УДК 004.056.5

Лаковський Б.А., Сиропятов О.А., Тимошенко Л.М.

Національний університет «Одеська політехніка»

ПОТОЧНИЙ СТАН ТА ПРОБЛЕМАТИКА ВПРОВАДЖЕНЯ ЗАХИСТУ ІНФОРМАЦІЇ У ДЕРЖАВНИХ ПРОМИСЛОВИХ СИСТЕМАХ

Вступ.У сучасних умовах цифровізації промисловості питання захисту інформації на державних об'єктах набуває стратегічного значення для національної безпеки. Особливу роль у цьому аспекті відіграють автоматизовані системи управління технологічними процесами (АСУ ТП), які забезпечують безперервне функціонування виробничих і енергетичних об'єктів.

На відміну від звичайних корпоративних мереж, більшість систем АСУ ТП на державних промислових підприємствах мають власну ізольовану мережеву інфраструктуру, спеціалізовані операційні системи, контролери та промислові протоколи зв'язку. Зазвичай такі системи не під'єднані безпосередньо до мережі Інтернет або корпоративних IT-мереж, що створює ілюзію високого рівня безпеки.

Проте ізольованість не гарантує абсолютного захисту. Практика міжнародних і вітчизняних кіберінцидентів свідчить, що навіть ізольовані технологічні системи можуть мати приховані канали зв'язку або бути скомпрометовані - через помилки конфігурації, неконтрольоване використання переносних носіїв, сервісні підключення, бездротові модулі або втручання внутрішніх користувачів. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» №2163-VIII від 5 жовтня 2017 року, державні промислові об'єкти, що забезпечують функціонування енергетичних, транспортних, оборонних і виробничих систем, відносяться до об'єктів критичної інформаційної інфраструктури (КІІ). Порушення роботи таких об'єктів може призвести до масштабних наслідків - від зупинки виробництва до виникнення техногенних аварій.

Дані аспекти роблять проблему захисту інформації АСУ ТП особливо складною та актуальною.

Мета: Оцінка актуального стану впровадження захисту інформації на державних промислових об'єктах, аналіз основних проблем та ризиків кібербезпеки в ізольованих автоматизованих системах управління технологічними процесами.

1. Поточний стан впровадження захисту інформації

Більшість державних промислових підприємств сьогодні реалізують заходи із впровадження комплексних систем захисту інформації (КСЗІ) відповідно до вимог Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ) України [1].

Основні кроки - створення локальних політик інформаційної безпеки, аудит технологічних сегментів, моніторинг доступу до контролерів та операторських станцій, а також фізичну ізоляцію критичних вузлів.

Однак значна частина обладнання функціонує на базі застарілих промислових операційних систем (наприклад, Windows XP Embedded, VxWorks,

QNX), для яких не існують актуальні оновлення безпеки. Додаткову загрозу становить можливість прихованого або несанкціонованого підключення таких систем до зовнішніх мереж - наприклад, через неналежне адміністрування доступу персоналу, використання сервісних ноутбуків або несанкціоноване втручання підрядних організацій.

Практика міжнародних інцидентів, таких як атака Stuxnet [2], доводить, що навіть повністю ізольовані мережі можуть стати об'єктом цілеспрямованого кібервпливу.

Тож навіть у закритих промислових середовищах існує ризик появи «мостів зв'язку», які потенційно можуть бути використані зловмисником для несанкціонованого доступу або проникнення шкідливого програмного забезпечення.

Сьогодні в Україні поступово впроваджується комплексна політика забезпечення кіберзахисту об'єктів критичної інфраструктури відповідно до вимог постанови КМУ № 518 [3].

Проте практична реалізація цих вимог у державних промислових системах часто наражається на нестачу фінансування, відсутність сертифікованих рішень, сумісних із застарілим обладнанням, та недостатній рівень підготовки персоналу у сфері кіберзахисту.

Таким чином, актуальність захисту інформації на державних промислових об'єктах зумовлена поєднанням високої технологічної залежності виробництва, інертності модернізації технічних систем та необхідності виконання сучасних нормативних вимог.

Подальший розвиток системи захисту інформації потребує поєднання заходів нормативного, технічного та організаційного характеру, зокрема розроблення адаптивних механізмів кіберзахисту для ізольованих мереж АСУ ТП без порушення їхньої функціональної стабільності.

2. Проблематика впровадження кіберзахисту в промислових системах

Інертність оновлення виробничих систем. Промислове обладнання має довгий життєвий цикл - 15-30 років, тому його модернізація або заміна є складним і витратним процесом. Це створює розрив між рівнем актуальних кіберзагроз і можливостями реагування.

Обмежена сумісність старих систем із сучасними засобами захисту. Часто контроллери, ПЛК та SCADA-сервери не підтримують нові стандарти безпеки або протоколи шифрування, що унеможливлює пряме впровадження типових IT-рішень.

Людський фактор та внутрішні загрози. Через відсутність централізованих політик безпеки персонал може несвідомо підключати до промислових систем зовнішні пристрої (USB-накопичувачі, модеми тощо), що створює потенційні канали зараження або віддаленого доступу.

Відсутність механізмів моніторингу в реальному часі. У багатьох АСУ ТП відсутня система відстеження аномалій або подій безпеки, що дозволяє виявляти підключення неавторизованих пристроїв.

Нормативна та організаційна фрагментарність. Попри наявність загальних законів і стандартів (наприклад, НП 306.2.237-2022 [4]), практичні методики

побудови кіберзахисту для ізольованих технологічних мереж у державному секторі поки що не мають уніфікованої регламентації, не встановлюють часові вимоги до модернізації обладнання, що не відповідає вимогам з точки зору захисту інформації [5].

Також варто зазначити, що документальна база розглядає захист інформації мережевих систем, обладнання «де-факто» в контексті кіберпростору, що зміщує важливість захисту ізольованих промислових систем на другий план.

Висновок. Промислові системи управління не є гарантовано захищеними лише через свою відокремленість від мереж загального користування. Навпаки, відсутність постійного контролю, обмежені механізми оновлення та людський фактор створюють приховані вектори загроз, які часто складно виявити.

З огляду на інертність модернізації обладнання, державним промисловим об'єктам необхідно реалізовувати поетапну стратегію підвищення кіберстійкості, що містить:

– аудит ізольованих мереж та виявлення потенційних каналів доступу;

– впровадження систем моніторингу (SIEM/IDS) у межах закритого сегменту;

– контроль дій персоналу та політику використання зовнішніх носіїв;

– розробку планів реагування на інциденти згідно з вимогами ISO/IEC 27035:2023.

Комплексний підхід до захисту інформації в ізольованих промислових системах повинен бути складовою державної стратегії з кібербезпеки, відповідно до Стратегії кібербезпеки України (Указ Президента №447/2021). Лише поєднання технічних, організаційних і кадрових заходів дозволить забезпечити належний рівень інформаційної безпеки в умовах сучасних загроз сьогодення.

Перелік використаних джерел.

1. ДССЗЗІ. Нормативні документи ТЗІ. URL: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024

2. Wikipedia. Stuxnet – malicious computer worm. URL:https://wikipedia.org/wiki/Stuxnet

3. Постанова Кабінету Міністрів України № 518 від 19.06.2019 року «Про затвердження Порядку забезпечення кіберзахисту об'єктів критичної інфраструктури».

4. НП 306.2.237-2022 "Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій" (2022 р.)

5. О.А. Сиропятов, Л.М. Тимошенко, І. В. Назарова, Н. Г. Козаченко. Експрес-аудит як інструмент оцінки вразливостей в системах обробки даних: підходи, методики та рекомендації. Інформатика та математичні методи в моделюванні. 2024.Том 14, № 4. С.391-404. DOI 10.15276/imms.v14.no4.391