МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Захист інформації в спеціалізованих ІТС

Практичне заняття №2

Інформаційний аналіз документів ЄС з питань кібербезпеки спеціалізованих систем

Перевірив:
Зубок В. Ю.

Виконав:
студент І курсу
групи ФБ-41мп
Сахній Н. Р.

Київ 2025

Завдання `(Варіант №10: Парний)`**:** Зробити аналіз документу «Protecting Industrial Control Systems. Recommendations for Europe and Member States» (Захист систем промислового управління. Рекомендації для Європи та країн членів) та зробити за ним анотований звіт.

1. Чому в захисті ICS багато уваги приділяється захисту інформації?

Як під час вторинного дослідження, так і під час аналізу анкет було виявлено, що однією з найбільших проблем, з якими стикаються оператори ІКС, є створення програм безпеки, які інтегрують усі аспекти кібербезпеки, поєднуючи настільні та бізнес-обчислювальні системи разом з промисловими системами автоматизації та управління. Багато організацій мають досить детальні та повні програми інформаційної безпеки для своїх бізнес-обчислювальних систем, але практики управління інформаційною безпекою для ІКС поки що не настільки ж повно розроблені.

Це призводить до інформаційного дисбалансу між бізнесом і виробництвом, тому захист інформації в ICS важливий через цей розрив між добре розвиненими програмами інформаційної безпеки в IT (офісні, бізнес-системи) і слабко охопленими практиками у сфері автоматизованого керування. Через злиття IT- та ICS-середовищ і виникає потреба у єдиній інтегрованій системі захисту, що охоплюватиме обидва світи.

“6.1.3 Challenge 3: The lack of integrated management of ICS security (KF 1.3)”, ст. 14

2. Які ключові висновки стосуються захисту інформації в ICS?

Окрім наведеного висновку у відповіді до попереднього завдання, також до ключових висновків (“Key Findings”), що стосуються захисту інформації в ICS (промислових системах) можна віднести наступне:

- Низький рівень впровадження стандартів та практик (*6.3.5 Low level of adoption of security guidelines and standards (KF 3.5), ст. 18*)

Учасники опитування ENISA вказали, що більшість з них або лише розробляє плани безпеки для ICS, або знаходиться на етапі початкового аналізу ризиків. Це свідчить про

недостатню зрілість підходів до захисту інформації в ІКС на відміну від ІТ-систем, де подібні практики є вже більш усталеними та перевіреними.

- Управління ризиками має бути включено до плану безпеки (*6.4.3 Risk Management to be included in the ICS security plan (KF 4.3), ст. 20*).

ENISA рекомендує організаціям здійснювати оцінку поточного рівня безпеки ІКС та аналіз наявних ризиків, враховуючи інформаційними потоками та залежності між компонентами системи. Адже саме ці зв'язки визначатимуть потенційний вплив інцидентів на фізичні процеси та стабільність функціонування підприємства.

- ICS імпортує ІКТ-рішення та проблеми цих ІКТ & Звичайні ІКТ-рішення потребують подальшої адаптації до сценаріїв ICS (*6.12.2 Regular ICT solutions need to be adapted further to the ICS scenario (KF 12.2), ст. 28* & *6.12.1 ICS importing the ICT solutions and the ICT problems (KF 12.1), ст. 28*).

Наголошується, що за останні роки в середовищі ІКС усе ширше використовуються ІКТ-рішення на основі TCP/IP, але водночас разом із цими перевагами – ICS «успадкували» й притаманні ІКТ-вразливості, зокрема баги, властиві комплексним ПЗ.

Попри поступову інтеграцію ІТ-рішень, більшість із них усе ще не адаптовані належним чином до специфічного ICS-середовища. Наприклад, Deep Packet Inspection (глибокий аналіз трафіку) в індустріальних міжмережевих екранах поки що підтримує лише обмежену кількість промислових протоколів. IDS/IPS-рішення також потребують створення спеціалізованих сигнатур та впровадження методів виявлення кібератак, орієнтованих на промислові системи. Інші технології, такі як Data Loss Prevention (захист від витоку даних), поки що мають низьку прийнятність у сфері ICS, хоча водночас вже можуть бути корисними при обробці історичних або бізнес-даних.

3. Які рекомендації запропоновані в результаті аналізу висновків?

На основі ключових висновків запропоновано 7 рекомендацій щодо покращення безпеки ICS для державного та приватного секторів, залучених до сфери промислових

систем керування. Сім рекомендацій пов’язані між собою та є однаково важливими, адже стосуються різних питань безпеки (*1. Executive summary: Recommendation 1-7, ст. 2-3*):

1) **Створення загальноєвропейської та національної стратегій безпеки ICS**

   Дана рекомендація представляє собою основу, відповідно до якої слід включити та тлумачити наступні рекомендації.

   Пропонується розробити загальноєвропейську та національні (для кожного з держав-членів) стратегії безпеки ICS. Ці стратегії мають узгоджуватися з існуючими нормами та використовувати існуючі ініціативи, державно-приватні партнерства, а також сприяти обміну ініціативами, стимулювати наукові дослідження.

2) **Створення посібника з передової практики безпеки ICS**

   ЄС пропонує розробити набір документів, який би включав фізичні та логічні аспекти безпеки, що служитимуть орієнтиром для впровадження передових практик безпеки ICS для зацікавлених сторін.

3) **Створення шаблонів планів безпеки ICS**

   Національні стратегії мають створювати шаблони планів безпеки ICS, які можна адаптувати під конкретні ситуації.

   Це дозволить знизити витрати на розробку планів безпеки та прискорить впровадження комплексних заходів безпеки в галузі.

4) **Сприяння обізнаності та навчанню**

   Сприяння розповсюдженню та просвітницькій діяльності, шляхом створення навчальних програм та освітніх заходів для будь-яких працівників.

5) **Створення спільного випробувального стенду або, як альтернатива, системи сертифікації безпеки ICS**

Спільна стратегія має призвести до створення випробувального стенду, на якому можна буде проводити випробування, щоб гарантувати, що взаємодія різних систем не призведе до збоїв у системі безпеки.

В якості альтернативи можна було б визначити модель системи безпеки, адаптовану для ICS, і на основі цієї системи проводити сертифікацію.

6) **Створення національних можливостей реагування ICS-інциденти**

Пропонується створити національні можливості для реагування на комп'ютерні інциденти в сфері ICS у співпраці з відповідною кількістю державних та приватних центрів реагування на надзвичайні ситуації (CERT).

7) **Сприяти дослідженням у сфері безпеки ICS, використовуючи існуючі науково-дослідницькі програми**

Національні та спільні стратегії безпеки ICS повинні сприяти проведенню досліджень для вирішення поточних і майбутніх загроз та викликів, таких як інтеграція ICS та ІКТ, наявність застарілого або небезпечного обладнання, цілеспрямовані атаки чи проблеми «розумних мереж».

Ці рекомендації призначені, перш за все, для державних органів та органів влади, а саме для національних та європейських. Однак вони також спрямовані на інших зацікавлених сторін, таких як виробники, інтегратори та оператори ICS, постачальники інструментів та послуг безпеки, академічні кола та науково-дослідні установи, а також органи стандартизації, що мають на меті надати корисні та практичні поради, спрямовані на вдосконалення поточних ініціатив, посилення співпраці, розробку нових заходів та передового досвіду, а також зменшення бар'єрів для обміну інформацією.