https://nure.ua/

The Ministry of Education and Science of Ukraine

Kharkiv National University of Radio Electronics

KITAM

2023

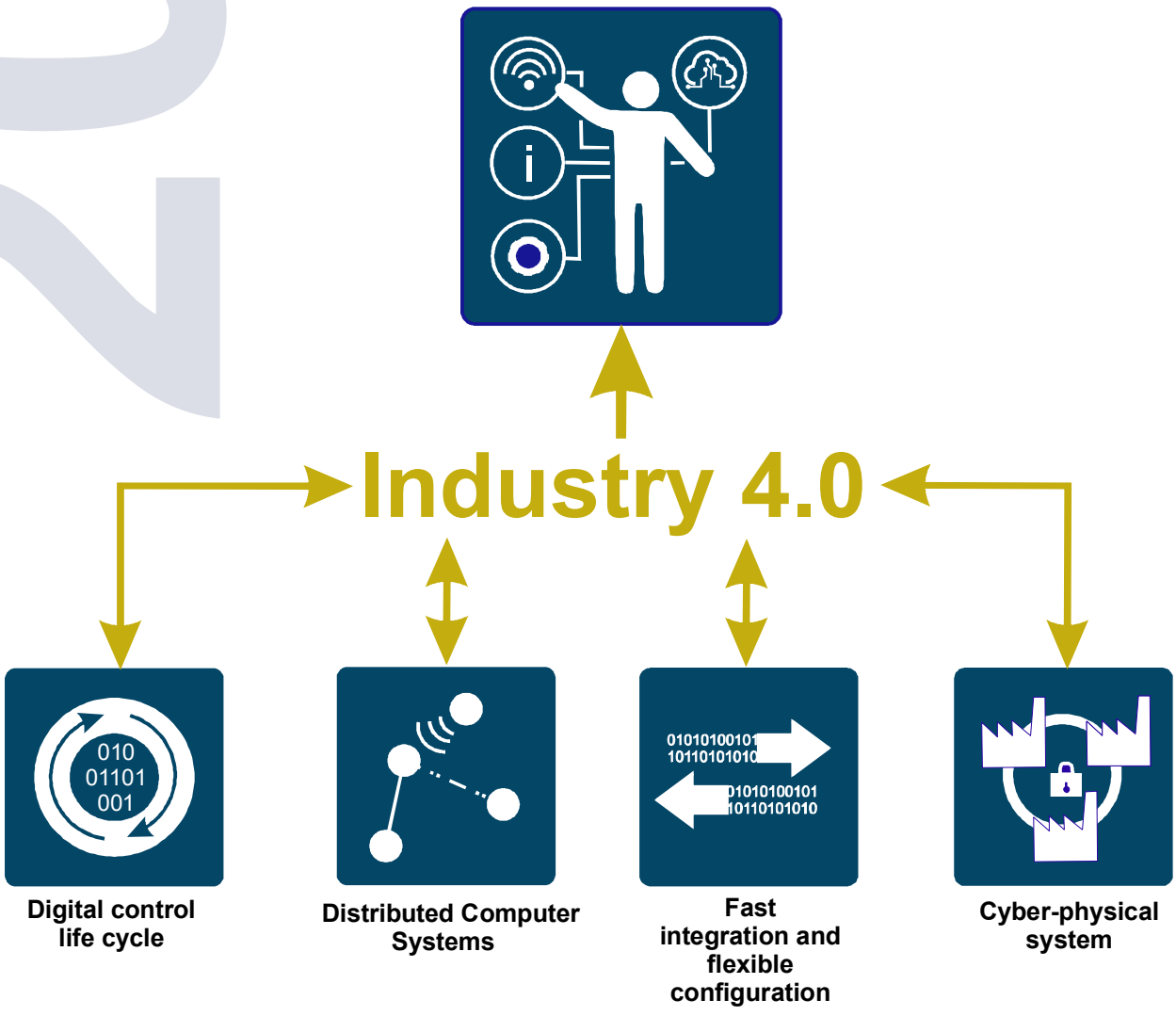
COLLECTION

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

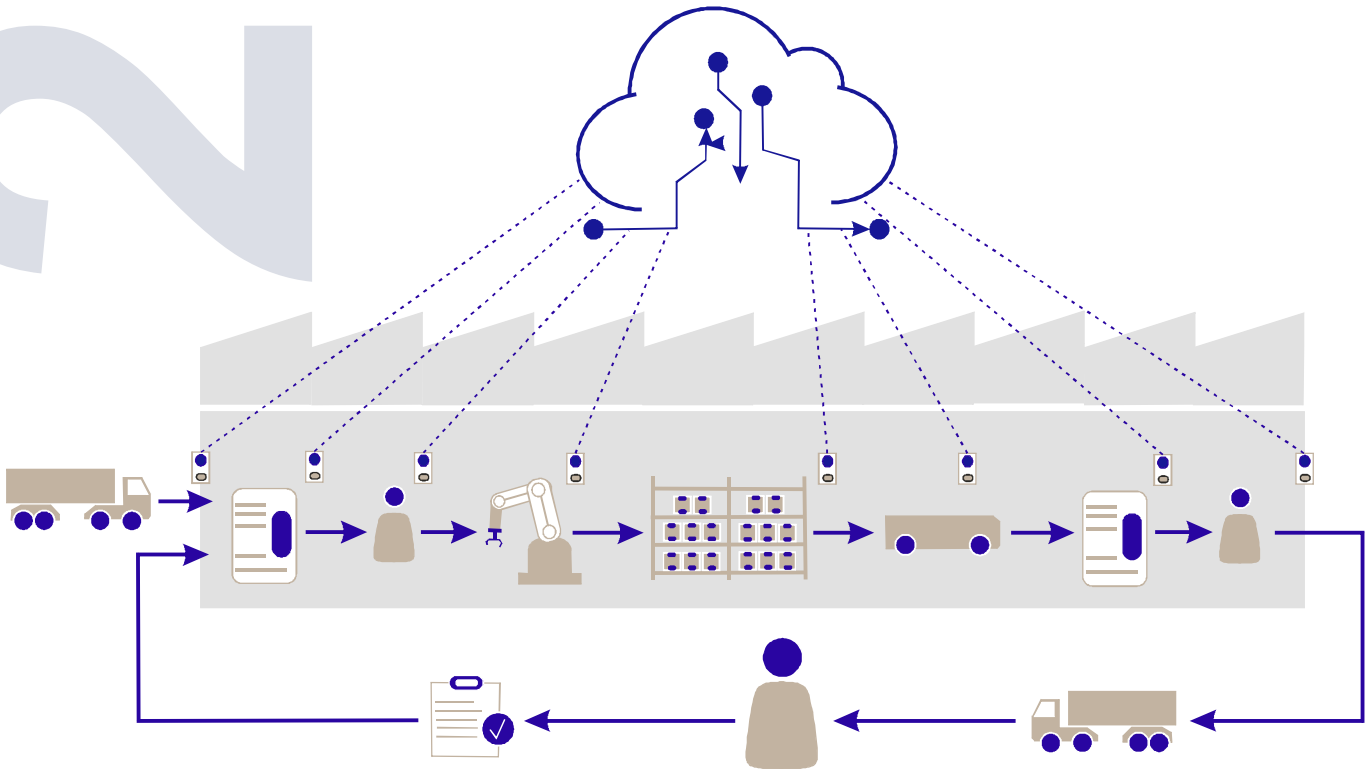
2023

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 338.2

АНАЛІЗ ПРИЧИН КІБЕРАТАК ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Д. М. Світайло
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки 14
E-mail: daria.svitailo@nure.ua

Анотація: У даній статі проведено аналіз причин кібератак та захисту даних. Виявлені основні причини загроз й варіанти запобігання цих загроз. Розглянуті рішення, які забезпечують захист інформації.

Ключові слова: інформаційна безпека, кібератака, захист інформації, загроза.

ANALYSIS OF CAUSES OF CYBER ATTACKS AND INFORMATION SECURITY

D. Svitailo
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Nauky av.,14
E-mail: daria.svitailo@nure.ua

Abstract: This article analyzes the causes of cyberattacks and data protection. The main causes of threats and options for preventing these threats are revealed. Considered solutions that ensure information protection.

Key words: information security, cyber-attack, information protection, threat.

У сучасному світі проблема кібербезпеки є однією з найбільш пріоритетних. Але у чому ж основні відмінності понять інформаційної безпеки й кібербезпеки? У першу чергу кібербезпека є підвидом інформаційної безпеки.

Інформація завжди відігравала надзвичайно важливу роль не тільки у житті людини, але й в виробничих процесах [1-6].

Інформаційна безпека – це інше вживання виразу «захист даних». Сукупність організаційних та інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Задачею інформаційної безпеки є захист й збереження дані будь-якої форми, у цьому й проявляється масштабність значення інформаційної безпеки порівняно з кібербезпекою.

Однією з різновидів загроз кібербезпеки є кібератака.

Кібератака – це масовий замах на інформаційну безпеку комп’ютерної системи. Атаки проводяться по різним направленням: SMTP, DNS, HTTP, SSL. Щоб захиститися від них, потрібні спеціальні рішення. Щоб почати кібератаку, необхідно створити комп’ютерну мережу. Вона може включати декілька сотень тисяч комп’ютерів. Ці комп’ютери направляють у ціль величезну кількість запитів. Сервери не витримують навантаження й відмовляють.

Зараз ніхто не заперечує важливість захисту інформації. Як для домашніх користувачів, так і для системних адміністраторів у великих корпораціях є різноманітні інструменти для збереження даних – ви просто вибираєте та використовуєте. Чому ми так часто чуємо, як компанії втрачають гроші та час через вірусні атаки, інформаційні витоки та подібні інциденти? Питання зовсім не риторичне.

Люди мають звичку недооцінювати ризики, пов’язані з порушенням конфіденційності, цілісності та доступності даних, або, що ще гірше, сподіватися на необмежену удачу. Для цього є кілька причин, перша з яких психологічна: людям легше оцінити негайний прибуток, ніж теоретичні втрати. Друга пов'язана з тим, що побудова та підтримка ефективної системи захисту інформації є дуже складним процесом, і придбання та налагодження технічних засобів захисту є лише малою його частиною. У підсумку ми маємо статистику аналітичного центру компанії «InfoWatch», який повідомив про 1395 інформаційних витоків у 2021 році [7, 8].

Середня вартість одного розливу оцінюється в 25,51 мільйона доларів. Менші випадки, сотні разів на день, не фіксуються, але ви можете порівняти наведені цифри з реальним станом і зробити відповідні висновки. Крім технічних засобів захисту, системи захисту інформації мають і інші складові. За статистикою, понад 90 % нещасних випадків відбувається з вини людей: брак знань і уваги співробітників призводить до витоку або повної втрати даних. Тому не варто забувати про регулярне проведення тренінгів з інформаційної безпеки, а також написанні зрозумілих і продуманих службових інструкцій.

Що стосується засобів технічного захисту, то їх кількість величезна, але змінився принцип використання. Поступова міграція інформаційних систем до хмарних середовищ розмила такі ключові поняття, як «межі мережі». Дійсно, більшість мереж у минулому будувалися за однією схемою: маршрутизатор із функціями безпеки стояв на краю корпоративної мережі, ізолюючи корпоративну мережу від зовнішнього світу. Зараз багато підприємств більш охоче переносять свої сервери в хмару, що робить поняття «периметр мережі» дуже умовним. У такій конфігурації захист від спаму, вірусних атак і підбору паролів бере на себе постачальник послуг, що дозволяє споживачам зосередитися на захисті робочих станцій і роботі з людьми.

Грамотне застосування сучасних security-рішень допоможе знизити потенційні ризики. Щоб визначитися з необхідними засобами забезпечення інформаційної безпеки, необхідно повністю усвідомлювати, що саме треба захищати, тому визначено набір стандартних рішень, який можна представити і без цього:

1. По-перше, необхідний антивірусний захист. Ще пам'ятний вірус «Petya», від якого лихоманило Україну та інші країни.
2. Другим фактором боротьби зі шкідливим кодом є своєчасне оновлення програмного забезпечення та використання ліцензійних версій операційної системи. Використання піратського ПЗ може призвести до повної зупинки роботи, що коштує врази більше заощаджених коштів.
3. Важливо також стежити за тим, що роблять співробітники на робочому місці: перераховувати відвідані веб-сайти, стежити за встановленням сторонніх додатків, контролювати копіювання даних на носії та надсилати дані за допомогою Messenger – усе це не варто випускати з уваги.
4. На випадок втрати пристроїв, дані на них повинні бути зашифровані або хоча б заблоковані паролем. Google, наприклад, дозволяє власнику домену змушувати власників смартфонів використовувати адекватні методи захисту: PIN-коди, паролі та інші.

Британська компанія Databarracks, яка спеціалізується на безперебійності бізнес-процесів та резервному копіюванні й аварійному відновленню даних, зробила щорічне дослідження Data Health Check.

Згідно з ним, у 2022 році вперше найпоширенішими причинами для втрати даних стали кібератаки (38 %), а найчастішою формою кібератак виявилося ransomware (програма-вимагач). У дослідженні також зазначається, що іншими частими причинами втрати даних залишається людський фактор та збій у роботі обладнання [7 - 9].

Для покращення безпеки даних треба діяти у двох напрямках: по-перше, застосовувати заходи та інструменти, які дозволяють попередити та відбити спроби атак. Цей напрямок роботи має на меті посилити кіберзахищеність.

І по-друге, на випадок якщо хакерська атака виявилася успішною та дані було втрачено чи скомпрометовано, треба мати протокол дій у разі атаки. Для цього великі компанії розробляють Business Continuity Plan, тобто план забезпечення безперебійної діяльності, а також Політику щодо зберігання даних.

На випадок втрати даних. Варто зазначити, що, згідно з доповіддю, Business Continuity Plan стали приймати все більше малих підприємств, а не тільки великі корпорації. І дійсно, навіть не на рівні компанії, а на рівні індивідуального користувача потрібно продумати можливі кроки – що ви будете робити у випадку шахрайської вимагацької атаки або втрати даних.

Регулярне резервне копіювання та декріптори. Згідно з дослідженням від Databarracks, 34 % учасників опитування, що зазнали успішної атаки від вимагацького програмного забезпечення, не платили викуп нападникам, а відновилися з бекапів. Власно, резервне копіювання є поширеною відповіддю на втрату даних з будь-яких причин – хоч через вимагачів, хоч через злам або крадіжку обладнання.

Крім того, ще 22 % змогли відновити свої дані завдяки програмам-декріпторам – інструментам для розшифрування вимагацького програмного забезпечення [7 - 9]. До речі, на вебсторінці проєкту Кіберполіції України «No More Ransom (тобто, «Ні – викупу») ви можете скористатися деякими інструментами для дешифрування шкідливих програм.

Звернемо увагу на дії для того, щоб запобігти кібератакам:

1. Горщик з медом. Це дослівний переклад терміну «honeypot», який означає «пастка». Він може бути реалізований як програмно (емульований), так і апаратно (на окремо виділених серверах) та діє як приманка. Мета honeypot полягає в тому, щоб видати себе за цінний об'єкт компанії, викликати на себе атаки хакерів й вивчити їхню поведінку. Таким чином сервер-приманка дізнається стратегії та методи зловмисників та допомагає виробити план дій з покращення кіберзахисту.

2. Регулярне оновлення ПЗ. Оновлення програм та застосунків для мобільних пристроїв та комп'ютерів, окрім суто поліпшення функціональності та усунення багів, також містять важливі покращення системи безпеки та засоби для відбивання відомих на той момент вірусів.

Щоб ці процедури не потребували додаткових дій, корисно налаштувати автоматичне оновлення ПЗ, що допоможе усунути принаймні деякі проблеми з безпекою.

3. Встановити антивірус та VPN. Антивірусна програма – це ПЗ для пошуку та знешкодження шкідливих програм, або комп'ютерних вірусів. За потреби антивіруси сканують файли та програми, інтернет-трафік, електронні листи тощо.

Ставлення до VPN серед широкого загалу зазнало швидкої еволюції – від «що таке VPN?» до «чи треба мені встановити VPN?» і врешті-решт до «який саме ВПН скачати?». Але все-таки нагадаємо, чим він корисний:

VPN робить присутність в Інтернеті анонімною завдяки шифруванню даних та можливості змінити на іншу IP-адресу користувача. Таким чином, ніхто не зможе відстежити історію ваших пошукових запитів або дізнатися, які Веб-ресурси ви відвідували. VPN приховує ваш цифровий слід, що є особливо критичним з точки зору комерційного шпигунства.

Якщо компанія застосовує на своїх корпораційних пристроях VNP та антивірус, є сенс рекомендувати її співробітникам також вживати аналогічних заходів безпеки на їхніх особистих пристроях. Це важливо, адже часто успішні атаки трапляються саме завдяки необережним діям окремих користувачів.

Тому обачні компанії вживають заходів, щоб забезпечити кібергігієну персоналу.

4. Антиспам – захист від спаму. Захиститися від спаму важливо не тільки для того, аби персонал не відволікався на різноманітні заманливі пропозиції у робочий час. Головна небезпека спам-листів полягає у тому, що посилання, які містяться у цих листах, з великою ймовірністю можуть або вести на фішингові Веб-сайти, або містити віруси, які стануть причиною втрати даних та призведуть до фінансових або репутаційних збитків.

Тому компанії мають подбати про те, щоб робітники знали, як правильно поводитися зі спамом.

5. Складні та надійно сховані паролі. По-перше, паролі мають бути надійними. Це означає, що не можна вказувати в якості пароля слово «пароль», своє ім'я або ім'я дітей, декілька однакових цифр (111111) чи цифри, що йдуть поспіль (12345678), або будь-яке слово, яке дійсно існує. Натомість пароль має складатися з рандомної комбінації цифр, букв у верхньому та нижньому регістрах та дозволених службових символів.

По-друге, треба зізнатися, що такі складні паролі важко запам'ятати. Але написати пароль на клаптику паперу і потім повісити на чільне місце на моніторі не є гаразд. Тому компанія має забезпечити, щоб співробітники вміли користуватися менеджерами паролів.

І наостанок – ще одна цифра з доповіді Databarracks: 44 % від тих, хто зазнав успішної атаки з боку вимагацького вірусу сплатили викуп, щоб повернути собі доступ до своїх даних. Тож, якщо у вас немає процедур для зберігання резервної копії даних, немає ресурсів, щоб успішно відбити атаки, а також немає запобіжно-профілактичних заходів, ви завжди маєте останній вибір – сплатити.

Проведений аналіз дає змогу побачити, що для покращення безпеки даних треба діяти у двох напрямках: по-перше, застосовувати заходи та інструменти, які дозволяють попередити та відбити спроби атак. І по-друге, на випадок якщо хакерська атака виявилася успішною та дані було втрачено чи скомпрометовано, треба мати протокол дій у разі атаки. Виявлені причини кібератак та інформаційної безпеки, знайдено рішення для усунення цих проблем у майбутньому.

ЛІТЕРАТУРА

1. Sotnik, S. Analysis of Existing Infliences in Formation of Mobile Robots Trajectory // International Journal of Academic Information Systems Research / S Sotnik, V Lyashenko. – 2022. – Vol. 6, Issue 1. – P. 13-20.
2. Deineko Z. Confidentiality of Information when Using QR-Coding // International Journal of Academic Information Systems Research (IJAISR) / S. Sotnik, V. Lyashenko, Z. Deineko. – 2022. – Vol. 6, Issue 9. – P. 10-15.
3. Al-Sherrawi, M.H. Corrosion of metal construction structures // International Journal of Civil Engineering and Technology / M.H. Al-Sherrawi, V. Lyashenko, E.M. Edaan, S. Sotnik. – 2018. – Vol. 9(6). – P. 437–446.
4. Sotnik, S. Prospects for Introduction of Robotics in Service // International Journal of Academic Engineering Research (IJAER). / S. Sotnik, V. Lyashenko. – 2022. – Vol. 6, Issue 5. – P. 4-9.
5. Lyashenko, V. Features of Database Types // International Journal of Engineering and Information Systems (IJEAIS) / S. Sotnik, Z. Deineko, O. Vovk, V. Lyashenko – 2021. – Т. 5. – №. 10. – С. 73-80.
6. Безкоровайний, В.В. Інформаційна технологія реінжинірингу корпоративних комп'ютерних мереж // Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку / В.В. Безкоровайний, С.В. Сотник. – 2020. – С. 134.
7. Magomedov, I.A. Cyber literacy as one of the main discipline necessary in modern time / I.A. Magomedov, H.A. Murzaev, A.L. Zolkin // European Proceedings of Social and Behavioural Sciences EpSBS. – 2020. – С. 1011-1015.
8. Digilina, O. Information Security in a Digital Economy Deployment / O. Digilina, I. Teslenko, N. Muravyova // Modern Global Economic System: Evolutional Development vs. Revolutionary Leap 11. – Springer International Publishing, 2021. – С. 1225-1230.
9. Onishchenko, O. Ensuring cyber resilience of ship information systems / O. Onishchenko, K. Shumilova, S. Volyanskyy, Y. Volyanskaya, Y. Volianskyi // TransNav: International Journal on Marine Navigation and Safety of Sea Transportation. – 2022. – Т. 16. – №. 1.