Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:681.5-047.36

КАЗЛОВСКИЙ
Евгений Александрович

СИСТЕМА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Автореферат
на соискание степени магистра
по специальности 1–98 80 01 Информационная безопасность

_____

Научный руководитель
доктор технических наук,
профессор
БОРБОТЬКО Тимофей
Валентинович

_____

Минск 2023

ВВЕДЕНИЕ

Автоматизированная система управления технологическим процессом —это человеко-машинная система управления, обеспечивающая автоматизированный сбор и обработку информации, необходимой для оптимизации управления технологическим объектом в соответствии с принятым критерием.

Стоит отметить, что участие оператора сведено к минимуму, но все же присутствует на уровне реализации и принятия наиболее ответственных решений.

Главными целями автоматизации технологического процесса являются:

— централизованный контроль управления технологическим оборудованием;

- сбор и первичная обработка данных о процессе для обеспечения персонала актуальной информацией;

— повышение безопасности и надежности функционирования объекта;

— уменьшение влияния человеческого фактора на управляемый процесс.

Таким образом, главной целью АСУ ТП является обеспечение оптимального функционирования технологического процесса.

Как правило, АСУ ТП состоит из трех уровней, которые представляют собой единую систему операторского управления технологическим процессом в виде одного или нескольких пультов управления, средства обработки информации о ходе процесса и типовые элементы автоматики (датчики, устройства управления и исполнительные устройства).

Предлагаю рассмотреть подробнее каждый уровень. Самый нижний, первый уровень — датчики и исполнительные механизмы, передают данные от устройств по линиям связи на средний уровень. Далее идет средний уровень, который включает в себя программируемые логические контроллеры и операторские панели. Контроллеры и панели получают данные с нижнего уровня и передают на верхний уровень для принятия решения по управлению объектом или процессом. Завершает процесс верхний уровень — это операторские автоматизированные рабочие места, промышленные серверы (SCADA-серверы) с установленным на них общесистемным и прикладным программным обеспечением, телекоммуникационное оборудование (маршрутизаторы, коммутаторы), а также каналы связи. На автоматизированных рабочих местах выводится состояние технологического процесса, и отсюда при необходимости оператором подаются команды на изменение какого-либо параметра.

Угрозы АСУ ТП

Современные АСУ ТП подвержены разнообразным угрозам со стороны внутренних и внешних нарушителей (террористические, экстремистские и враждебно настроенные группы) с целью вывести систему из строя.

Необходимо отметить, что сами производители и потребители не всегда обеспечивают должную безопасность, при этом не выполняя необходимые требования по безопасности своих систем. Из-за непрерывности технологических процессов базовые компоненты систем управления (индустриальные протоколы, операционные системы, системы управления базами данных) регулярно не обновляются. Все вышесказанное в совокупности приводит к появлению уязвимостей в системе, в результате которых реализуются новые угрозы.

Сегодня для АСУ ТП наиболее актуальны угрозы сбоя, отказов и нарушения режима работы, распространение вредоносного программного обеспечения.

Реализация этих угроз непосредственно связана с:

– ошибочными действиями пользователей;

– устаревшим ПО или средствами защиты;

– подключением зараженного USB-устройств к автоматизированным рабочим местам;

– несанкционированным подключением USB-устройств к автоматизированным рабочим местам пользователей, а также к сети Интернет.

Решение данной проблемы сводится к комплексу мер, направленных на обеспечение безопасности информации в целом. Стоит отметить, что на производстве необходимо уделять внимание не только обеспечению конфиденциальности данных и информации, но и обеспечению непрерывности и целостности самого технологического процесса. Ведь мало кому будут полезны и интересны данные с датчиков, а если нарушителю удастся вывести из строя и остановить производство, это может нанести огромные ущерб предприятию.

Поэтому задача обеспечения безопасности АСУ ТП — это прежде всего обеспечение безопасности технологических процессов. Обезопасить технологические процессы — это значит оградить их от любых несанкционированных воздействий информационного характера, которые создают возможность некорректного выполнения технологических процессов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научной, научно-технической и инновационной деятельности

Тема диссертационной работы соответствует разделу 6 «Обеспечение

безопасности человека, общества и государства» приоритетных направлений научной, научно-технической и инновационной деятельности в Республики Беларусь на 2021–2025 гг., утверждённых Указом Президента Республики Беларусь 7 мая 2020 г., № 156. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке системы мониторинга информационной безопасности АС ТП.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Произвести анализ типовых АСУ ТП;
2. Определить модель нарушителя для АСУ ТП;
3. Разработать систему мониторинга информационной безопасности АСУ ТП.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XVIII Международной научно-практической конференции «Управление информационными ресурсами» (Минск, 2022).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 1 работа, в том числе 1 статья в сборнике материалов XVIII международной научно-практической конференции Академии управления при Президента Республики Беларусь.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно. Методы обеспечения информационной безопасности для АСУ ТП были разработаны соискателем.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении рассмотрены проблемы необходимости осуществления информационной безопасности в автоматизированных системах управления технологическими процессами.

В общей характеристике работы показана связь работы с приоритетными направлениями научных исследований, цель и задачи

исследования, личный вклад соискателя ученой степени, апробация результатов диссертации.

В первой главе был проведен анализ типовых автоматизированных систем управления технологическими процессами. Была рассмотрена архитектура и состав типовых автоматизированных систем управления технологическими процессами.

Во второй главе рассматривался вопрос информационной безопасности автоматизированных систем управления технологическими процессами. Приводились основные типы угроз и нарушений информационной безопасности, рассматривались стадии атаки на автоматизированные системы управления технологическими процессами, цели обеспечения информационной безопасности и стратегии защиты автоматизированных систем управления технологическими процессами

В третьей главе рассматривалась модель нарушителя в автоматизированных системах управления технологическими процессами. Была охарактеризована матрица MITRE ATT&CK для составления модели нарушителя, были определены основные TTP нарушителя и рассматривался анализ событий информационной безопасности возникающих вследствие действий нарушителя.

В четвертой главе были определены события подлежащие регистрации системой мониторинга информационной безопасности и разрабатывалась непосредственна сама система.

ЗАКЛЮЧЕНИЕ

В заключении также можно отметить следующее. Информационная безопасность является одним из наиболее актуальных и важных направлений развития современных информационных технологий. Особенно важно обеспечить безопасность в системах автоматизированного управления технологическими процессами, где нарушение безопасности может привести к серьезным последствиям, включая чрезвычайные ситуации.

Разработка системы мониторинга информационной безопасности в АСУ ТП является необходимым условием для обеспечения безопасности таких систем. Она позволяет своевременно обнаруживать угрозы безопасности, предотвращать их реализацию и минимизировать последствия нарушений.

В ходе данной работы был проведен анализ типовых автоматизированных систем управления технологическими процессами. После чего, было раскрыто понятие информационное безопасности и разобраны основные типы угроз для автоматизированных систем управления

технологическими процессами. Далее, была определена модель нарушителя для АСУ ТП.

После чего были разобраны вопросы, которые касаются непосредственно событий, которые необходимо регистрировать разрабатываемой системой. Были приведены варианты получения несанкционированного доступа нарушителем к объектам технологического процесса и исполнительным механизмам.

В ходе определения поведения нарушителя и получения им несанкционированного доступа, разрабатываемая система показала, что она удовлетворяет всем необходимым требования, для осуществления безопасности на предприятии.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

XVIII международной научно-практической конференции Академии управления при Президента Республики Беларусь, «Управление информационными ресупсами», стр. 247.