

# АНАЛІЗ ВЗАЄМОЗВ'ЯЗКУ МІЖ ЗАГРОЗАМИ, ВРАЗЛИВОСТЯМИ ТА РИЗИКОМ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

С. А. Леус<sup>1</sup>, О. Є. Архипов<sup>1</sup>

<sup>1</sup>Національний технічний університет України «Київський політехнічний інститут»

## Анотація

В роботі проведено аналіз загроз захисту інформації в автоматизованих системах управління технологічними процесами та джерел їх виникнення. Здійснено аналіз вразливостей інформаційної безпеки автоматизованих систем управління технологічними процесами, класифікація та причини їх виникнення. Досліджено взаємозв'язки між загрозами, вразливостями і ризиком для автоматизованих систем управління технологічними процесами.

**Ключові слова:** Ключові слова: загроза, захист інформації, автоматизовані системи управління, вразливості, ризик.

## Вступ

На момент появи автоматизовані системи керування технологічними процесами (АСУ ТП) мали вигляд ізольованих автоматизованих систем, які функціонували на базі вузькоспеціалізованого обладнання і програмного забезпечення. Тому задача забезпечення інформаційної безпеки (ІБ) АСУ ТП достатньо успішно вирішувалась організаційними методами – в основному шляхом забезпечення фізичного захисту компонентів системи і роботою з обслуговуючим персоналом. Проте, для скорочення витрат на створення і впровадження систем, забезпечення взаємодії з бізнес-додатками і підтримки віддаленого доступу системи все частіше стали інтегруватись з корпоративною інформаційною інфраструктурою. Цей підхід приніс не лише переваги, а й нові ризики – АСУ ТП зазнали впливу нових загроз. Для вирішення задач по забезпеченню інформаційної безпеки АСУ ТП необхідні дослідження їх загроз, вразливостей, ризиків та взаємозв'язків між ними.

## 1. Загрози захисту інформації в АСУ ТП

Загрози інформації класифікують за результатом їх впливу на інформацію. Всі деструктивні впливи на інформацію є похідними від трьох найбільш загальних: порушення конфіденційності (витік інформації), цілісності (модифікація) та доступності (відмова в обслуговуванні) [1]. Деструктивні впливи на АСУ ТП:

- втрата керованості технологічного процесу (блокування керування, несанкціоноване керування);
- втрата спостереженості технологічного процесу (фальсифікація вимірів датчиків);
- модифікація параметрів технологічного процесу (параметри нормального режиму, установки протиаварійного захисту);

- відмова в обслуговування (аварія чи зупинка технологічного процесу, деградація обчислювальних ресурсів).

Тобто, на відміну від атак на автоматизовані системи інших видів, атака на АСУ ТП має на меті не викрадення інформації, а вплив на фізичний об'єкт або технологічний процес.

## 2. Джерела загроз інформаційної безпеки АСУ ТП

Джерела загроз інформаційної безпеки АСУ ТП не відрізняються від інших АС. Навмисні джерела загроз:

### 1) Зовнішні:

- розвідки іноземних держав;
- терористи;
- злочинні спілки;
- промисловий шпіонаж;
- хакери шляхом шкідливого ПЗ (віруси, трояни, черви) і різних інструментів.

### 2) Внутрішні:

- нинішні і колишні працівники.

Ненавмисні джерела загроз:

- складність системи;
- помилки працівників;
- аварії;
- відмови обладнання.

Природні джерела загроз:

- стихійні лиха;
- кліматичні умови.

## 3. Вразливості АСУ ТП

Вразливістю є недолік або слабе місце інформаційної системи, системи безпеки, процедур внутрішнього контролю, які можуть бути використані для порушення цілісності або доступності системи та її коректної роботи [2]. Класифікація вразливостей ІБ АСУ ТП показана на рис. 1.

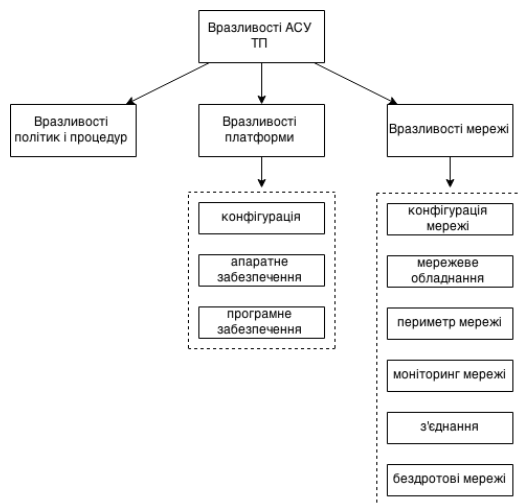


Рис. 1. Класифікація вразливостей інформаційної безпеки АСУ ТП

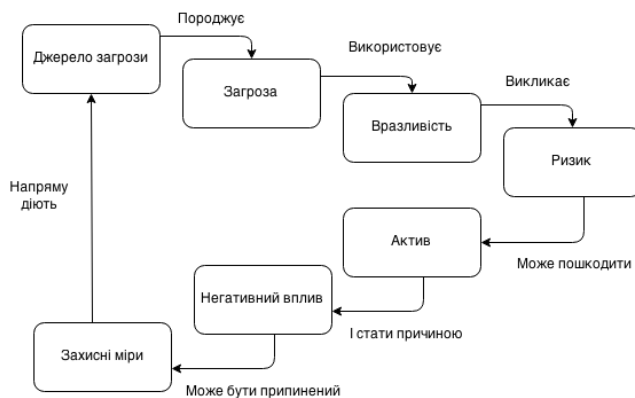


Рис. 2. Взаємозв'язок між загрозами, вразливостями і ризиком

#### 4. Взаємозв'язок між загрозами, вразливостями і ризиком

Причинами виникнення загроз інформації являються дестабілізуючі фактори — явища чи події, які можуть з'являтися на будь-якому етапі життєвого циклу системи. Наслідком виникнення дестабілізуючих факторів може бути ризик інформаційної безпеки — ймовірність того, що певна загроза використає уразливість системи, в результаті чого буде нанесено шкоду компонентам системи [3]. Отже, порушення інформаційної безпеки — це виникнення і реалізація загроз. Загроза, яка не має відповідної уразливості, може не призводити до ризику. І навпаки, наявність уразливості не завдає шкоди сама по собі, так як необхідна наявність загрози, яка скористається нею. Взаємозв'язок між загрозами, вразливостями і ризиком приведений на рис. 2 [4].

#### 5. Результати досліджень

Вразливості політик і процедур в промислових автоматизованих системах управління виникають через відсутність або неповну, неадекватну документацію в галузі безпеки, у тому числі політик і керівництва (процедур), адміністрування аудиту, відновлення. Вразливості платформ в АСУ ТП можуть виникати через недоліки, помилки, або неякісне обслуговування своїх платформ, у тому числі обладнання (апаратні засоби, операційні системи і додатки), відсутність контролю фізичного доступу. Вразливості мережі в промислових автоматизованих системах управління можуть виникати через недоліки, помилки, погане адміністрування мереж. Ці уразливості можуть бути усунені або нівельовані за допомогою правильного проектування мережі, шифрування мережевих з'єднань, забезпечення контролю фізичного доступу до мережевих компонентів.

#### Висновки

З метою вирішення задач по забезпеченню інформаційної безпеки автоматизованих систем управління технологічними процесами проведено аналіз загроз захисту інформації та детальний опис джерел загроз. Здійснено аналіз вразливостей інформаційної безпеки автоматизованих систем управління технологічними процесами, класифікація та причини їх виникнення. Дані рекомендації щодо усунення або нівелювання даних вразливостей. Досліджено взаємозв'язки між загрозами, вразливостями і ризиком для автоматизованих систем управління технологічними процесами. Отримані результати в подальшому можна використовувати для оцінки ризиків інформаційної безпеки в АСУ ТП.

#### Перелік використаних джерел

1. Power systems management and associated information exchange — Data and communications security: IEC 62351-1. — Part 1: Communication network and system security — Introduction to security issues. — 2007. — с.12. —
2. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. — Recommendations of the National Institute of Standards and Technology. — 2011. — с.3.
3. Information technology — Security techniques — Information security risk management: BS ISO/IEC 27005:2010. — 2010. — с.5.
4. Industrial communication networks — Network and system security: IEC 62443, Part 3. — 2005. — с.6.