https://nure.ua/

The Ministry of Education and Science of Ukraine

Kharkiv National University of Radio Electronics

KITAM

2023

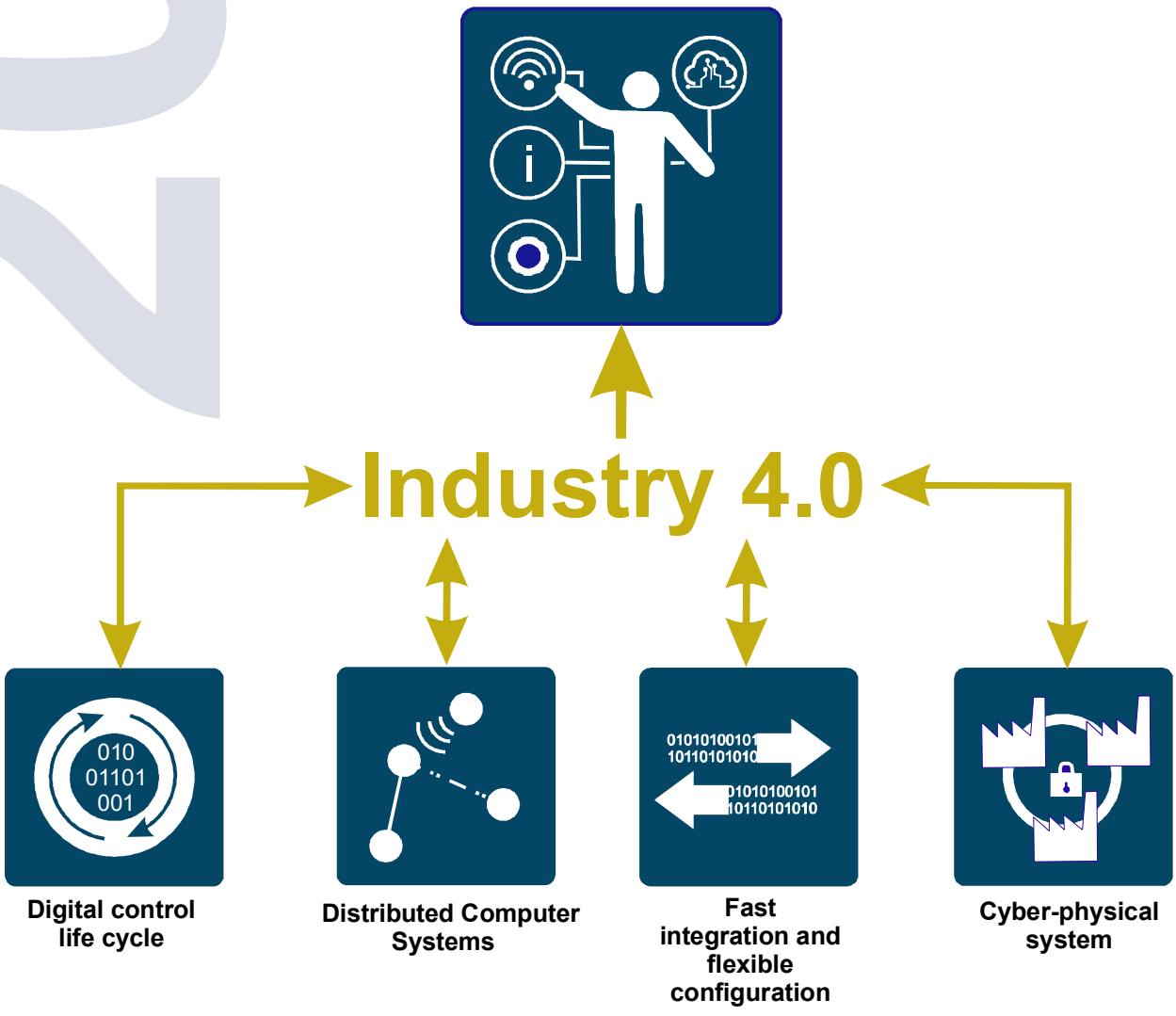
COLLECTION

OF STUDENTS' SCIENTIFIC PAPER

«Automation and Development of Electronic Devices»

ADED-2023

(Part 1)



https://nure.ua/

кафедра
Комп'ютерно-інтегрованих
технологій, автоматизації та мехатроніки

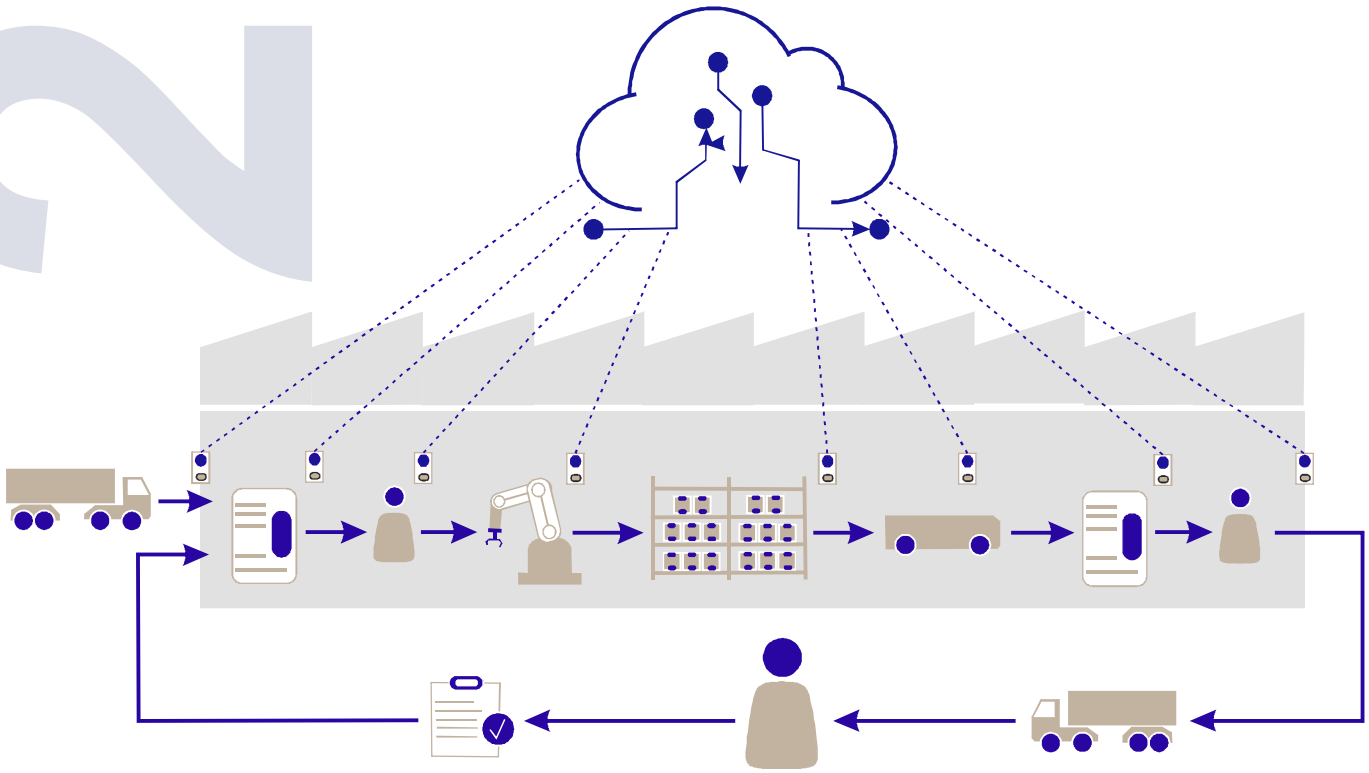
2023

ХНУРЕ

ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»
ADED-2023
(Випуск 1)
[електронне видання]



Industry 4.0

Автоматизація та Приладобудування («Automation and Development of Electronic Devices» ADED-2023) [Електронний ресурс] : збірник студентських наукових статей / Харківський національний університет радіоелектроніки ; [редкол.: І.Ш. Невлюдов та ін.]. – Харків : ХНУРЕ, 2023. – Вип. 1. – 336с.

Collection of Students' Scientific Paper «Automation and Development Of Electronic Devices» ADED-2023 Part 1 (Key infrastructure 2023) - Kharkiv/ The Editorial.: Nevlyudov I.Sh. (head), that all. Kharkiv: Kind of Kharkiv National Universitety of Radio Elektronics [electronic edition], 2023. – 336p 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 № 6 від 01.05.2023

Збірник містить наукові статті здобувачів першого (бакалаврського), другого (магістерського) рівнів вищої освіти 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. Статті надані в авторській редакції.

ЗМІСТ

УДК 004.738

ОГЛЯД МОЖЛИВИХ РИЗИКІВ КІБЕРАТАКИ ДЛЯ ВІРТУАЛЬНОГО ПІДПРИЄМСТВА ТА СПОСОБІВ ЇХ ЗАПОБІГАННЯ

С.О. Вінниченко
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки 14
E-mail: sofiia.vinnychenko@nure.ua

Анотація: У даній статті наведено огляд загроз для віртуального підприємства. Проведено їх аналіз та надано рекомендації щодо усунення. Розглянуто основні підходи для захисту системи, описано принцип роботи та доцільність використання.

Ключові слова: кібербезпека, загроза, аналіз, система, захист.

OVERVIEW OF CYBER ATTACK POSSIBLE RISKS FOR VIRTUAL ENTERPRISE AND WAYS TO PREVENT THEM

S. Vinnychenko
Kharkiv Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Nauky av, 14
E-mail: sofiia.vinnychenko@nure.ua

Abstract: This article provides overview of threats to virtual enterprise. Their analysis was carried out and recommendations for elimination were provided. The main approaches to system protection are considered, principle of operation and feasibility of use are described.

Key words: cyber security, threat, analysis, system, protection.

Протягом всього свого існування люди намагалися зберегти в секреті важливу для них інформацію. Раніше проблема її захисту розглядалася в забезпеченні охорони поштових повідомлень, надійного зберігання паперових носіїв, використання шифрування, тощо. Швидкий розвиток інформаційних технологій (ІТ) та глобальної мережі Інтернет призвели до формування середовища, яке вплинуло на всі сфери людської діяльності [1-6]. Нині кожен має доступ до різноманітних ресурсів та додатків в мережі. Але поява нових технологій зазвичай супроводжується як позитивними, так і негативними наслідками. Тепер інформацію про необхідну особу знайти набагато легше, адже всі дані про неї знаходяться в мережі Інтернет. Цим і користуються зловмисники, які за допомогою різних махінацій отримують несанкціонований доступ до секретних даних.

Найбільше від витоку інформації страждають підприємства, банки, малий та великий бізнес. Нині майже кожна компанія використовує ІТ для підвищення ефективності всіх сторін діяльності компанії, включаючи виробництво, маркетинг, продажі, пошук працівників, підтримку клієнтів та фінансовий аналіз.

Важливою умовою існування бізнесу є інформаційна безпека (ІБ), яка являє собою захищеність корпоративної інформації та інфраструктури від випадкових та навмисних впливів, які здатні зашкодити власникам або користувачам інформації. Шкода від порушення ІБ може призвести до значних фінансових втрат і навіть до повного закриття компанії. Тому проблеми забезпечення безпеки привертають увагу не тільки спеціалістів в галузі комп'ютерних систем і мереж, а й численних організацій.

Для забезпечення конфіденційності інформації кожна компанія в першу чергу повинна провести аналіз можливих загроз з метою визначення повного набору вимог до створюваної системи захисту. Його доцільно проводити на основі класифікації загроз за низкою ознак. Кожна з ознак відображає одну з узагальнених вимог до системи захисту.

Необхідність класифікації загроз інформаційної системи (ІС) обумовлена тим, що інформація в системі схильна до впливу на неї значної кількості факторів, тому описати повний перелік загроз у вигляді однієї задачі неможливо.

Незалежно від цього, ІС задовольняє потреби користувачів, якщо для інформаційних ресурсів в системі наявні такі рівні:

- доступність (можливість отримати необхідну інформацію за короткий проміжок часу);
- цілісність (відсутність можливості випадкової або несанкціонованої модифікації інформації);
- конфіденційність (відсутність можливості несанкціонованого отримання інформації).

Відповідно, для автоматизованих ІС необхідно насамперед класифікувати загрози за рівнями, наведеними вище:

- загрози порушення доступності (відмова в обслуговуванні) – направлені на створення ситуацій, при яких блокується доступ до деяких ресурсів ІС, або знижується її працездатність;
- загрози порушення цілісності інформації, які призводять до її спотворення та повного знищення в подальшому. Цілісність може бути порушена зловмисником, або в результаті дій зі сторони середовища, яке оточує систему. Ця загроза є особливо актуальною для комп'ютерних мереж та систем телекомунікації [7];
- загрози порушення конфіденційності – направлені на розповсюдження секретної інформації. При цьому інформація стає відомою особам, які не повинні мати до неї доступ.

Дані види загроз є первинними, оскільки їх реалізація веде до безпосереднього впливу на захищену інформацію.

Класифікація можливих загроз може бути проведена також за іншими ознаками:

1. За природою виникнення розділяють:
- природні (викликані впливом фізичних процесів або природних явищ);
- штучні (викликані діяльністю людини).
2. За розташуванням джерела загроз:
- поза зоною, контрольованою ІС (перехоплення даних з каналів зв'язку, тощо);
- в межах контрольованої зони ІС (використання пристроїв для прослуховування, викрадення записів, носіїв інформації);
- безпосередньо в ІС (некоректне використання ресурсів).
3. За ступенем дії на ІС:
- активні загрози (вносять зміни в зміст та структуру, наприклад, завантаження вірусу);
- пасивні загрози (не впливають на структуру системи, наприклад, копіювання секретних даних).
4. За поточним місцем розташування інформації, яка зберігається в інформаційній системі:
- загрози доступу до інформації на зовнішніх е програм пристроях (несанкціоноване копіювання інформації з жорсткого диску);
- загрози доступу до інформації в оперативній пам'яті (зчитування залишкової інформації з неї; доступ до системної області ОП зі сторони прикладних програм);
- загрози доступу до інформації, яка циркулює в лініях зв'язку (незаконне підключення до ліній зв'язку з подальшим введенням хибних повідомлень або їх модифікацією);
- загрози доступу до інформації, що відображається на терміналі або друкується принтером (запис інформації на відеокамеру).

Найбільш поширеним видом комп'ютерних порушень є несанкціонований доступ (НСД). Його суть полягає в тому, що користувач отримує доступ до об'єкту, порушуючи правила політики безпеки. Із всіх можливих порушень розглянемо ті, які відбуваються найчастіше: перехоплення паролів, маскарад, шкідливі програми, незаконне користування привілеями.

Перехоплення паролів здійснюється програмами, які створені для цього спеціально. Коли законний користувач намагається ввійти в систему – програма імітує на екрані поля для вводу логіну та пароля, інформація з яких одразу надсилається власнику перехопника, після чого на екран виводиться повідомлення про помилку і управління повертається до системи.

Користувач знову вводить дані і отримує доступ до системи. А власник програми зможе використовувати викрадені дані в своїх цілях.

Маскарад – виконання будь-яких дій одним користувачем від імені іншого. Ціллю порушення є привласнення дій зловмисника законному працівнику. Наприклад, вхід в систему під його е прог та паролем.

Незаконне користування привілеями. Більшість систем захисту встановлюють набори привілегій для користувачів: адміністратори – максимальні, звичайні робітники – мінімальні. Несанкціоноване використання привілей надає можливість зловмисникам виконувати дії в обхід системи захисту.

Шкідливі програми. До них відносять: комп'ютерні віруси (програми, які можуть заражати інші, модифікуючи їх внесенням своєї копії, яка зберігає здатність розмножуватися), е програ «хробаків» (різновид програми-віруса, який розповсюджується мережею), програму «троянський кінь» (непомітно виконує дії, які призводять до порушення роботи системи) (рис. 1.1).

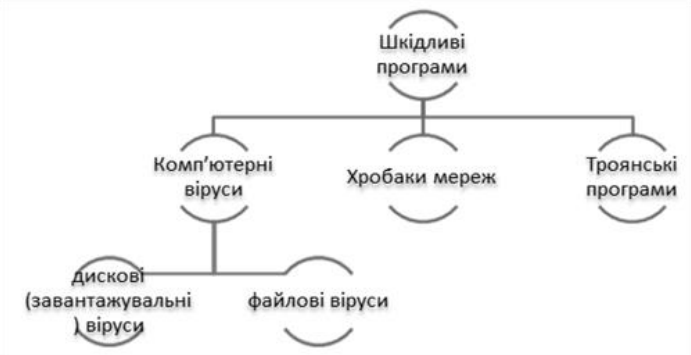


Рисунок 1.1 – Схематичне зображення різновидів шкідливих програм

Варто зазначити, що наведені вище програми відносяться до одної з найнебезпечніших загроз для ІС. Особливістю їх є те, що вони орієнтовані на конкретне прикладне ПО, в першу чергу Microsoft Outlook. Масове створення вірусів для його продуктів пояснюється не лише низьким рівнем безпеки, а й розповсюдженістю їх серед користувачів. Для захисту від шкідливих програм необхідні такі міри:

- виключення несанкціонованого доступу до виконуваних файлів;
- тестування щойно придбаних програмних засобів;
- контроль цілісності виконуваних файлів та системних областей;
- створення замкненого середовища виконання програм.

Боротьба з вірусами, «хробаками» та «троянськими конями» ведеться за допомогою ефективного антивірусного програмного забезпечення, яке працює на користувальницькому рівні та на рівні мережі. За ним потрібно слідкувати та часто оновлювати.

До е програмних загроз можна віднести спам (масове розсилання комерційної, політичної реклами та інших повідомлень особам, які не бажають їх отримувати). Він може створювати загрозу доступності інформації, блокуючи поштові сервери, або використовуватися для розповсюдження шкідливого програмного забезпечення.

Тепер поговоримо про засоби забезпечення загальної інформаційної безпеки в комп'ютерних системах. Існує два підходи до проблеми: фрагментарний та комплексний.

Фрагментарний підхід – направлений на протидію чітко визначеним загрозам з заданих умовах. В якості прикладів реалізації такого підходу можна зазначити автономні засоби шифрування, спеціалізовані антивірусні програми, тощо. Перевагою такого підходу є висока вибірковість до конкретної загрози. Головним недоліком його є відсутність єдиного захищеного середовища обробки інформації. Фрагментарні засоби забезпечують захист конкретних об'єктів лише від заданої загрози. Мінімальна її видозміна призводить до втрати ефективного захисту.

Комплексний підхід орієнтований на створення захищеного середовища обробки в комп'ютерній системі, яке об'єднує в єдиний комплекс різні засоби протидії загрозам. Головною перевагою даного підходу є те, що організація середовища дозволяє гарантувати певний рівень безпеки. До недоліків можна віднести обмеження свободи дій користувачів, чутливість до помилок встановлення та налаштування засобів захисту, складність управління. Комплексний підхід застосовують для захищення комп'ютерних систем крупних організацій або невеликих систем, які виконують відповідальні задачі і обробляють важливу інформацію. Порушення безпеки інформації в них може завдати серйозних матеріальних збитків як організаціям, так й їх клієнтам. Тому компанії повинні приділяти особливу увагу гарантіям безпеки та реалізовувати комплексний захист. Цим підходом користуються більшість державних та крупних комерційних підприємств та закладів.

Комплексний підхід до проблеми заснований на політиці безпеки, розробленій для конкретної системи. Вона охоплює всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях.

Для захисту інтересів суб'єктів інформаційних відносин необхідно поєднувати засоби наступних рівнів:

- законодавчого (комплекс засобів, направлених на підтримку в суспільстві негативного ставлення до порушень та порушників ІБ);
- адміністративно-організаційного (основною мірою є політика безпеки, направлена на захист інформації, та комплекс організаційних заходів, тобто набір регламентів для персоналу);
- програмно-технічного (повинні бути доступні: ідентифікація користувачів, аудит, криптографія, керування доступом, протоколювання, екранування).

Таким чином, у статті наведено основні загрози інформаційній безпеці віртуального підприємства, проведено їх аналіз та класифікацію, детально розглянуто деякі порушення інформаційної безпеки та надано рекомендації щодо їх усунення. Також проаналізовано основні підходи для захисту системи, визначено їх переваги та недоліки і принцип роботи.

ЛІТЕРАТУРА

1. Sotnik, S. Features of Database Types / Z. Deineko, S. Sotnik, O. Vovk, V. Lyashenko // International Journal of Engineering and Information Systems (IJEAIS). – 2021. – Vol. 5 (10). – P. 73-80.

2. Al-Sherrawi, M.H. Information model of plastic products formation process duration by injection molding method / M.H. Al-Sherrawi, A.M. Saadoon, S. Sotnik, V. Lyashenko // International Journal of Mechanical Engineering and Technology. –2018. – Vol. 9 (3). – P. 357–366.

3. Lyashenko, V., Sotnik S. Semantic Model Workspace Industrial Robot / V. Lyashenko, S. Sotnik // International Journal of Academic Engineering Research (IJAER). – 2021. – Vol. 5, Issue 9.– P. 40-48.

4. Sotnik, S. Recognition of Voice Commands Based on Neural Network / V. Lyashenko, F. Laariedh, S. Sotnik, M. A. Ahmad // TEM Journal. – 2021. – Vol. 10, Iss. 2. – P. 583-591.

5. Lyashenko, V. Dynamic and Static QR Coding / Zh. Deineko, S. Sotnik, V. Lyashenko // International Journal of Academic Engineering Research (IJAER). – 2023. – Vol. 6, Iss. 11. – P. 1-6.

6. Sotnik, S. Development Features Web-Applications / S. Sotnik, T. Shakurova, V. Lyashenko // International Journal of Academic and Applied Research (IJAAR). – 2023. – Vol. 7 Iss. 1. – 2023. – P. 79-85.

7. Остапов С. Кібербезпека: сучасні технології захисту: навч. Посіб. Львів: «Новий Світ-2000». – 2020. – 678 с.