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
Рецензент, главный специалист Отдела Сетевых Технологий УИТ
АО «ЧЭМК»
_____ Н.В. Тюрин
_____ 2019 г.

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

Автоматизированная система обнаружения целевых атак в промышленных сетях

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ - 10.05.03.2019.386.ПЗ ВКР

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

Руководитель проекта,
н.с. НОЦ «Информационная безопасность»
_____ А.Е. Баринов
_____ 2019 г.

Экономическая часть,
ст. преп.
_____ С.А. Сабельников
_____ 2019 г.

Автор проекта,
студент группы КЭ-570
_____ Л.А. Рагрин
_____ 2019 г.

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

Челябинск 2019

АННОТАЦИЯ

Рагрин Л.А. Автоматизированная система обнаружения целевых атак в промышленных - Челябинск: ЮУрГУ, КЭ-570, 70 с., 20 ил., 11 табл., библиогр. список - 11 наим., 4 прил.

Выпускная квалификационная работа выполнена с целью анализа существующей автоматизированной системы обнаружения целевых атак, нахождения ее уязвимостей и предоставления способов их устранения.

В выпускной квалификационной работе отражены все этапы анализа системы, от изучения программных компонентов KICS и KTMD до предоставления трех путей устранения обнаруженных в ходе анализа уязвимостей.

В процессе выполнения квалификационной работы был представлен типовой АСУ ТП объект с перечнем используемого оборудования, изучены и описаны продукты KICS и KTMD, разработанные «Лабораторией Касперского». Были приведены уязвимости компонентов АСУ ТП, проанализирована работа KICS при борьбе с сложнодетектируемыми атаками и представлены способы модернизации имеющейся системы защиты.

ОГЛАВЛЕНИЕ

ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

АСУ ТП - автоматизированная система управления технологическим процессом;
КИИ - критическая информационная инфраструктура;
ФСТЭК - федеральная служба по техническому и экспортному контролю;
IT система - информационная система;
ПО - программное обеспечение;
АСУ - автоматизированная система управления;
ИБ - информационная безопасность;
ICS – промышленная система управления;
СМИБ - система менеджмента информационной безопасности;
SCADA - система диспетчерского управления и сбора данных;
РСУ - распределенные системы управления;
ПЛК - программируемые логические контроллеры;
УСО - устройство связи с объектом;
АРМ - автоматизированное рабочее место;
ИЭУ - интеллектуальное электронное устройство;
ЧМИ - человеко-машинный интерфейс;
СУП - система управления процессом;
СБ - система безопасности;
MES - система управления производственными процессами;
ERP - планирование ресурсов предприятия;
BI - системы бизнес-аналитики;
НСС - несанкционированное сетевое соединение;
KICS - Kaspersky Industrial CyberSecurity;
KTMD - Kaspersky Endpoint Detection and Response;
KATA - Kaspersky Anti Targeted Attack Platform;
KEDR - Kaspersky Endpoint Detection and Response
KSC - Kaspersky Security Center;
KSN - Kaspersky Security Network;
KSPN - Kaspersky Private Security Network;
SPAN - Switch Port Analyzer.

ВВЕДЕНИЕ

По мере развития технологий люди становятся все более зависимы от услуг автоматизированных систем управления.

Развитие современного общества сопряжено с все большими и большими темпами роста технологий во всех сторонах жизни как государств в целом, так и отдельных людей в частности. Одна из основных особенностей века информации состоит в развитии и использовании промышленного комплекса: строятся новые заводы, вырабатываются новые и действующие месторождения, ищутся способы замены исчерпаемых материалов неисчерпаемыми, внедряются новые технологии совершенствования производственного процесса. Например, современные печи любого металлургического комбината оснащаются рядом программируемых логических контроллеров (ПЛК), позволяющих автоматизировать технологический процесс путем мониторинга состояния печи (или любого другого объекта) и удаленного управления ею. Соответственно, общество становится все более и более зависимо от использования автоматизированных систем управления технологическим процессом (АСУ ТП).

В связи с тем, что АСУ ТП влияет на непосредственную работу и функционирование промышленных объектов по всей стране, а сбой многих таких систем может привести опасным последствиям для государства и его населения, значит, что АСУ ТП является неотъемлемой частью критической информационной инфраструктуры (КИИ). Следовательно, подобные системы должны обладать необходимым уровнем защищенности, особенно при учете того, что они зачастую поставляются на предприятия со множеством уязвимостей. Некоторые уязвимости возможно устранить, используя регулярные обновления разработчиков, однако многие уязвимости во-первых сложно обнаружить, во-вторых, они могут быть не устранимы и в-третьих, существует человеческий фактор, при котором АСУ ТП, поставленные в определенной базовой комплектации, в дальнейшем не обновляются и работают в своей первоначальной версии, а значит уязвимы для большего числа угроз.

Число атак на промышленные системы растет. Согласно исследованию «Кибербезопасность систем промышленной автоматизации» 2018 [7], если еще несколько лет назад эта проблема носила «умозрительный характер», то сейчас она вполне реальна. Исследования показали, что «более трех четвертей опрошенных» специалистов по информационной безопасности определяют уровень угроз АСУ ТП как критический или высокий, хотя, к примеру, в 2015 году такого мнения придерживалось 43% специалистов, а в 2016 уже 67%. Чтобы обеспечить безопасность АСУ ТП, разрабатывается и внедряется новое программное обеспечение, позволяющее контролировать работу системы, а также регулировать и мониторить подключения к ней. Одним из таких программных средств является разработанный Лабораторией Касперского KICS (Kaspersky Industrial Cyber Security) - ПО, позволяющее контролировать, но не нарушать бесперебойную работу технологического процесса. KICS с полным пакетом компонентов стоит достаточно до-

рого, но хорошо выполняет свою работу и, как следствие, получило распространение в различных компаниях на территории РФ (АО «МОСГАЗ»; нефтеперерабатывающая компания «Танеко», Татарстан).

Однако, даже KICS не может предотвратить все сложнодетектируемые целевые атаки, направленные на промышленные сети, и использующие уязвимости АСУ ТП предприятия. Согласно исследованию «Уязвимости в АСУ ТП: итоги 2018 года» [8], число уязвимостей АСУ ТП на 2018 год резко возросло по сравнению с предыдущими годами (рис.1).

Таблица 1 - Число уязвимостей, обнаруженных в компонентах АСУ ТП

Год исследования	Общее число уязвимостей, обнаруженных в компонентах АСУ ТП
2013	158
2014	181
2015	212
2016	115
2017	197
2018	257

Согласно исследованию «Кибербезопасность систем промышленной автоматизации в 2018 году»[7] проведенному компанией CXP Group по заказу «Лаборатории Касперского» 66% респондентов из всего перечня угроз большего всего опасались именно целевых атак, что говорит об актуальности поднятой темы.

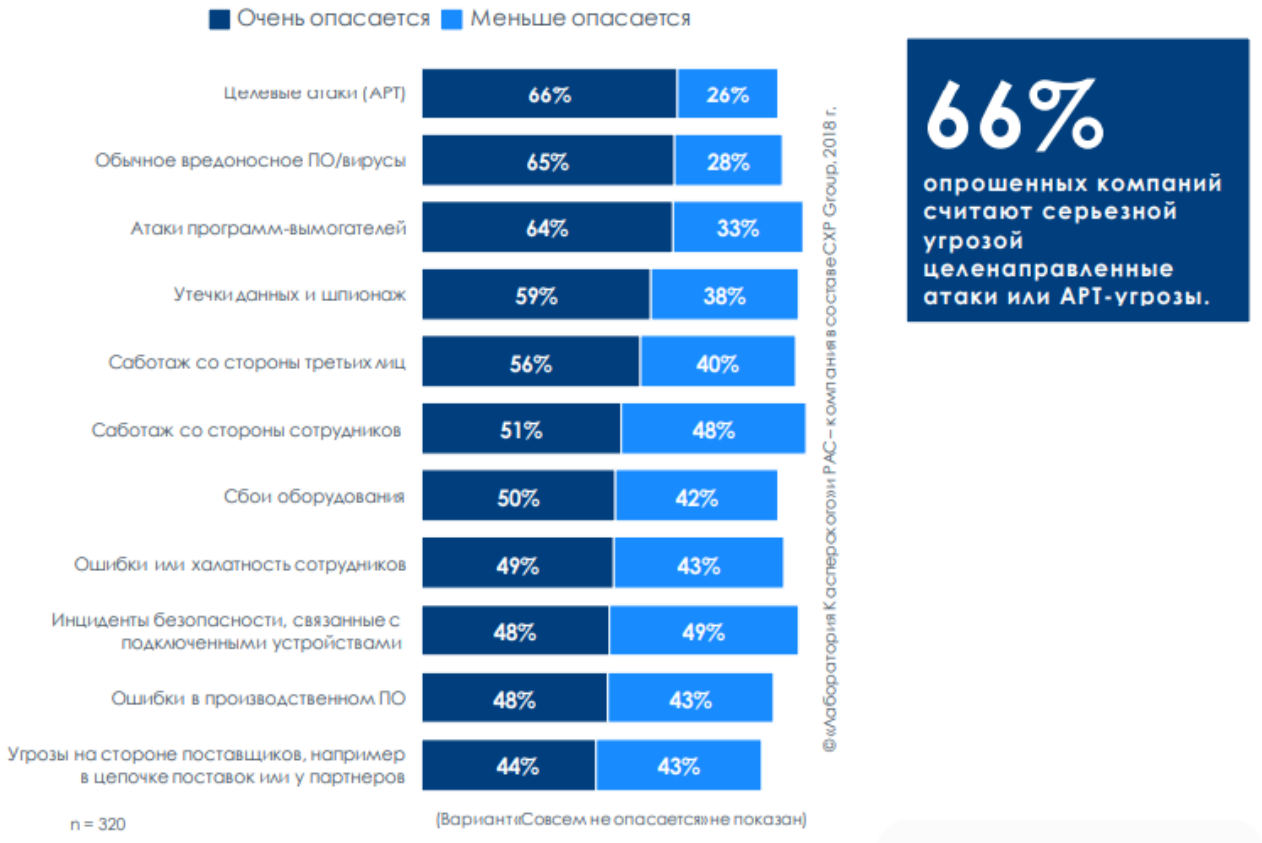

Рис. 1. - Исследование CXP Group

А значит, нужны определенные совершенствования, дополнительные правила, позволяющие KICS либо какому-либо другому средству обнаруживать эти отдельные, индивидуальные атаки.

Цель дипломной работы состоит в выявлении уязвимостей АСУ ТП, нахождении способов их реализации и предложении путей совершенствования АС обнаружения целевых атак в промышленных сетях.

Для достижения этой цели необходимо выполнить ряд задач:

- описать структуру АСУ ТП типового объекта;
- описать структуру и принцип работы KICS и KTMD;
- найти уязвимости АСУ ТП оборудования;
- найти open-source эксплойты, задействующие данные уязвимости для осуществления несанкционированного доступа (НСД) в промышленную сеть и убедиться в том, что они не распознаются стандартными средствами KICS, также найти любые другие примеры атак, не распознающихся KICS;
- предложить варианты решения, позволяющие, при реализации, сделать детект необнаруженных ранее целевых атак (YARA-правила, средства KTMD, другие вендоры).