**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Лабораторная работа № 2

по дисциплине

«Подтверждение соответствия, сертификация, анализ безопасности программного обеспечения»

на тему: «Разработка программы и методики испытаний межсетевого экрана по требованиям безопасности информации»

|  |  |  |
| --- | --- | --- |
| **Выполнил**  **обучающийся**  Курс 5  Группа КИБ-012 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | Г.Е. Груздев |
|  |  |  |
| **Проверил** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | С.В. Корниенко |

Санкт-Петербург

|  |  |
| --- | --- |
| **УТВЕРЖДЕНО** | **СОГЛАСОВАНО** |
| Генеральный директор  АО «НПО «Эшелон»  (подпись) И.И. Иванов  12.12.2024 | Глава отдела разработки  ОАО «Компания»  (подпись) П.П. Петров  12.12.2024 |

ОАО «Лаборатория ППШ»

Межсетевой экран «PfSense»

ЛИСТ УТВЕРЖДЕНИЯ

Программа и методика испытаний

643.1037804000563.001001.00001-01 51 01-ЛУ

Листов 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  | **СОГЛАСОВАНО:** | |  | Генеральный директор  ОАО «Гранит-Электрон»  (подпись) Попов А.А  12.12.2024 | |  |

Санкт-Петербург

2024

УТВЕРЖДЕНО

643.1037804000563.001001.00001-01 51 01-ЛУ

ОАО «Лаборатория ППШ»

Межсетевой экран «PfSense»

ПРОГРАММА И МЕТОДИКА ИСПЫТАНИЙ

643.1037804000563.001001.00001-01 51 01

Листов 19

Санкт-Петербург

2024

**Оглавление**

[1. Объект испытаний 4](#_Toc1809385471)

[2. Цель испытаний 5](#_Toc1838524600)

[3. Требования к программе 6](#_Toc2024946823)

[4. Требования к программной документации 9](#_Toc1331385280)

[5. Состав и порядок испытаний 10](#_Toc2047019028)

[6. Методы испытаний 13](#_Toc1576797522)

[Лист регистрации изменений 23](#_Toc1858241128)

Объект испытаний

Наименование испытуемой программы: 643.1037804000563.001001.00001 межсетевой экран PfSense.

Программный комплекс межсетевого экрана (далее ПК МЭ) PfSense предназначен для контроля информационных потоков и защиты локальной сети от внешних угроз с использованием сетевого фильтра. Фильтрация осуществляется на основе множества характеристик сетевых протоколов. Программа проводит алгоритмическую обработку и анализ данных в соответствии с заданными настройками, принимая индивидуальные решения для каждого сетевого пакета. Все операции с пакетами фиксируются в системном журнале, расположенном в **/var/log/filter.log**.

**Область применения испытуемой программы:**

Программный комплекс PfSense используется для обеспечения информационной безопасности в корпоративных и частных локальных сетях. Основное назначение — защита от несанкционированного доступа, сетевых атак и вредоносных действий в реальном времени. PfSense может быть эффективно применён в организациях с различными требованиями к уровню безопасности сетей, включая малый и средний бизнес, государственные учреждения и крупные корпоративные сети.

Обозначение испытуемой программы: 643.1037804000563. 001001.00001

Цель испытаний

Целью сертификационных испытаний является определение соответствия программного изделия требованиям для межсетевого экрана (МЭ) по 4 классу защищенности, изложенным в руководящем документе ФСТЭК «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» от 25 июля 1997 года.

Требования к программе

Для межсетевого экрана должны быть реализованы следующие функциональные возможности:

* межсетевое экранирование — пакетная фильтрация сетевого трафика до 4-го уровня модели OSI включительно;

**- IP-фильтрация:** фильтрация на основе IP-адресов, сетевых масок, источников и получателей.

**- TCP/UDP-портовая фильтрация:** контроль доступа к определенным портам на основе TCP и UDP.

**- ICMP:** управление доступом к ICMP-пакетам для ограничения работы сетевых утилит вроде ping.

**- IPv4/IPv6:** поддержка обоих версий IP протокола для совместимости с различными сетями.

* контроль приложений — определение используемых приложений независимо от используемого сетевого порта;

**- DPI (Deep Packet Inspection):** глубокий анализ пакетов для идентификации приложений вне зависимости от порта.

**- Протоколы уровня приложения:** такие как HTTP, HTTPS, DNS, FTP, SMTP, POP3 и другие, для более точной фильтрации на основе типов приложений и служб.

**- Application Layer Gateways (ALG):** позволяет межсетевому экрану "понимать" специфичные для приложений протоколы, такие как SIP или FTP, что упрощает их контроль.

* контентная фильтрация — анализ посещаемых пользователем интернет-страниц (URL) с целью предотвращения доступа к запрещенным или вредоносным ресурсам;

- **URL-фильтрация:** контроль доступа к веб-ресурсам с использованием баз данных запрещённых сайтов (URL Blacklist).

**- HTTP/HTTPS фильтрация:** анализ заголовков и содержимого запросов в HTTP и HTTPS для предотвращения доступа к нежелательным сайтам.

**- SNI (Server Name Indication) фильтрация:** позволяет блокировать сайты на основе имени сервера, даже если соединение зашифровано

* анализ сетевого трафика на предмет вторжений — сигнатурный анализ сетевого трафика с целью обнаружения активности вредоносов или попыток эксплуатации уязвимостей программного обеспечения;

**- IDS/IPS системы:** использует сигнатурный и аномальный анализ для выявления угроз, таких как Snort или Suricata.

**- Сигнатуры и базы данных угроз:** база данных известных сигнатур атак, таких как SQL-инъекции, DDoS, brute force, и других типов атак.

**- Протоколы уровня приложения и транспортного уровня:** контроль специфических протоколов (HTTP, FTP, DNS) для обнаружения и предотвращения попыток эксплуатации уязвимостей.

* аутентификация пользователей — аутентификация пользователей при сетевом доступе в интернет;

**- LDAP (Lightweight Directory Access Protocol):** для интеграции с корпоративными базами пользователей.

**- Kerberos:** безопасный протокол аутентификации, часто используемый в корпоративных сетях.

**- SAML/OAuth/OpenID Connect:** для реализации единого входа (SSO) и аутентификации пользователей.

* антивирусная проверка передаваемых файлов — сигнатурный анализ передаваемых файлов на предмет вредоносных программ;

**- HTTP/HTTPS/FTP сканирование:** проверка загружаемых файлов при помощи прокси и DPI для обнаружения вредоносного кода.

**- Сигнатурные антивирусные движки:** использование известных сигнатур вирусов для анализа содержимого файлов (например, ClamAV, Kaspersky).

**- ICAP (Internet Content Adaptation Protocol):** протокол, который позволяет интеграцию межсетевого экрана с антивирусными системами для сканирования контент

* встроенный почтовый сервер — сконфигурированный и настроенный корпоративный почтовый сервер;

**- SMTP (Simple Mail Transfer Protocol):** для отправки электронной почты.

**- POP3/IMAP:** для получения и управления электронной почтой.

**- SPF, DKIM, DMARC:** для защиты от спама и фальсификации исходных адресов.

**- Антивирусная и антиспам проверка:** фильтрация писем на наличие спама и вредоносных вложений.

* встроенный VPN-сервер — обеспечение возможности подключения удаленных пользователей к корпоративной сети.

**- IPSec (Internet Protocol Security):** защищенный протокол для туннелирования данных между удалёнными узлами.

**- SSL/TLS VPN (Secure Sockets Layer/Transport Layer Security):** шифрование для защиты данных на уровне транспортного слоя.

**- L2TP (Layer 2 Tunneling Protocol) с IPSec:** для туннелирования на втором уровне с дополнительной защитой IPSec.

**- OpenVPN:** широко используемый VPN-протокол с поддержкой SSL/TLS для шифрования трафика.

Требования к программной документации

Состав программной документации должен включать в себя:

1. Руководство администратора МЭ:

* Межсетевой экран PfSense. Руководство администратора 643.1037804000563.001001.00001-01 91 01.

2. Тестовая документация:

* Межсетевой экран PfSense. Программа и методика испытаний по передаче в опытную эксплуатацию МЭ PfSense 643.1037804000563.001001.00001-01 51 02.
* Межсетевой экран PfSense. Протокол тестовых испытаний 643.1037804000563.001001.00001-01 92 02.

3. Конструкторская документация:

* Техническое задание на разработку СЗИ PfSense 643.1037804000563.001001.00001-01 90 01.

Состав и порядок испытаний

Место проведения испытаний: АО «Лаборатория ППШ»

(Российская Федерация, Санкт-Петербург, наб. реки Смоленки, 25Е, телефон 8 (812) 555-5555).

Период проведения испытаний: с 12.11.2024 по 13.12.2024.

**5.1 Технические и программные средства, используемые во время испытаний**

Для проведения испытаний необходимо собрать стенд (рис.1), имитирующий 2 сегмента сети (внешний и внутренний).

В состав внутреннего сегмента сети входят:

• 2 пользовательских узла (компьютер 1 и 2);

• Коммутатор (Switch);

• Узел администратора (компьютер 3) с установленным МЭ.

В состав внешнего сегмента сети входит:

• Компьютер 4;

• Маршрутизатор (Router).

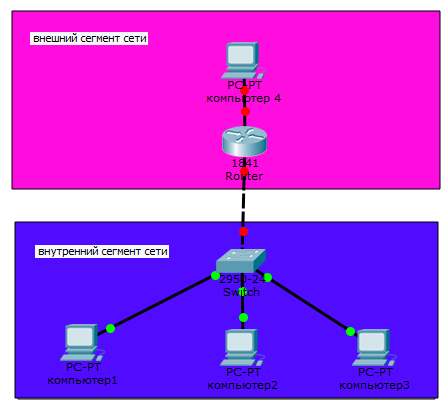


Рисунок 1 - Структурная схема стенда

Требования к техническим характеристикам рабочих станций:

**Для компьютеров 1, 2, 4:**

- процессор: AMD Ryzen 5 3500 OEM, 6 x 3.6 ГГц

- оперативная память: Kingston FURY Beast Black

- SATA накопитель: 240 ГБ 2.5" SATA накопитель ADATA SU650

- Сетевая карта TP-Link TG-3468

- Материнская плата MSI PRO H610M-E DDR4

**Для компьютера 3 (сервера):**

- процессор: Intel Xeon Silver 4214 OEM, 12 x 2.2 ГГц

- оперативная память: Kingston FURY Beast Black

- SATA накопитель: 960 ГБ 2.5" SATA накопитель Kingston A400

- Сетевая карта TP-Link TG-3468

- Материнская плата Supermicro X12DPL-i6 ATX LGA 4189

**Маршрутизатор (Router):**

- модель MikroTik hEX PoE

**Коммутатор (Switch):**

- модель MikroTik hEX S RB760iGS

**5.2 Программные средства, используемые во время испытаний**

Для проведения испытаний необходимо установить:

* На пользовательские узлы – систему Windows 10.
* На сервер – межсетевой экран;
* Для генерации пакетов – утилиты ping, curl, nmap, snmpwalk, sshd на внешний узел.
* Для анализа трафика – программу tcpdump на сервер.

**5.3 Порядок проведения испытаний**

1. Испытания управления доступом;

2. Испытания процесса регистрации;

3. Испытания процесса администрирования: идентификация и аутентификация;

4. Испытания процесса администрирования: регистрация;

5. Испытания процесса контроля за целостностью;

6. Испытания процедуры восстановления;

7. Испытания регламентного тестирования;

8. Проверка руководства администратора безопасности;

9. Проверка тестовой документации;

10. Проверка конструкторской документации;

Методы испытаний

**1) Управление доступом**

* ПК МЭ PfSense должен обеспечивать фильтрацию на сетевом уровне: решение по фильтрации может приниматься независимо для каждого сетевого пакета на основе, по крайней мере, сетевых адресов отправителя и получателя, или на основе других эквивалентных атрибутов.
* ПК МЭ PfSense должен обеспечивать фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.
* ПК МЭ PfSense должен обеспечивать фильтрацию с учетом входного и выходного сетевого интерфейса посредством проверки подлинности сетевых адресов.
* ПК МЭ PfSense должен обеспечивать фильтрацию с учетом любых значимых полей сетевых пакетов.

Для проверки фильтрации на различных уровнях должна быть проведена проверка фильтрации основных протоколов:

* Сетевого уровня: IPv4/IPv6, ICMP
* Транспортного уровня: TCP, UDP
* Прикладного уровня: HTTP, SNMP

Проверка проводится с помощью последовательной генерации пакетов, указанных выше протоколов и отправкой их с компьютера 4 с помощью утилиты Scapy во внутренний сегмент сети (компьютеры 1, 2, 3) при предварительной настройке запрета трафика с данного удаленного узла (пакеты не должны проходить в сеть) и при разрешении трафика с данного узла (пакеты должны свободно доходить до адресатов).

Порядок проведения:

1. Перейти в Firewall -> Rules
2. Настроить правила для:

* Разрешения и блокировки трафика по IP-адресам.
* Фильтрации трафика служебных протоколов ICMP, SNMP.
* Проверки значимых полей сетевых пакетов (портов, флагов TCP и т.д.).

1. Проверить проходят ли пакеты от внешнего узла к вунтренним.
2. Включить правила фильтрации.
3. С помощью утилит ping (для ICMP), snmpwalk (для SNMP), nmap (для TCP сегментов с флагами SYN и ACK), curl (для HTTP и IP запросов).

Результат испытания считается положительным, если пакеты с разрешёнными параметрами успешно прошли фильтрацию, а пакеты с запрещёнными параметрами были заблокированы.

**2) Регистрация**

ПК МЭ PfSense должен обеспечивать возможность регистрации и учета фильтруемых пакетов, при этом в параметры регистрации должны включаться адрес, время и результат фильтрации (пакет заблокирован, разрешен или перенаправлен (NAT)).

Проверка проводится с помощью просмотра результатов фильтрации пакетов из испытания прошлого пункта, то есть просмотра журнала фильтрации, который в веб-интерфейсе расположен во вкладке Firewall (Status -> System Logs -> Firewall). На самой машине с межсетевым экраном результаты фильтрации записываются в файл /var/log/filter.log.

Порядок проведения испытания:

1. Включить опцию “Log packets that are handled by this rule” для каждого правила, созданного для испытания управления доступом.
2. Включить tcpdump для прослушивания порта сервера, на который приходя пакеты
3. Провести испытания управления доступом.
4. Открыть логи в Status -> System Logs -> Firewall и сверить с выводом tcpdump

Результат испытания считать положительным, если система не пропускает пакеты без логирования и регистрирует их с минимальной задержкой.

**3) Администрирование: идентификация и аутентификация**

Проверить корректность работы функции идентификации и аутентификации администратора межсетевого экрана PfSense при локальном доступе, включая запрос учётных данных (логина и пароля) и повторный запрос пароля при изменении настроек.

ПК МЭ PfSense должен обеспечивать возможность идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.

Порядок проведения испытания:

1. Идентификация и аутентификация при запуске

1.1 Открыть веб-интерфейс PfSense (например, через браузер по адресу http://<IP-адрес PfSense>).

1.2 Убедиться, что система запрашивает ввод логина и пароля администратора.

1.3 Ввести правильные учётные данные. Убедиться, что система выдала доступ к интерфейсу.

1.4 Выйти из системы (Logout).

1.5 Попробовать ввести неверные учётные данные. Убедиться, что система не выдала доступ к интерфейсу.

1. Повторная аутентификация при изменении параметров

2.1 Войти в веб-интерфейс с учётными данными администратора.

2.2 Перейти в раздел настройки System -> General Setup.

2.3 Попробовать изменить любой из параметров (например, настройки DNS).

2.4 Убедиться, что система запрашивает повторный ввод пароля администратора.

1. Локальный доступ через терминал

3.1 Подключиться к PfSense через локальную консоль.

3.2 Убедиться, что система запрашивает ввод логина и пароля администратора.

1. Ограничение доступа после неудачных попыток

4.1 Ввести неправильный логин или пароль несколько раз подряд (5 попыток).

4.2 Убедиться, что система временно блокирует доступ.

1. Изменение учётных данных

5.1 В веб-интерфейсе перейти в раздел System -> User Manager.

5.2 Попробовать изменить пароль администратора. Убедиться, что система запрашивает текущий пароль перед применением изменений.

Результат испытания считать положительным, если при запуске программы требуется ввод учётных данных администратора (логина и пароля), а также при изменении настроек параметров программы система требует повторный ввод пароля администратора.

**4) Администрирование: регистрация**

ПК МЭ PfSense должен обеспечивать регистрацию входа (выхода) администратора ПК МЭ PfSense, либо загрузки и инициализации системы и ее программного останова. Регистрация выхода не проводится в моменты аппаратурного отключения ПК МЭ PfSense;

В параметрах регистрации должны указываться:

* дата, время и код регистрируемого события;
* результат попытки осуществления регистрируемого события - успешная или неуспешная;
* идентификатор администратора ПК МЭ PfSense, предъявленный при попытке осуществления регистрируемого события.

ПК МЭ PfSense должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).

Порядок проведения испытания:

1. Регистрация входа и выхода администратора

1.1 Войти в веб-интерфейс с использованием учётных данных администратора.

1.2 Выйти из системы (Logout).

1.3 Войти в систему.

1.4 Перейти в раздел Status → System Logs → General и выбрать вкладку Authentication. Убедиться, что появились записи о входе и выходе администратора с датой и временем события, статусом (успешно/неуспешно) и логином (идентификатором) администратора.

1. Регистрация запуска и завершения системы

2.1 Перезагрузить PfSense через веб-интерфейс (Diagnostics-> Reboot).

2.2 После перезагрузки зайти в веб-интерфейс и проверить журнал событий (System Logs -> General). Убедиться, что в журнале отображаются записи о запуске системы и её программном завершении.

1. Попытка входа с неверными данными

3.1 На экране входа ввести некорректные учётные данные (неверный логин или пароль).

3.2 Проверить журнал событий (Authentication) на наличие записи о неуспешной попытке входа. Убедиться, что записывается информация о неуспешной попытке входа с датой и временем, статусом (неуспешно) и идентификатором, введённым в качестве логина.

1. Регистрация запуска процессов

4.1 Запустить дополнительный процесс или службу через интерфейс PfSense (например, VPN-сервер или настройку файрвола).

4.2 Перейти в журнал событий (Status -> System Logs -> General) и выбрать вкладку Service. Убедиться, что отображается информация о запуске процессов с датой и временем событий, именем процесса и статусом (успешный/неуспешный запуск).

Результат испытания считать положительным, если в журнале верно отображается информация об успешных и неуспешных попытках входа администратора в систему и запусках программы или её отдельных сервисов.

**5) Целостность**

ПК МЭ PfSense должен содержать средства контроля целостности своей программной и информационной части.

Проверка производится путем проверки наличия модуля контроля целостности в составе программы, путем изучения технической документации и проверки функциональности.

Порядок проведения испытания:

1. В веб-интерфейсе PfSense перейти в меню Diagnostics → File System Check
2. Убедиться, что система предоставляет инструмент для проверки файловой системы или встроенной проверки целостности файлов/настроек.

Результат испытания считать положительным, если программа содержит модуль контроля целостности.

**6) Восстановление**

ПК МЭ PfSense должен предусматривать процедуру восстановления после сбоев и отказов оборудования, обеспечивая тем самым восстановление своих свойств.

Проверка проводится аварийным завершением работы системы с последующим её перезапуском.

Порядок проведения испытания

1. Создать резервную копию текущей конфигурации через веб-интерфейс PfSense (меню Diagnostics -> Backup/Restore).
2. Принудительно завершить работу системы (например, отключить питание устройства).
3. Подключить устройство заново и запустить PfSense. Убедиться, что после перезапуска система должна загрузиться без ошибок, сохранить основные настройки и восстановить сетевые функции.

Результат испытания считать положительным, если МЭ предусматривает процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.

**7) Тестирование**

ПК МЭ PfSense должен обеспечивать возможность регламентного тестирования:

* реализации правил фильтрации;
* процесса идентификации и аутентификации администратора ПК МЭ PfSense;
* процесса регистрации действий администратора ПК МЭ PfSense;
* процесса контроля за целостностью программной и информационной части ПК МЭ PfSense;
* процедуры восстановления;
* процесса регистрации.

Результат испытания считать положительным, если были получены успешные результаты испытаний вышеперечисленных пунктов (6.1-6.6).

**8) Руководство администратора безопасности**

Производится визуальный контроль документа.

Состав руководства администратора безопасности:

* Руководство по эксплуатации СЗИ PfSense 643.1037804000563.001001.00001-01 91 01.

Документ должен содержать:

* описание контролируемых функций ПК МЭ PfSense;
* руководство по настройке и конфигурированию ПК МЭ PfSense;
* описание старта ПК МЭ PfSense и процедур проверки правильности старта;
* руководство по процедуре восстановления.

Результат испытания считать положительным, если руководство администратора МЭ содержит вышеперечисленные пункты.

**9) Тестовая документация**

Производится визуальный контроль документов.

Состав тестовой документации:

* Межсетевой экран PfSense. Программа и методика испытаний по передаче в опытную эксплуатацию МЭ PfSense 643.1037804000563.001001.00001-01 51 02.
* Межсетевой экран PfSense. Протокол тестовых испытаний 643.1037804000563.001001.00001-01 92 02.

Результат испытания считать положительным, если тестовая документация содержит описание тестов и испытаний, которым подвергался ПК МЭ PfSense, и их результаты.

**10) Конструкторская (проектная) документация**

Производится визуальный контроль документа.

Состав конструкторской документации:

* Техническое задание на разработку СЗИ PfSense (PfSense) 643.1037804000563.001001.00001-01 90 01.

Документация должна содержать:

* общую схему ПК МЭ PfSense;
* общее описание принципов работы ПК МЭ PfSense;
* описание правил фильтрации;
* описание средств и процесса идентификации и аутентификации;
* описание средств и процесса регистрации;
* описание средств и процесса контроля за целостностью программной и информационной части ПК МЭ PfSense;
* описание процедуры восстановления свойств ПК МЭ PfSense.

Результат испытания считать положительным, если конструкторская документация содержит вышеперечисленные пункты.

**7 ИНТЕГРАЛЬНАЯ ОЦЕНКА ИСПЫТАНИЙ**

После проведения испытаний, требуется составить протокол об их проведении с указанием полученных результатов:

|  |  |
| --- | --- |
| Испытание | Результат испытания |
| Управление доступом |  |
| Реализация процесса регистрации |  |
| Реализация процесса администрирования: идентификация и аутентификация |  |
| Реализация процесса администрирования: регистрация |  |
| Реализация процесса контроля за целостностью |  |
| Реализация процедуры восстановления |  |
| Тестирование |  |
| Руководство администратора безопасности |  |
| Тестовая документация |  |
| Конструкторская документация |  |
| Итого |  |

Если по итогам проведенных испытаний все десять проверок имеют положительный результат, то исследуемый межсетевой экран соответствует требованиям руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации» – по 4 классу защищенности информации от несанкционированного доступа.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Заместитель начальника  АО «Лаборатория ППШ» | | | | |  | | | | Серов А.В. | | |
|  | Лист регистрации изменений | | | | | | | | | | |
|  | Номер листов (страниц) | | | | | Всего листов (страниц) | № докум | Входящий номер сопроводит. документа и дата | | Подпись | Дата |
|  | Изм | изменен | заменен | новых | аннулир |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | 9 | 10 |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |