**УДК 004.056.53**

**Кучер Ростислав Юрьевич, студент гр. 125м-16-1,**
**Научный руководитель Кручинин А.В., ст. преп. кафедры безопасности информации и телекоммуникаций**
*(Государственное ВУЗ «Национальный горный университет», г. Днепр, Украина)*

# СПОСОБЫ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ЗАПУСКА ПРИЛОЖЕНИЙ С USB-УСТРОЙСТВ

В данных тезисах анализируются способы защиты от несанкционированного доступа в компьютерные системы по USB-каналу, особенности их работы, разработка рекомендаций, которая удовлетворит большинству запросам безопасности.

*Ключевые слова: кибербезопасность, операционная система, взлом, Windows, USB.*

## ВВЕДЕНИЕ

В операционной системе Windows 95 существует функция автозапуска. Целью данного инструмента было упрощение запуска и установки приложений, программного обеспечения и драйверов устройств не квалифицированными пользователями и для уменьшения количества звонков в службу поддержки. Когда записанный особым образом диск вставляли в привод, система Windows определяла наличие специального файла с инструкциями. Но эта функция открыла возможность злоумышленнику модифицировать устройство переносного хранения информации и установить набор инструкций для получения прав администратора с целью хищения, изменения или удаления информации в системе[6].

## СПОСОБЫ ЗАЩИТЫ ОС ОТ ВЗЛОМА С ПОМОЩЬЮ USB-НАКОПИТЕЛЕЙ

За реализацию функции автозапуска в Windows системах ответственен файл autorun.inf, с помощью которого злоумышленники достаточно эффективно обходили защиту системы. Компании Microsoft пришлось избавиться от этой функции и уже через 3 месяца после отключения автозапуска, количество атак, использующих его в Windows XP и Vista, снилось на 1.3 миллиона. Теперь, начиная с Windows 7, этот функционал отключен по умолчанию. Это является одним из способов защиты ОС от взлома с помощью ЮСБ носителей. На сегодняшний день, актуальный следующие способы защиты[1,7]:

1. Физическое отключение портов.
2. Отключение портов в BIOS/UEFI.
3. Удаление драйверов контроллера USB[5,8].
4. Блокировка отдельных устройства USB.
5. Ограничение прав на чтение файлов usbstor.inf и usbstor.pnf в каталоге \Windows\Inf.
6. Контроль подключений устройств с использованием дополнительного ПО[4,5].

## СРАВНЕНИЕ СПОСОБОВ ЗАЩИТЫ

Для сравнения представленных способов предлагается использовать следующие основные критерии:

- удобство – комфорт работы с примененной мерой защиты;
- простота – соотношение количества ресурсов и времени, необходимых для установки и настройки;
- надежность – насколько хорошо меры безопасности могут защитить от взлома.

Так использование способа редактирования реестра, позволяет заблокировать возможность использования USB-накопителей, однако при этом сканеры, клавиатура, мышь и подобное оборудование продолжит свою роботу. Кроме этого, ошибочные действия могут повлечь повреждение системы. Отключение устройств в диспетчере более удобно, однако очень ненадежно и требует времени для полной реализации. Также неоднозначен и способ с удалением драйверов. Система всегда будет пытаться восстановить свой функционал. Подключая USB-устройство, система проверит наличие драйвера и при их отсутствии предложит установить драйвер. Это в свою очередь откроет доступ к USB-устройству. При физическом отключении на материнской плате кабеля, может заблокировать только переднюю панель, при этом остается активной задняя панель. Необходимо заблокировать доступ к задней панели системного блока, иначе защита не имеет смысла. Ограничение прав на чтение файлов usbstor.inf и usbstor.pnf способ делегирования с правами NTFS. Если невозможно обратиться к этим файлам в ограниченной учетной записи, то не будут подключаться флешки, но необходимо удостоверится что пользователь не получит возможности перемещения файлов в другое место. Способ подключения устройств по USB с использованием дополнительного ПО предлагает сохранить разрешенные флешки по номеру тома (VSN) [2,3]. Существует возможность использовать кремниевые диоды с встречно-параллельным включением. Каждый такой диод понизит напряжение на 0,7 В. В некотором роде это можно использовать в защитных целях, принудительно понижая ток.

На основе выполненного анализа, была составлена сравнительна таблица. В этой таблице критерии ранжируются от 1 до 3.

Таблица 1. Сравнения способов защиты:

| **Способ** | **Критерии** | | |
|---|---|---|---|
| | **Надежность** | **Простота** | **Удобство** |
| Редактирование реестра | 2 | 3 | 2 |
| Диспетчер устройств | 1 | 3 | 3 |
| Удаление драйверов | 2 | 1 | 2 |
| Физическое отключение | 3 | 2 | 2 |
| Ограничение прав на чтение файлов | 2 | 3 | 2 |
| Контроль подключений устройств с помощью доп. ПО | 1 | 1 | 2 |

Полученные результаты позволяют выбрать способ или группу способов защиты наиболее подходящих для решения конкретных задач. В большинстве случаев, используя редактирование реестра и контроля подключения устройств с помощью доп. ПО, можно добиться достаточно высокого уровня защиты ОС от взлома с помощью USB-накопителей.

## ВЫВОДЫ

В данной работе рассмотрен вопрос о способах реализации несанкционированного доступа с использованием USB-устройств к компьютерной системе под управлением ОС Windows, первопричинах появления данной уязвимости. Выполнен анализ существующих способов защиты, предложены критерии и выполнена их оценка. Предложены рекомендации по выбору способов защиты.

## СПИСОК ИСТОЧНИКОВ

1. Википедия: Несанкционированный доступ [Электронный ресурс] – [Веб-сайт]- Режим доступа: https://uk.wikipedia.org/wiki/Несанкціонованийдоступ

2. Способы блокировки клавиатуры ноутбука [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://wd-x.ru/kak-zablokirovat-klaviaturu-na-noutbuke/

3. Способы обхода паролей BIOS [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://habrahabr.ru/post/128466/

4. DeviceLock 5.61: периферия под контролем [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://www.osp.ru/winitpro/2004/07/177240/

5. Вскрываем Windows. Легкие способы получить права админа на рабочем компьютере [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://xakep.ru/2016/09/29/bypassing-office-pc-restrictions/

6. Чем UEFI лучше обычного BIOS и каковы отличия [Электронный ресурс] – [Веб-сайт] - Режим доступа: http://vindavoz.ru/poleznoe/128-chem-uefi-luchshe-obychnogo-bios-i-kakovy-otlichiya.html

7. Википедия: Доверенная загрузка [Электронный ресурс] – [Веб-сайт] - Режим доступа: https://ru.wikipedia.org/wiki/Доверенная_загрузка_(аппаратные_средства)

8. Википедия: Ubuntu [Электронный ресурс] – [Веб-сайт] - Режим доступа: wiki.ubuntu.com/Security/Features.

ShmooCon 2011: USB Autorun attacks against Linux [Электронный ресурс] – [Веб-сайт] - Режим доступа: youtube.com/watch?v=ovfYBa1EHm4.