

УДК 681.51

Малюков М. К.¹, Зайко Т. А.²

¹студ. гр. КНТ-120м НУ «Запорізька політехніка»

²канд. техн. наук, доц. НУ «Запорізька політехніка»

ВРАЗЛИВОСТІ ПРОМИСЛОВИХ SCADA-СИСТЕМ

Промислові системи за останні десятиліття стали використовувати звичайні персональні комп'ютери, операційні системи Windows та Linux, мережеві протоколи TCP/IP, доступ до мережі Інтернет, а також веб-браузери. Це стало причиною появи нових вразливостей, недоліків та розширення можливих загроз для таких систем. Існує велика кількість вразливостей, характерних для промислових систем в АСУ ТП, які можуть бути використані зловмисником. До них належить у першу чергу людський фактор. Дослідження показали, що ті, хто відповідає за безпеку промислових систем, часто мають або недостатній рівень компетентності, або навмисно нехтують безпекою таких систем, щоб забезпечити надійність, підвищити ефективність, доступність, вирішити технологічні проблеми, що виникають під час роботи системи і мінімізувати витрати системи в цілому.

Якщо розглядати вразливості операційної системи, виправлення операційної системи часто не робляться операторами свідомо, оскільки вони не можуть вносити корективи без належної сертифікації оновлень. Тому операційні системи з добре відомими вразливими місцями часто використовуються для забезпечення безперебійної роботи SCADA-систем.

Також існує недолік у автентифікації. Використання загальних паролів є звичайною практикою для промислових систем. Багатофакторні системи автентифікації використовуються рідко, і інформація часто передається по мережі відкрито.

Для управління SCADA-системами співробітники часто встановлюють віддалений доступ через комутацію каналів або через VPN через інтернет. Це може призвести до серйозних інцидентів з інформаційною безпекою.

Незважаючи на те, що зовнішні з'єднання вкрай не рекомендуються для SCADA-систем, в інформаційному звіті CyberX зазначено, що близько 40% АСУ ТП мають пряме підключення до інтернету. Це робить такі системи легкою мішенню для зловмисників.

В АСУ ТП часто використовуються різні типи бездротового зв'язку, включаючи протоколи 802.11, які, як відомо, не забезпечують достатніх можливостей захисту.

Деякі класи пристроїв дистанційного керування, що використовуються в промислових системах для управління технологічними процесами, мають такі характеристики, які не завжди дозволяють виконувати функції безпеки.

Програмне забезпечення для промислових систем зазвичай не містить достатньо функцій безпеки. Крім того, він часто містить значну кількість архітектурних дефектів.

Також, слід враховувати, що якщо обладнання знаходиться поза контрольованою зоною, то за таких умов він не може фізично контролюватися персоналом, і єдиним механізмом фізичного захисту є використання залізних замків та дверей, що, очевидно, не є серйозною перешкодою для зловмисників.

Успішна атака може призвести до несправності SCADA-системи, пошкодження промислового обладнання, порушення виробничого процесу, зниження його якості, шкоди здоров'ю людей, флорі та фауні, порушенню екологічної безпеки та охорони праці.

Більшість SCADA-систем, які використовуються на даний момент, були розроблені більше ніж двадцять п'ять років тому і не захищені як слід, оскільки тоді не розраховували на виникнення корпоративних мереж. Оскільки вони не призначені для роботи в мережі, більшість SCADA-систем, що використовуються у критичній інфраструктурі, не захищені належним чином, саме тому при проєктуванні нових необхідно враховувати усі вищезазначені недоліки задля створення якісного програмного продукту.