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»

РАБОТА ПРОВЕРЕНА
Старший системный администратор,
ИП «Аксенов»
_____М.А. Кочуров
_____ 2019 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2019 г.

Система аудита и контроля средств удаленного администрирования автоматизированных систем управления технологическим процессом

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2019.380.ПЗ ВКР

Консультанты

Безопасность жизнедеятельности,
к.т.н., доцент
_____ Н.В. Глотова
_____ 2019 г.

Руководитель проекта,
н. с. НОЦ «Информационной безопасности»
_____ А.Е. Баринов
_____ 2019 г.

Автор проекта,
студент группы КЭ-570
_____ Д.В. Ермолаев
_____ 2019 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2019 г.

Челябинск 2019

АННОТАЦИЯ

Ермолаев Д.В. Система аудита и контроля средств удаленного администрирования автоматизированных систем управления технологическим процессом - Челябинск: ЮУрГУ, КЭ-570, 104 с., 20 ил., 6 табл., библиогр. список - 26 наим., 6 прил.

Выпускная квалификационная работа выполнена с целью создания системы аудита и контроля средств удаленного администрирования автоматизированных систем управления технологическим процессом.

В выпускной квалификационной работе отражены все этапы создания системы, от изучения структуры сетевых пакетов и поиска уникальных отличительных особенностей протоколов удаленного управления до разработки политики использования программ удаленного администрирования и тестирования системы на АСУ ТП.

В процессе выполнения квалификационной работы были выбраны распространенные протоколы удаленного управления, определены их уникальные отличительные особенности, создана система для обнаружения использования протоколов удаленного управления, найдены файлы учетных данных для авторизации на серверной части программ удаленного администрирования и установлен контроль целлостности.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В наш век информационных технологий все предприятия стремятся автоматизировать производственные и технологические процессы, для удешевления рабочей силы, улучшения качества и скорости производства продукции. Этот процесс привёл к возникновению автоматизированных систем управления технологическим процессом, которые состоят из комплекса технических и программных средств, предназначенный для автоматизации управления технологическим оборудованием на промышленных предприятиях. Человеческое участие при внедрении АСУ ТП при этом сведено к минимуму, но всё же присутствует на уровне принятия наиболее ответственных решений.

Как мы знаем, в любой незащищённой информационной системе существуют уязвимости, при обнаружении которых разработчики выпускают патчи, закрывающие данные уязвимости. Но не всегда эти уязвимости обнаруживают разработчики, иногда в этом преуспевают преступные группировки, хакеры. После ущерба, который всем известный компьютерный червь Stuxnet нанёс ядерной программе Ирана на заводе работающим с АСУ ТП, эксперты кибербезопасности всего мира начали создавать промышленные решения безопасности автоматизированных систем.

К сожалению, информационной безопасности промышленных объектов до последнего времени уделялось недостаточно внимания как со стороны эксплуатирующих организаций, так и со стороны организаций, занимающихся проектированием систем индустриальной автоматизации. Это, безусловно, негативно отразилось на фактическом уровне защищенности инфраструктуры критических производств, которые в реальности оказались не готовы противостоять современным киберугрозам. К сожалению, осознание этого факта всеми участниками процесса пришло лишь после нескольких крупных международных инцидентов.

В ближайшие годы промышленности предстоит преодолеть этот разрыв. К сожалению, современные продукты ИБ, к использованию которых мы привыкли в офисных инфраструктурах, зачастую просто не применимы для защиты промышленных инфраструктур по ряду объективных причин. Поэтому, в свою очередь,

производители систем информационной безопасности должны предложить продукты, которые помогли бы решить основные задачи в контексте защиты индустриальных объектов. Эксперты «Лаборатории Касперского» создали Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team - глобальный проект, нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур, а также создали продукты Kaspersky Industrial Cyber Security, состоящие из KICS for Nodes, Kics for Networks.

В попытках удешевить обслуживание АСУ и уменьшить время реагирования в случае возникновения неполадок отделы информационных технологий многих предприятий устанавливают на автоматизированные рабочие места инженеров и операторов средства удалённого управления. Согласно исследованию «Лаборатории Касперского» за первое полугодие 2018 года, в котором обрабатывались данные полученные из отчётов работы программы для защиты инфраструктуры промышленных предприятий от угроз информационной безопасности и для обеспечения непрерывности технологических процессов KICS for Networks на каждом третьем компьютере АСУ установлены легитимные средства администрирования ПК. В ряде расследованных «Лабораторией Касперского» инцидентов средства администрирования (Remote Administration Tool – RAT) были использованы злоумышленниками для атаки на промышленные организации. В некоторых случаях это были RAT, скрыто установленные злоумышленниками на компьютеры атакованных организаций, в других случаях злоумышленники могли использовать средства RAT, которые уже присутствовали в организации на момент атаки. Беря во внимание этот факт, возникает потребность в создании системы контроля и фиксирования подобных подключений.

Первый шаг к пресечению деятельности по несанкционированному доступу – это своевременное пресечение такового.

Проанализировав различную техническую литературу, специализированные источники, статьи и иные источники информации, не удалось обнаружить ни одного средства обнаружения использования протоколов удалённого управления, оптимизированного под обработку большого объёма сетевого трафика, удобного в работе для администратора информационной безопасности.

В ходе своей работы я рассмотрел разнообразные протоколы и программы для удалённого доступа и выявил их отличительные особенности, по которым можно обнаруживать принадлежащие им сетевые пакеты. На основании этого на базе программного продукта «Лабораторией Касперского» KICS for Networks была реализована программа регистрирующая удалённые подключения во локальной сети предприятия, имитирующей стенд НОЦ “Информационной безопасности”.

Объектом исследования является локальная сеть предприятия, в частности АСУ ТП.

Предметом исследования является удалённые подключения в локальной сети предприятия, а частности АСУ ТП.

Целью дипломной работы является обнаружение всех активных средств удалённого управления HMI, SCADA, проанализировать их соответствие политикам Информационной Безопасности, и дать какое-либо предупреждение администратору информационной безопасности.

Для достижения этой цели необходимо выполнить ряд задач:

- описать тестовую информационную систему, которая будет подвергаться защите;

- провести анализ самых распространённых средств удалённого управления в АСУ ТП;

- описать политику Информационной безопасности предприятия для пользователей информационной системы работающими с программами удалённого доступа;

- разработать правила для обнаружения средств удалённого доступа и оповещения администратора Информационной безопасности.

Практическая значимость работы заключается в том, что на данный момент большая часть программных продуктов для предприятий не оснащена системой обнаружения средств удалённого управления и оповещения администратора на соответствие политики Информационной безопасности.