УДК 004.777

ПРОГРАММНЫЙ МОДУЛЬ ОБНАРУЖЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕЕСТРЕ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА WINDOWS

Боровец Н.О.

гр. 367241

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Пулко Т.А. – канд. техн.наук, доцент

Аннотация. Данная статья представляет обзор программного модуля, который будет разработан для обнаружения угроз информационной безопасности в реестре операционных систем семейства Windows. Модуль специализируется на обнаружении нежелательного подключения мобильных телефонов и незарегистрированных USB-накопителей в локальной сети организации, которые могут представлять серьезную угрозу для безопасности информации. Анализ основных проблем безопасности, связанные с такими устройствами, и предлагают решение в виде программного модуля, основанного на мониторинге реестра

Windows и анализе идентификационных данных подключенных устройств.

Ключевые слова: программный модуль, локальная вычислительная сеть, операционные системы семейства Windows, администратор, язык Python.

Введение. В современном цифровом мире, где информационные технологии играют ключевую роль в деятельности организаций, обеспечение безопасности информации становится неотъемлемой задачей для любого предприятия. Особенно актуальным остается обеспечение защиты от внутренних угроз, таких как нежелательное подключение мобильных устройств и USB-накопителей к корпоративным сетям. Именно здесь встает задача разработки эффективных инструментов для обнаружения и предотвращения подобных угроз.

Одним из наиболее распространенных средств хранения конфиденциальной информации и настроек операционной системы Windows является ее реестр. Именно в этом ключевом компоненте системы скрыты потенциальные угрозы, связанные с нежелательным доступом и внесением изменений. В связи с этим возникает необходимость в разработке программного модуля, способного надежно обнаруживать угрозы информационной безопасности в реестре операционных систем семейства Windows.

Основная часть. Целью разработки программного модуля является предоставление администраторам информации о подключенных устройствах, проверка их легитимности и обеспечение безопасности информационной среды организации.

Работа модуля будет иметь следующие особенности, он может работать как в ручном режиме, т.е администратор запускает модуль вручную через интерфейс или командную строку. Модуль начинает свою работу по анализу реестра Windows и сбору информации о подключенных устройствах и сетевых параметрах. Модуль сканирует реестр Windows на наличие записей о подключенных устройствах и сетевых настройках компьютера. После завершения анализа, модуль извлекает необходимую информацию о времени подключения мобильных телефонов и USB-накопителей, а также о сетевых параметрах компьютера, таких как IP-адрес и MAC-адрес, его имени в локальной сети организации. Полученная информация представляется администратору в удобном формате, возможно, через интерфейс программы или вывод в консоль. В зависимости от настроек модуля, администратор может выполнять дополнительные действия, такие как сохранение результатов в файл.

Также модуль может работать, как и в автоматическом режиме совместно с установленным антивирусном программным обеспечением на предприятии (к примеру, Kaspersky Endpoint Security), где создается задача на основании которой модуль запускается на всех компьютерах организации, где установлен антивирус.

Текстовое описание диаграммы вариантов использования модуля обнаружения угроз в реестре Windows:

- Администратор устанавливает и настраивает модуль;
- Администратор определяет параметры мониторинга реестра;
- Администратор настраивает журналирование действий модуля;
- Модуль мониторит реестр Windows на наличие новых записей о подключенных устройствах;
- Модуль анализирует идентификационные данные новых устройств;
- Модуль проверяет права доступа к подключенным устройствам;
- Модуль анализирует активность подключенных устройств;
- Модуль сравнивает идентификационные данные с зарегистрированными устройствами;

- Модуль ведет журнал действий для последующего анализа.

Для реализации поставленных целей принято решение об использовании в работе языка программирования Python. Данное решение обусловлено тем, что данный язык программирования легкий в освоении с простым и понятным синтаксисом. Это позволяет в перспективе упростить процесс сопровождения итогового решения, в случае смены разработчика.

Заключение. Разработка и внедрение программных модулей для обнаружения угроз информационной безопасности в реестре Windows является важным шагом для обеспечения безопасности информации в современном бизнесе. Эти модули обеспечивают непрерывный мониторинг системы, анализируют активность и идентифицируют потенциальные угрозы, что позволяет оперативно реагировать на возможные инциденты и минимизировать риски для организации. Данный программный модуль разрабатывается на языке программирования Python.

Список литературы

1. Климов Александр, Чеботарев Игорь Реестр Windows – 2002-2012. Справочные материалы – 325с.
2. Денис Колисниченко Секреты, настройка и оптимизация реестра Windows – Санкт-Петербур 2010г. – 320с
3. Язык программирования Python : учеб.-метод. пособие / Д. Ю. Косицин. – Минск: БГУ, 2019. – 136с.

UDC 004.777

SOFTWARE MODULE FOR DETECTING INFORMATION SECURITY THREATS IN THE REGISTRY OF OPERATING SYSTEMS OF THE WINDOWS FAMILY

Borovets N.O.

gr. 367241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Pulko T.A. – Ph.D. technical sciences, associate professor

Annotation. This article provides an overview of a software module that will be developed to detect information security threats in the registry of Windows operating systems. The module specializes in detecting unwanted connections of mobile phones and unregistered USB drives on the enterprise local network, which can pose a serious threat to information security. They analyze the main security problems associated with such devices and offer a solution in the form of a software module based on monitoring the Windows registry and analyzing the identification data of connected devices.

Keywords: software module, local area network, Windows operating systems, administrator, Python language.