Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2020 г.

Разработка серверной части программного обеспечения инвентаризации и контроля целостности программной среды автоматизированных рабочих мест локальной сети

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2020.114.ПЗ ВКР

Руководитель проекта,
специалист по защите
информации ООО
«Стратегия безопасности»
_____ С. В. Скурлаев
_____ 2020 г.

Автор проекта,
студент группы КЭ-555
_____ А. П. Левакин
_____ 2020 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2020 г.

Челябинск 2020

АННОТАЦИЯ

Левакин А.П. Разработка серверной части программного обеспечения инвентаризации и контроля целостности программной среды автоматизированных рабочих мест локальной сети – Челябинск: ЮУрГУ, КЭ-555, 98с., 47 ил., 3 табл., библиогр. список – 27 наим., 1 прил.

Выпускная квалификационная работа выполнена с целью создания серверной части программного обеспечения инвентаризации и контроля целостности программной среды автоматизированных рабочих мест локальной сети.

В выпускной квалификационной работе отражены все этапы создания программы, от сбора теоретических данных о работе программного обеспечения такого рода до практической реализации.

В процессе выполнения квалификационной работы был проведен поиск аналогов, исследование необходимой функциональности, поиск методов реализации поставленных задач, программирование, отладка и тестирование изделия.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Роль информационной безопасности в современном мире неукоснительно возрастает с каждым днём. Об этом свидетельствует стремительное развитие информационных технологий в различных сферах жизнедеятельности в мировом социуме. Ведь там, где присутствует какая-либо информация, несущая в себе определённую ценность для её владельца и/или третьих лиц, регулярно требуется обеспечение безопасности этой самой информации. В зависимости от того, насколько важна сохранность каких-либо сведений для их держателя, может быть предпринят ряд мер по защите этой информации. Такими мерами по обеспечению информационной безопасности могут являться: организационные, правовые, программно-технические и другие меры. В свою очередь, любая из перечисленных мер является неотъемлемой частью единого процесса обеспечения информационной безопасности вычислительных систем.

Для обеспечения информационной безопасности на рабочих местах локальной сети перед специалистами встают такие проблемы как:

- централизованное управление;
- защита данных на удаленных компьютерах;
- защита компьютеров на уровне программной среды;
- защита удаленных компьютеров на уровне сети;
- защита удаленных компьютеров на уровне операционной системы.

Пользователи могут получить вредоносный код во многих формах, от собственных исполняемых файлов Windows (exe-файлы) до макросов в документах (таких как файлы .doc), в скрипты (например, vbs-файлы). Злоумышленники часто используют методы социальной инженерии, чтобы пользователи запустили код, содержащий вирусы и черви. Если такой код активирован, он может создавать атаки типа «отказ в обслуживании» на сеть, отправлять конфиденциальные или закрытые данные в Интернет, обеспечивать безопасность компьютера под угрозой или повредить содержимое жесткого диска.

Ответственные организации и пользователи должны иметь возможность определить, какое программное обеспечение можно безопасно использовать для своей деятельности, а какое нет. Благодаря множеству форм и вариантов создания вредоносных программ, это довольно сложная задача. Таким образом возникает необходимость каким-то образом отслеживать целостность программ и контролировать их работу.

Возможны и другие ситуации. К примеру, существуют так называемые «портативные» версии программ, не требующие установки. С их помощью пользователи могут применять запрещенное программное обеспечение, вроде различных программ общения в сети Интернет, или использовать не контролируемый администратором установленный веб-браузер, а свой собственный. Злоумышленник может применить различные программы, предназначенные для сетевой разведки и взлома.

В целом, пользователи могут приносить и использовать различного рода специальное ПО для личных целей, что так же может навредить работодателю, однако будет обнаружено антивирусами. Примером такого программного обеспечения могут послужить так называемые «майнеры» (англ. «Miner»), используемые для добычи криптовалют путем утилизации мощностей компьютеров.

Исходя из сказанного выше, можно обнаружить, что контроль происходящего на автоматизированном рабочем месте является важной частью информационной безопасности предприятия. Существует множество программ, позволяющих обеспечить необходимый результат, все они имеют свои недостатки и преимущества. Зачастую, крупнейшим недостатком становится стоимость программного комплекса, слишком крупная для предприятия, как финансово, так и психологически. Кроме того, такие программы имеют закрытый исходный код и не позволяют системному администратору или другому ответственному лицу редактировать их возможности при необходимости.

Таким образом, вышеобозначенная проблема актуальна по следующим причинам:

– существование различных не вирусных программ, способных тем или иным способом навредить работодателю;

– возможность подмены программных файлов злоумышленниками;

– закрытость исходного кода программ инвентаризации и контроля целостности;

– стоимость программ инвентаризации и контроля целостности.

На фоне актуальности этой проблемы, руководителем было предложено разработать собственный вариант программного обеспечения для учебно-практических целей. Такая программа может быть использована в ЮУрГУ как по прямому назначению, так и в качестве каркаса для дальнейших студенческих разработок в области защиты информации.

Целью работы является разработка серверной части программного обеспечения инвентаризации и контроля целостности программной среды автоматизированных рабочих мест локальной сети.

В соответствии с поставленной целью необходимо решить следующие задачи:

– разработать систему контроля работающих в системе процессов;

– разработать систему обнаружения изменений в исполняемых файлах;

– разработать систему обнаружения новых сетевых адаптеров и оповещения администратора об этом событии;

– исследовать актуальные подходы к решению проблемы;

– развернуть всю систему, состоящую из сервера, административной панели, базы данных и клиента в программном обеспечении для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации.