УДК 004.056.5

С. П. Киргизбаев [1], В. П. Киргизбаев [1], А. А. Бутин [1]

[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

ПРИМЕНЕНИЕ СКАНЕРОВ УЯЗВИМОСТЕЙ ДЛЯ ОБНАРУЖЕНИЯ ПОТЕНЦИАЛЬНЫХ УГРОЗ ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ И АНАЛИЗА ЕЁ ЗАЩИЩЕННОСТИ

Аннотация. В статье освещается актуальная тематика информационной безопасности, связанная с использованием сканеров уязвимостей для защиты программного и аппаратного обеспечения. Анализируется проблема обнаружения более 10 тысяч уязвимостей ежегодно, которые могут привести к значительным экономическим и финансовым потерям. Подчеркивается важность внедрения сканеров уязвимостей для оперативного нахождения и исправления уязвимостей в цифровых активах организаций. Описывается принцип работы и методы, используемые сканерами уязвимостей, включая footprinting, эксплуатацию уязвимостей, сканирование конфигураций и аутентифицированные сканирования. В статье также делается сравнение зарубежных и отечественных сканеров уязвимостей, включая продукты таких компаний как Tenable (Nessus), Greenbone AG (OpenVAS), Positive Technologies (XSpider, MaxPatrol 8), Профиль Защиты (Ревизор Сети 3.0) и НПО Эшелон (Сканер-ВС). Анализируются их ключевые особенности, преимущества и недостатки. В частности, обсуждаются различные подходы к лицензированию, совместимость с операционными системами, а также специфика использования в различных типах организаций. Сделан вывод о необходимости использования сканеров уязвимостей для обеспечения безопасности корпоративных сетей и минимизации рисков, связанных с информационной безопасностью. Акцентируется внимание на том, что выбор подходящего сканера уязвимостей зависит от конкретных потребностей и возможностей организации.

Ключевые слова: информационная безопасность, сканирование уязвимостей, цифровые активы, анализ защищённости, конфигурация сети, сетевая инфраструктура, тестирование на проникновение.

S. P. Kirgizbaev [1], V. P. Kirgizbaev [1], A. A. Butin [1]

[1] *Irkutsk State Transport University, Irkutsk, Russian Federation*

APPLICATION OF VULNERABILITY SCANNERS FOR DETECTING POTENTIAL THREATS TO INFORMATION IN THE CORPORATE NETWORK AND ANALYZING ITS PROTECTION

Abstract. The article addresses the current topic of information security, related to the use of vulnerability scanners for the protection of software and hardware. It analyzes the problem of detecting more than 10,000 vulnerabilities annually, which can lead to significant economic and financial losses. The importance of implementing vulnerability scanners for the prompt finding and fixing of vulnerabilities in digital assets of organizations is emphasized. The article describes the working principle and methods used by vulnerability scanners, including footprinting, vulnerability exploitation, configuration scanning, and authenticated scans. It also compares foreign and domestic vulnerability scanners, including products from companies such as Tenable (Nessus), Greenbone AG (OpenVAS), Positive Technologies (XSpider, MaxPatrol 8), Profil Zashchity (Revisor Seti 3.0), and NPO Eshelon (Scanner-VC). Their key features, advantages, and

disadvantages are analyzed. In particular, different approaches to licensing, compatibility with operating systems, and the specifics of use in various types of organizations are discussed. The article concludes with the necessity of using vulnerability scanners to ensure the security of corporate networks and minimize risks associated with information security. It highlights that the choice of a suitable vulnerability scanner depends on the specific needs and capabilities of the organization.

Keywords: information security, vulnerability scanning, digital assets, security analysis, network configuration, network infrastructure, penetration testing.

Введение

Ежегодно специалисты по информационной безопасности обнаруживают в программном и аппаратном обеспечении более 10 тысяч уязвимостей, несвоевременное устранение которых может привести к большим экономическим и финансовым потерям. Вследствие этого компаниям важно внедрять решения, которые смогут оперативно находить уязвимости в цифровых активах организации. Одним из таких решений является сканер уязвимостей. Сканер уязвимостей (сканер безопасности, сканер защищенности) – это средство защиты, предназначенное для выявления слабых мест в приложениях, операционных системах и телекоммуникационных сетях [1]. Сканеры уязвимостей могут использоваться в законных или незаконных целях:

1) законные цели – эксперты по компьютерной безопасности применяют сканеры уязвимостей для нахождения и исправления проблем в компьютерах и телекоммуникационных системах;

2) незаконные цели – злоумышленники используют сканеры уязвимостей для нахождения слабых мест в информационной системе перед подготовкой атаки на организацию.

В настоящее время сканеры защищённости поставляются в нескольких вариантах: программа, устанавливаемая на локальный компьютер; предварительно настроенная виртуальная машина; облачное SaaS-решение (программное обеспечение как услуга).

Принцип работы сканера уязвимостей состоит из следующих этапов:

1. Пользователь вводит одну или несколько целей (доменное имя, IP-адрес или диапазон IP-адресов) для сканирования внутренней сети или внешнего периметра компании.

2. Проверка доступности целей с использованием различных протоколов ARP, ICMP, TCP.

3. Сканирование открытых TCP и UDP портов.

4. Обнаружение запущенных сетевых служб (SSH, HTTP и т.д.) на открытых портах.

5. Использование предварительно заданных учётных данных для доступа к устройствам и проверки установленных на них программ.

6. Тестирование доступных веб-приложений и построение древовидной структуры веб-сайта.

7. Генерация отчета по результатам сканирования с указанием критичности каждой уязвимости и номера из баз CVE, NVD или БДУ ФСТЭК России.

Для определения слабых мест в цифровых активах компании сканер безопасности использует следующие методы:

1. Footprinting (сетевой след) – это наиболее распространённый метод, используемый специалистами по информационной безопасности для сбора как можно большего количества данных о конкретной целевой компьютерной системе, инфраструктуре и сетях для выявления возможностей проникновения в них. Существует два основных типа сетевого следа: пассивный и активный [1]. Пассивный след – это сбор информации из общедоступных источников, таких как веб-сайты, новостные статьи и профили компаний. Активный след – это использование более интрузивных (грубых) методов для доступа к конфиденциальным данным, таких как взлом систем или применение методов социальной

инженерии. Однако этот метод подвержен ложноположительным и ложноотрицательным результатам:

1) ложноположительный результат – это ситуация, когда сканер сообщает, что есть уязвимость, но на самом деле её нет: это может привести к потере времени специалистов службы информационной безопасности, пытающихся устранить уязвимость, которой просто не существует.

2) ложноотрицательный результат – это ситуация, когда сканер сообщает, что уязвимости нет, но на самом деле она есть: если при сканировании обнаружено ноль уязвимостей, это не означает, что уязвимостей нет.

2. Эксплуатация уязвимостей. Сканер уязвимостей может использовать общедоступный эксплойт для проверки наличия уязвимости. В этом случае сканеру не нужно полагаться на версию программы, которую он проверяет, он полагается на успех или неудачу эксплойта. Эксплойт – это специально созданный код, который злоумышленники используют, чтобы воспользоваться определенной уязвимостью и скомпрометировать ресурс. Существует несколько баз данных эксплойтов, таких как Exploit-DB от компании Offensive Security (разработчик дистрибутива Kali Linux, предназначенного для тестирования на проникновение) или Metasploit Framework от компании Rapid7 (разработчик сканера уязвимостей Nexpose).

Этот метод показывает очень высокую эффективность по обнаружению уязвимостей, но в тоже время имеет два существенных недостатка. Во-первых, существуют уязвимости, для которых недоступны эксплойты. Например, разработчики Metasploit Framework зарегистрировали около 200 тысяч уязвимостей и 4 тысячи эксплойтов. Во-вторых, некоторые эксплойты могут нарушать работу проверяемого цифрового актива компании, что может привести к потере данных и остановке бизнес-процессов. Поэтому специалистам по информационной безопасности следует использовать их с осторожностью.

3. Сканирование конфигурации. Некоторые уязвимости происходят не из-за ошибок в исходном коде программы, а из-за плохой её настройки IT-специалистами. Сканеры безопасности способны обнаружить некорректные настройки, анализируя конфигурацию проверяемого оборудования организации [1]. Например, сканеры защищённости могут проверять параметры файлов cookies, настройки наборов шифров в SSL, конфигурацию передачи зоны для DNS-сервера, установленные пароли по умолчанию, ненужные открытые порты, неверные настройки удалённого доступа, оставленные включенные службы по умолчанию, некорректные параметры на межсетевом экране.

Этот метод безопасен для цифровых активов компании, так как не создаёт лишней нагрузки на корпоративную сеть, и база данных правильных конфигураций проста в обслуживании. Но проверка паролей, установленных по умолчанию, может заблокировать учётные записи после слишком большого числа попыток входа. Также существуют риски ложных срабатываний, поскольку сканер уязвимостей не всегда может знать особенности конкретной сети и, следовательно, судить о правильности конфигурации. Например, передача зоны DNS опасна в глобальной сети, но относительно безопасна в корпоративной сети компании.

4. Аутентифицированные сканирования. Большинство сканеров уязвимостей являются безагентными, то есть они не требуют установки агента на целевое устройство. Сканеры безопасности могут использовать учётные данные пользователей для проведения сканирования.

Во время аутентифицированного сканирования сканер защищённости использует модуль «локальная проверка безопасности», который состоит из проверки версий установленных программ. Например, запрос реестра Windows или запрос менеджеров пакетов apt для Debian Linux, pacman для Arch Linux, emerge для Gentoo Linux. На основе предупреждений безопасности от баз CVE, NVD или БДУ ФСТЭК России сканер может определить наличие программ с известными уязвимостями.

Важное преимущество этого метода в том, что он не ограничивается видимой поверхностью устройства из сети [1]. Действительно, компьютер с устаревшим браузером может быть легко скомпрометирован вредоносным ПО, но браузер является программой, а не службой, поэтому не передает информацию о себе через открытый сетевой порт. Таким образом, при отсутствии аутентифицированного сканирования уязвимость может остаться незамеченной сканером безопасности. Аутентифицированное сканирование является надёжным, так как при его работе нет ложных срабатываний, не вызывает нестабильности в проверяемой системе и имеет высокую скорость работы. Он может заменить методы сетевого следа и эксплуатации уязвимостей, а метод сканирование конфигурации является дополняющим методом в аутентифицированном сканировании. Но этот метод требует предоставления действительных учетных данных для каждого проверяемого устройства.

Отображение результатов сканирования и создание отчётов базируется на двух принципах. Во-первых, вывод общего списка уязвимостей с указанием затронутых цифровых активов компании. Во-вторых, указание у каждого цифрового актива компании списка найденных уязвимостей.

В информационной безопасности уязвимости классифицируются по четырём уровням опасности: критический уровень, высокий уровень, средний уровень, низкий уровень. Каждой уязвимости присваивается оценка от 0 до 10, называемая CVSS (Common Vulnerability Scoring System, общая система оценки уязвимостей), которая зависит от характеристик этой уязвимости [2]. Версия CVSS V3.1 учитывает следующие элементы:

1. Вектор атаки (AV) – эта метрика отражает степень удаленности нарушитель от атакуемого устройства.
2. Сложность атаки (AC) – эта метрика описывает сложность реализации атаки.
3. Требуемые привилегии (PR) – эта метрика показывает уровень привилегий, требуемый злоумышленнику для успешного использования уязвимости.
4. Взаимодействие с пользователем (UI) – эта метрика фиксирует требование к наличию пользователя системы для совершения злоумышленником успешной атаки.
5. Влияние на другие компоненты системы (S) – эта метрика показывает влияние уязвимости в одной цифровом активе компании на другие системы в корпоративной сети компании.
6. Влияние на конфиденциальность (C) – эта метрика измеряет влияние на конфиденциальность информации вследствие успешно использованной уязвимости злоумышленником.
7. Влияние на целостность (I) – эта метрика измеряет влияние на целостность информации вследствие успешно использованной уязвимости злоумышленником.
8. Влияние на доступность (A) – эта метрика измеряет влияние на доступность информации вследствие успешно использованной уязвимости злоумышленником.

Оценка CVSS регулярно используется сканерами уязвимостей для оценки рисков, связанных с цифровыми активами компании [2]. Сканеры безопасности формируют отчёт о работе, который включает в себя следующие элементы:

1. Название уязвимости.
2. Критичность уязвимости.
3. Уязвимый актив компании.
4. Краткое описание уязвимости.
5. Ссылка на номера из баз CVE, NVD или БДУ ФСТЭК России.
6. Степень простоты эксплуатации уязвимости.
7. Описание воздействия в случае успешной эксплуатации уязвимости.
8. Рекомендации по устранению уязвимости.

Отчеты можно экспортировать в различные форматы, например, PDF, CSV, HTML, XML.

Зарубежные решения

Для поиска уязвимостей в цифровых активах организации на международном рынке представлены различные сканеры безопасности.

Nessus (Tenable)

В 1998 году семнадцатилетний подросток Рено Дерайсон разработал первую версию сканера безопасности Nessus. Программа была с открытым исходным кодом и распространялась бесплатно [3]. В 2002 году Рено стал соучредителем и главным техническим директором компании Tenable Network Security, Inc. 5 октября 2005 года с выпуском Nessus 3 проект был изменен с общедоступной лицензии GNU GPL на проприетарную лицензию (исходный код программы стал закрытым).

В современном мире специалистам информационной безопасности трудно уследить за появлением новых и неизвестных угроз цифровым активам компании. Поэтому сотрудникам службы информационной безопасности нужен простой и быстрый способ упреждающего поиска уязвимостей. Nessus от компании Tenable – это самое надежное решение в отрасли для оценки уязвимостей, разработанное специалистами-практиками в области безопасности. Nessus создан с глубоким пониманием того, как работают специалисты по безопасности. Каждая функция Nessus делает оценку уязвимости простой, легкой и интуитивно понятной.

Особенности Tenable Nessus:

1. Развёртывание на любой платформе – Nessus можно развернуть на различных платформах (Windows, macOS, Linux), включая Raspberry Pi.

2. Эффективность и точность – динамически скомпилированные подключаемые модули повышают производительность и эффективность сканирования корпоративной сети компании.

3. Получение видимости поверхности атаки через Интернет – компания не может защитить то, чего не видит, поэтому она должна найти и оценить свои цифровые активы прежде, чем их найдут злоумышленники.

4. Защита облачной инфраструктуры перед развёртыванием – выявление проблем безопасности в рамках жизненного цикла разработки систем (SDLC).

5. Приоритизация наиболее важных угроз – Tenable Nessus позволяет сортировать и приоритизировать самые опасные уязвимости в цифровых активах компании.

6. Предварительно настроенные политики и шаблоны – более 450 шаблонов в Nessus помогают организации быстро обнаружить уязвимости в цифровых активах.

7. Простая генерация отчётов – Nessus позволяет гибко настраивать отчёты для удовлетворения конкретных потребностей и экспортировать их в различные форматы.

8. «Живые» результаты (Live Results) – при каждом обновлении плагина Tenable Nessus автоматически выполняет автономную оценку уязвимостям на основе истории сканирования компании.

9. Простота использования – Nessus использует интуитивно понятный интерфейс взаимодействия с пользователем.

10. Сгруппированный вид – Tenable Nessus группирует похожие проблемы или категории в списки, что упрощает исследование и определение приоритетов проблем для устранения.

Сегодня Nessus от компании Tenable пользуется доверием более десяти тысяч организаций по всему миру как один из наиболее широко используемых сканеров безопасности на планете и как золотой стандарт оценки уязвимостей [3]. Главное окно Tenable Nessus представлено на рисунке 1.

Рис. 1. Главное окно Tenable Nessus

OpenVAS (Greenbone AG, Open Source)

В 2005 году разработчики сканера уязвимостей Tenable Nessus изменили лицензию с общедоступной GNU GPL на проприетарную. В ответ на прекращение поддержки решения с открытым исходным кодом в 2006 году было создано несколько форков (ответвлений) Nessus. Из них на 2023 год только OpenVAS от компании Greenbone AG продолжает активно развиваться [4]. OpenVAS зарегистрирован в некоммерческой организации Software in the Public Interest, Inc. (SPI) для защиты домена openvas.org. Бизнес-план Greenbone AG состоит из трех краеугольных камней:

1. Эволюция сканера уязвимостей в комплексное решение для управления уязвимостями.
2. Создание готового устройство «под ключ» для корпоративных клиентов.
3. Продолжение разработки сканера с открытым исходного кода для создания прозрачной технологии безопасности.

В процессе разработки продукта OpenVAS Scanner было написано множество модулей, которые вместе с сканером стали называться «OpenVAS framework». В 2017 году «OpenVAS framework» получил новое название «Greenbone Vulnerability Management» (GVM), архитектура которого состоит из трех основных частей:

1. Исполняемые приложения-сканеры, запускающие тесты на уязвимости в целевых системах.
2. Служба диспетчера уязвимостей Greenbone (gvmd).
3. Помощник по безопасности Greenbone (GSA) со службой помощника по безопасности Greenbone (gsad).

Greenbone Vulnerability Manager (gvmd) – это центральная служба, которая объединяет простое сканирование уязвимостей в полноценное решение по управлению уязвимостями [5]. Диспетчер уязвимостей управляет сканером OpenVAS через протокол Open Scanner Protocol (OSP). Служба предлагает протокол без сохранения состояния Greenbone Management Protocol (GMP) основанный на XML. Диспетчер уязвимостей также управляет базой данных PostgreSQL.

Greenbone Security Assistant (GSA) – это веб-интерфейс, с помощью которого пользователь управляет сканированием и получает доступ к информации об уязвимостях. Помощник по безопасности подключается к gvmd через веб-сервер Greenbone Security Assistant Daemon для предоставления полнофункционального веб-приложения управления уязвимостями.

Главный сканер OpenVAS Scanner – это полнофункциональное ядро сканирования, которое выполняет тесты на уязвимости в целевых системах. Для этого сканер использует ежедневно обновляемые каналы: коммерческий канал Greenbone Enterprise или бесплатный

канал Greenbone Community. Сканер безопасности состоит из компонентов ospd-openvas и openvas-scanner. Сканер OpenVAS управляется через протокол OSP.

В 2022 году в Greenbone Vulnerability Management появился новый сканер Notus. Обычно сканер OpenVAS загружает каждую локальную проверку безопасности (LSC) на основе NASL (Nessus Attack Scripting Language) индивидуально и выполняет её одну за другой для каждого хоста. Затем сканер сравнивает установленное на хосте программное обеспечение с одной известной уязвимостью ПО. Это повторяется для всех LSC. Сканер Notus заменяет логику всех локальных проверок безопасности на основе NASL. Вместо запуска сценария теста на уязвимость для каждого LSC выполняется сравнение установленного на хосте программного обеспечения со списком известного уязвимого ПО. Главное окно Greenbone AG OpenVAS представлено на рисунке 2.

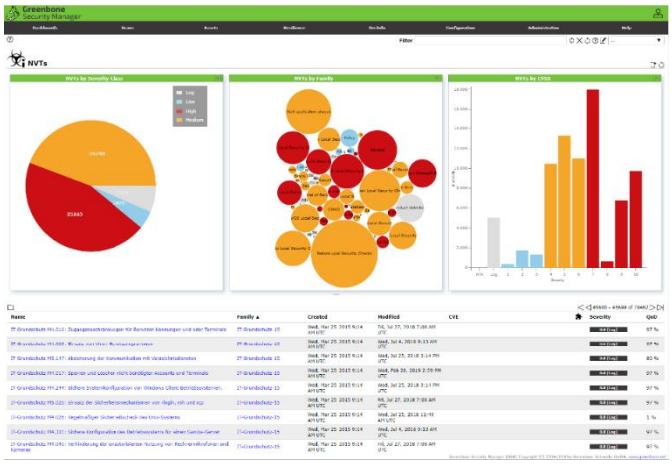

Рис. 2. Главное окно Greenbone AG OpenVAS

Отечественные решения

Для сканирования цифровых активов компании на российском рынке представлены различные сканеры уязвимостей.

XSpider (Positive Technologies)

В 1998 году программист Дмитрий Максимов разработал несколько утилит для сканирования корпоративной сети и на их основе создал сканер уязвимостей XSpider. Программа была выложена в отрытый доступ и распространялась бесплатно [6]. В течение первого года было произведено полмиллиона скачиваний XSpider, и программа получила большое число положительных отзывов в сети Интернет. В 2002 году, после создания Дмитрием Максимовым и Евгением Киреевым компании Positive Technologies, началась разработка коммерческой версии сканера уязвимостей XSpider. В 2008 году компания прекратила разработку XSpider, и на его основе была создана система контроля защищенности и соответствия стандартам MaxPatrol. Но в 2011 году на основе MaxPatrol была выпущена новая версия XSpider. На 2023 год Positive Technologies предлагает три продукта для поиска уязвимостей в корпоративной сети компании: XSpider, MaxPatrol 8 и MaxPatrol VM.

XSpider – это программный продукт, предназначенный для удалённого сканирования сети и поиска уязвимостей на серверах, рабочих станциях, сетевом оборудовании. На проверяемые хосты не требуется устанавливать дополнительное программное обеспечение [7]. Продукт XSpider имеет сертификат ФСТЭК России №3247 от 24 октября 2014 года, действительный до 24 октября 2025 года, который позволяет применять продукт для сканирования на уязвимости в государственных информационных системах, информационных системах персональных данных, значимых объектов критической информационной инфраструктуры, автоматизированных системам управления технологическим процессом; сертификат МО РФ №2910 от 25 августа 2015 года, который позволяет применять продукт для сканирования на уязвимости в сетях Министерства

обороны РФ. XSpider входит в реестр отечественного программного обеспечения (запись в реестре №786 от 16.05.2016). Ключевыми достоинствами сканера XSpider являются:

1) наглядный и удобной многооконный графический интерфейс;
2) низкие требования к оборудованию;
3) широкое покрытие программного обеспечения и операционных систем;
4) сканирование по расписанию без вмешательства специалиста;
5) выявление уязвимости для системного и прикладного программного обеспечения;
6) проведение анализ web-приложений;
7) применение эвристического алгоритм анализа, который способен выявлять ещё не опубликованные уязвимости;
8) выведение чётких рекомендаций по устранению обнаруженных уязвимостей;
9) низкий уровень ложного срабатывания;
10) формирование отчётов с различными уровнями детализации;
11) хранение всех результатов сканирования.

Продукт XSpider лицензируется по числу IP-адресов (минимум 4 IP-адреса). Срок действия лицензии составляет один год и стоимость её продления равна 40% от первоначальной стоимости. Лицензию можно продлить только в течение года после окончания её срока действия. Главное окно XSpider от компании Positive Technologies представлено на рисунке 3.

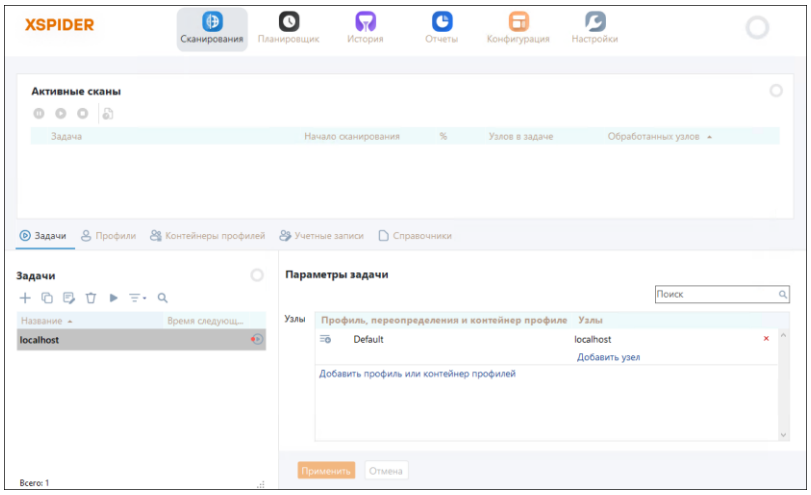

Рис.3. Главное окно XSpider от компании Positive Technologies

MaxPatrol 8 (Positive Technologies)

В 2008 году компания Positive Technologies на основе сканера уязвимостей XSpider создала продукт для комплексного анализа сетевой инфраструктуры компании MaxPatrol 8. Данный продукт удовлетворяет потребности крупных организаций, имеющих большую и распределённую корпоративную сеть [8]. Комплексная защита достигается путем установки сканеров в различных сегментах сети, и консолидации полученных данных об уязвимостях в центральном офисе предприятия. Также MaxPatrol 8 позволяет автоматически сравнивать результаты сканирований, выполненных в различное время.

Продукт MaxPatrol 8 имеет сертификат ФСТЭК России № 2922 от 8 июля 2013 года, действительный до 8 июля 2024 года, который позволяет применять продукт для контроля защищенности в государственных информационных системах, информационных системах персональных данных, значимых объектов критической информационной инфраструктуры, автоматизированных системам управления технологическим процессом, информационных системах общего пользования; сертификат МО РФ № 2635 от 21 августа 2014 года, который позволяет применять продукт для сканирования на уязвимости в сетях Министерства обороны РФ; сертификат на соответствие Общим критериям безопасности информационных технологий (Common Criteria) v.3.1 № BSI-DSZ-CC-0931-2015 от 29

августа 2015 года. MaxPatrol 8 входит в реестр отечественного программного обеспечения (запись в реестре №785 от 16.05.2016) и обеспечивает соответствие требованиям стандарта Payment Card Industry Data Security Standard (PCI DSS).

Продукт MaxPatrol 8 состоит из трёх модулей:

1. Модуль Pentest – режим тестирования на проникновение. Он позволяет реализовать инвентаризацию всех цифровых активов, «баннерные» проверки (проверки по заголовкам), фаззинг (передача на вход программы неправильных данных), подбор учетных записей. Также в MaxPatrol 8 проводит анализ защищенности веб-приложений и систем управления базами данных (СУБД).

2. Модуль Audit – режим системного сканирования. Он позволяет выявить уязвимости и ошибки конфигурации в операционных системах, службах, СУБД, прикладных системах, средствах защиты информации и контролировать установку актуальных обновлений.

3. Модуль Compliance – режим контроля соответствия стандартам. Он позволяет проверять выполнение требований российского законодательства, международных стандартов и корпоративных регламентов.

Архитектура MaxPatrol 8 от компании Positive Technologies состоит из ядра системы MP Server, сканера MP Scanner, сервера консолидации MaxPatrol Consolidation Server и локального сервера обновлений MaxPatrol Local Update Server (LUS) [9]. MP Server регулирует конфигурацию системы и её настройку. MP Scanner сканирует, собирает и обрабатывает данные.

В MaxPatrol 8 содержится большая и непрерывно обновляемая база уязвимостей. Эксперты Positive Technologies регулярно пополняют её данными из исследований угроз и способов их обнаружения. Так можно проверить, насколько IT-системы компании соответствуют общепринятым политикам безопасности. Требования могут быть как простые, например, к длине пароли, так и более сложные, например, к настройкам программного обеспечения. Пользователь может использовать готовые политики безопасности или с учётом особенностей компания задавать собственные. Главное окно MaxPatrol 8 от компании Positive Technologies представлено на рисунке 4.

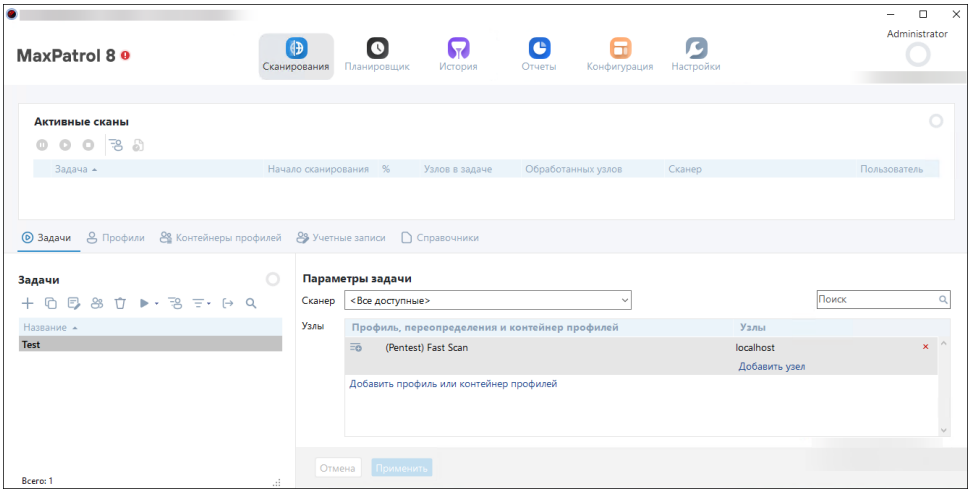

Рис. 4. Главное окно MaxPatrol 8 от компании Positive Technologies

Ревизор Сети 3.0 (Профиль Защиты)

Сетевой сканер «Ревизор Сети» версия 3.0 от компании Профиль Защиты – это система анализа защищённости программного и аппаратного обеспечения TCP/IP сетей. Сетевой сканер проводит тестирование сетевых устройств и операционных систем, которые используют технологии пакетной передачи информации Ethernet [10]. Сканер ищет уязвимости, которые включены в Банк данных угроз безопасности информации ФСТЭК России и которые содержатся в операционных системах Microsoft Windows и Linux. Ревизор Сети также проводит поиск уязвимостей в международных базах microsoft.com, ovaldb.altx-

soft.ru, cve.mitre.org. Для определения типов операционных систем и выявления сетевых сервисов на открытых TCP- и UDP-портах Ревизор Сети от компании Профиль Защиты использует сетевой сканер Nmap.

Продукт «Ревизор Сети» версия 3.0 имеет сертификат ФСТЭК России № 3413 от 2 июня 2015 года, действительный до 2 июня 2023 года, и срок технической поддержки, оканчивающийся 2 июня 2026 года. Данный сертификат позволяет применять сканер для контроля защищенности в государственных и муниципальных информационных системах, информационных системах персональных данных, значимых объектов критической информационной инфраструктуры, автоматизированных системам управления технологическим процессом, информационных системах общего пользования. Ревизор Сети входит в реестр отечественного программного обеспечения (запись в реестре №6729 от 09.06.2020).

Функции и возможности Ревизора Сети 3.0:

1. Продукт содержит базу уязвимостей на языке OVAL (открытый язык описания и оценки уязвимостей) для автоматической проверки наличия уязвимостей и установленных обновлений безопасности программного и аппаратного обеспечения.
2. Программа проводит одновременное тестирование нескольких узлов сети.
3. Сканер объединяет узлы сети в группы по IP-адресам.
4. Продукт сохраняет настройки пользователя для следующего сеанса.
5. Тестирование проводится в диапазоне IP-адресов, заданном оператором.
6. Проверка осуществляется только для доступных в текущий момент времени узлов сети.
7. Параметры проверок в плане проверок можно редактировать.
8. Программа отображает на гистограммах процесс выполнения плана проверок.
9. Продукт позволяет визуализировать обмен информацией между узлами сети.
10. Результаты проверок сохраняются в базе данных Ревизора Сети версии 3.0.
11. Результаты проверок можно посмотреть в виде дерева объектов.
12. Программа отображает итоговый результат своей работы для всех узлов сети.
13. Продукт формирует отчёты в формате HTML.
14. Для каждого сеанса работы сканер формирует отчёты об обнаруженных уязвимостях.

Ревизор Сети позволяет определить: доступность узлов сети различными методами, открытые TCP и UDP порты, тип операционной системы, NetBios-имя, DNS-имя [11]. Сканер позволяет проводить проверки: учетных записей, наличия общих сетевых ресурсов, уязвимостей операционных систем, неустановленных обновлений, FTP, RPC, сервисов электронной почты, сетевых сервисов, удаленного доступа к приложениям, удаленного получения прав администратора. Главное окно сканера «Ревизор Сети» версии 3.0 от компании Профиль Защиты представлено на рисунке 5.

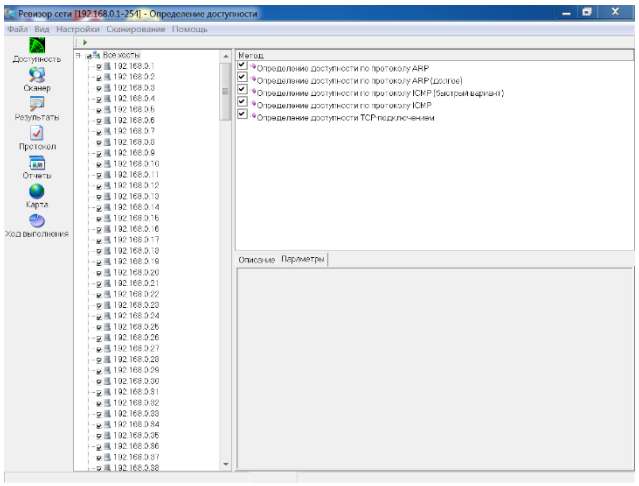

Рис. 5. Главное окно сканера «Ревизор Сети» версии 3.0 от компании Профиль Защиты

Сканер-ВС (НПО Эшелон)

В 2005 году было создано научно-производственное объединение «Эшелон», президентом которого является доктор технических наук Марков Алексей Сергеевич. НПО Эшелон разработало программный комплекс «Сканер-ВС», который позволяет провести комплексное тестирование защищённости автоматизированной системы [12]. Сканер-ВС проводит тестирование на проникновение, анализирует конфигурацию, выполняет сканирование на наличие уязвимостей и позволяет организовать постоянный мониторинг состояния защищённости IT-инфраструктуры компании.

Сканер-ВС от компании НПО Эшелон имеет сертификат Минобороны России №3872, подтверждающий выполнение требований Приказа МО РФ и действительный до 03.02.2028 года, и Сертификат ФСТЭК России №2204, действительный до 13.11.2024 года, который позволяет применять сканер для контроля защищенности в государственных и муниципальных информационных системах, информационных системах персональных данных, значимых объектов критической информационной инфраструктуры, автоматизированных системам управления технологическим процессом, информационных системах общего пользования. Сканер-ВС входит в реестр отечественного программного обеспечения (запись в реестре №231 от 18.03.2016 года).

Сканер-ВС от компании НПО Эшелон обладает особенностями:

1. Продукт содержит базу уязвимостей, обновляемую каждую неделю и совместимую с БДУ ФСТЭК России, содержащей более 50 тысяч проверок;
2. Сканер имеет понятный для пользователя интерфейс;
3. Продукт легко интегрируется с SIEM-системами;
4. Сканер-ВС работает в режиме Live USB, то есть установка продукта на компьютер необязательна;
5. Продукт включает в себя инструмент для создания отчётов по уязвимостям, по хостам и по изменения их состояния;
6. Сканер может генерировать отчёты в различных форматах PDF, CSV, DOC, HTML:
7. Продукт лицензируется по количеству одновременно сканируемых IP-адресов;
8. Лицензия продукта не привязана к конкретным IP-адресам;
9. Сканер можно применяться для проведения сертификации и аттестации;
10. Продукт совместим с отечественной операционной системой Astra Linux Special Edition;

Сканер-ВС от компании НПО Эшелон позволяет проводить инвентаризацию сетевой инфраструктуры компании. Также сканер ищет уязвимости с помощью безагентного сканирование. Сканер может проверять пароли на стойкость любого сетевого сервиса благодаря словарям распространённых паролей [13]. Сканер-ВС автоматически подбирать эксплойты на основе результатов сканирования сетевого узла. Сканер может перехватывать и анализировать сетевой трафик. Также сканер проводит аудит обновлений операционных систем Windows и настроек операционной системы Astra Linux Special Edition. Продукт может искать остаточную информацию на различных носителях и гарантированно очищать информацию. Сканер-ВС выполняет аудит уставленного на узле программного и аппаратного обеспечения. Продукт имеет возможность сравнения отчётов для поиска появившихся изменений в конфигурации сети. Также сканер может считать контрольные суммы для проверки целостности указанных файлов и папок. Главное окно продукта Сканер-ВС от компании НПО Эшелон представлено на рисунке 6.

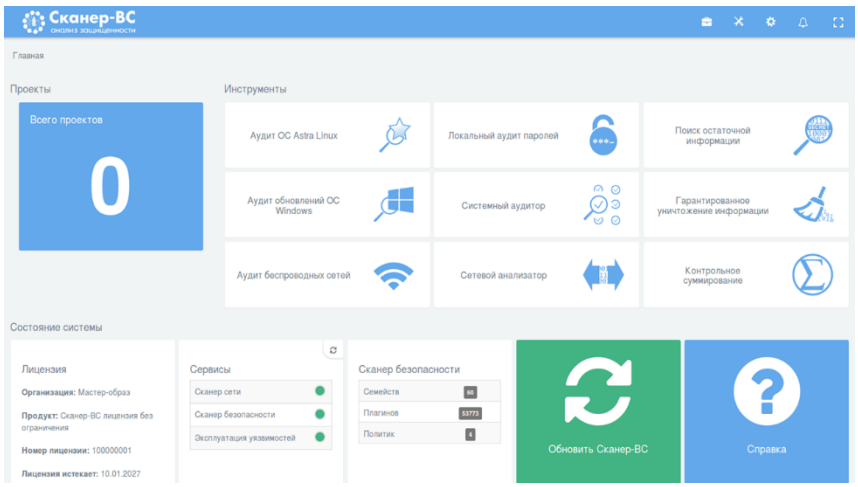

Рис. 6. Главное окно продукта Сканер-ВС от компании НПО Эшелон

Сравнение зарубежных и отечественных решений

В таблицах 1, 2 и 3 приведено сравнение сканеров уязвимостей по важным для бизнеса характеристикам [14, 15].

Таблица 1.

Сравнение сканеров уязвимостей Nessus и OpenVAS

	Nessus	OpenVAS
Масштаб компании	Любой	Любой
Количество проверяемых сетевых узлов	Нет ограничений	Нет ограничений
Лицензирование	Фиксированная цена	Бесплатно
Поддерживаемые платформы	Windows, macOS, Linux	Linux
Ценовая политика (цены указаны на годовую лицензию 2023 года)	Неограниченное число IP-адресов стоит 4375 евро (примерно 430 тысяч рублей)	Бесплатно (исходный код открыт)

Таблица 2.

Сравнение сканеров уязвимостей XSpider и MaxPatrol 8

	XSpider	MaxPatrol 8
Масштаб компании	Средний	Любой
Количество проверяемых сетевых узлов	До 10 000	Нет ограничений
Лицензирование	По числу хостов	По числу серверов
Поддерживаемые платформы	Windows	Windows
Ценовая политика (цены указаны на годовую лицензию 2023 года)	Минимум: 4 IP-адреса стоят 18 тысяч рублей Максимум: 10240 IP-адресов стоят 3 миллиона рублей	Открыто не публикуется

Таблица 3.

Сравнение сканеров уязвимостей Ревизор сети 3.0 и Сканер-ВС

	Ревизор сети 3.0	Сканер-ВС
Масштаб компании	Небольшой	Любой
Количество проверяемых сетевых узлов	До 1 000	Нет ограничений
Лицензирование	По числу хостов	По числу хостов
Поддерживаемые платформы	Windows	Дистрибутив Linux
Ценовая политика (цены указаны на годовую лицензию 2023 года)	Минимум: 5 IP-адресов стоят 8 тысяч рублей Максимум: 1000 IP-адресов стоят 140 тысяч рублей	Минимум: 4 IP-адреса стоят 6 тысяч рублей Максимум: неограниченное число IP-адресов стоят 900 тысяч рублей

Из сравнения видно, что Nessus имеет самый большой охват операционных систем. OpenVAS – это продукт с открытым исходным кодом. XSpider подходит для организаций среднего размера, а MaxPatrol 8 – для крупных предприятий. Важными недостатками решений XSpider и MaxPatrol 8 являются высокие цены на лицензию и отсутствие возможности установки на отечественные операционные системы. У Ревизор сети 3.0 также отсутствует возможность установки на отечественные операционные системы, но он имеет невысокие цены на лицензию. Сканер-ВС является дистрибутивом Linux, вследствие чего его запуск и функционирование возможен без установки на жёсткий диск.

Заключение

Авторами данной статьи был проведён глубокий и всесторонний анализ существующих сканеров уязвимостей, как отечественных, так и зарубежных, с целью оценки их эффективности в контексте информационной безопасности. Были изучены и систематизированы ключевые функциональные характеристики, методы сканирования и аспекты лицензирования каждого рассмотренного сканера. Особое внимание было уделено анализу их применимости в различных сферах бизнеса и соответствия требованиям специфических информационных систем. Результаты исследования демонстрируют, что современные сканеры уязвимостей предлагают широкий спектр возможностей для обеспечения информационной безопасности, от пассивного и активного сетевого следа, до эксплуатации уязвимостей и сканирования конфигураций. Каждый из рассмотренных сканеров обладает уникальными характеристиками, которые делают его подходящим для определенных типов задач и организаций. Сравнительный анализ зарубежных и отечественных сканеров показал, что несмотря на некоторые преимущества зарубежных продуктов в плане охвата операционных систем, отечественные решения предлагают значительную функциональность, адаптированную под специфику российских нормативных требований и стандартов. Также было выявлено, что вопрос стоимости лицензий и совместимости с отечественными операционными системами остается актуальным для многих российских продуктов. В целом, результаты исследования подчеркивают значимость выбора подходящего сканера уязвимостей в зависимости от конкретных потребностей и возможностей компании. Это позволит максимально эффективно обеспечить защиту информационных ресурсов и минимизировать потенциальные риски, связанные с информационной безопасностью.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2005. 256 с.

2. Common Vulnerability Scoring System v3.1: Specification Document [Электронный ресурс]. – Режим доступа: URL: https://www.first.org/cvss/v3.1/specification-document (дата обращения: 12.12.2023)

3. Tenable Nessus – The global gold standard in vulnerability assessment built for the modern attack surface [Электронный ресурс]. – Режим доступа: URL: https://www.tenable.com/products/nessus (дата обращения: 12.12.2023).

4. Greenbone OpenVAS [Электронный ресурс]. – Режим доступа: URL: https://openvas.org/ (дата обращения: 12.12.2023).

5. OpenVAS Background [Электронный ресурс]. – Режим доступа: URL: https://greebone.github.io/docs/latest/background.html (дата обращения: 12.12.2023).

6. XSpider – Выяви уязвимости в сетевых ресурсах до того, как это будет сделано злоумышленниками [Электронный ресурс]. – Режим доступа: URL: https://www.ptsecurity.com/ru-ru/products/xspider/ (дата обращения: 12.12.2023).

7. Краткое описание продукта XSpider [Электронный ресурс]. – Режим доступа: URL: https://www.ptsecurity.com/upload/corporate/ru-ru/products/xspider/XSpider_PB.pdf (дата обращения: 12.12.2023).

8. MaxPatrol 8 – Система контроля защищенности и соответствия стандартам [Электронный ресурс]. – Режим доступа: URL: https://www.ptsecurity.com/ru-ru/products/mp8/ (дата обращения: 12.12.2023).

9. Краткое описание продукта MaxPatrol 8 [Электронный ресурс]. – Режим доступа: URL: https://www.ptsecurity.com/upload/corporate/ru-ru/products/mp8/MaxPatrol-8_PB_09-2022.pdf (дата обращения: 12.12.2023).

10. Сетевой сканер «Ревизор Сети» версия 3.0 [Электронный ресурс]. – Режим доступа: URL: http://prp.su/products/sertifitsirovannyie-produktyi-profil-zashhityi/setevoy-skaner-revizor-seti-3-0 (дата обращения: 12.12.2023).

11. Описание продукта «Ревизор Сети» версия 3.0 [Электронный ресурс]. – Режим доступа: URL: https://prp.su/files/support/rseti/rseti3.0_opisanie_funktsionalnih_harakteristik.pdf (дата обращения: 12.12.2023).

12. Сканер-ВС – анализ защищённости [Электронный ресурс]. – Режим доступа: URL: https://scaner-vs.ru/ (дата обращения: 12.12.2023).

13. Сканер-ВС [Электронный ресурс]. – Режим доступа: URL: https://npo-echelon.ru/production/65/4291 (дата обращения: 12.12.2023).

14. Compare Nessus with industry vulnerability assessment solutions [Электронный ресурс]. – Режим доступа: URL: https://www.tenable.com/nessus/competitive-comparison (дата обращения: 12.12.2023).

15. XSpider или MaxPatrol 8 – что выбрать? [Электронный ресурс]. – Режим доступа: URL: https://www.ptsecurity.com/upload/corporate/ru-ru/products/xspider/XSpider-vs-MaxPatrol8-rus.pdf (дата обращения: 12.12.2023).

REFERENCES

1. Khorev P.B. Methods and means of protecting information in computer systems. M.: Academy, 2005. 256 p.

2. Common Vulnerability Scoring System v3.1: Specification Document [Electronic resource]. – Access mode: URL: https://www.first.org/cvss/v3.1/specification-document (date of access: 12/12/2023)

3. Tenable Nessus – The global gold standard in vulnerability assessment built for the modern attack surface [Electronic resource]. – Access mode: URL: https://www.tenable.com/products/nessus (date of access: 12/12/2023).

4. Greenbone OpenVAS [Electronic resource]. – Access mode: URL: https://openvas.org/ (date of access: 12/12/2023).

5. OpenVAS Background [Electronic resource]. – Access mode: URL: https://greebone.github.io/docs/latest/background.html (date of access: 12/12/2023).
6. XSpider – Identify vulnerabilities in network resources before it is done by attackers [Electronic resource]. – Access mode: URL: https://www.ptsecurity.com/ru-ru/products/xspider/ (date of access: 12/12/2023).
7. Brief description of the product XSpider [Electronic resource]. – Access mode: URL: https://www.ptsecurity.com/upload/corporate/ru-ru/products/xspider/XSpider_PB.pdf (date of access: 12/12/2023).
8. MaxPatrol 8 – System for monitoring security and compliance with standards [Electronic resource]. – Access mode: URL: https://www.ptsecurity.com/ru-ru/products/mp8/ (date of access: 12/12/2023).
9. Brief description of the product MaxPatrol 8 [Electronic resource]. – Access mode: URL: https://www.ptsecurity.com/upload/corporate/ru-ru/products/mp8/MaxPatrol-8_PB_09-2022.pdf (date of access: 12/12/2023).
10. Network scanner “Revizor Seti” version 3.0 [Electronic resource]. – Access mode: URL: http://prp.su/products/sertifitsirovannyie-produktyi-profil-zashhityi/setevoy-skaner-revizor-seti-3-0 (date of access: 12/12/2023).
11. Product description “Revizor Seti” version 3.0 [Electronic resource]. – Access mode: URL: https://prp.su/files/support/rseti/rseti3.0_opisanie_funktsionalnih_harakteristik.pdf (date of access: 12.12.2023).
12. Scanner-VS - security analysis [Electronic resource]. – Access mode: URL: https://scaner-vs.ru/ (date of access: 12/12/2023).
13. Scanner-VS [Electronic resource]. – Access mode: URL: https://npo-echelon.ru/production/65/4291 (date of access: 12.12.2023).
14. Compare Nessus with industry vulnerability assessment solutions [Electronic resource]. – Access mode: URL: https://www.tenable.com/nessus/competitive-comparison (date of access: 12/12/2023).
15. XSpider or MaxPatrol 8 – what to choose? [Electronic resource]. – Access mode: URL: https://www.ptsecurity.com/upload/corporate/ru-ru/products/xspider/XSpider-vs-MaxPatrol8-rus.pdf (date of access: 12/12/2023).

Информация об авторах

Станислав Павлович Киргизбаев – студент, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: s.p.kirgizbaev@gmail.com

Владислав Павлович Киргизбаев – аспирант, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: v.p.kirgizbaev@gmail.com

Александр Алексеевич Бутин – к.ф.-м.н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: butin_aa@mail.ru

Authors

Stanislav Pavlovich Kirgizbaev – student, Irkutsk State Transport University, Irkutsk, e-mail: v.p.kirgizbaev@gmail.com

Vladislav Pavlovich Kirgizbaev – post-graduate student, Irkutsk State Transport University, Irkutsk, e-mail: v.p.kirgizbaev@gmail.com

Alexander Alekseevich Butin – Cand. Sc. (Physics and Mathematics), Associate Professor of the Department of Information Systems and Information Security, Irkutsk State Transport University, Irkutsk, e-mail: butin_aa@mail.ru

Для цитирования

С. П. Киргизбаев, В. П. Киргизбаев, А. А. Бутин. Применение сканеров уязвимостей для обнаружения потенциальных угроз информации в корпоративной сети и анализа её

защищенности // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2023. – №4. – С. 17-31 – Режим доступа: https://ismm.irgups.ru/toma/420-2023, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 12.12.2023)

For citations

S. P. Kirgizbaev, V. P. Kirgizbaev, A. A. Butin. Application of vulnerability scanners for detecting potential threats to information in the corporate network and analyzing its protection // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2023. No. 4. P. 17-31. [date of access: 12/12/2023]