Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ   
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Архитектура вычислительных систем

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовой работе

на тему

ПРОГРАММА-ВИРУС С ИСПОЛЬЗОВАНИЕМ АППАРАТНЫХ ПРЕРЫВАНИЙ

БГУИР КП 1-40 04 01 01 003

Студент Киселёв А.В.

Руководитель Марков А.Н.

Минск 2023

СОДЕРЖАНИЕ

Определения и сокращения

Введение

1 Архитектура вычислительной системы

2 Платформа программного обеспечения

3 Теоретическое обоснование разработки программного продукта

4 Проектирование функциональных возможностей программы

5 Архитектура разрабатываемой программы

Заключение

Список литературных источников

Приложение А (обязательное) Исходный код

**ВВЕДЕНИЕ**

В современном мире, где цифровые технологии проникают во все сферы нашей жизни, безопасность информации становится приоритетом. Все больше людей, как в личной, так и в корпоративной среде, осознают важность защиты данных. Однако, чтобы защититься от угроз, нужно хорошо понимать, как эти угрозы работают. В этом контексте изучение аспектов создания вредоносных программ может оказаться необычным, но важным инструментом для повышения кибербезопасности. Сегодняшние компьютеры и сети предоставляют нам невероятные возможности, но также подвергают нашу конфиденциальность и безопасность риску.

Применение вредоносных программ приводит к различным последствиям: от создания мелких неполадок в системе, до полного прекращения работоспособности компьютерных систем или кражи важных данных. В результате действия таких программ огромное количество людей испытывает критические неудобства при использовании своих систем, а крупные предприятия имеют большие финансовые убытки.

Цель данного курсового проекта состоит в том, чтобы разобраться в тонкостях работы компьютера, понять, каким образом вредоносное программное обеспечение может использовать аппаратные прерывания и другие механизмы для достижения своих целей. Изучая процесс создания вирусов с точки зрения их авторов, мы сможем лучше понимать их методы, что в свою очередь поможет разработать более эффективные меры по защите информации.

Создание вирусов позволяет сделать свой вклад в обеспечение безопасности информации, ибо только понимая уязвимости, можно разработать меры защиты от них. Изучение аспектов создания вирусов может сделать более осведомленным и помочь избежать стать жертвой злоумышленников.

**1 АРХИТЕКТУРА ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ**

**Структура и архитектура вычислительной системы**

Процессор *Intel Celeron N3350* является важным компонентом семейства процессоров *Intel Apollo Lake*, предназначенных для использования в ноутбуках и мобильных устройствах. Он представляет собой двухъядерный процессор с низким энергопотреблением, что обеспечивает оптимальный баланс между производительностью и энергосбережением.

Архитектура процессора *Intel Celeron N3350* основана на микроархитектуре *Intel Goldmont*, которая представляет собой существенное улучшение по сравнению с предыдущими поколениями процессоров *Celeron* и обеспечивает ряд ключевых преимуществ:

1. Исполнение команд "*out-of-order*": микроархитектура *Goldmont* использует принципы исполнения команд с префиксом "*out-of-order*", что означает способность процессора выполнять команды вне последовательности исходного кода программы. Это улучшает эффективность выполнения команд и ускоряет обработку задач.
2. Поддержка 64-битных вычислений: архитектура *Goldmont* обеспечивает поддержку 64-битных вычислений, что позволяет работать с большим объемом памяти и обеспечивает совместимость с 64-битными операционными системами и приложениями.
3. Эффективное управление энергопотреблением: архитектура *Goldmont* разрабатывалась с акцентом на эффективное управление энергопотреблением. Процессор может автоматически регулировать частоту и напряжение для минимизации энергопотребления в режимах простоя.

Семейство процессоров *Intel Apollo Lake* с микроархитектурой *Goldmont* представляет значительное усовершенствование в мире мобильных и встроенных устройств. Процессор *Intel Celeron N3350*, как один из его представителей, объединяет выдающуюся эффективность энергопотребления, производительность и современные технологии.

**История, версии и достоинства**

Процессоры *Intel Celeron* с кодовым названием *N3350* были представлены компанией *Intel* в 2016 году и стали частью архитектуры *Apollo Lake*. Эти процессоры продолжили линейку *Celeron*, спроектированную для устройств с низким энергопотреблением. С момента своего выпуска процессоры *N3350* приобрели популярность в ноутбуках и мобильных устройствах благодаря своей эффективности и хорошей производительности в данном классе устройств.

Процессоры *Intel Celeron N3350* имеют разные версии, которые могут немного отличаться по характеристикам и возможностям. Тем не менее, основные характеристики, такие как наличие двух вычислительных ядер, использование архитектуры *Goldmont* и интегрированное графическое ядро *Intel HD Graphics 500*, остаются общими для всех версий данного процессора.

**Анализ выбранной вычислительной системы для написания программы**

Процессор *Intel Celeron N3350* обладает двухъядерной архитектурой, что предоставляет возможность параллельного выполнения двух независимых задач. Это важное преимущество для вредоносных программ, так как они могут использовать одно ядро для своей деятельности, при этом второе ядро остается доступным для других процессов. Эффективное использование многозадачности может увеличить степень скрытности вредоносных приложений.

Процессор *Celeron N3350* также поддерживает механизм аппаратных прерываний, который позволяет внешним устройствам взаимодействовать с процессором и операционной системой. Это свойство может быть использовано вредоносными программами для вмешательства в работу аппаратуры и перехвата управления важными событиями.

Аппаратные характеристики процессора *Intel Celeron N3350*, такие как его двухъядерная архитектура и поддержка аппаратных прерываний, делают его потенциально привлекательным для создания вредоносных программ.

**2 ПЛАТФОРМА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

**Структура и архитектура платформы**

*Linux Ubuntu* - это один из популярных дистрибутивов операционной системы Linux, основанный на *Debian*. Структура и архитектура *Ubuntu* обладают своими уникальными особенностями. В основе *Ubuntu* лежит ядро *Linux*, которое обеспечивает взаимодействие с аппаратным обеспечением компьютера и управляет ресурсами. В рамках структуры *Ubuntu* существуют разнообразные модули ядра, подсистемы, оболочки, пакетные менеджеры, графические оболочки и системные демоны.

**История, версии и достоинства**

Операционная система *Ubuntu* была впервые выпущена в октябре 2004 года фирмой *Canonical Ltd*. и её основателем Марком Шаттлвортом. Основной целью создания Ubuntu было предоставление пользователям бесплатной и простой в использовании альтернативы коммерческим операционным системам. С момента своего появления *Ubuntu* активно развивается и завоевывает популярность благодаря своей открытости и бесплатности.

*Ubuntu* имеет регулярный цикл выпуска новых версий. Номер версии определяется годом и месяцем выпуска. Каждая версия поддерживается в течение определенного периода времени, что обеспечивает регулярные обновления и патчи безопасности для пользователей.

Достоинства *Ubuntu* включают в себя стабильность, безопасность и поддержку сообщества, а также наличие большого количества программного обеспечения и инструментов для разработки. *Ubuntu* известна своей стабильностью и надежностью, что делает её популярным выбором для серверов и рабочих станций. Операционная система регулярно обновляется для устранения уязвимостей, и в ней внедрены различные механизмы безопасности, такие как *AppArmor*.

*Ubuntu* имеет активное и преданное сообщество пользователей и разработчиков. Это обеспечивает доступ к бесценным знаниям и поддержке для пользователей на всех уровнях опыта. Операционная система предоставляет широкий выбор программного обеспечения и инструментов для разработки, которые могут быть установлены с помощью удобного софтверного центра. *Ubuntu* также совместима с *Debian* и поддерживает большинство пакетов и репозиториев *Debian*, что расширяет доступность программного обеспечения для пользователей *Ubuntu*.

**Обоснование выбора платформы**

Для написания программы-вирус была выбрана именно *Ubuntu*, поскольку это один из наиболее популярных дистрибутивов *Linux* с активным сообществом и доступом к открытому исходному коду. *Ubuntu* обеспечивает удобную среду для разработки и тестирования программного обеспечения, включая вредоносное, и предоставляет доступ к богатому набору инструментов и библиотек. Кроме того, *Ubuntu* широко используется как на рабочих станциях, так и на серверах, что делает его интересной целью для исследования уязвимостей и методов защиты. Выбор *Ubuntu* обусловлен как его популярностью, так и возможностью более полного понимания работы операционной системы и механизмов защиты, что поможет разработать более эффективные меры по обеспечению кибербезопасности.

**3. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ РАЗРАБОТКИ ПРОГРАММНОГО ПРОДУКТА**

**4 ПРОЕКТИРОВАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММЫ**

**5 АНАЛИЗ СРАВНЕНИЯ ПРОЦЕССОРОВ**