Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»

«Automation and Development of Electronic Devices»

ADED-2020

(Випуск 2)

[електронне видання]

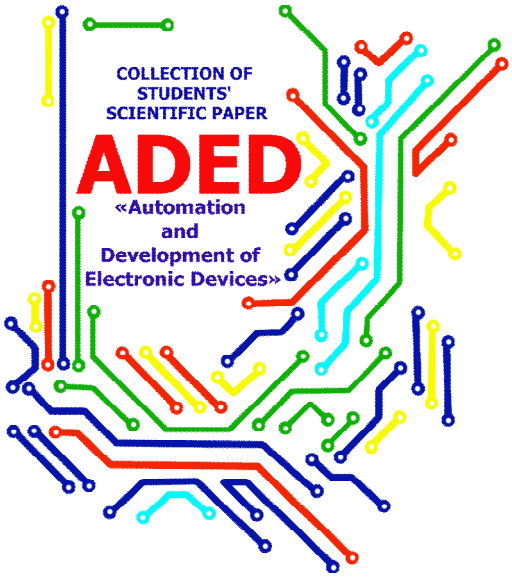
http://nure.ua/department/kafedra-komp-yuterno-integrovanih-tehnologiy-avtomatizatsiyi-ta-mehatroniki-kitam

http://itez.zntu.edu.ua/

http://kafea.kdu.edu.ua

Харків 2020

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
кафедра комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки
(КІТАМ)



ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»

«Automation and Development of Electronic Devices»

ADED-2020

(Випуск 2)

[електронне видання]

Харків 2020

АВТОМАТИЗАЦІЯ ТА ПРИЛАДОБУДУВАННЯ («Automation and Development of Electronic Devices» ADED-2020) [Електронний ресурс] : збірник студентських наукових статей / Харківський національний університет радіоелектроніки ; [редкол.: І.Ш. Невлюдов та ін.]. – Харків : ХНУРЕ, 2020. – Вип. 2. – 298 с.

COLLECTION OF STUDENTS' SCIENTIFIC PAPER «AUTOMATION AND DEVELOPMENT OF ELECTRONIC DEVICES» ADED-2020 Part 2 (Key infrastructure 2020) - Kharkiv/ The Editorial.: Nevlyudov I.Sh. (head), that all. Kharkiv: Kind of Kharkiv National Universitety of Radio Elektronics [electronic edition], 2020.- 298 p with.

Рекомендовано рішенням
Науково-технічної ради
Харківського національного
університету радіоелектроніки
протокол №6 від 29.11.2018

Рекомендовано рішенням Вченої ради
факультету Автоматики і комп'ютеризованих
технологій
Харківського національного
університету радіоелектроніки
протокол № 2 від 23.11.2020

Збірник містить наукові статті студентів кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки (КІТАМ) Харківського національного університету радіоелектроніки, кафедри Інформаційних технологій електронних засобів (ІТЕД) Запорізького національного технічного університету та кафедри Електронних апаратів (ЕА) Кременчуцького національного університету ім. М. Остроградського які навчаються за спеціальностями: 151 Автоматизація та комп'ютерно-інтегровані технології, 172 Телекомунікації та радіотехніка, 171 Електроніка та 163 Біомедична інженерія, першого (бакалаврського), другого (магістерського) рівнів вищої освіти. Статті надані в авторській редакції.

7. Мікросистемна техніка та нанотехнології [Текст]: монографія/ І. Ш. Невлюдов, В. А. Палагін,/ Київ НАУ, 2017. – 528 с.
8. Емельянович А. А., Коваль С. В. Современные технологии продвижения продукции: промышленный дизайн //ББК 65.9 (2Рос) я43 А43. – 2019. – С. 364.

Науковий керівник: *Чала Олена Олександрівна, старший викладач кафедри КІТАМ Харківського національного університету радіоелектроніки*

УДК 621.315

ЗАСОБИ ЗАХИСТУ СИСТЕМ ПРОМИСЛОВОЇ АВТОМАТИЗАЦІЇ ТА УПРАВЛІННЯ

Шило Н. Ю.
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки, 14
E-mail: nazar.shylo@nure.ua

Анотація: Системи промислової автоматизації та управління (IACS) завжди було вразливі до загроз ззовні. Одним із ключових чинників стабільної роботи таких систем є забезпечення безпеки та надійності за допомогою різних засобів та персоналу.

Ключові слова: загроза, захист, демілітаризована зона.

MEANS OF PROTECTION OF INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS

N. Shylo
Kharkiv National University of Radioelectronics
Ukraine, 61166, Kharkiv, Nauky av., 14
E-mail: nazar.shylo@nure.ua

Abstract: Industrial automation and control systems (IACS) have always been vulnerable to external threats. One of the key factors in the stable operation of such systems is to ensure security and reliability through a variety of tools and staff.

Key words: загроза, захист, демілітаризована зона.

Промислові системи автоматизації та управління є невід'ємною рушійною силою розвитку та нових технологій. Але в той же час вони є вразливими і досить нестабільними через загрози ззовні. Як і раніше, так і зараз особливе місце в працездатності таких систем посідає захист та запобігання атакам ззовні.

Дана стаття вводить деякі рекомендації, спрямовані на висвітлення того, які аспекти безпеки слід враховувати під час проектування систем автоматизації. Обов'язкова безпека, яка не враховується на даному етапі (безпека на етапі розробки), часто випробовується і в той же час з багатьма помилками. Однак важливо розуміти, що неможливо створити повністю безпечну систему проти будь-якої кібератаки.

У цій галузі проводиться багато досліджень. Організація стандартів NIST надає деякі стратегії проектування в цьому напрямку [1]. Але вони теж є вразливими. У США ICS-CERT [2] націлений на зменшення ризиків у межах усієї критичної інфраструктури секторів. Так само у Великобританії Центр захисту Національної інфраструктури (CPNI) забезпечує захист рекомендацій щодо безпеки [3]. Прийняття Індустріального Інтернету у всьому світі вивчається Індустріальним Інтернет-консорціумом. Там представлений документ, покликаний розширити розуміння основних архітектурних питань та створити консенсус з особливою увагою щодо безпеки, довіри та конфіденційності в промислових умовах.

Ці вказівки щодо кібербезпеки спрямовані на технічний характер та нетехнічні профілі, щоб показати їх чіткою і зрозумілою мовою, яка є основним пунктом, що слід врахувати, з точки зору кібербезпеки, при побудові систем промислової автоматизації та управління.

Існує декілька способів захистити такі системи від зовнішніх загроз. Класифікуємо їх в наступних блоках (рис. 1):

1) мережева архітектура;
2) конфігурація брандмауера;
3) контроль доступу та захищений зв'язок;
4) моніторинг мереж систем промислової автоматизації та управління;
5) запобігання зловмисному програмному забезпеченню;
6) політика та процедури;
7) аудит безпеки.

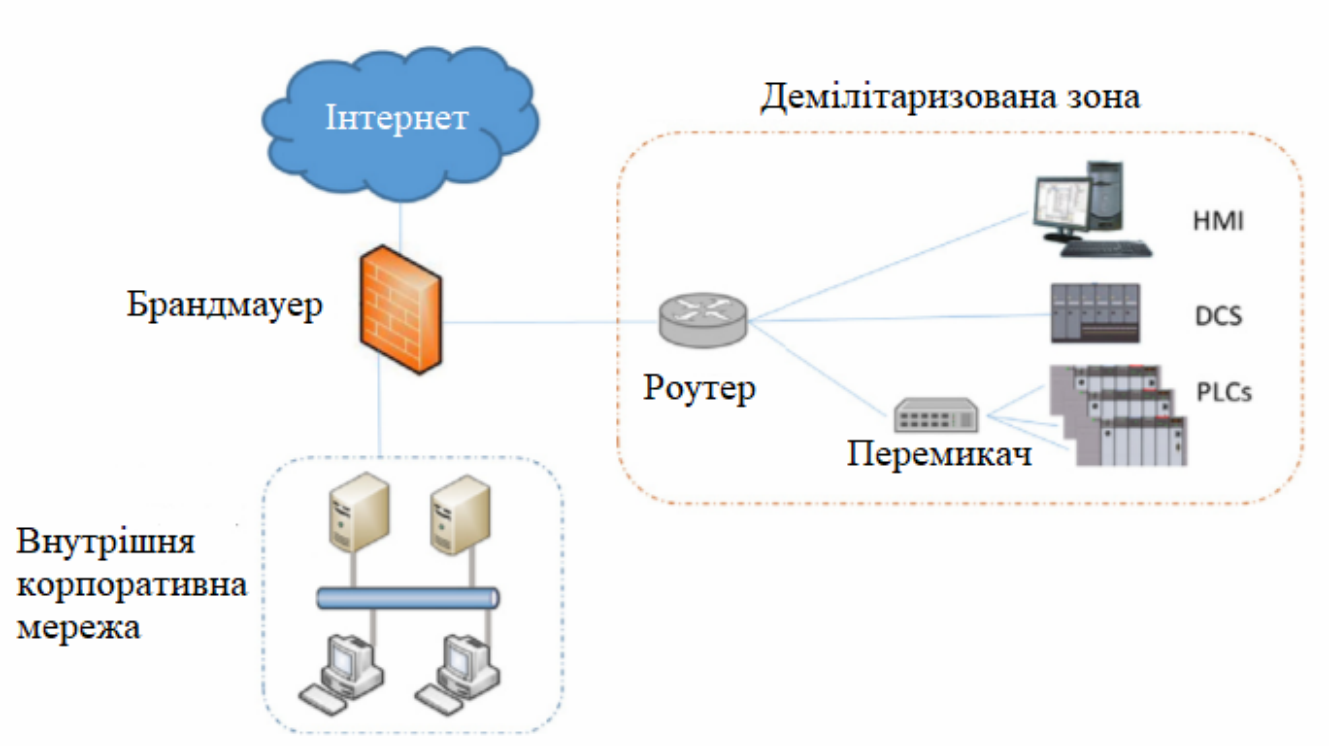


Рисунок 1 – Базова схема демілітаризованої зони з брандмауером

Мережева архітектура. Корпоративні мережі та мережі систем промислової автоматизації та управління повинні бути відокремлені для поліпшення комп'ютерної безпеки, використовуючи різні конфігурації. Вони вимагають використання і реалізацію одного або декількох брандмауерів та створення демілітаризованої зони [4].

Демілітаризована зона – це ізольована зона, яка відповідає приватній мережі між корпоративною мережею та ззовні. При правильному налаштуванні, зона захищає безпосередній доступ та доступ до обчислювальних ресурсів всередині від зовнішніх користувачів, забезпечуючи більш високий рівень надійності, контролю та фільтрації.

Для прийнятного рішення безпеки дві області можуть бути реалізовані з використанням двох брандмауерів, але їх слід застосовувати з особливою обережністю. Найбезпечніше, кероване та масштабоване рішення для сегрегації систем промислової автоматизації та управління і корпоративних мереж, як правило, засноване на створенні щонайменше з трьох областей, включаючи одну або декілька демілітаризованих зон, як показано на рис.2.

Конфігурація брандмауера. Правильно налаштований брандмауер може значно обмежити небажаний доступ до/з комп'ютерів та контролерів-хостів систем промислової автоматизації та

управління, покращуючи безпеку та потенційно покращуючи реагування мережі управління шляхом усунення несуттєвого мережевого трафіку.

Дана конфігурація дозволяє створювати правила для конкретних сервісів, як DNS, HTTP, FTP або TFTP, Telnet, SMTP, SNMP, DCOM, SCADA та промислові протоколи. Для систем промислової автоматизації та управління необхідно врахувати ряд питань, пов'язаних з конфігурацією брандмауера, таких як віддалений доступ, багатоадресний трафік, одиничні точки відмови, відмовостійкість та надмірність.

Рис. 2 – Брандмауер та демілітаризована зона між мережею систем промислової автоматизації та управління

Базова конфігурація, яка працює у багатьох випадках, незважаючи на покарання за продуктивність, викликану брандмауером, включає наступні правила:

1) неприйняття усіх зв’язків (повідомлень) окрім тих, які позначені як відомі або допущені раніше;

2) визначення джерела та призначення IP-адреси;

3) використання даних перевірки для моніторингу активних з'єднань і вирішення, які пакети дозволені;

4) використання глибокої перевірки пакетів для моніторингу вмісту трафіку зв'язку, а не лише заголовків.

Використання різних протоколів в окремих мережах, коли це можливо, наприклад, між демілітаризованою зоною та корпоративною мережею або мережами систем промислової автоматизації та управління показано на рис. 2

Контроль доступу та захищений зв’язок. Контроль доступу включає політику автентифікації та авторизації для управління мережевим доступом, захист віддаленого доступу. Іншим важливим питанням є введення методів шифрування для надсилання важливих даних.

Політика автентифікації та авторизації запроваджує механізми захисту в додатках, перевіряючи унікальна ідентичність користувачів (автентифікація) та надаючи доступ до пристроїв та операцій (авторизація). Заходи безпеки повинні забезпечувати будь-які механізми автентифікації мережевого доступу. Часто системи промислової автоматизації та управління включають лише механізми автентифікації низької ємності. Вищий рівень безпеки повинен включати не тільки використання чогось, що знає користувач (наприклад, пароль), але також і те, що користувач має (наприклад, документи або будь-яка біометрична характеристика), щоб переконатися, що це дійсно той користувач.

Контроль доступу повинен дозволяти ідентифікувати режим доступу та походження, дотримуючись унікальних рекомендацій ідентифікації, рольового дозволу та принципу найменшого привілею з обмеженими підключеннями ,які визначаються фільтрацією за портами, додатками, користувачами, а також зашифрованим зв'язком.

У цьому випадку рекомендується створення віртуальних приватних мереж (VPN), щоб захистити трафік між кінцевими точками і, таким чином, захистити інформацію від перехоплення. У таких мережах необхідно шифрувати дані, які переходять від однієї точки до іншої. Шифрування – це процес перетворення з використанням алгоритму, який надає інформацію, яку можна розшифрувати лише за допомогою ключа. VPN може базуватися на наборі протоколів для забезпечення захисту даних IPSec [5-9]. Крім того, використання захищених протоколів, таких як SSH або SFT, рекомендується для всіх з'єднань.

Рекомендується використовувати найпоширеніші промислові протоколи без надсилання та отримання інформації до/від корпоративнтх мереж. Створення різних робочих зон з правилами через брандмауери та моніторинг руху дозволить контроль доступу.

Особливу обережність слід дотримуватися при шифруванні механізмів, оскільки вони можуть перевантажувати елементи обробки. Крім того, ефекти введеної затримки та тремтіння повинні враховуватись, щоб відповідати вимогам програм реального часу.

Моніторинг мереж систем промислової автоматизації та управління. Агресори можуть атакувати деякі специфічні зони пристрої систем промислової автоматизації та управління (слабкі зони) з метою збору інформації не тільки від цього технологічного пристрою, але самої мережі, компрометуючи всю систему. У більшості випадків дії, що здійснюються зловмисником, як правило, генерують мережу та активність пристрою, яку можна відстежувати за допомогою спеціалізованих систем.

Системи виявлення вторгнень дозволяють здійснювати моніторинг мережі для виявлення неправильного використання або ненормальних операцій. У першому випадку мережеві з'єднання порівнюються з великими базами даних відомих атак. У другому випадку визначається базовий рівень, порівнюючи його показники з іншими сегментами мережі для виявлення ненормальних дій. У будь-якому випадку потрібно визначити, які саме закономірності відстежувати та аналізувати, порівнювати та приймати рішення. Деякі класичні правила включають наступне:

1) Блокування всіх даних мережевих протоколів систем промислової автоматизації та управління з неправильним розміром або довжиною

2) Блокування всього вхідного/вихідного мережевого трафіку будь-якої області, яка не передбачається або не допускається

3) Блокування мережевих пакетів протоколів систем промислової автоматизації та управління, які виявлені там, де їх не очікують або не дозволяють

4) Повідомлення про невдалі спроби автентифікації та ненормальні ситуації

Запобігання зловмисному програмному забезпеченню. Шкідливе програмне забезпечення – це будь-яке шкідливе або надокучливе програмне забезпечення, яке може бути встановлене в комп’ютерних системах для виконання дій без відома користувачів. Існують різні типи шкідливих програм, включаючи віруси, хробаків, троянських коней, шпигунське та рекламне програмне забезпечення.

Пакети антивірусного програмного забезпечення аналізують файли на накопичувачах і порівнюють їх із переліком раніше відомих шкідливих програм. Програму для захисту від шкідливих програм можна розгорнути на робочі станції, сервери, брандмауери. Їх використання в системах промислової автоматизації та управління потребує прийняття спеціальних практик, включаючи перевірку сумісності, управління змінами та показники впливу на ефективність.

Особливу увагу слід звертати на звичайне програмне забезпечення для захисту від шкідливих програм, щоб уникнути компрометації чуйності систем. Тільки конкретні рішення слід розглянути для такого роду систем.

Усередині мережі систем промислової автоматизації та управління впровадження зловмисного програмного забезпечення має бути централізоване за допомогою шкідливого програмного забезпечення або антивірусного сервера в демілітаризованій зоні, як показано на рис. 3. Конфігурація пристроїв може бути згрупована таким чином, щоб її можна було легко розділити на критичні та некритичні пристрої та аналізувати.

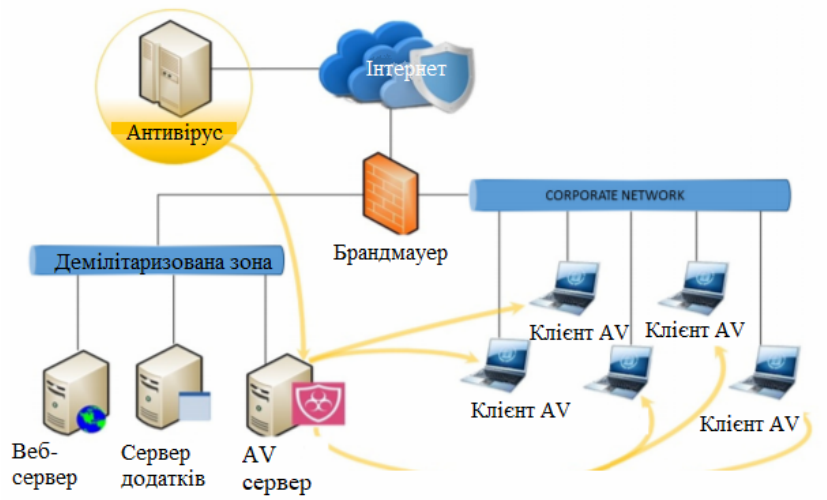


Рисунок 3 – Схема централізованої антивірусної системи

Впровадження новітніх технологій в системи промислової автоматизації та управління, включаючи появу Інтернету та рішень на основі TCP/IP, ризикує швидкістю реагування, продуктивністю та безперервністю таких середовищ, що відкриває нові проблеми та ризики. Занадто часто цим системам загрожують кібератаки через погані або відсутні заходи безпеки. Наразі більшість підходів базуються на використанні безпеки за допомогою неясності, реалізованої завдяки ізоляції цих систем від зовнішніх для них систем.

ЛІТЕРАТУРА

1. K. Stouffer, J. Falco, and K. Scarfone, “Guide to industrial control systems (ICS) security,” NIST special publication (2011): 800-82.

2. ICS-CERT, “ICS-CERT Monitor Newsletters,” October– December 2012. https://ics-cert.us-cert.gov/monitors.

3. CPNI. Centre for the Protection of National Infrastructure. http://www.cpni.gov.uk/.

4. H. Flynn, Designing and building enterprise DMZs, Syngress, 2006.

5. Y. Heng and H. Wang, “Building an application-aware IPsec policy system,” IEEE/ACM Trans on Networking, 15:6 pp. 1502- 1513, 2007.

6. Основи наукових досліджень: Навч. посібник / І.Ш. Невлюдов, Ю.М. Олександров, А.О. Андрусевич, О.О. Чала. – Кривий Ріг: Криворізький коледж НАУ, 2019. – 396 с.

7. Невлюдов, І. Ш., Демська, Н. П., Чала, О. О., & Демська, А. І. ГРУПОВЕ УПРАВЛІННЯ ГНУЧКИМИ ВИРОБНИЧИМИ СИСТЕМАМИ У ВИГОТОВЛЕННІ МЕМС ВИРОБІВ. ББК: У 290-21, 101.

8. Невлюдов І. Ш. Трансфер технологій у сучасній науці, освіті та виробництві в умовах четвертої промислової революції «ІНДУСТРІЯ 4.0» / І. Ш. Невлюдов, О. О. Чала, Ю. М. Олександров // Сучасний рух науки: тези доп. VIII міжнародної науково-практичної інтернет-конференції, 3-4 жовтня 2019 р. – Дніпро, 2019. – Т.2 С.: 604-608

9. Невлюдов И.Ш., Палагин В.А., Чалая Е.А. «Технологиии микросистемной техники (часть II)», НТЖ «Технология приборостоения». – Х., 2015. №2.

10. Nevliudov, V. Bortnikova, O. Chala, and S. Maksymova, “Modeling MEMS Membranes Characteristics,” 2018 XXVI-th International Ukrainian-Polish Scientific and Technical Conference CAD in machinery design implementation and educational issues (CADMD), Lviv, 2018, pp. 61-68.

Науковий керівник: *Чала Олена Олександрівна, старший викладач кафедри КІТАМ Харківського національного університету радіоелектроніки.*