Задачи информационной безопасности автоматических систем управления

Д.А. Корнюшкин, А.А. Крылов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Аннотация: В данной работе проведен обзор основных проблем безопасности современных автоматизированных систем управления технологическими процессами (АСУ ТП) и сформулированы задачи по их устранению. Цель работы заключалась в рассмотрении безопасности современных АСУ ТП. Аварийные ситуации, связанные с последовательными ошибочными действиями обслуживающего персонала, должны предотвращать системы управления. До начала 2000-х годов АСУ ТП считались самыми безопасными системами, вследствие их работы по жесткому и выверенному алгоритму, человеческий фактор не мог на них повлиять. Для возможности дистанционного управления и мониторинга появилась необходимость подключения к сети Интернет. Вследствие увеличения количества кибератак на автоматизированные системы управления технологическим процессом, незащищенное подключение к сети Интернет стало не безопасным, и появилась новая возможность воздействовать на систему извне. Вопрос безопасности и надежности современных АСУ ТП стал еще более актуален.
Ключевые слова: Автоматизированная система управления технологическими процессами, безопасность, уязвимость

Введение

Необходимость защиты от внешних угроз - это важнейшая задача безопасности автоматизированных систем управления технологическими процессами (АСУ ТП). Тем не менее, информационной безопасности обычно уделяется недостаточно внимания. Ранее считалось, что данные информационные системы будут эксплуатироваться внутри некой локальной вычислительной сети, с управлением оператором с рабочего места, расположенного непосредственно на предприятии, и даже в непосредственной близости перед блоками индикации и внешнего управления. Большинство старых систем имело управление с внешней приборной панелью, имеющий клавиатуру ограниченной функциональности, а также жидкокристаллический индикатор, использующий режим работы либо статический режим работы, либо с бегущей строкой. Начиная с 2000-х годов, вследствие появления массового доступа в сеть Интернет, возникла

необходимость удалённого доступа к АСУ ТП, однако большинство производителей таких систем АСУ ТП не стали коренным образом перерабатывать концепцию работы устройств, а просто внедрили дополнительный блок внешнего управления, подключаемый сначала к телефонной линии и работающей по принципу передачи данных с помощью модема, а, далее, сделав блок с возможностью высокоскоростной передачи данных, осуществили его непосредственное подключение к сети Интернет [1,2]. Несмотря на явную уязвимость такого подключения, должное внимание системе безопасности соединения, и, в частности, защите от несанкционированного доступа должное внимание не уделялось. Одной из основных угроз для современных поколений АСУ ТП являются целевые внешние атаки, которые могут привести к техногенным катастрофам, огромным финансовым потерям и человеческим жертвам [3].

Возможные уязвимости АСУ ТП.

При построении АСУ ТП в России до недавнего времени было принято использовать аппаратно-программные средства и комплексы зарубежного производства, поэтому вероятность вмешательства в технологический цикл иностранными преступниками с целью разрушения критической инфраструктуры и работы социально значимых предприятий крайне высока [4,5].

Изучив опыт стран, использующих АСУ ТП, можно выделить следующие потенциальные уязвимости:

выполнение произвольного «битого» кода (загрузка вредоносных файлов);

загрузка случайных файлов;

открытие информации для доступа к базе данных.

Перечисленные вмешательства могут остановить производство и привести к аварийной ситуации.

Одной из основных причин этих уязвимостей является персонал, отвечающий за информационную безопасность. Вмешательство человека, намеренное и не преднамеренное, чаще всего служит одной из основных причин возникновения аварийных ситуаций на предприятиях. Так же не стоит забывать о «факторе руководителя», в интересах которого не останавливать работу предприятия [6,7].

Помимо аварийных ситуаций, которые происходят по вине персонала или сбоев в работе АСУ ТП, существует угроза промышленного шпионажа, целью которого является выявление слабых мест в производственном цикле и нарушение нормального цикла работы предприятия [8].

Основные элементы защиты и противодействия.

Аварийные ситуации, связанные с последовательными ошибочными действиями обслуживающего персонала, должна предотвращать система управления.

Исходя из приведенной выше статистики, можно выделить основные элементы системы защиты АСУ ТП:

управление доступом (УД)

обеспечение целостности (ОЦ)

регистрация и учет (РУ)

антивирусная защита (АЗ)

обнаружение вторжений (система ОВ)

анализ защищенности (система АЗ)

Требования к системе защиты АСУ ТП.

Безопасность систем и исправное функционирование оборудования напрямую зависит от уровня безопасности процессов. При возникновении внешних воздействий, система обязана обеспечивать безопасное функционирование во всех режимах работы. В случае ошибочных действий работников, АСУТ ТП не должна допустить создания аварийной ситуации. [9]

Защищенный закрытый доступ к данным и к управлению АСУ ТП.

Система оповещения о несанкционированном вторжении в систему, автоматическая блокировка действий злоумышленников.

Выявление отклонения в режиме работы оборудования, АСУ ТП и объекта наблюдения в целом, при помощи использования системы анализа технического состояния [10].

Все основные требования безопасности направлены на снижение риска возможного возникновения аварий и катастроф в течение различных технологических процессов.

Методы защиты АСУ ТП.

Комплексная информационная защита АСУ ТП – это совокупность методов, направленных на защиту от несанкционированного входа в систему, ее использования, уничтожения и копирования информации.

Контроль, за уровнем квалификации персонала в сфере информационной безопасности, позволит увеличить уровень безопасности АСУ ТП.

Минимизация зависимости в поставках АСУ ТП от европейских производителей и развитие отечественных систем аппаратно-программные средств АСУ ТП [9,10].

Заключение

В представленной работе был проведен краткий обзор информационной безопасности автоматизированных систем управления технологическими процессами, изучена статистика уязвимостей, а также предложены способы их устранения.

Безопасность АСУ ТП – актуальная и основополагающе важная тема. Возникновение аварийных ситуаций на предприятиях оборонно-промышленного комплекса и градообразующих предприятиях может привести к катастрофам мирового масштаба и нанести непоправимый вред всему отраслевому комплексу. С каждым годом актуальность проблемы информационной и физической безопасности АСУ ТП будет только возрастать.

Развитие технологий в области автоматизации напрямую зависит от уровня безопасности систем, чем выше будет уровень, тем более совершенными будут становиться системы АСУ ТП.

Литература

1. АСУ ТП обеспечивает безопасность технологических комплексов URL: cnews.ru/reviews/free/security2008/articles/asu.shtml. (дата обращения 4.12.21)

2. Защита информации в автоматизированных системах управления технологическими процессами (АСУ ТП) URL: arinteg.ru/services/asutp.php. (дата обращения 06.12.21)

3. Синещук. М.Ю. Особенности обеспечения информационной безопасности АСУ ТП потенциально опасных объектов URL: cyberleninka.ru/article/n/osobennosti-obespecheniya-informatsionnoy-bezopasnosti-asu-tp-potentsialno-opasnyh-obektov/viewer. (дата обращения 28.11.21)

4. Надеждин Ю. Безопасность АСУ ТП критически важных объектов URL: secuteck.ru/articles2/security-director/bezopasnost-asu-tp-kriticheski-vazhnyh-obektov. (дата обращения 28.11.21)

5. Чернов Д.В., Сычугов А.А. Современные подходы к обеспечению информационной безопасности АСУ ТП. URL: cyberleninka.ru/article/n/sovremennye-podhody-k-obespecheniyu-informatsionnoy-bezopasnosti-asu-tp. (дата обращения 26.11.21)

6. Безопасность от кибератак и аварий в АСУ ТП. URL: automation-system.ru/main/11-asutp/asu-tp/468-security-asutp.html (дата обращения 06.12.21)

7. Ибрагимова З.М., Батчаева З.Б., Ткаченко А.Л. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона, 2022, №11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010.

8. Полевщиков И.С., Боброва И.А. Автоматизация оценки эффективности обучения операторов на компьютерных тренажерах с применением статистических методов // Инженерный вестник Дона, 2022, №3. URL: ivdon.ru/ru/magazine/archive/N3y2020/6373.

9. Верлингер Р., Малднер К., Хоуки К., Безносов К. Подготовка, обнаружение и анализ: диагностическая работа по реагированию на инциденты ИТ-безопасности. Inf Manag Вычисление, раздел 18 (1): С. 26-42. URL: emerald.com/insight/content/doi/10.1108/09685221011035241/full/html.

10. Фрейтас Л., Уотсон П. (2014) Формализация разделения рабочих процессов по федеративным облакам: многоуровневая безопасность и затраты. Int J Вычислительная математика 91 (5): С. 881-906. URL: tandfonline.com/doi/abs/10.1080/00207160.2013.820282.

References

1. ASU TP obespechivaet bezopasnost` texnologicheskix kompleksov [The process control system ensures the safety of technological complexes]. URL: cnews.ru/reviews/free/security2008/articles/asu.shtml. (date assessed: 4.12.21)

2. Zashhita informacii v avtomatizirovanny`x sistemax upravleniya texnologicheskimi processami (ASU TP) [Information security in automated process control systems (APCS)] URL: arinteg.ru/services/asutp.php. (date assessed: 06.12.21)

3. Sineshhuk M.Yu. Osobennosti obespecheniya informacionnoj bezopasnosti ASU TP potencial`no opasny`x ob``ektov URL: cyberleninka.ru/article/n/osobennosti-obespecheniya-informatsionnoybezopasnosti-asu-tp-potentsialno-opasnyh-obektov/viewer (date assessed: 28.11.21)

4. Nadezhdin Yu. Bezopasnost` ASU TP kriticheski vazhny`x ob``ektov [Security of critical control systems]. URL: secuteck.ru/articles2/security-director/bezopasnost-asu-tp-kriticheski-vazhnyh-obektov. (date assessed : 28.11.21)

5. Chernov D.V., A.A. Sy`chugov. Sovremenny`e podxody` k obespecheniyu informacionnoj bezopasnosti ASU TP URL: cyberleninka.ru/article/n/sovremennye-podhody-k-obespecheniyu informatsionnoy-bezopasnosti-asu-tp (date assessed 26.11.21)

6. Bezopasnost` ot kiberatak i avarij v ASU TP [Safety from cyber-attacks and accidents in the APCS]. URL: automation-system.ru/main/11-asutp/asu-tp/468-security-asutp.html. (date assessed:06.12.21)

7. Ibragimova Z.M., Batchaeva Z.B., Tkachenko A.L. Inzhenernyj vestnik Dona, 2022, №11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010.

8. Polevshchikov I.S., Bobrova I.A. Inzhenernyj vestnik Dona, 2022, №3. URL: ivdon.ru/ru/magazine/archive/N3y2020/6373.

9. Verlinger R., Maldner K., Houki K., Beznosov K. 2010. Podgotovka, obnaruzhenie i analiz: diagnosticheskaya rabota po reagirovaniyu na incidenty IT-bezopasnosti. Inf Manag Vychislenie, razdel 18 (1): pp. 26-42. URL: emerald.com/insight/content/doi/10.1108/09685221011035241/full/html.

10. Frejtas L., Uotson P. 2014. Int J Vychislitel'naya matematika 91 (5): pp. 881-906. URL: tandfonline.com/doi/abs/10.1080/00207160.2013.820282.