

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 тех-
нологическим 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 целостности.

					ЮУрГУ - 10.05.03.2019.380.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Ермолаев			<i>Система аудита и контроля средств удаленного администрирования автоматизированных систем управления технологическим процессом</i>	Лит.	Лист	Листов
Пров.		Баринов					6	104
Реценз.		Кочуров				ЮУрГУ		
Н. Контр.		Мартынов				Кафедра ЗИ		
Утв.		Соколов						

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	9
ГЛАВА 1. АНАЛИТИЧЕСКОЕ ОБОСНОВАНИЕ НЕОБХОДИМОСТИ СОЗДАНИЯ СРЕДСТВА ОБНАРУЖЕНИЯ УДАЛЁННЫХ ПОДКЛЮЧЕНИЙ..	13
1.1 Аналитическое описание частей АСУ ТП.....	13
1.2 Обзор работы ПО KICS for Networks.....	17
1.3 Обзор международных стандартов в области защиты промышленных сетей передачи данных	20
1.4 Аналитика угрозы удалённых подключений на АСУ ТП.....	21
1.5. Выводы по главе.....	28
ГЛАВА 2. СЕТЕВЫЕ ПРОТОКОЛЫ УДАЛЁННОГО ДОСТУПА.....	30
2.1 RDP.....	31
2.2 VNC.....	32
2.3. Radmin.....	35
2.4. TeamViewer	37
2.5. Ammyu Admin	38
2.7. Выводы по главе	39
ГЛАВА 3. МЕТОДЫ ОБНАРУЖЕНИЯ ИСПОЛЬЗОВАНИЯ ПРОТОКОЛОВ УДАЛЕННОГО УПРАВЛЕНИЯ КОМПЬЮТЕРНОЙ СИСТЕМОЙ. СРАВНЕНИЕ СУЩЕСТВУЮЩИХ ПРОГРАММНЫХ И ПРОГРАММНО- АППАРАТНЫХ ПРОДУКТОВ	41
3.1 Методы обнаружения протоколов удалённого управления.....	41
3.2 Сравнение существующих программных и программно-аппаратных продуктов, позволяющих обнаруживать сетевые протоколы прикладного уровня.....	43
3.3 Выводы по главе	46
ГЛАВА 4. РАЗРАБОТКА СИСТЕМЫ АУДИТА И КОНТРОЛЯ СРЕДСТВ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ	47
4.1 Требования к разработанной системе, разработка политики использования программ удаленного администрирования.....	47
4.2 Описание программного обеспечения, использованного в реализации системы	49

4.3. Методология нахождения отличительных особенностей протоколов удаленного управления RDP.....	56
4.4 Отличительные особенности удаленных протоколов и программ для удаленного управления.....	60
4.5 Создание системы аудита и контроля программ удаленного администрирования.....	62
4.6 Создание механизма контроля целостности настроек программ удаленного администрирования.....	66
4.7 Выводы по главе	72
ГЛАВА 5. БЕЗОПАСНОСТЬ ЖИЗНИ ДЕЯТЕЛЬНОСТИ	74
5.1. Общие требования к организации рабочих мест пользователей.....	75
5.2. Требования к помещениям для размещения рабочего места.....	77
5.3. Требования к уровням шума на рабочих местах.....	78
5.4. Требования к освещению на рабочих местах.....	78
5.5. Требования к микроклимату	80
5.6. Требования к электробезопасности.....	81
5.7. Пожарная безопасность	82
5.8. Рекомендации по организации режима труда и отдыха.....	85
5.9. Сравнения параметров рабочего места с допустимыми нормами	87
5.10. Выводы по главе	89
ЗАКЛЮЧЕНИЕ	90
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	92
ПРИЛОЖЕНИЕ А	95
ПРИЛОЖЕНИЕ Б.....	100
ПРИЛОЖЕНИЕ В	101
ПРИЛОЖЕНИЕ Г.....	102
ПРИЛОЖЕНИЕ Д	103
ПРИЛОЖЕНИЕ Е.....	104

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 защищённости 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 промышленных объектов. Эксперты «Лаборатории Касперского» создали Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team - глобальный проект, направленный 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 фиксации 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.