Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
(ФГАОУ ВО «ЮФУ»)
Инженерно-технологическая Академия
Институт компьютерных технологий и информационной безопасности
Кафедра Систем Автоматизированного Проектирования
им. В. М. Курейчика

РЕФЕРАТ №1

на тему: «Угрозы безопасности ОС и их особенности»

по дисциплине «Операционные системы»

Выполнил
студент КТбо2-4 _____ А. А. Воронов

Принял
профессор каф. САПР, к. т. н. _____ Е. В. Нужнов

Таганрог 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современные операционные системы (ОС) играют ключевую роль в информационных технологиях, обеспечивая работу как персональных устройств, так и сложных серверных инфраструктур. С развитием технологий увеличивается не только их функционал, но и количество угроз, нацеленных на нарушение работы ОС или компрометацию данных. Вопросы безопасности становятся все более актуальными, поскольку уязвимости в ОС могут привести, например, к утечке конфиденциальной информации, финансовым потерям и срыву бизнес-процессов, если речь идет об использовании ОС внутри крупных предприятий. Утечки информации могут, также, повлиять и на обыкновенного пользователя — он может стать жертвой мошенников.

Цель данного реферата — изучение основных угроз безопасности операционных систем и анализ их особенностей. В рамках работы рассматриваются классификации угроз, примеры атак, а также методы, используемые для их предотвращения. Это позволит понять, как эффективно защитить ОС от современных рисков, и выявить направления для дальнейшего улучшения технологий безопасности.

Значимость исследования обусловлена растущей зависимостью общества от цифровой инфраструктуры и необходимостью обеспечения надежной защиты данных в условиях увеличивающегося количества кибератак.

1 КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ОС

Угрозы безопасности операционной системы можно классифицировать по различным аспектам их реализации [1]:

– по цели атаки;

– по принципу воздействия на операционную систему;

– по типу используемой злоумышленником уязвимости защиты;

– по характеру воздействия на операционную систему.

Далее рассмотрим каждый вид угроз более подробно.

1.1 Классификация по цели атаки

По цели атаки угрозы безопасности ОС делятся на следующие виды:

1. Несанкционированное чтение информации;
2. Несанкционированное изменение информации;
3. Несанкционированное уничтожение информации;
4. Полное или частичное разрушение ОС [2].

1.2 Классификация по принципу взаимодействия на операционную систему

По принципу взаимодействия на ОС угрозы делят следующим образом:

1. Использование известных (легальных) каналов получения информации; например, угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно — разрешен доступ пользователю, которому согласно адекватной политике безопасности доступ должен быть запрещен;

2. Использование скрытых каналов получения информации; например, угроза использования злоумышленником недокументированных возможностей операционной системы;

3. Создание новых каналов получения информации с помощью программных закладок [2].

1.3 Классификация по типу используемой злоумышленником уязвимости защиты

В классификации угроз безопасности ОС по типу используемой уязвимости выделяют пункты:

1. Неадекватная политика безопасности, в том числе и ошибки администратора системы;

2. Ошибки и недокументированные возможности программного обеспечения операционной системы, в том числе и так называемые «люки» - случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты; обычно люки создаются разработчиками программного обеспечения для тестирования и отладки, и иногда разработчики забывают их удалить или оставляют специально;

3. Ранее внедренная программная закладка [2].

1.4 Классификация по характеру взаимодействия на ОС

1. Активное воздействие — несанкционированные действия злоумышленника в системе;

2. Пассивное воздействие — несанкционированное наблюдение злоумышленника за процессами, происходящими в системе.

2 ОСОБЕННОСТИ УГРОЗ СОВРЕМЕННЫХ ОС

2.1 Отличия в безопасности между настольными, серверными и мобильными ОС

Отличия в безопасности между настольными, серверными и мобильными операционными системами обусловлены их предназначением и архитектурой.

2.1.1 Настольные ОС (Windows, macOS, Linux)

Такие системы предназначены в основном для индивидуального использования, поэтому основной акцент идет на защиту именно личных данных пользователя, обеспечения простоты работы для него, а также на совместимость с большим количеством разных программ. Угрозами для настольных ОС являются частые атаки вредоносного ПО, фишинг и эксплойты уязвимостей ПО. С угрозами борются, например, такие технологии как Windows Defender в Windows, FileVault в macOS, SELinux в Linux [3].

2.1.2 Серверные ОС (Red Hat Enterprise Linux, Windows Server)

Созданы, чтобы управлять серверными задачами, такими как базы данных или веб-серверы. Уровень безопасности достигается за счет тщательной настройки доступа, использования систем мониторинга и шифрования данных. Частыми угрозами для серверных ОС являются DDoS-атаки, SQL-инъекции и попытки НСД — несанкционированного доступа [4].

2.1.3 Мобильные ОС (Android, iOS)

Ориентированы на работу на мобильных устройствах. Они оптимизированы для высокой энергоэффективности и защищенности пользовательских данных. Особенно много внимания уделяется безопасной работе с приложениями и шифрованию для защиты пользовательских данных. Угрозы представляются злоупотреблением привилегиями установленных приложений, кража данных и взлом через незащищенные сети.

2.2 Роль политики безопасности и администрирования

Политика безопасности операционных систем (ОС) играет ключевую роль в обеспечении защиты данных и ресурсов от различных угроз. Она включает в себя определение правил, процедур и технических решений, направленных на предотвращение несанкционированного доступа, утечек данных и вредоносного воздействия на операционную систему.

Ниже перечислены основные аспекты роли политики безопасности:

– Управление доступом. Политика безопасности регулирует права доступа пользователей и процессов к системным ресурсам. Она обеспечивает строгий контроль за доступом к файлам, сетям и приложениям.

– Минимизация уязвимостей. Внедрение политики безопасности помогает минимизировать потенциальные уязвимости. Например, помочь убрать уязвимости может регулярное обновление ОС и настройка встроенных механизмов.

– Мониторинг и аудит. Современные политики безопасности включают системы мониторинга активности и ведения статистики. Это упрощает выявление инцидентов безопасности и их расследование.

– Снижение человеческого фактора. Политики безопасности нацелены на то, чтобы пользователь научился безопасному поведению, например — использовал сложные пароли, регулярно обновлял ПО и избегал подозрительных и опасных действий в системе.

– Соответствие стандартам. Реализация эффективной политики безопасности позволяет соответствовать международным и национальным стандартам. Это может быть критично для организаций, которые работают с конфиденциальными данными [5].

Эффективная политика безопасности — это неотъемлемая часть стратегии защиты операционных систем в условиях современных угроз, включая кибератаки, вредоносное ПО и утечки данных.

3 ПРИМЕРЫ ИЗВЕСТНЫХ УГРОЗ И ИХ ПОСЛЕДСТВИЙ

3.1 Угрозы на уровне ядра ОС

Угрозы на уровне ядра операционной системы (ОС) представляют собой одни из самых серьезных рисков для информационной безопасности, так как ядро контролирует взаимодействие между оборудованием и программным обеспечением, а также управляет критически важными процессами системы. Далее рассмотрим основные угрозы и их последствия.

3.1.1 Руткиты ядра

Руткиты — это вредоносные программы, которые встраиваются в ядро ОС. Это позволяет им скрываться от стандартных средств защиты, таких как антивирусы. Руткиты могут перехватывать системные вызовы, что позволяет злоумышленникам скрывать свои действия и устанавливать полный контроль над системой. Их обезвреживание особенно сложно из-за их глубокой интеграции в системные процессы [6].

3.1.2 Эксплуатация уязвимостей ядра

Уязвимости, такие как переполнение буфера или ошибки в обработке протоколов, могут использоваться для получения привилегий администратора или выполнения произвольного кода. Например, ошибки в обработке сетевых пакетов могут позволить злоумышленнику внедрить вредоносный код на этапе обработки данных в ядре, еще до их фильтрации брандмауэром.

3.1.3 Атаки через драйверы

Атаки через драйверы представляют собой угрозу, когда злоумышленники используют уязвимости в системных или аппаратных драйверах. Путем их модификации или подмены можно получить привилегированный доступ к системе.

3.1.4 Последствия реализации угроз на уровне ядра

При реализации угроз на уровне ядра, злоумышленник получает полный контроль над системой: может читать, изменять или удалять данные, включая системные файлы. К тому же, из-за сложности обнаружения вредоносные программы на уровне ядра могут оставаться активными в системе долгое время.

3.2 Угрозы, связанные с управлением доступом

Угрозы, которые связаны с управлением доступом в операционных системах, представляют собой одну из ключевых областей риска для информационной безопасности. Управление доступом направлено на то, чтобы только авторизованные пользователи имели доступ к определенным данным и ресурсам. Нарушения в этой области могут привести к утечке конфиденциальной информации, нарушению работоспособности системы и другим негативным последствиям. Как и в прошлом подразделе, ниже рассмотрим основные виды таких угроз и их влияние на ОС [7].

3.2.1 Несанкционированный доступ

Несанкционированный доступ (НСД) возникает, когда злоумышленник получает доступ к ресурсам системы без должных прав. Это может быть результатом использования уязвимостей в механизмах аутентификации, использования слабых паролей или обхода систем защиты, таких как многофакторная аутентификация.

3.2.2 Эскалация привилегий

Эксплуатация уязвимостей в программном обеспечении может позволить пользователю с низкими привилегиями получить доступ на уровне администратора. Это дает злоумышленнику возможность изменить критически важные настройки, удалить или похитить данные, а также деактивировать защитные механизмы системы.

3.2.3 Вредоносное программное обеспечение и внутренние угрозы

Злоумышленники, имеющие доступ к учетным записям с высокими привилегиями, могут использовать их для установки вредоносных программ, удаления данных или нарушения работы системы. Внутренние угрозы также представляют проблему, так как сотрудники с законным доступом могут злоупотребить своими правами.

3.2.4 Последствия реализации угроз управления доступом

При реализации угроз управления доступом, злоумышленник может нанести ощутимый вред для системы и пользователя. Например, может произойти утечка конфиденциальной информации: персональных данных или коммерческой тайны.

3.3 Угрозы, связанные с программным обеспечением

Угрозы, связанные с программным обеспечением — это основная и самая распространенная категория рисков для операционных систем. Они связаны с уязвимостями, ошибками или преднамеренно вредоносным поведением программ, работающих на устройстве. Такие угрозы могут привести к повреждению или утечке данных и даже полному выходу системы из строя. Ниже приведены основные типы угроз на уровне ПО. Рассмотрим несколько типов таких угроз [7].

3.3.1 Уязвимости в программном обеспечении

Программные уязвимости возникают из-за ошибок в коде, недостаточной проверки входных данных или недоработок в архитектуре приложения. Злоумышленники могут использовать их для получения НСД, запуска вредоносного кода или создания отказов в обслуживании (DoS). Примером таких атак является эксплуатация уязвимостей нулевого дня, т.е. тех, которых еще не обнаружили или не исправили разработчики.

3.3.2 Вредоносное программное обеспечение (вирусы, трояны и др.)

Вредоносные программы специально разрабатываются для компрометации систем. Например, вирусы могут заражать файлы, трояны предоставляют удаленный доступ злоумышленникам, а программы-вымогатели блокируют данные до уплаты выкупа. Эти угрозы могут нанести значительный ущерб как отдельным пользователям, так и организациям.

3.3.3 Необновленное или неподдерживаемое ПО

Использование устаревших программ повышает риск атак, так как такие программы могут содержать известные, но не исправленные уязвимости. Устройства с неподдерживаемым программным обеспечением, например, с устаревшими версиями ОС, часто становятся целью атак.

3.3.4 Поддельное или ненадежное ПО

Установка программ из ненадежных источников может привести к проникновению вредоносного кода. Поддельные приложения часто используются для кражи данных или установки другого вредоносного ПО.

3.4 Злоупотребления механизмами виртуализации и контейнеризации

Последствия злоупотребления механизмами виртуализации и контейнеризации — это класс угроз безопасности операционных систем, которые связанны с использованием технологий виртуальных машин и контейнеров для изоляции приложений и сред выполнения. Эти технологии предоставляют мощные средства управления ресурсами, но также создают дополнительные направления атак. Основные типы угроз и последствия их реализации представлены далее [6].

3.4.1 Выход за пределы виртуальной среды (escape)

Злоумышленник может использовать уязвимости в гипервизоре или контейнерном движке, чтобы выйти за пределы изолированной среды и получить доступ к гостевой ОС или другим виртуальным машинам. Например, атаки на

гипервизоры Xen или VMware позволяли обойти изоляцию и получить желаемый контроль над гостевой системой.

3.4.2 Атаки на слабую изоляцию контейнеров

Контейнеры используют ядро гостевой ОС, что делает их изоляцию менее надежной по сравнению с виртуальными машинами. Если одно приложение в контейнере будет скомпрометировано, существует риск компрометации всей гостевой системы или других контейнеров.

3.4.3 Проблемы с управлением образами контейнеров

Использование ненадежных или устаревших образов может привести к внедрению вредоносного ПО. Также есть риск того, что контейнеры содержат незащищенные зависимости или открытые порты, через которые может быть выполнена атака.

3.4.4 Угрозы от привилегированных пользователей

Если злоумышленник получает доступ к гипервизору или контейнерному оркестратору с привилегиями администратора, он может управлять всеми виртуальными машинами и контейнерами, создавать или удалять их, а также использовать ресурсы гостевой системы. Неправильная настройка ограничений доступа между виртуальными машинами или контейнерами может привести к утечке данных или перегрузке ресурсов, что может негативно повлиять на производительность системы и её безопасность.

3.4.5 Последствия злоупотребления виртуализации

Последствиями злоупотребления виртуализацией и реализации связанных с ней угроз являются:

– Утечка конфиденциальных данных из изолированных сред;

– Нарушение работы систем и приложений из-за перегрузки ресурсов;

– Неавторизованный доступ к другим виртуальным машинам или контейнерам;

– Потеря контроля над гостевой ОС.

3.5 Атаки с использованием систем обновлений

Атаки через системы обновлений представляют собой серьёзную угрозу для пользователей и организаций. Злоумышленники могут заменить официальные обновления вредоносным ПО (например, атака на цепочку поставок) [8]. Такой метод позволяет внедрить вирус на устройства конечных пользователей, используя доверие к разработчику программного обеспечения.

Основные риски включают распространение вредоносных программ, кражу данных и нарушение работы IT-инфраструктуры. Примером может служить атака с использованием вируса NotPetya в 2017 году, которая парализовала работу множества компаний в восточной Европе. Этот вирус использовал уязвимость в программном обеспечении компании MEDoc для распространения, что привело к значительным финансовым потерям и остановке операций у организаций. Или еще один яркий пример — атака через обновление SolarWinds в 2020 году, когда хакеры получили доступ к системам многих крупных компаний и государственных структур, включая ведомства США. В результате десятки тысяч систем подверглись компрометации.

3.6 Целевые атаки на встроенные системы безопасности ОС

Целевые атаки направлены на обход встроенных защитных механизмов, таких как ASLR (рандомизация расположения в памяти) и DEP (предотвращение выполнения данных). Злоумышленники используют методы, позволяющие подстроить вредоносный код под особенности системы жертвы. Например, уязвимость Spectre позволила атакующим обойти защиту процессоров, выполняя побочные атаки через кеш системы. Обход ASLR и DEP делает систему подверженной кражам данных и внедрению эксплойтов [9].

4 МЕТОДЫ ЗАЩИТЫ ОТ УГРОЗ БЕЗОПАСНОСТИ ОС

4.1 Контроль доступа к операционной системе

Контроль доступа — основа информационной безопасности, обеспечивающая управление правами пользователей на взаимодействие с ресурсами системы. Реализуется через методы аутентификации и авторизации. Например, ОС Windows NT/2000/XP применяют модель контроля доступа, включающую учет пользователей, группы и объектов. Для повышения безопасности применяются многоуровневые политики, такие как DAC (Discretionary Access Control) — назначение прав владельцем объекта, и MAC (Mandatory Access Control) — обязательное распределение доступа на основе ролей и политики. Внедрение современных систем управления доступом, включая IAM (Identity and Access Management), помогает автоматизировать настройку прав доступа и предотвращает несанкционированное использование данных [10].

4.2 Обеспечение целостности системы

Целостность ОС гарантируется через контроль изменений в системных файлах и реестре, мониторинг процессов и использование технологий, таких как контроль целостности файлов (FIM). ОС UNIX и Windows поддерживают встроенные средства, проверяющие контрольные суммы данных. Программные решения, например, Tripwire, анализируют изменения в ключевых файлах, а защита через хэширование (SHA-256 и другие алгоритмы) предотвращает манипуляции. Важной составляющей является регулярное резервное копирование, позволяющее восстановить систему после сбоев или атак [10].

4.3 Применение встроенных средств защиты

Современные ОС, включая Windows и UNIX, оснащены встроенными инструментами защиты. Например, в Windows реализованы DEP (Data Execution Prevention) для предотвращения выполнения вредоносного кода и ASLR (Address

Space Layout Randomization) для защиты памяти. ОС также поддерживают средства шифрования данных (BitLocker в Windows), защиту на уровне файловой системы (NTFS) и управление резервным копированием. Использование этих технологий повышает стойкость системы к атакам и упрощает управление безопасностью. Однако, как было упомянуто ранее в подразделе 3.6, даже встроенные системы защиты не обеспечивают полную безопасность системы.

4.4 Изоляция и виртуализация

Метод изоляции предполагает использование технологий виртуализации для защиты системных ресурсов от вредоносных воздействий. Виртуализация позволяет разделить физическую систему на несколько изолированных виртуальных машин (ВМ), каждая из которых работает независимо. Это снижает вероятность распространения угроз между виртуальными машинами и физическим хостом, но как было выяснено в подразделе 3.4, тоже не приравнивает эту вероятность к нулю — риск есть всегда. Ниже представлены основные аспекты виртуализации:

– Гипервизоры обеспечивают управление ВМ, но также представляют собой потенциальную точку отказа. Использование проверенных решений и обновлений минимизирует риски взлома гипервизора;

– Изоляция сетей через VLAN и сегментацию трафика предотвращает атаки, такие как ARP-спуфинг, которые направлены на определение MAC-адресов (физических сетевых адресов) устройств по их IP-адресам;

– Контроль доступа и использование многофакторной аутентификации (MFA) обеспечивают защиту от несанкционированного доступа к ВМ и гипервизору.

4.5 Резервное копирование и аварийное восстановление

4.5.1 Резервное копирование

Резервное копирование и аварийное восстановление являются важными методами защиты операционных систем от угроз, направленных на нарушение целостности данных, кражу информации или выход оборудования из строя. Эти меры обеспечивают восстановление работоспособности системы и минимизацию потерь в случае инцидентов безопасности. Данные в резервных копиях шифруются для предотвращения несанкционированного доступа, а использование программ для автоматического резервного копирования минимизирует человеческие ошибки. Резервное копирование включает в себя несколько методов:

– Полное резервное копирование сохраняет всю информацию, обеспечивая максимальную защиту, но требует значительных ресурсов;

– Дифференциальное копирование фиксирует изменения с момента последнего полного бэкапа, снижая нагрузку на систему;

– Инкрементальное копирование сохраняет только изменения, минимизируя объем данных, но усложняет восстановление.

При копировании также важно учитывать месторасположение копий. Локальные копии обеспечивают быстрое восстановление после сбоев. Облачные копии защищают от физических повреждений оборудования, таких как пожары или затопления.

4.5.2 Аварийное восстановление

Аварийное восстановление — это комплекс мер, направленных на восстановление работы ОС после инцидентов. При восстановлении требуется определить тип повреждений и выбрать подходящий резервный образ.

Резервные копии обеспечивают защита от вредоносных программ, таких как шифровальщики, которые могут блокировать доступ к данным. Например, они позволяют восстановить информацию без уплаты выкупа. Также они могут

предотвратить потери данных в результате внутренних угроз, например, неумышленного или умышленного удаления файлов.

Резервное копирование и аварийное восстановление являются неотъемлемой частью стратегии обеспечения информационной безопасности. Регулярное выполнение этих процедур и их интеграция в комплексную систему защиты помогают минимизировать ущерб от кибератак и технологических инцидентов.

4.6 Журналирование и аудит

Журналирование обеспечивает запись событий, связанных с деятельностью системы, что позволяет выявлять аномалии и потенциальные угрозы. Этот метод охватывает ключевые аспекты, которые рассмотрены ниже.

4.6.1 Централизация логов

Сбор данных с различных систем в едином репозитории позволяет оперативно анализировать информацию и исключает необходимость поиска журналов вручную. SIEM-системы (Security Information and Event Management — решения для управления событиями информационной безопасности), такие как Splunk и ELK Stack, обрабатывают логи в режиме реального времени и уведомляют администраторов о подозрительных активностях.

4.6.2 Подробный мониторинг событий

Фиксация событий входа в систему, изменений конфигурации, неудачных попыток авторизации и других критичных действий позволяет отслеживать подозрительную активность. Автоматизированные системы уведомлений ускоряют реакцию на инциденты.

4.6.3 Аудит безопасности

Регулярные проверки журналов выявляют уязвимости, например, устаревшее ПО, слабые пароли или незащищенные порты. Результаты аудитов используют для обновления политики безопасности и устранения найденных недостатков.

4.6.4 Долгосрочное хранение логов

Хранение данных о состоянии системы (логов) обеспечивает возможность анализа прошлых событий, что полезно для расследований инцидентов и соблюдения нормативных требований. Данные хранятся в зашифрованном виде, чтобы предотвратить их утечку или компрометацию.

ЗАКЛЮЧЕНИЕ

В процессе написания реферата была проанализирована актуальная проблема угроз безопасности операционных систем и их особенностей. Установлено, что операционные системы, являясь основой работы современных цифровых устройств, подвергаются разнообразным видам угроз, начиная от вирусов и вредоносного ПО до сложных атак с использованием эксплойтов и социальной инженерии.

Была выделена классификация угроз, описаны примеры реальных атак и их последствия, а также рассмотрены подходы к защите ОС. Особое внимание уделялось необходимости использования актуальных методов безопасности, таких как регулярные обновления, строгая система управления доступом и антивирусные решения.

Проведенный анализ позволяет сделать вывод о том, что комплексный подход к безопасности операционных систем является важным условием устойчивой работы любой ИТ-инфраструктуры. Несмотря на стремительное развитие технологий, ключевым остается взаимодействие человека и системы, поскольку человеческий фактор остается одной из основных уязвимостей. Для обеспечения надежной защиты необходимо как развитие новых технологий, так и повышение осведомленности пользователей о киберугрозах и способах их предотвращения.

Таким образом, результаты исследования подчеркивают необходимость дальнейшего изучения и совершенствования методов защиты операционных систем в условиях постоянно изменяющегося ландшафта угроз.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Климов Д.А. БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ В КОРПОРАТИВНЫХ СЕТЯХ \ Климов Д.А. [Электронный ресурс] \\ Репозиторий БГУИР: [сайт]. — URL: https://libeldoc.bsuir.by/bitstream/123456789/40042/1/Klimov_Bezopasnost.pdf (дата обращения: 24.11.2024).

2. Общие вопросы обеспечения информационной безопасности \ [Электронный ресурс] \\ StudFile.net: [сайт]. — URL: https://studfile.net/preview/5163176/ (дата обращения: 24.11.2024).

3. Обзор основных видов операционных систем. — Текст : электронный \\ Geekon : [сайт]. — URL: https://geekon.media/vidy-operacionnyh-sistem-raznye-os-na-kompyuter-i-smartfon/#respond (дата обращения: 02.12.2024).

4. Какую операционную систему выбрать для сервера? — Текст : электронный \\ Cloud4box : [сайт]. — URL: https://cloud4box.com/blog/os-dlya-servera/ (дата обращения: 02.12.2024).

5. Гуз В. В. Безопасность в современных операционных системах: вызовы и решения \ В. В. Гуз. — Текст : электронный \\ Научно-издательский центр Аспект : [сайт]. — URL: https://na-journal.ru/3-2024-informacionnye-tekhnologii/10109-bezopasnost-v-sovremennyh-operacionnyh-sistemah-vyzovy-i-resheniya (дата обращения: 02.12.2024).

6. Кирилова, К. С. Проблема обезвреживания руткитов уровня ядра в системах специального назначения \ К. С. Кирилова, В. Н. Волкогонов, А. Ю. Цветков. — Текст : непосредственный \\ i-methods. — 2020. — № 3 Том 12. — С. 1-7.

7. Анализ CVE-2024-38063: удаленная эксплуатация ядра Windows. — Текст : электронный \\ Хабр : [сайт]. — URL: https://habr.com/ru/companies/bizone/articles/839302/ (дата обращения: 02.12.2024).

8. Распространенные риски в цепочке поставок программного обеспечения и способы их смягчения. — Текст : электронный \\ Scribe : [сайт]. — URL:

https://scribesecurity.com/ru/software-supply-chain-security/supply-chain-risks/#how-to-mitigate-the-risks-in-the-software-supply-chain (дата обращения: 02.12.2024).

9. Обход ASLR/DEP. — Текст : электронный \\ SecurityLab.ru : [сайт]. — URL: https://www.securitylab.ru/analytics/413398.php (дата обращения: 02.12.2024).

10. Что такое управление доступом? — Текст : электронный \\ Microsoft : [сайт]. — URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-access-control (дата обращения: 02.12.2024).