Министерство Образования Республики Беларусь

Белорусский Национальный Технический Университет

Факультет информационных технологий и робототехники

Кафедра **“**Технология разработки программного обеспечения**”**

Исследовательская работа:

Изучение рынка ПО

Выполнили: студенты группы 10701322

ФИТР БНТУ

Бородкин Дмитрий Владимирович

Серов Данил Викторович

Минск, 2024

Цель работы: исследовать рынок антивирусного ПО и придумать функционал для достижения конкурентоспособности собственного ПО на рынке.

Почему антивирусное ПО активно используется?

- Информационная безопасность

- Защита устройства

- Безопасность сёрфинга

- Защита от некомпетентности пользователя

Информационная безопасность

Компании становятся более бдительными в защите своих конфиденциальных бизнес-данных. Такие отрасли, как финансовые услуги и банковское дело, являются очевидными местами, где важно обеспечить безопасность данных. Но хакеры нацелены на самые разные компании и частных лиц, поскольку почти все организации и люди имеют в своих сетях тот или иной уровень ценных данных.

Защита устройства

В современном мире компьютеры разрознены и многочисленны. Компании часто предоставляют пользователям доступ к бизнес-данным и приложениям на любом устройстве, которое у них есть под рукой. Однако важно обеспечить безопасность каждой из этих конечных точек. Кросс-платформенная доступность важна для многих компаний. Но антивирусные инструменты помогают защитить вашу бизнес-сеть от опасных программ и хакеров, независимо от типа устройства, которое они используют.

Безопасность сёрфинга

Сотрудники часто просматривают Интернет и попадают на потенциально опасные сайты. Если сеть вашей компании не блокирует несанкционированные сайты или сотрудники пользуются своей собственной сетью, вполне вероятно, что они в конечном итоге столкнутся с каким-либо вредоносным ПО. Антивирусные решения — это полезные инструменты для выявления потенциально опасных материалов и предотвращения их получения пользователями. Это включает в себя нажатие на опасную рекламу, загрузку подозрительных файлов или попадание в зону фишинга. Все эти действия пользователей могут в конечном итоге привести к проникновению вредоносного ПО в сеть и поставить под угрозу бизнес-данные.

Защита от некомпетентности

Как и в случае с браузером, сотрудники не всегда владеют лучшими практиками интернет-безопасности. Многие пользователи загружают расширение или программу просто потому, что сайт требует этого; антивирусные решения помогают затруднить или даже сделать невозможной загрузку вредоносной программы. Эти загрузки могут легко содержать вредоносное ПО и нанести ущерб сети компании. Это подвергает риску данные отдельных пользователей. А из-за способности вируса размножаться и распространяться, мишенью становится вся сеть компании.

Основные функции, требуемые для создания антивирусного ПО:

1. Сканирование системы
2. Постоянное наблюдение за системой
3. Файерволл
4. Веб-безопасность
5. Защита почты
6. Автообновление ПО
7. Кроссплатформинг

Новые функции нашего ПО, для достижения конкурентоспособности:

1. Адаптивная нагрузка (в зависимости от функций используемых компьютером изменять приоритет работы модулей антивируса)
2. Мониторинг процессов компьютера для выявления вредоносных. (Уведомление пользователя о подозрительном процессе и возможность заморозки процесса. Также предусмотреть работу с мониторингом скрываемых процессов. К примеру сделать историю нагрузки за последний час)
3. Партнёрство с издателями ПО (для поиска уязвимостей и пользования нелицензированным ПО)

Вывод

Изучив рынок ПО, мы смогли выделить обязательные функции для антивирусного ПО и придумать новые, которые позволяют нашему ПО обрести конкурентоспособность.