УДК 004.056.5
Зайко Т.А.[1], Мироненко Н.В.[2]
[1]канд. техн. наук, доц. НУ «Запорізька Політехніка»
[2]студ. гр. КНТ-120м НУ «Запорізька політехніка»

АНАЛІЗ ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АСК ТП

В останні роки питання інформаційної безпеки систем керування технологічними процесами постало дуже гостро. Особливий інтерес виник після інцедентів з комп'ютерними вірусами, які атакували ядерні об'єкти, держустанови і промислові об'єкти у різних країнах світу.

Також великого резонансу набув випадок в Україні, який трапився у 2015 році. Тоді невідомі хакери зламали систему керування телемеханікою компанії «Прикарпаттяобленерго», яка спеціалізується на передачі та забезпеченні електроенергією споживачів Івано-Франківської області. У результаті, протягом декількох годин більша частина області і місто залишалося без електроенергії [1].

До цих випадків вважалося, що в роботу АСК ТП досить важко втрутитися, адже програмне забезпечення кожної АСК ТП є унікальним і закритим; локальна мережа АСК ТП вирішує проблеми обмеження доступу; проникнення в АСК ТП пов'язано з великими інтелектуальними витратами [2]. Однак, усіх цих обмежень виявилося недостатньо, щоб забезпечити повний захист і тому на сьогодні важливою задачею є підвищення інформаційної безпеки таких систем.

Для підвищення безпеки необхідно спочатку розглянути проблеми, які призводять до виникнення ризиків:

– слабкий захист від несанкціонованого доступу;
– недекларовані можливості SCADA;
– використання слабко захищених бездротових комунікацій;
– відсутність чітких границь між різними сегментами мережі;
– несвоєчасне чи некоректне оновлення програмного забезпечення;
– дистанційні методи керування;

– відмова або недостатня кількість засобів захисту (наприклад, відсутність антивірусу чи паролю);

– створення систем без урахування кращих практик розробки безпечного коду;

– людський фактор [3].

Для зменшення та уникнення розглянутих ризиків необхідно відслідкувати тенденції розвитку кіберзагроз при проєктуванні і розробці нових АСК ТП. Однак, оскільки змінити склад і якість АСК ТП, які введено в експлуатацію, для підвищення інформаційної безпеки є досить складне і дороге завдання, то потрібно проводити регулярну роботу з контролю та попередження потенційних загроз.

Для нейтралізації потенційних загроз використовується дві групи заходів: адміністративно-організаційні та програмно-технічні.

Перша група пов'язана з формуванням програми робіт із надання інформаційної безпеки (ІБ) АСК ТП і розробкою набору документів, які регламентують високорівневий підхід до забезпечення ІБ, а також описують політику розвитку АСК ТП [4]. Основна мета ІБ – підтримувати необхідний рівень безпеки на підприємстві, а також підтримувати неперервність виробництва

Основний набір засобів забезпечення ІБ утворюють програмно-технічні заходи. До них відносяться наступні дії:

– керування доступом;

– забезпечення цілісності;

– створення безпечної міжмережевої взаємодії;

– антивірусний захист;

– аналіз захищеності;

– виявлення вторгнень;

– неперервний моніторинг стану системи ІБ, виявлення інцедентів, реагування [5].

Перелічені дії дозволять знизити ризики та попередити потенційні загрози. Це є особливо актуальною задачею у теперішній час інформаційної війни, коли атака на небезпечний виробничий об'єкт або критично важливий об'єкт може призвести до невиправних дій.

Підводячи підсумки, варто сказати, що проблема інформаційної безпеки АСК ТП є дуже великою проблемою на сьогодні. Вона потребує негайних дій, бо незахищеність у даній сфері призводить не тільки до значної втрати грошових та часових ресурсів, а і до спричинення дискомфорту або навіть створення загрози людині.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. В Украине зафиксирована первая в истории государства успешная хакерская атака на АСУ ТП [Электрон. ресурс] – Режим доступа: http://digitalsubstation.com/blog/2015/12/25/v-ukraine-zafiksirovana-pervaya-v-istorii-gosudarstva-uspeshnaya-hakerskaya-ataka-na-asu-tp/.

2. Пищик, Б. Н. Безопасность АСУ ТП [Текст] / Б. Н. Пищик // Вычислительные технологии. 2013. – №18. – С. 170–175.

3. Стандарты безопасности АСУ ТП [Электрон. ресурс] – Режим доступа: https://www.slideshare.net/CiscoRu/ss-8690963.

4. Демидович Д. И. Современые технологии защиты информации в АСУ ТП [Текст] / Д. И. Демидович. // Сборник 56-ой научной конференции аспирантов, магистрантов и студентов БГУИР. – 2020. – С. 15–17.

5. Роль АСУ ТП на нефтеперерабатывающем заводе [Электрон. ресурс] – Режим доступа: https://cccp-online.ru/rol-asu-tp-na-neftepererabatyvayushhem-zavode/.