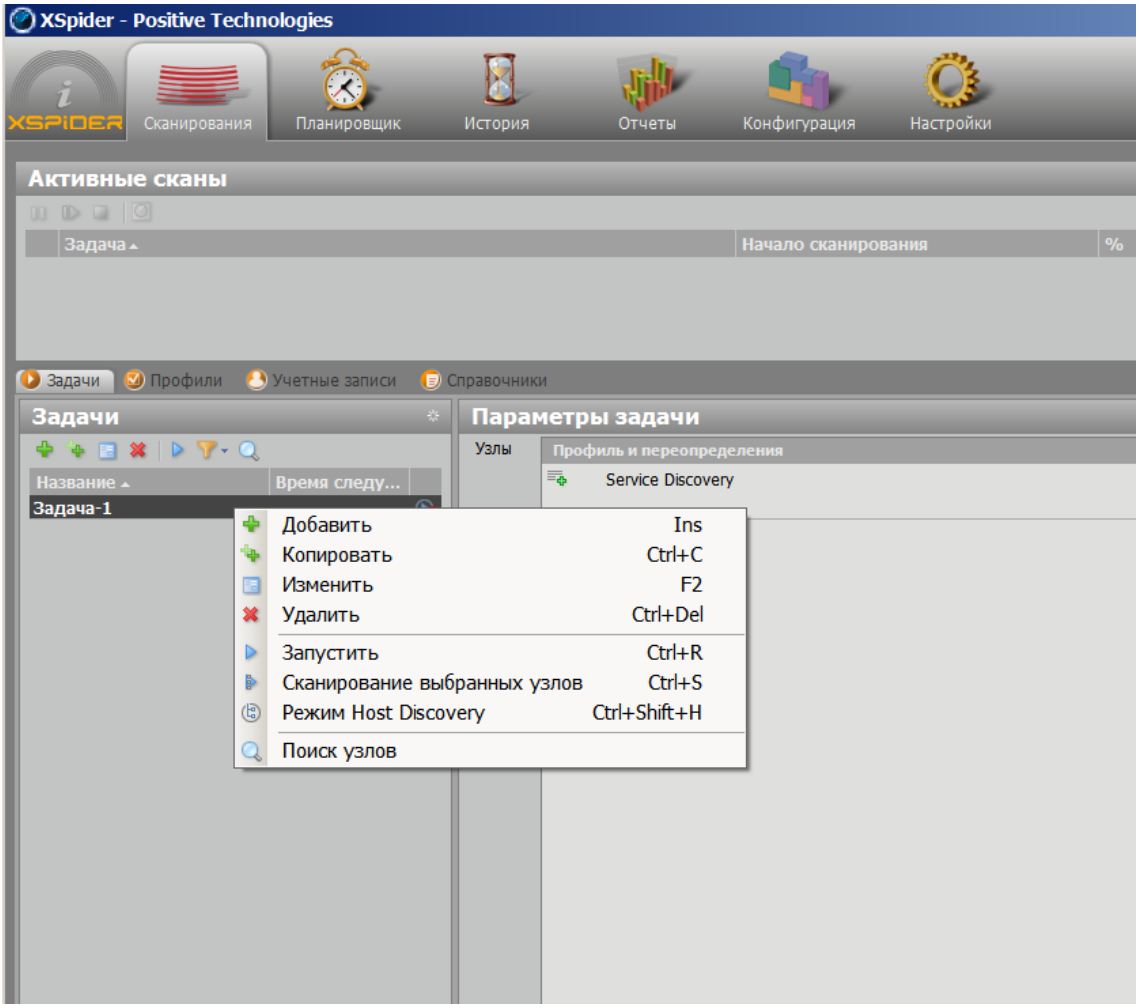

Рис. 2 – Выбор режима запуска задач

Выбор режима запуска задачи осуществляется из меню, появляющегося при нажатии правой кнопкой мыши на конкретной задаче (см. Рис. 2).

Режим «запустить» непосредственно осуществляет запуск задачи с параметрами и адресами, указанными в профиле.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Режим «сканирование выбранных узлов» позволяет осуществить запуск задачи с параметрами указанными в профиле, при этом выбрать только адреса интересующих нас узлов.

Режим Host discovery позволяет провести сканирование, направленное только на определение доступности узлов, указанных в задаче, и некоторых ключевых для сканирования параметров. Доступность узлов определяется по следующим параметрам:

- ICMP ping – проверить доступность узла по ICMP ping
- TCP ping – проверить доступность узла по TCP ping
- ICMP и TCP ping - проверить доступность узла по ICMP и TCP ping
- Определение имен – определить имена доступных узлов.

3.2 Планирование и автоматизация сканирования

Для формирования запланированных действий используется вкладка «Планировщик». Предусмотрена возможность выполнить следующие сценарии запуска задачи:

- Последовательный запуск;
- Выпуск отчета;
- Host Discovery.

Для создания нового расписания необходимо на панели инструментов выбрать кнопку *Создать*. Откроется новое диалоговое окно *Создание расписания*, в котором можно выбрать необходимый сценарий запуска и указать параметры его запуска.

3.3 Формирование отчетов

Результаты работы Программы называются «сканами». Сканы можно посмотреть на вкладке «История» (см. Рис. 3).

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

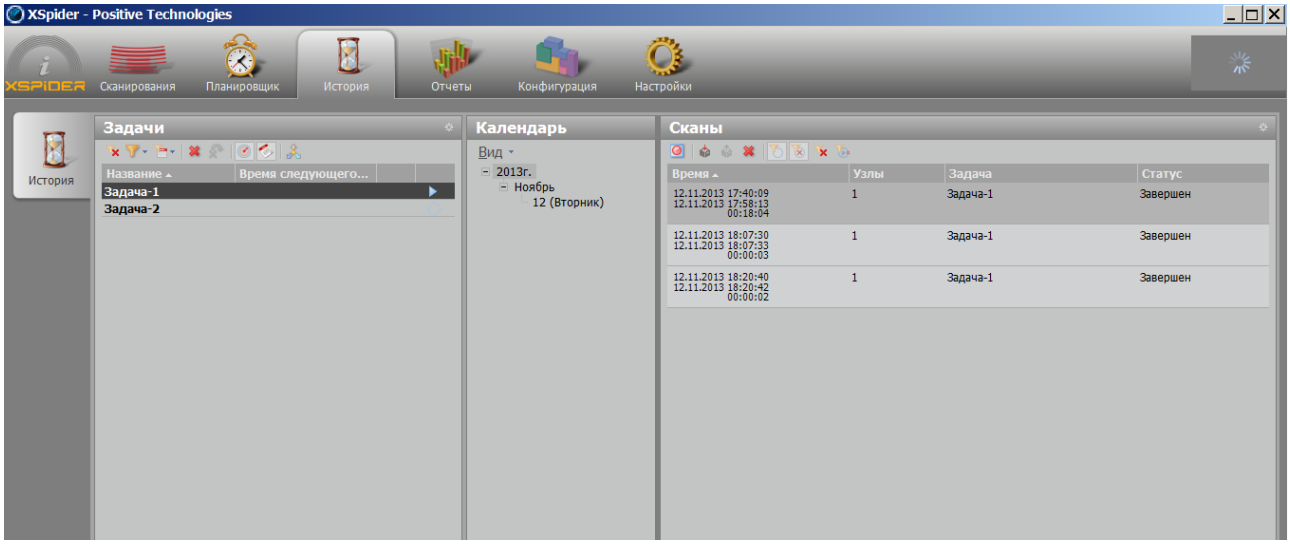

Рис. 3 – Вкладка «История» с результатами сканирования

Существует возможность сформировать отчет по текущему скану непосредственно из вкладки История. Для этого на выбранном скане необходимо щелкнуть правой кнопкой мыши и указать в контекстном меню пункт «Отчеты».

После генерации отчета отобразится диалоговое окно, позволяющее просмотреть или доставить отчет.

Модуль отчетов в Программе позволяет получать в структурированном виде данные о результатах сканирования одной или нескольких задач (сканов) с возможностью фильтрации и группировки, сравнивать данные различных сканирований, получать общие оценки состояния системы и строить регламентированные отчеты. Отчет позволяет получить требуемые сведения для детального анализа текущей ситуации в системе или для составления общего отчета.

Отчет строится на основании данных сканирования. Пользователь может выбрать необходимый ему тип отчета. Использование конкретного типа зависит от задач. Программа позволяет проводить сканирование и генерировать отчеты по расписанию. Системный планировщик по указанному расписанию запускает задачи, по результатам сканирования которых выпускается указанный отчет. Этот отчет можно сохранить в сетевой папке или отправить по электронной почте указанному адресату.

Программа позволяет формировать 2 типа отчетов:

– Информационный;
– Дифференциальный.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Для построения отчета используется шаблон, содержащий его (отчета) параметры. В Программе возможно использование шаблонов 2-х типов:

– Системный шаблон;
– Пользовательский шаблон.

Для формирования отчетов используется вкладка «Отчеты» (см. Рис. 4).

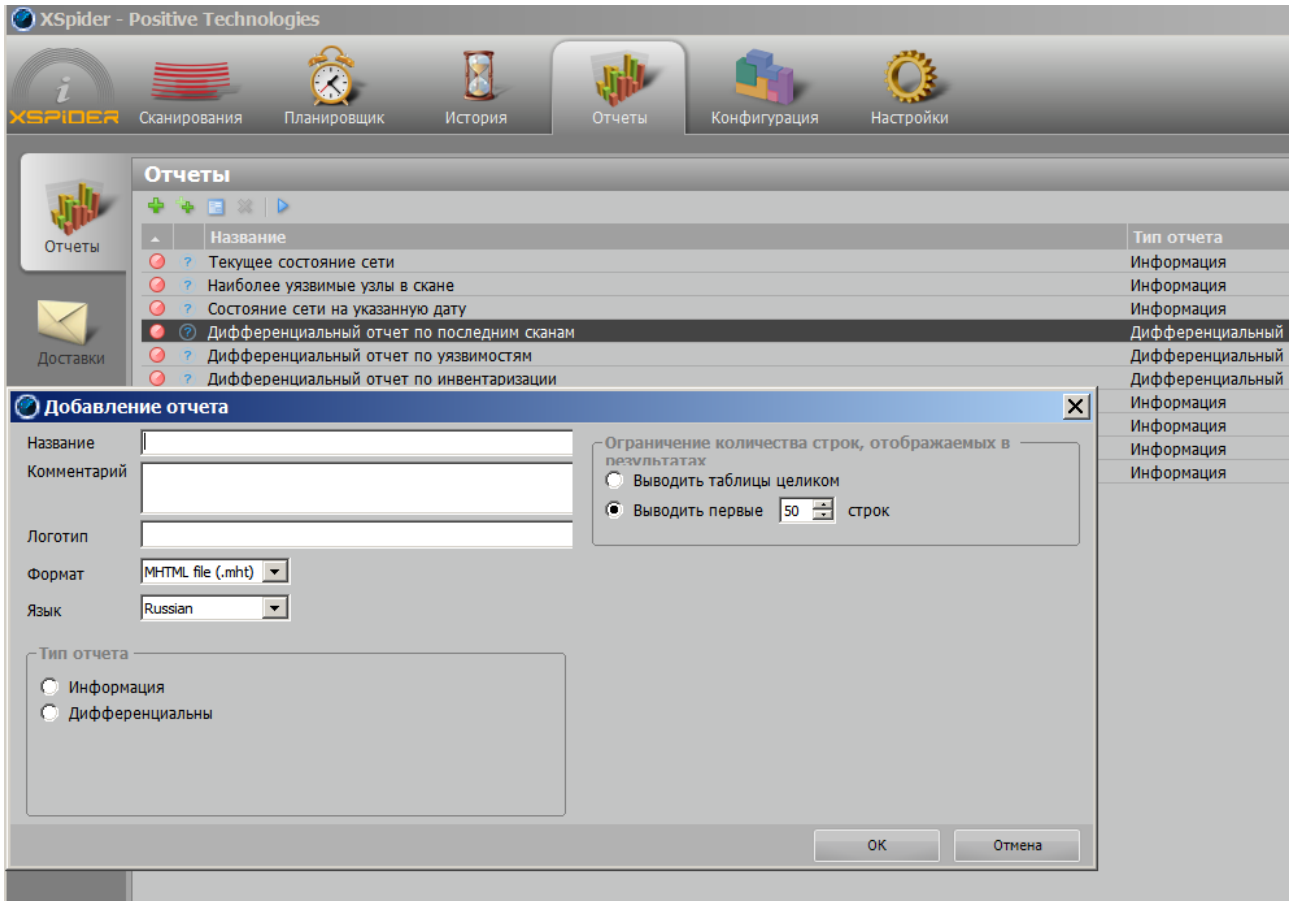

Рис. 4 – Вкладка отчеты

3.4 Разграничение доступа к функциям программы

Программа представляет собой однопользовательскую прикладную систему. Пользователь Программы работает под учетной записью «Administrator». Учетная запись Administrator имеет максимальные привилегии по отношению к Программе. Пароль администратора задается при установке Программы.

В Программе реализованы следующие собственные механизмы защиты:

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

– Авторизация пользователя. При запуске Программы пользователю предлагается ввести пароль (см. Рис. 5). В случае, если пользователь вводит верный пароль, ему предоставляется возможность работы с Программой. Если пароль введен неверно, то в допуске для работы с Программой будет отказано;

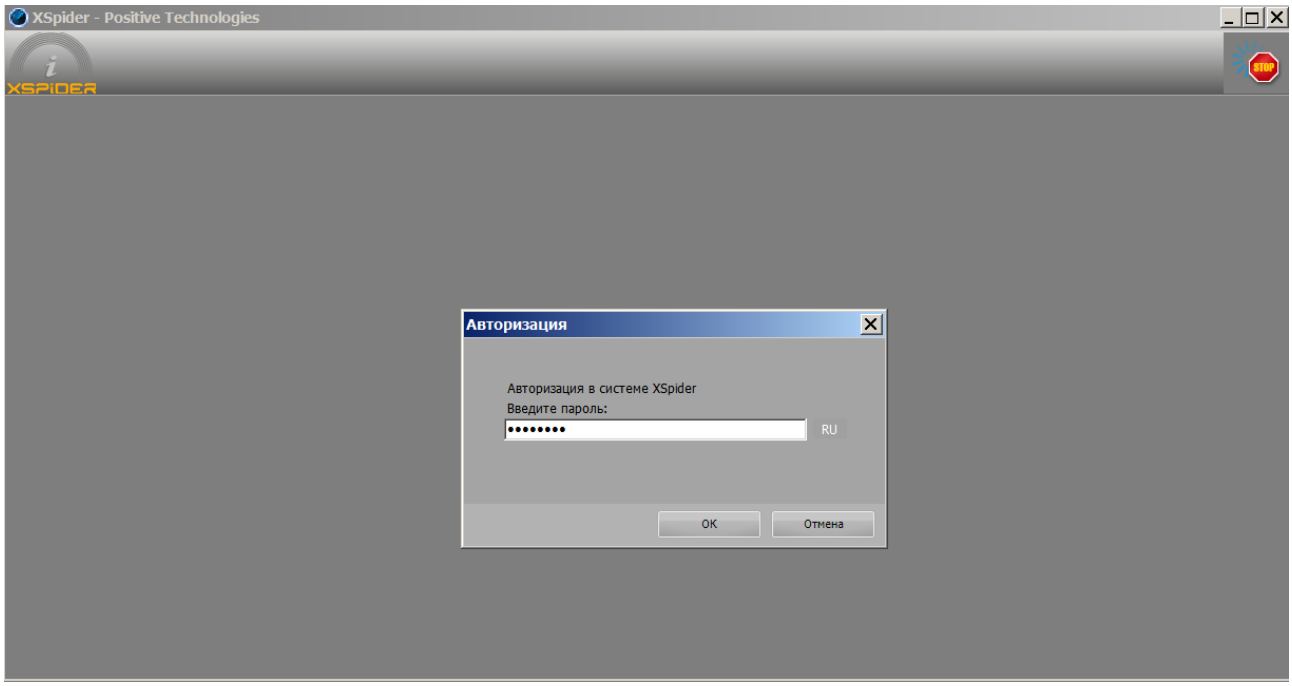

Рис. 5 – Окно авторизации пользователя

– Смена пароля пользователя. В процессе работы авторизованный пользователь может изменить пароль;

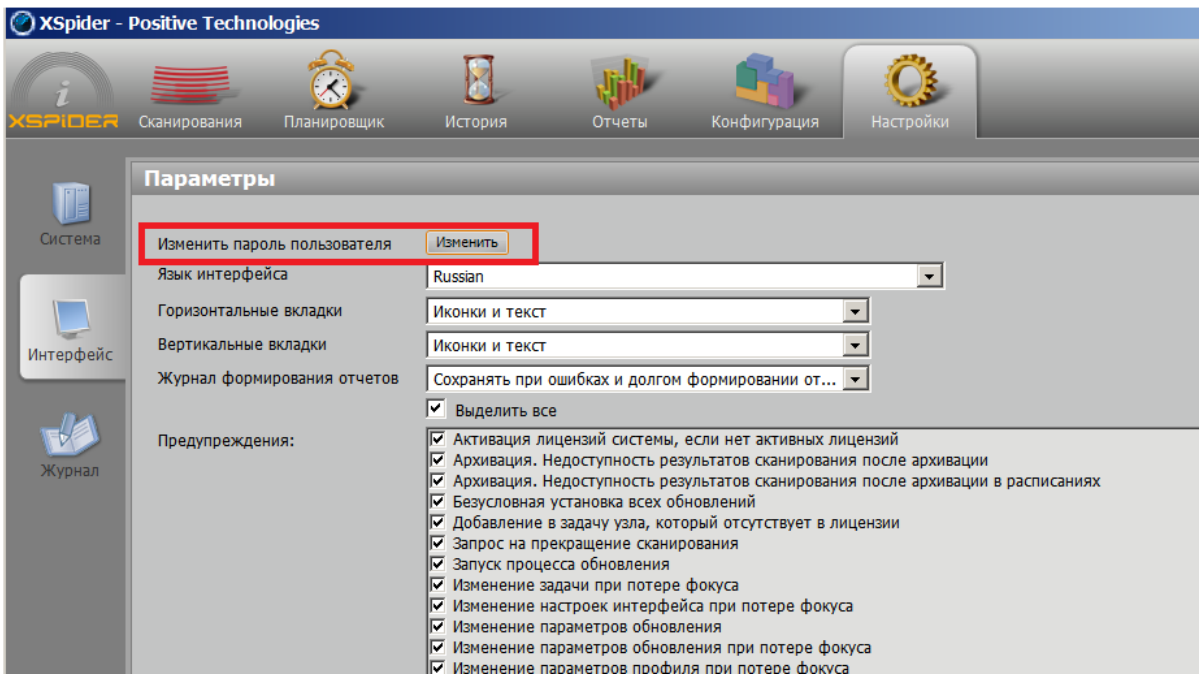

Рис. 6 – Окно смены пароля пользователя

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

– Регистрация событий. В процессе работы с Программой осуществляется регистрация событий, связанных с информационной безопасностью (см. Рис. 7).

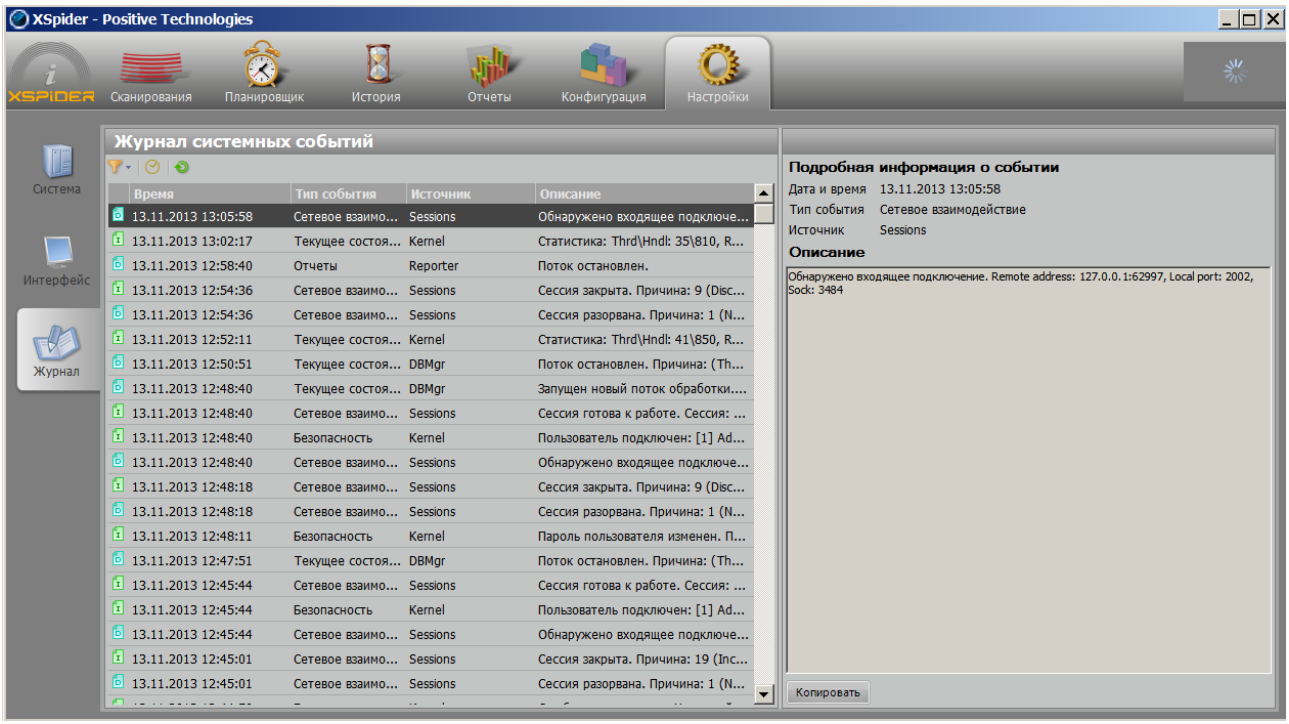

Рис. 7 – Окно «Журнал системный событий»

Более подробно работа с Программой описана в документе «Сетевой сканер безопасности XSpider. Руководство администратора», входящем в комплект поставки Программы.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1 Общие характеристики входных и выходных данных

Входными данными для работы Программы является информация вводимая пользователем с клавиатуры и с использованием манипулятора «мышь»:

– при формировании задачи на сканирование;

– при формировании отчетов.

При описании входных и выходных данных используются следующие специализированные термины:

– профиль сканирования;

– задача сканирования;

– скан;

– шаблон отчета;

– отчет.

Профили и задачи сканирования представляют собой формализованное описание проверок, выполняемых Программой при запуске процедуры сканирования. В программе предусмотрено несколько разработанных профилей сканирования. Пользователь так же имеет возможность самостоятельно разрабатывать собственные профили сканирования.

Шаблоны отчетов представляют собой файлы, содержащие параметры (формы), используемые Программной при формировании отчетов по результатам сканирования. В программе предусмотрено несколько системных шаблонов отчетов. Пользователь так же может разрабатывать собственные шаблоны отчетов.

Выходными данными Программы являются сканы и отчеты.

Скан представляет собой структурированную совокупность данных, полученных Программной в процессе сканирования.

Отчет является результатом обработки скана с использованием шаблона отчета и пользовательских настроек.

4.2 Входные данные

4.2.1 Сканирование объектов

Задача на сканирование объектов содержит имя задачи, перечень объектов сканирования и соответствующие этим объектам профили, время и периодичность запуска сканирований (для заданий, запускаемых по расписанию).

Имя задачи – произвольная, задаваемая оператором строка.

Объект сканирования – узел или группа узлов, идентифицируемых доменным именем, перечнем доменных имен, IP-адресом, перечнем или диапазоном IP-адресов.

Профиль содержит информацию о параметрах сканирования данной группы объектов, включая:

- название профиля;
- учетные записи (пары «имя-пароль»), используемые при сканировании;
- ограничения на сканирование (диапазоны сканируемых портов, время ожидания отклика от узла);
- словари для подбора паролей.

Результатом сканирования является файл с данными (скан).

4.2.2 Формирование отчетов

Входными данными для формирования отчетов являются:

- результаты сканирования (сканы) (см. раздел 4.3.1);
- шаблон отчета;
- параметры отчета.

Параметрами отчета являются:

- имя отчета;
- формат выходных данных отчета (*.mht, *.pdf, *.xml);
- язык отчета (русский, английский, корейский);
- тип отчета (см. раздел 4.3.2);
- источник исходных данных (скан, задача);
- параметры, относящиеся к отчетам данного типа.

4.3 Выходные данные

4.3.1 Результаты сканирования

Результаты сканирования (сканы) сохраняются в СУБД Программы. Ниже приведен перечень результатов сканирования, доступных пользователю через графический интерфейс Программы:

– перечень сетевых служб, предоставляемых сканируемым узлом (протокол, порт, идентификатор службы – если по результатам сканирования ее удалось идентифицировать);

– перечень выявленных уязвимостей (отдельно по каждой службе) с информацией по каждой уязвимости;

– информация об операционной системе;

– перечень идентифицированных программных средств;

– перечень выявленных уязвимостей (отдельно по каждому программному средству).

Информация о выявленных уязвимостях включает в себя:

– описание уязвимости;

– индекс уязвимости в каталоге CVE (если уязвимость присутствует в каталоге);

– оценку критичности уязвимости;

– рекомендации по устранению уязвимости;

– ссылки на публикации об уязвимости.

4.3.2 Отчеты

Программа формирует отчеты следующих типов:

– Информационный отчет;

– дифференциальный отчет.

Отчет по скану включает в себя результаты сканирования (смотри предыдущий раздел) и статистическую информацию по этим результатам (если задано в параметрах генерации отчета).

Отчет по задаче/группе задач включает в себя совокупные результаты сканирования по всем указанным в параметрах отчета задачам на указанную дату.

Дифференциальный отчет содержит:

– информацию об изменении состава узлов сети (если в задаче в качестве объекта сканирования указана группа узлов);

– информацию об изменении состава и конфигурации программных и аппаратных средств, идентифицированных в ходе сканирования узлов;

– перечень и описания устраненных, сохранившихся и появившихся уязвимостей.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм	измененных	замененных	новых	анулированных					

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения