KAPITEL 6 / *CHAPTER 6* [20]
COMPREHENSIVE STRENGTHENING OF INFORMATION SECURITY: POLICIES, CONFIGURATION AUDITS, AND OPERATIONAL RESPONSE PROCEDURES

DOI: 10.30890/2709-2313.2025-42-04-044

Вступ

Зростання складності корпоративних IT-середовищ і динаміка кіберзагроз висувають підвищені вимоги до політик та процедур, що гарантують конфіденційність, цілісність і доступність інформаційних активів [1–5]. Практика показує, що уразливості часто виникають не лише через технічні чинники, а й через людський фактор, тобто, недостатню обізнаність користувачів та неуніфіковані процеси життєвого циклу доступу [6–11]. Цей розділ монографії пропонує цілісну рамку підвищення зрілості системи ІБ організації [12–13]. Сформовано набір рекомендацій з удосконалення ключових політик (обізнаність користувачів, контроль доступу, оновлення ПЗ, паролі, ідентифікація та автентифікація, використання ПЗ, резервне копіювання). Проведено прикладний аудит конфігурацій мережевих пристроїв та серверних служб у типових топологіях (головний офіс і два віддалені підрозділи) з конкретними діями з "ужорсточення" (hardening). Подано рекомендовану операційну процедуру реагування на інциденти ІБ - від повідомлення і класифікації до ескалації, відновлення та післяінцидентного аналізу зі збором свідчень. **Мета розділу монографії** – надати узгоджений, практично застосовний набір політик, технічних налаштувань і процедур, що знижують імовірність інцидентів і скорочують час виявлення та реагування. Предметом є політики, конфігурації мережевих/серверних компонентів і процеси реагування; об'єктом - корпоративна мережа з центральним офісом і віддаленими майданчиками. Практична цінність полягає у готових рекомендаціях і послідовностях дій, які можна безпосередньо імплементувати в експлуатаційне середовище. З

[20] ***Authors:*** *Korobeinikova Tetiana Ivanivna, Zhuravel Ihor Myhailovych*
Number of characters: *29842*
Author's sheets: *0,75*

урахуванням стрімкого розвитку технологій та постійного зростання загроз кібербезпеці, актуальність ефективного аудиту мережевої безпеки на основі Security Design Review (SDR) набуває особливого значення. Розробка належних рекомендацій для проведення такого аудиту стає стратегічним завданням для забезпечення високого рівня захисту наших інформаційних ресурсів.

6.1 Рекомендації щодо покращення політик безпеки

Для посилення загальної безпеки та захисту конфіденційності, цілісності та доступності інформаційних ресурсів, нижче будуть наведені рекомендації щодо вдосконалення політики безпеки. Ці рекомендації ґрунтуються на передових стандартах та кращих практиках галузі. Їхнє впровадження сприятиме оптимізації захисту від потенційних загроз та забезпеченню стійкої оборони від кіберзагроз. Важливість імплементації цих рекомендацій є важливим елементом стратегії інформаційної безпеки, спрямованої на забезпечення надійності та безпеки даних і систем.

Політика обізнаності користувачів. Людина є одним із ключових елементів забезпечення інформаційної безпеки у будь-якій інфраструктурі, але і одночасно – найслабшою ланкою у забезпеченні ІБ. Щоб підвищити рівень обізнаності користувачів щодо забезпечення інформаційної безпеки на підприємстві, пропонується схема (рис. 1), у якій передбачено найважливіші аспекти навчання персоналу та роботи з ним.

Рисунок 1 - Схема дій при прийнятті нового співробітника

Період виконання робочих обов'язків. Щоб завжди орієнтуватися у знаннях та вміннях працівників підприємства, потрібно регулярно проводити перевірки їх компетенцій. Взагалі перевірки можуть бути такими, які проводяться за наперед складеним графіком і такими, які можна проводити без попередження і лише для певної категорії працівників, наприклад. Переважна більшість працівників мала б пройти такі перевірки успішно, але й, напевно, знайдуться й такі, що провалять їх. Якщо перевірка проходила за таким сценарієм, що припущена шкода буде незначною і співробітник її не пройшов, його слід відправити «вчитися» і застосувати до нього не жорсткі дисциплінарні стягнення (позбавлення премії). З рештою працівників потрібно провести бесіду, на якій розібрати помилки їхнього колеги та пояснити їм послідовність дій (рис. 2).

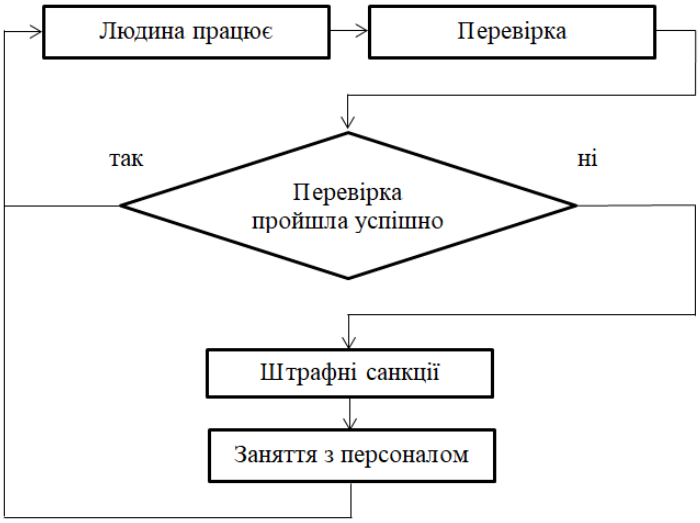

Рисунок 2 - Схема дій для перевірки рівня обізнаності користувачів

Якщо ж припущена шкода могла бути серйозною штрафні санкції щодо порушника повинні бути суворішими. Знову ж таки потрібно буде зібрати колектив чи його частину і обговорити помилки, які було допущено та шляхи їх усунення.

Припинення чи зміна трудових відносин. Відповідальність і обов'язки, які залишаються в силі після завершення трудових відносин, повинні бути вказані в умовах трудової угоди з співробітником у контракті.

Якщо працівник вирішив більше не працювати в організації, повинна початися процедура звільнення. Спочатку працівник повинен здати усі ключі, ключ-карти, флешки, відповідні документи і т.д., тобто все те, що належить організації і звільнити своє робоче місце. Таким чином, блокується доступ такого працівника до будь-якої інфраструктури організації. Далі блокується доступ до робочих облікових записів працівника. При потребі всі вони чи частина з них можуть бути видаленими. Після цього проводиться робота з документацією для звільнення цього працівника.

Політика контролю доступу. Для того щоб вберегтися від несанкціонованого проникнення на підприємство чи незаконного використання ресурсів, на допомогу приходять політики контролю доступу. До інформаційних активів, якими володіє організація, доступ має бути обмеженим. Це робиться для того, щоб відповідною інформацією могли користуватися лише працівники об’єкту. Процес застосування політики контролю доступу може бути трудомістким, а також може потребувати фінансових затрат.

Принцип цієї політики полягає у тому, що ніхто не повинен мати більше привілеїв, ніж це необхідно для виконання його посадових обов’язків. Вибір моделі управління доступом – це важливий елемент захисту, який забезпечує необхідний рівень безпеки для підприємства та інформаційних систем будь-якого призначення. Існує 4 основних моделі, де враховані як специфіки суб'єктів, так і ступінь важливості безпеки об'єктів або ресурсів.

Моделі управління доступом поділяються на такі категорії:

1. дискреційне (виборче) управління (DAC);
2. обов'язковий (мандатний) метод управління (MAC);
3. рольова модель управління (RBA);
4. управління доступом на основі правил (RBA).

Політика процедури оновлень. Оновлення програмного забезпечення є надзвичайно важливою складовою інформаційної безпеки будь-якого підприємства. Розробники ПЗ намагаються виправити всі відомі допущені помилки попередніх версій програм та захистити їх від будь-яких відомих загроз,

які стосуються цих продуктів. Оновлення програмного забезпечення і додатків, які використовуються в організації повинно виконуватися тільки навченими адміністраторами за наявності відповідного розпорядження керівництва, але при цьому попередні версії ПЗ повинні зберігатися як міра страхування. Також повинен вестися журнал всіх оновлень. Можливим є використання автоматичних оновлень. При цьому має бути врахований ризик для цілісності і готовності системи до роботи в порівнянні з швидкістю їх встановлення. Проте, автоматичні оновлення для критичної інфраструктури повинні бути забороненими тому, що встановлення деяких оновлень призводить до примусового припинення роботи відповідного ПЗ.

Політика паролів. Паролі – це типовий засіб перевірки справжності користувача. Паролі повинні бути стійкими і при цьому мати мінімально можливу довжину. Вони повинні бути такими, що:

– не використовувати чогось такого, про що будь-хто може здогадатися на основі особистої інформації (номер телефону, дати народження, імена);

– не містяться у словниках;

– не містять послідовностей однакових літер чи/та цифр;

– змінюються в першій ж сесії.

Паролі не можна передавати у відкритому вигляді по мережі та небажано відображати при введені. Проте варто зауважити, що фахівці радять використовувати довші та складніші паролі, але дозволяти користувачу візуально контролювати те, що він вводить у відповідне поле. У першому випадку під час процедури входу, пароль може бути перехоплений аналізаторами трафіку. У другому – його підглянути. Не можна використовувати один і той самий пароль для доступу до різних ресурсів чи сервісів. Це може привести до значного зниження рівня безпеки. Для забезпечення інформаційної безпеки в організації повинні функціонувати системи керування паролями. Інколи, деякі додатки потребують встановлення паролів незалежним системним адміністратором, але переважна більшість програм дозволяють вибирати і змінювати паролі самостійно.

Паролі потрібно змінювати регулярно. Бувають випадки, коли користувачі забувають змінити пароль вчасно. Щоб уникнути такого потрібно розсилати їм електронні листи за 5 днів, а потім за 1 день до закінчення терміну дії паролю.

Політика ідентифікації та аутентифікації. Для початку потрібно навести визначення основних понять. Ідентифікація – процедура розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Автентифікація – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора. Правильно продумана політика ідентифікації та аутентифікації забезпечує безпечну процедуру входу у систему. Процедура для входу в систему чи додаток повинна мінімізувати можливість несанкціонованого доступу. Це означає, що процедура входу має містити мінімально можливу кількість інформації про систему чи програму. Така вимога висувається для того, щоб ненавмисно не допомогти зловмиснику. Надійна система ідентифікації та авторизації повинна:

- не відображати ідентифікатори до успішного входу;
- не давати ніяких підказок під час входу;
- бути стійкою до спроби входу методом повного перебору ідентифікаторів;
- реєструвати усі спроби входу (як вдалі, так і невдалі);
- завершувати сесію після нетривалого періоду бездіяльності.

Якщо потрібно застосувати строгу перевірку інформації про аутентифікацію та ідентифікацію, застосовуються додаткові заходи аутентифікації, такі як смарт-карти, біометрія чи апаратні ключі.

Політика дозволеного і забороненого ПЗ. Відповідно до потреб організації, потрібно визначити, яке програмне забезпечення є необхідним для виконання працівниками своїх посадових обов’язків.

Головний принцип такої політики – принцип мінімальних привілеїв. Перелік дозволених програмних продуктів може встановити лише підприємство, виходячи зі своїх поточних цілей та задач.

Такі строгі правила повинні діяти тому, що неконтрольоване встановлення програмного забезпечення на робочі станції працівників може привести до появи вразливостей і, тим самим, до витоку конфіденційної інформації, втрати цілісності або інших інцидентів, які стосуються інформаційної безпеки. Неконтрольоване встановлення ПЗ є також причиною появи шкідливих програмних засобів у системі і, навіть, порушення авторських прав.

Політика резервного копіювання. Резервне копіювання інформації, програмного забезпечення та образів операційної системи повинно відбуватися регулярно – щодня часткове резервне копіювання та раз на тиждень – повне в неробочий час. Для резервного копіювання має бути виділено окремий сервер. Це гарантуватиме відновлення інформації і програмного забезпечення після аварійної ситуації чи збою. Сервер для бек-апів повинен розміщуватися на значній відстані, оскільки, у випадку аварійної ситуації у головному будинку ці дані можуть бути відновлені пізніше. Потрібно забезпечити надійний фізичний захист та захист від зовнішніх дій для пристрою, на якому буде зберігатися резервна інформація. Окрім цього, носії для резервних копій повинні регулярно тестуватися для гарантій того, що на них можна буде покластися при застосуванні у випадку надзвичайної необхідності. Також потрібно забезпечити тестування можливості відновити збережені дані на нових пристроях, а не перезаписати інформацію на оригінальні у випадку, якщо в процесі резервного копіювання стався збій чи було виявлено серйозне пошкодження чи навіть втрату даних. Для критично важливих систем та служб резервне копіювання застосовується для всієї системної інформації, додатків і даних, необхідних для відновлення всієї системи у випадку аварії. Відповідно до ступеня важливості для підприємства інформації, дані повинні зберігатися із урахуванням вимог архівування копій та згідно із чинним законодавством.

6.2 Аудит конфігурацій та розробка рекомендацій

У архітектурі мережевої безпеки, мережеві пристрої виступають як

невід'ємна складова корпоративної інфраструктури, невідкладною стає необхідність ефективного контролю та аудиту їхніх конфігурацій. На меті аудиту конфігурацій мережевих пристроїв стоїть не лише виявлення потенційних ризиків та вразливостей, але і надання конкретних рішень для їхнього усунення та підтримки високого рівня безпеки в контексті захисту корпоративних мереж. Розглядається модель корпоративної мережі рис. 3 яка складається з головного офісу (ГО) рис. 3 та двох віддалених офісів (ВО1, ВО2), мережі яких повторюють топологію мережі ГО.

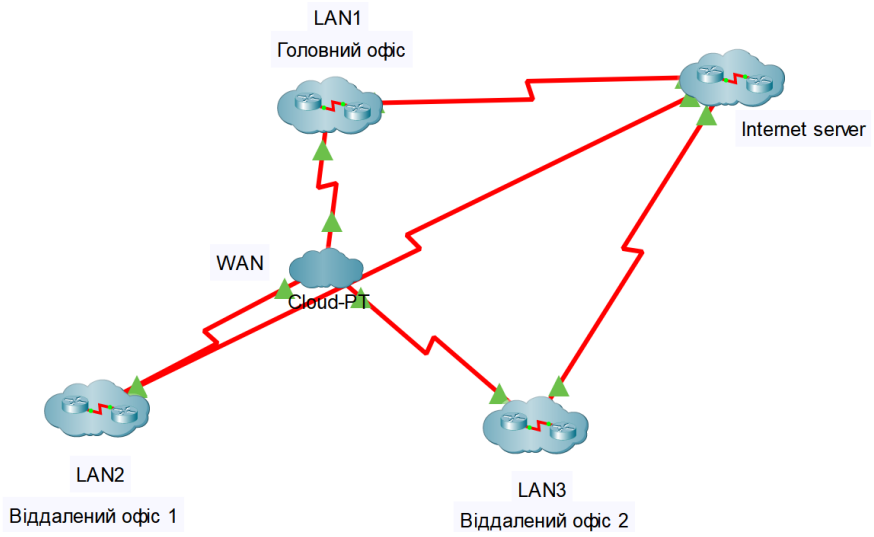

Рисунок 3 - Структурна схема мережі, що розглядається

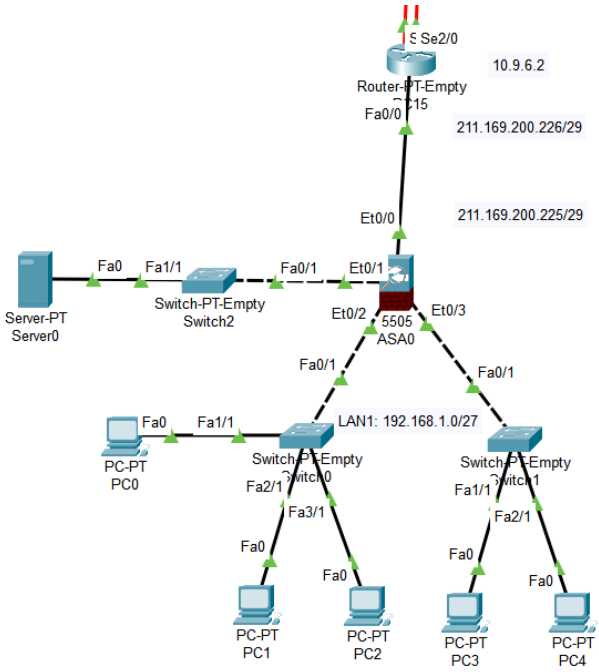

Рисунок 4 - Структурна схема головного офісу мережі, що розглядається

Така мережа складається з головного офісу (ГО) та двох віддалених офісів (ВО1, ВО2), мережі яких повторюють топологію мережі ГО. На рис. 4 наведено топологію мережі головного офісу. Така мережа складається з мережевих пристроїв (маршрутизатор, який відіграє роль шлюзу, Cisco ASA 5505 та комутаторів), кінцевих пристроїв (персональні комп'ютери та сервер) та провідникових з'єднань.

Пристроями, які підтримують безпеку в мережі виступають маршрутизатор та пристрій адаптивної безпеки Cisco ASA 5505. Тепер проведемо аудит конфігурації цих мережевих пристроїв та сервера.

Аудит конфігурації маршрутизаторів та рекомендації. Аудит конфігурації маршрутизаторів мережі, яка розглядається в якості прикладу потрібен для визначення неправильних або небезпечних конфігурацій, що можуть бути причиною компроментації конфіденційної інформації. Використовуючи командний рядок було введено команду `show running-config` за допомогою якої було виведено поточну конфігурацію, яку використовує роутер. Результат роботи команди – всі налаштування, які зараз активні (рис. 5).

Судячи з отриманого результату, видно, що в налаштуваннях роутера є ряд порушень, що можуть стати причиною витоку інформації. Нижче наведемо виявлені проблеми і рекомендації для їх усунення.

- Використання застарілої версія Cisco IOS (version 12.2) – потрібно оновити версію IOS до version 17.11
- Відсутні паролі для входу в консоль і термінальні лінії – потрібно використати такі набори команд відповідно:

```
line console 0
password <пароль>
login
line vty 0 15
password <пароль>
login
```

- Відсутній пароль для привілейованого режиму – потрібно ввести таку команду: `enable secret <пароль>`

```
Rt1-LAN1>en
Rt1-LAN1#show running-config
Building configuration...

Current configuration : 1324
bytes
!
version 12.2
no service timestamps log
datetime msec
no service timestamps debug
datetime msec
no service password-encryption
!
hostname Rt1-LAN1
!
no ip cef
no ipv6 cef
!
interface FastEthernet0/0
ip address 211.169.200.226
255.255.255.248
duplex auto
speed auto
!
interface Serial1/0
ip address 10.9.6.2 255.0.0.0
!
interface Serial2/0
no ip address
encapsulation frame-relay
!
interface Serial2/0.102 point-
to-point
ip address 172.20.1.1
255.255.255.252
frame-relay interface-dlci 102
!
interface Serial2/0.103 point-
to-point
ip address 172.20.3.2
255.255.255.252
frame-relay interface-dlci 103
!
interface Serial3/0
no ip address
clock rate 2000000
shutdown
!
router eigrp 100
network 172.20.0.0
network 211.169.200.0
network 192.168.1.32 0.0.0.31
network 192.168.1.0 0.0.0.31
network 211.169.200.224
0.0.0.7
network 172.20.3.0 0.0.0.3
network 172.20.1.0 0.0.0.3
network 210.170.201.224
0.0.0.7
no auto-summary
!
router rip
!
ip classless
ip route 8.8.8.0 255.255.255.0
10.9.6.1
ip route 210.170.201.224
255.255.255.252
210.170.201.225
ip route 192.168.1.64
255.255.255.224
210.170.201.225
ip route 192.168.1.32
255.255.255.224
212.168.191.225
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
end
```

Рисунок 5 Поточна конфігурація, яку використовує роутер

- Відсутнє шифрування паролів – потрібно скористатися командою `service password-encryption`
- Для віддаленого доступу використовується Telnet – потрібно перейти на SSH для захищеного з'єднання і для цього використовують такі команди:

```
ip domain-name <домен>
crypto key generate rsa
line vty 0 15
transport input ssh
```

  - Вимкнене журналювання подій – потрібного його увімкнути командою: `logging buffered 51200`
- Можливе налаштування списків контролю доступу (ACL) на маршрутизаторі за необхідності

- Використання застарілих протоколів маршрутизації – потрібно замінити протоколи RIP та EIGRP на OSPF, на альтернативні OSPF чи BGP, що вважаються більш безпечними.
- Відсутність захисту від DDoS атак – потрібно використати механізм Control Plane Policing (CoPP), який встановлюється командами:

```
control-plane
service-policy input <назва_політики>
```

Прийнявши до уваги рекомендації, які наведені вище, можна істотно збільшити рівень захищеності даних, що циркулюють в даній мережі.

Аудит конфігурації пристрою адаптивної безпеки Cisco ASA 5505 та рекомендації. Cisco ASA (Adaptive Security Appliances) представляє собою пристрій адаптивної безпеки компанії Cisco, об'єднуючи в собі різноманітні потужні інструменти, такі як міжмережевий екран, система запобігання вторгнень та концентратори VPN. Цей пристрій можна налаштовувати і керувати через SSH, Telnet, веб-інтерфейс або використовуючи відповідне ПЗ. Загалом ASA є уніфікованим пристроєм, що об'єднує кілька засобів безпеки. Так само як і з маршрутизатор, проведемо аудит Cisco ASA (рис. 6).

Загалом, даний пристрій налаштовано не погано, проте тут також було виявлено деякі проблеми. Детальніше розглянемо конфігурація обраного пристрою адаптивної безпеки:

- Відсутній пароль для привілейованого режиму – потрібно ввести таку команду: `enable secret <пароль>`
- Налаштування SSH. Загалом, конфігурація SSH-з’єднання виглядає прийнятно, але рекомендується наступне для підвищення безпеки реалізації SSH-з’єднання:
    - Обмеження доступу SSH: Зараз налаштовано доступ до SSH з будь-якої IP-адреси в мережі INSIDE (192.168.1.0/27). Безпечнішим буде дозволити доступ лише з конкретних IP-адрес.
- Мережеві інтерфейси та VLAN. Конфігурація VLAN виглядає належним чином

```
ASA1-LAN1# show running-config
: Saved
:
ASA Version 8.4(2)
!
hostname ASA1-LAN1
domain-name asa1.com
enable password
4IncP7vTjpaba2aF encrypted
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif INSIDE
security-level 100
ip address 192.168.1.1
255.255.255.224
!
interface Vlan2
nameif OUTSIDE
security-level 0
ip address 211.169.200.225
255.255.255.248
!
object network INSIDE
subnet 192.168.1.0
255.255.255.224
nat (INSIDE,OUTSIDE) dynamic
interface
!
route OUTSIDE 0.0.0.0 0.0.0.0
211.169.200.226 1
!
aaa authentication ssh console
LOCAL
!
username admin password
4IncP7vTjpaba2aF encrypted
!
class-map inspection_default
match default-inspection-
traffic
!
policy-map global_policy
class inspection_default
inspect icmp
!
service-policy global_policy
global
!
telnet timeout 5
ssh 192.168.1.2
255.255.255.255 INSIDE
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.2-
192.168.1.30 INSIDE
dhcpd dns 8.8.8.8 interface
INSIDE
dhcpd enable INSIDE
!
ASA1-LAN1#
```

Рисунок 6 Аудит Cisco ASA

- Firewall Policy. Політика перевірки пакетів є надто простою (перевіряються лише ICMP-пакети: inspect ICMP). Рекомендується ретельніше налаштувати політику, додавши необхідні правила:
  - Використання Application Layer Inspection:

```
policy-map global_policy
class inspection_default
inspect icmp
inspect ftp
inspect http
```

  - Створення VPN-правил:

```
access-list outside_cryptomap_20 extended permit ip 192.168.1.0
255.255.255.224 10.0.0.0 255.0.0.0
crypto map outside_map 20 match address outside_cryptomap_20
```

  - Встановлення контролю над DDoS-атаками:

```
policy-map global_policy
class class-default
```

```
set connection per-client-max 10
```

- Моніторинг та журналювання:

```
logging enable
logging buffered informational
```

- Інтеграція з IDS/IPS:

```
ips (inside) inline
```

- Розгортання стратегії реагування на інциденти:

```
threat-detection basic-threat
threat-detection scanning-threat
threat-detection statistics host
```

- NAT (Network Address Translation): Конфігурація NAT виглядає належним чином.
- DHCP: Конфігурація DHCP виглядає належним чином.
- Використання застарілої версія Cisco IOS (version 8,4(2)) – потрібно оновити версію IOS до version 17.11.

Врахувавши перелічені проблеми і прислухавшись до рекомендацій можна повною мірою використати потенціал Cisco ASA 5505, чим можна значно ускладнити завдання потенційним зловмисникам.

Аудит налаштувань мережевих сервісів на сервері та рекомендації. Дослідимо налаштування мережевих сервісів на сервері. Перевіримо та оцінимо параметри і конфігурацію, що пов'язані з мережевими службами, які працюють на сервері. Ці рекомендації допоможуть підвищити рівень безпеки мережевих служб на сервері. Нижче наведено виявлені проблеми в налаштуваннях мережевих сервісів та деякі рекомендації:

1) Перевірка активних служб. На сервері налаштовані такі пережеві служби:

- HTTP (Hypertext Transfer Protocol): Вразливість передачі незашифрованих даних, що може призвести до перехоплення і читання інформації. Рекомендується вимкнути цей протокол і замінити його на HTTPS, який використовує шифрування TLS/SSL для захисту передачі даних.
- HTTPS (Hypertext Transfer Protocol Secure): В теорії безпечний, але

можливість атак на приватні ключі або використання застарілих криптографічних протоколів.

- FTP (File Transfer Protocol): Передача незашифрованих даних, включаючи паролі, що робить її вразливою до перехоплення. Рекомендується вимкнути цей протокол і замінити його на SFTP (SSH File Transfer Protocol) або FTPS (FTP Secure), котрі використовують шифрування для безпечної передачі файлів
- SNMP (Simple Network Management Protocol): Небезпека використання SNMP без аутентифікації або шифрування, що дозволяє несанкціонованому доступу до інформації про мережеві пристрої. Рекомендується вимкнути цей протокол і замінити його на SNMPv3, що забезпечує аутентифікацію та шифрування для безпечного керування мережевими пристроями, або перейти на IMAP з високим рівнем безпеки (з використанням SSL/TLS) і який залишає копії повідомлень на сервері, дозволяючи отримати доступ до них з різних пристроїв, а також шифрує передачу даних між клієнтом і сервером.
- POP3 (Post Office Protocol 3): Відсутність шифрування може призвести до витоку конфіденційної інформації, так як дані передаються у незашифрованому вигляді. Рекомендується вимкнути цей протокол.
- DNS (Domain Name System): Можливість атак на протокол DNS, такі як DNS Spoofing або DNS Cache Poisoning, що може спричинити перенаправлення та маніпуляцію мережевим трафіком. Рекомендується замінити цей протокол на DNS over HTTPS (DoH) або DNS over TLS (DoT), що захищає конфіденційність та цілісність даних DNS через шифрування.

2) Перевірка мережевих портів. У даній мережі застосовуються вище перелічені мережеві служби, а отже і прослуховуються їх порти (80, 433, 21, 25, 110, 53) для передачі даних. *Рекомендація*: Здійснювати контроль над доступністю перелічених портів.

3) Параметри безпеки мережевих служб. Використовуються паролі для

доступу до відповідних служб, застосовано принцип мінімальних привілеїв для користувачів. *Рекомендація*: змінити політику паролів, використовуючи більш надійні, контролювати доступ дозволених IP-адрес та їх права до відповідних мережевих служб.

4) Журналювання подій. Здійснюється інструментарієм пристрою адаптивної безпеки Cisco ASA 5505, проте, можлива імплементація самостійної SIEM.

5) Оновлення та патчі. Рекомендація: Постійний контроль над виходом оновлень і їх встановленням для усунення відомих вразливостей.

6) Мережеві фільтри. Здійснюється інструментарієм пристрою адаптивної безпеки Cisco ASA 5505, проте, можлива імплементація окремого міжмережевого екрану перед сервером.

7) Моніторинг мережевого трафіку. Здійснюється інструментарієм пристроєм адаптивної безпеки Cisco ASA 5505, проте, можлива імплементація окремого міжмережевого екрану перед сервером.

6.3 Рекомендована операційна процедура дій при інциденті ІБ

У разі виникнення критичної ситуації, пов'язаної з ІБ, потрібно гарантувати послідовний і результативний підхід до керування інцидентами ІБ. На випадок інциденту, наперед вже повинні бути прийняті обов'язки керівництва та процедур, пов'язаних з керуваннями інцидентами ІБ:

- в обов'язки керівництва входить забезпечення проведення процедури планування та підготовки реакції на інцидент; процедури моніторингу, аналізу та інформування про подію; процедури реєстрації події; процедури дій у відповідь.
- дана операційна процедура гарантує, що проблему вирішить компетентний персонал, контактний центр з питань виявлення та інформування про інциденти ІБ працює.

Стратегія дій при інциденті ІБ повинна виглядати так:

1. Якомога швидше сповістити про подію ІБ по відповідних каналах. Усі співробітник повинні знати це, а також знати процедуру передачі повідомлення про подію ІБ. До ситуацій, які передбачають передачу відповідного повідомлення належать: нерезультативний контроль безпеки; невідповідності до політик та інструкцій; порушення доступу; неконтрольовані зміни у системі; порушення очікуваного рівня конфіденційності, цілісності чи доступності.

2. Усі співробітники повинні повідомити про виявлену ними уразливість в ІБ контактному центру якнайшвидше. Це робиться для того, щоб попередити можливий інцидент. Механізм передачі повідомлень такого роду повинен бути настільки простим, доступним та дієздатним, наскільки це можливо. Працівникам забороняється самотужки перевіряти уразливість захисту. Такі дії можуть сприйнятися некоректно.

3. Контактний центр повинен оцінювати кожну подію про, яку було повідомлено, використовуючи класифікаційну шкалу. Далі центр приймає рішення про те, чи повинна подія бути класифікована як інцидент. Якщо підприємство зможе виділити кошти для утримання групи реагування на інциденти ІБ, оцінка та прийняте рішення контактним центром, передається групі для підтвердження чи повторної оцінки. Результати оцінювання повинні бути зафіксовані.

4. Реакція на інцидент ІБ. Такі дії виконують за призначенням контактного центру або інших уповноважених осіб. Реакція на інцидент ІБ повинна включати в себе: якомога швидше зібрати відомості про те, що сталося; за потреби провести ретроспективний аналіз; за потреби передати рішення на вищий рівень; зареєструвати усі дії, які були виконані у відповідь на інцидент; сповістити про інцидент, тих осіб, які мають про нього знати, виходячи зі службової необхідності; усунення вразливості/вразливостей ІБ, які спричинили інцидент; офіційне закриття та документація інциденту.

5. Необхідно виконати аналіз після інциденту.

6. Дані, отримані після аналізу інциденту, повинні використовуватися для зменшення ймовірності виникнення інцидентів та легшого виявлення повторних

чи схожих інцидентів.

7. Збір свідчень. Потрібно провести ідентифікацію, збір та зберігання даних щодо інциденту, який мав місце. Така процедура повинна передбачати: порядок передачі та зберігання; компетентність персоналу; ролі та обов'язки задіяного персоналу; компетентність персоналу; документацію; інструктаж. Якщо є можливість, потрібно оцінити придатність персоналу та інструментарію, для підвищення цінності зібраних свідчень.

Висновки

У даному розділі монографії представлено комплекс рекомендацій для вдосконалення політики інформаційної безпеки. Ретельний аудит конфігурацій мережевих пристроїв виявив низку проблем, які можуть вплинути на стійкість і ефективність заходів безпеки. Було наведено рекомендації та конкретні кроки для усунення виявлених вразливостей. Проведення сканування хостів на вразливості, з використанням популярних інструментів етичного хакінгу, допомогло ідентифікувати потенційні ризики. Також було надано ряд настанов для впровадження заходів щодо усунення недоліків. Було запропоновано оптимальну оперативну процедуру для дій при інцидентах інформаційної безпеки, що передбачає швидке та координоване реагування на випадки порушення безпеки.

Загальна інтеграція цих рекомендацій стане ключовим кроком у забезпеченні надійності та стійкості інформаційного середовища організації перед сучасними викликами в галузі кібербезпеки.

Verweise / References

Chapter 1.

1.Kuklin V. M. (2023) On the question of the appearance of consciousness in neural networks // Philosophical peripeteias, Karazin Kharkov University 68, 2023. P. 32-38; DOI: 10.26565/2226-0994-2023-68-3

2. Gushchin I. V.(2017 Modeling of physical processes using CUDA technology / I.V. Gushchin I. V., Kuklin V. M., Mishin O. V., Priymak O. V. – Kh.: KhNU named after V. N. Karazin, 2017. – 116 p.

3.OpenAI. GPT (2023)– 4 technical report, 2023. arXiv preprint arXiv:2303.08774 [cs.CL] https://doi.org/10.48550/arXiv.2303.08774.

4.Linda S. et all. (1997) Mainstream science on intelligence: An editorial with 52 signs, history, and bibliography, 1997.

5.Bubeckar S. (2023) Sparks of Artificial General Intelligence: Early experiments with GPT –4/ arXiv:2303.12712v2 [cs.CL] 24 Mar 2023.

6. Hochreiter, S., Bengio, Y., Frasconi, P., & Schmidhuber, J. (2001). Gradient flow in recurrent nets: the difficulty of learning long-term dependencies. A Field Guide to Dynamical Recurrent Neural Networks. IEEE Press.

7. Chung, J., Gulcehre, C., Cho, K., & Bengio, Y. (2014). Empirical evaluation of gated recurrent neural networks on sequence modeling. ArXiv:1412.3555.

8. Abramov GS. Gushchin IV, Sirenka T.O. (2024) On the evolution of recurrent neural systems System research and information technologies. 2024;4;77-85.

9. Bahdanau, D., Cho, K., & Bengio, Y. (2014). Neural machine translation by jointly learning to align and translate. ArXiv:1409.0473.

10. Charniak E. Introduction to deep learning (2003,) - The MIT Press Cambridge, Massachuset. Bengio Y., Ducharme R., Vincent P. A Neural Probabilistic Language Model // Journal of Machine Learning Research, 2003, vol. 3. - P. 1137–1155.

11. Sutskever, I., Martens, J., Dahl, G., & Hinton, G. (2013). On the importance of initialization and momentum in deep learning. International Conference on

Machine Learning (pp. 1139–1147).

12. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems (pp. 5998–6008).
13. Gushchyn I.V. Kirichok A.V, Kuklin V.M. (2024) Introduction to Methods of Organization and Optimization of Neural Networks. Kharkiv: V. N. Karazin Kharkiv National University, 2024,229 (in print).
14. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., … Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems (pp. 5998–6008).
15. Altarabichi MG. (2024) Dropkan: Regularizing kans by masking post-activations. arXiv preprint arXiv:2407.13044, 2024.
16. Willison S.(2024) Things we learned about LLMs in 2024 by Simon Willison, posted on 31st December 2024.
17. Kaplan J., et all. (2001) Scaling Laws for Neural Language Models, arXiv:2001.08361v1 [cs.LG]. https://doi.org/10.48550/arXiv.2001.08361yu
18. Amir Gholami A. et all., (2024) AI and Memory Wall / arXiv:2403.14123 [cs.LG]. https://doi.org/10.48550yu
20. Hooper C. et al. (2025) KVQuant: Towards 10 Million Context Length LLM Inference with KV Cache Quantization / arXiv:2401.18079v6 [cs.LG] 28 May 2025.
21. Valmeekam K., Stechly K, Kambhampati S. (2024) LLMS still can't plan; can LRMS? A preliminary evaluation of openai's o1 on PLANBENCH. arXiv:2409.13373v1 [cs.AI] 20 Sep 2024.
22. Valmeekam K., Stechly K, Gundawar A. Evaluating and Improving the Planning and Scheduling Capabilities of LRM o1 arXiv:2410.02162v1 [cs.AI] 3 Oct 2024.
23. Lightman H. et all. (2023) Let's Verify Step by Step. arXiv:2305.20050v1 [cs.LG] 31 May 2023.
24. Narayanan A. and Kapoor S. (2020) Start reading the AI Snake Oil book online. https://www.aisnakeoil.com/p/starting-reading-the-ai-snake-oil.

25. Hoffman R. (2023) Impromptu: Amplifying Our Humanity Through AI Paperback – March 15, 2023 248p.
26. Chen R. T. Q., Rubanova Y., Bettencourt J., Duvenaud D. (2019)) Neural Ordinary Differential Equations, arXiv:1806.07366 (2019). doi:10.48550/arXiv.1806.07366
27. Lev Semenovich Pontryagin, EF Mishchenko, VG Boltyanskii, and RV Gamkrelidze (1962). The mathematical theory of optimal processes. 1962.
28. LeCun Y, Touresky D, G Hinton G, and T Sejnowski T. (1988) A theoretical framework for back-propagation. In Proceedings of the 1988 connectionist models summer school, volume 1, pages 21–28. CMU, Pittsburgh, Pa: Morgan Kaufmann, 1988.
29. Bao-Bing Li, Yi Gu, and Shao-Feng Wu (2024) Discover Physical Concepts and Equations with Machine Learning / arXiv:2412.12161v1 [cs.LG] 11 Dec 2024.
30. Chen, R., Rubanova Y., Bettencourt J. & Duvenaud, D.(2018) Neural ordinary differential equations. Advances In Neural Information Processing Systems. 31 (2018); arXiv:1806.07366 (2019). doi:10.48550/arXiv.1806.07366.
31. Brunton S. L., Proctor J. L., Kutz J. N. (2016) Discovering governing equations from data by sparse identification of nonlinear dynamical systems, Proceedings of the National Academy of Sciences 113 (15) (2016) 3932–3937. doi:10.1073/pnas. 1517384113.
32. Iten, R., Metger, T., Wilming, H., Del Rio, L. & Renner, R. (2020)) Discovering physical concepts with neural networks. Physical Review Letters. 124, 010508 (2020).
33. Liu, Z., Madhavan, V. & Tegmark, M. (2022) Machine learning conservation laws from differential equations. Physical Review E. DOI: https://doi.org/10.1103/PhysRevE.106.045307

Chapter 2.

1. Автомобіль Бенца 1886. *ICM:* веб-сайт. URL: https://icm.com.ua/ua/technique/benz-patent-motorwagen-1886-easy-version-2/ (дата звернення 18.09.2025).

2. Smith G.M. What Is CAN Bus (Controller Area Network) and How It Compares to Other Vehicle Bus Networks. *Dewesoft d.o.o.:* веб-сайт. URL: https://dewesoft.com/blog/what-is-can-bus (дата звернення 18.09.2025).
3. History of CAN technology. *CAN in Automation:* веб-сайт. URL: https://www.can-cia.org/can-knowledge/history-of-can-technology (дата звернення 18.09.2025).
4. Institute of Industrial Information Technology. *KIT – The Research University in the Helmholtz Association:* веб-сайт. URL: https://www.iiit.kit.edu/english/kiencke.php (дата звернення 18.09.2025).
5. CAN Bus Explained - A Simple Intro [2025]. *CSS Electronics:* веб-сайт. URL: https://www.csselectronics.com/pages/can-bus-simple-intro-tutorial (дата звернення 18.09.2025).
6. Storia della Tecnologia CAN. *Cabletronic SRL:* веб-сайт. URL: https://www.cabletronicsrl.com/approfondimenti/storia-della-tecnologia-can (дата звернення 18.09.2025).
7. The Basics of CANopen. *National Instruments CORP.:* веб-сайт. URL: https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/the-basics-of-canopen.html (дата звернення 18.09.2025).
8. DeviceNet Frequently Asked Questions. *MKS Inc.:* веб-сайт. URL: https://www.mks.com/n/devicenet-frequently-asked-questions (дата звернення 18.09.2025).
9. DeviceNet - A Comprehensive Overview. *Chipkin:* веб-сайт. URL: https://store.chipkin.com/articles/devicenet-a-comprehensive-overview (дата звернення 18.09.2025).
10. ControlNet. *Keyence Corporation:* веб-сайт. URL: https://www.keyence.com/ss/products/controls/network/fieldnetwork/controlnet.jsp (дата звернення 18.09.2025).
11. ControlNet : Architecture, Working, Differences & Its Applications. *Elprocus:* веб-сайт. URL: https://www.elprocus.com/controlnet/ (дата звернення 18.09.2025).
12. What Is Controlnet? *RealPars B.V.*: веб-сайт. URL:

https://files.valinonline.com/userfiles/documents/turck-sds.pdf (дата звернення 18.09.2025).

13. SDS (Smart Distributed System). *Valinonline*: веб-сайт. URL: https://www.realpars.com/blog/controlnet (дата звернення 18.09.2025).
14. SDS###: A CAN Protocol for Plant Floor Control. *CAN-CiA*: веб-сайт. URL: https://www.can-cia.org/fileadmin/cia/documents/proceedings/1995_beck.pdf (дата звернення 18.09.2025).
15. Kvaser's History. *Kvaser*: веб-сайт. URL: https://kvaser.com/about-us/history/ (дата звернення 18.09.2025).
16. A CAN Kingdom Rev. 3.01. *Kvaser*: веб-сайт. URL: https://kvaser.com/wp-content/uploads/2014/02/ck301p.pdf (дата звернення 18.09.2025).
17. CANaerospace. *Scribd Inc.*: веб-сайт. URL: https://www.scribd.com/document/164772863/CANaerospace-Presentation (дата звернення 18.09.2025).
18. History and trends: CAN in air and space. *CAN-CiA*: веб-сайт. URL: https://www.can-cia.org/fileadmin/cia/documents/publications/cnlm/june_2022/cnlm_22-2_p18_can_in_air_and_space_cindy_weissmueller_cia.pdf (дата звернення 18.09.2025).
19. Time-Triggered CAN: TTCAN Benefits. *Scribd Inc.*: веб-сайт. URL: https://www.scribd.com/document/42270919/TTCAN (дата звернення 18.09.2025).
20. TTCAN explained. *Kvaser*: веб-сайт. URL: https://kvaser.com/wp-content/uploads/2014/08/ttcan-explained.pdf (дата звернення 18.09.2025).
21. General Motors Local Area Network Enhanced Diagnostic Test Mode Specification. *Scribd Inc.*: веб-сайт. URL: https://www.scribd.com/document/514484019/MNHJ (дата звернення 18.09.2025).
22. SafetyBUS p. *Academic,*: веб-сайт. URL: https://en-academic.com/dic.nsf/enwiki/5121287 (дата звернення 18.09.2025).
23. Pilz Safety PLC. *Scribd Inc.*: веб-сайт. URL:

https://www.scribd.com/document/51036745/pilz-safety-plc (дата звернення 18.09.2025).

24. NMEA2000 - How it works and why it's a must on board. *SVB*: веб-сайт. URL: https://www.svb24.com/en/guide/nmea2000-networks.html (дата звернення 18.09.2025).
25. Мережа NMEA-2000 і прилади що мають такий роз'єм. *Сейл Моторс*: веб-сайт. URL: http://sail.com.ua/statti/52-merezha-nmea-2000.html (дата звернення 18.09.2025).
26. What is it that makes DUOTECNO so much more? *Duotecno*: веб-сайт. URL: https://www.duotecno.be/en/
27. Grodans Paradis AB: VSCP & The Very Simple Control Protocol. *Grodans Paradis AB*: веб-сайт. URL: https://www.grodansparadis.com/ (дата звернення 18.09.2025).
28. VSCP: Very Simple Control Protocol. *VSCP*: веб-сайт. URL: https://www.vscp.org/ (дата звернення 18.09.2025).
29. J1939 Explained - A Simple Intro [2025]. *CSS Electronics*: веб-сайт. URL: https://www.csselectronics.com/pages/j1939-explained-simple-intro-tutorial/ (дата звернення 18.09.2025).
30. A Brief Introduction to the SAE J1939 Protocol. *Copperhill*: веб-сайт. URL: https://copperhilltech.com/a-brief-introduction-to-the-sae-j1939-protocol/ (дата звернення 18.09.2025).
31. J2366/1_200111 - ITS Data Bus—IDB-C Physical Layer. *SAE International*: веб-сайт. URL: https://www.sae.org/standards/j23661_200111-data-bus-idb-c-physical-layer (дата звернення 18.09.2025).
32. Kim C. Information Networking: Convergence in Broadband and Mobile Networking. *Springer*: веб-сайт. URL: https://books.google.com.ua/books?id=3xX6BwAAQBAJ&pg=PA552&lpg=PA552&dq=IDB-C+protocol&source=bl&ots=vVOWJamyIr&sig=-vkazMUKw73d94gs-P3ZNeSGTeo&hl=uk&sa=X&ved=0ahUKEwigucCj95zVAhUkCpoKHZH6Dm

8Q6AEINDAC#v=onepage&q=IDB-C%20protocol&f=false (дата звернення 25.01.2023).

33. iNELS: Intelligent Electric Installation Systems for Buildings Installation Manual. iNELS. - 62 p.
34. iNELS: Intelligent Electroinstallation System. ELKO EP S.R.O. - 136 p.
35. iNELS Highlights. INELS. - 10 p.

Chapter 3.

1. Ştefănescu E., Chelaru V.F., Chira D., Mureşanu D. (2024). Eye Tracking Assessment of Parkinson's Disease: a Clinical Retrospective Analysis. J. Med. Life, vol. 17, no. 3, p. 360.

DOI: https://doi.org/10.25122/jml-2024-0270.

2. Jansson D., Rosén O., Medvedev A. (2015). Parametric and nonparametric analysis of eye-tracking data by anomaly detection. IEEE Trans. Control Syst. Technol., vol. 23, pp. 1578–1586.

DOI: https://doi.org/10.1109/TCST.2014.2364958.

3. Keehn B., Monahan P., Enneking B., et al. (2024). Eye-Tracking Biomarkers and Autism Diagnosis in Primary Care. JAMA Netw Open, vol. 7, no. 5, e2411190, pp. 1–14.

DOI: https://doi.org/10.1001/jamanetworkopen.2024.11190.

4. Dostálová N., Pátková Daňsová P., Ježek S., Vojtechovska M., Šašinka Č. (2024). Towards the Intervention of Dyslexia: a Complex Concept of Dyslexia Intervention System using Eye-Tracking. Proc. of the 2024 Symp. on Eye Tracking Research and Applications (ETRA '24), Article 84, pp. 1-6.

DOI: https://doi.org/10.1145/3649902.3656490.

5. Sun W., Wang Y., Hu B., Wang Q. (2024). Exploring the Connection between Eye Movement Parameters and Eye Fatigue. J. Phys.: Conf. Ser., vol. 2722.

DOI: https://doi.org/10.1088/1742-6596/2722/1/012013 .

6. Sevcenko N., Appel T., Ninaus M., et al. (2023). Theory-based approach for assessing cognitive load during time-critical resource-managing human–computer

interactions: an eye-tracking study. J. Multimodal User Interfaces, vol. 17, pp. 1-19.

DOI: https://doi.org/10.1007/s12193-022-00398-y

7. Mézière D.C., Yu L., Reichle E.D., Von Der Malsburg T., McArthur G. (2023). Using eye-tracking measures to predict reading comprehension. Reading Research Quarterly, vol. 58, no. 3, pp. 425-449.

DOI: https://doi.org/10.1002/rrq.498

8. Li S., Duffy M.C., Lajoie S.P., Zheng J., Lachapelle K. (2023). Using eye tracking to examine expert–novice differences during simulated surgical training: a case study. Computers in Human Behavior, vol. 144, 107720.

DOI: https://doi.org/10.1016/j.chb.2023.107720

9. Sun J., Liu Y., Wu H., Jing P., Ji Y. (2022). A novel deep learning approach for diagnosing Alzheimer's disease based on eye-tracking data. Front. Hum. Neurosci., vol. 16, Article 972773.

DOI: https://doi.org/10.3389/fnhum.2022.972773.

10. Kalla B.V., Mandava N., Surya C. (2024). Eye Disease Detection Using Deep Learning Models with Transfer Learning Techniques. ICST Trans. on Scalable Inf. Syst., vol. 11, 2024.

DOI: https://doi.org/10.4108/eetsis.5971.

11. Solodusha S., Kokonova Y., Dudareva O. (2023). Integral Models in the Form of Volterra Polynomials and Continued Fractions in the Problem of Identifying Input Signals. Mathematics, vol. 11, no. 23, 4724.

DOI: https://doi.org/10.3390/math11234724.

12. Bro V., Medvedev A. (2023). Continuous and Discrete Volterra-Laguerre Models with Delay for Modeling of Smooth Pursuit Eye Movements. IEEE Trans. Biomed. Eng., vol. 70, no. 1, pp. 97-104.

13. Doyle F.J., Pearson R.K., Ogunnaike B.A. (2001). Identification and Control Using Volterra Models. Communications and Control Engineering, Springer, London.

14. Weiss K., Kolbe M., Lohmeyer Q., Meboldt M. (2023). Measuring teamwork for training in healthcare using eye tracking and pose estimation. Front. Psychol., vol.

14, Article 1169940.

DOI: https://doi.org/10.3389/fpsyg.2023.1169940.

15. Yin J., Sun J., Li J., Liu K. (2022). An Effective Gaze-Based Authentication Method with the Spatiotemporal Feature of Eye Movement. Sensors, vol. 22, Article 3002, pp. 1-18.

DOI: https://doi.org/10.3390/s22083002.

16. Lanata L., Sebastian L., Di Gruttola F., et al. (2020). Nonlinear Analysis of Eye-Tracking Information for Motor Imagery Assessments. Front. Neurosci., vol. 13, Article 1431.

DOI: https://doi.org/10.3389/fnins.2019.01431.

17. Porras M.M., Campen C.A.N. Kv., González-Rosa J.J., et al. (2024). Eye Tracking Study in Children to Assess Mental Calculation and Eye Movements. Sci. Rep., vol. 14, Article 18901.

DOI: https://doi.org/10.1038/s41598-024-69800-x.

18. Chandran P., Huang Y., Munsell J., et al. (2024). Characterizing learners' complex attentional states during online multimedia learning using eye-tracking, egocentric camera, webcam, and retrospective recalls. Proc. of the 2024 Symp. on Eye Tracking Research and Applications (ETRA '24).

DOI: https://doi.org/10.1145/3649902.3653939.

19. Pardhu T., Deevi N. (2023). EEG Artifact Removal Strategies for BCI Applications: A Survey. Int. J. Electr. Eng. Comput. Sci., vol. 5, pp. 57-72.

DOI: https://doi.org/10.37394/232027.2023.5.8

20. Tablatin C.L.S. (2023). Visual Attention Patterns in Finding Source Code Defects. WSEAS Trans. on Inf. Sci. and Appl., vol. 20, pp. 375-389.

DOI: https://doi.org/10.37394/23209.2023.20.40.

21. Hämäläinen R., De Wever B., Sipiläinen K., Zemblys R. (2024). Using eye tracking to support professional learning in vision-intensive professions: a case of aviation pilots. Educ. Inf. Technol., 2024.

DOI: https://doi.org/10.1007/s10639-024-12814-9.

22. Pavlenko V., Lukashuk D. (2025). Machine Learning Effectiveness of a

Psychophysiological State Classification System based on Eye Tracking Technology. WSEAS Trans. on Systems, vol. 24, pp. 424-437.
DOI: https://doi.org/10.37394/23202.2025.24.37

23. Pavlenko V., Pavlenko S. (2018). Deterministic Identification Methods for Nonlinear Dynamical Systems Based on the Volterra Model. Applied Aspects of Information Technology, vol. 1, no. 1, pp. 9-29.
DOI: https://doi.org/10.15276/aait.01.2018.1.
24. Pavlenko V., Milosz M., Dzienkowski M. (2020). Identification of the Oculo-Motor System Based on the Volterra Model Using Eye Tracking Technology. J. Phys.: Conf. Ser., vol. 1603, pp. 1-8.
DOI: https://doi.org/10.1088/1742-6596/1603/1/012011.
25. Pavlenko V., Shamanina T., Chori V. (2024). Nonlinear dynamic model of the oculo-motor system human based on the Volterra series. In: Awrejcewicz J. (ed) Perspectives in Dynamical Systems II — Numerical and Analytical Approaches. Springer Proc. in Mathematics & Statistics, vol. 454, Cham: Springer, pp. 1-12.
DOI: https://doi.org/10.1007/978-3-031-56496-3_27.
26. Sundararajan D. (2016). Discrete Wavelet Transform: A Signal Processing Approach. John Wiley & Sons, 344 p.

Chapter 4.

1. AIIM, 2020. State of the IIM Industry 2020, https://surl.li/woyxdf
2. ARMA International, 2019. Generally Accepted Recordkeeping Principles, Kansas city, MO: https://sosmt.gov/Portals/142/ARM/2015/notices/the-principles_executive-summaries_final.pdf.
3. European Union, 2025. Artificial Intelligence Act. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689
4. European Union, 2025. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Available at: https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

5. EY, 2025. How EY is navigating global AI compliance: The EU AI Act and beyond. Available at: https://www.ey.com/en_gl/insights/ai/how-ey-is-navigating-global-ai-compliance-the-eu-ai-act-and-beyond
6. International Journal of Public Administration, 2025. Digital Transformation of Public Services: The Case of the Document Management Application. Available at: https://www.tandfonline.com/doi/full/10.1080/01900692.2025.2520522?utm_source=chatgpt.com#abstract
7. KPMG, 2025. AI IN FINANCE: US REPORT. Available at: https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/audit/ai-in-finance-us-report-dec-2024.pdf
8. OECD.AI, 2025. The OECD.AI Policy Navigator. Available at: https://oecd.ai/en/
9. OECD, 2025. ICT Access and Usage by Businesses. Available at: https://surl.li/rjbzcv
10. Online Browsing Platform (OBP), 2025. ISO 15489-1:2016 Information and documentation — Records management. Available at: https://www.iso.org/obp/ui/en/#iso:std:iso:15489:-1:ed-2:v1:en

Chapter 5.

1. DSTU ISO/IEC 12207:2016. Systems and software engineering. Software life cycle processes (ISO/IEC 12207:2008, IDT). Kyiv: DP "UkrNDNTs", 2016. 156 p.
2. DSTU ISO/IEC 25010:2023. Systems and software. Product quality model (ISO/IEC 25010:2011, IDT). Kyiv: DP "UkrNDNTs", 2023. 36 p.
3. DSTU ISO/IEC 90003:2006. Software engineering. Guidelines for the application of ISO 9001:2000 to software (ISO/IEC 90003:2004, IDT). Kyiv: DP "UkrNDNTs", 2006. 68 p.
4. DSTU ISO/IEC 27001:2022. Information security. Information security management systems. Requirements (ISO/IEC 27001:2022, IDT). Kyiv: DP "UkrNDNTs", 2022. 40 p.

5. ISO/IEC 12207:2017. Systems and software engineering — Software life cycle processes. Geneva: ISO/IEC, 2017. 160 p.
6. ISO/IEC 25010:2023. Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model. Geneva: ISO/IEC, 2023. 36 p.
7. ISO/IEC 20000-1:2018. Information technology — Service management — Part 1: Service management system requirements. Geneva: ISO/IEC, 2018. 52 p.
8. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022. 36 p.
9. ISO/IEC 90003:2018. Software engineering — Guidelines for the application of ISO 9001:2015 to computer software. Geneva: ISO/IEC, 2018. 92 p.
10. Law of Ukraine "On Standardization" dated 05.06.2014 No. 1315-VII (as amended as of 2025). Official Gazette of the Verkhovna Rada of Ukraine. 2014. No. 28. Art. 950.
11. Zaitsev I., Golubenko O., Tkachenko O., Pidmohylnyi O. (2023). Exploring advanced hypothesis generation in astronomy through the implementation of a mathematical model of linguistic neural networks. CEUR Workshop Proceedings, 2023, 3687, 121–128
12. Shevchenko R. I. Activities of technical committees for ICT standardization in Ukraine. Bulletin of the NAS of Ukraine. 2024. No. 2. P. 55–62.
13. Benediko I. V., Vichkaruk A. I., Lysenko K. V., & Syzhko O. Yu. (2023). Classifications of Machine Learning Application Models in Cybersecurity. Tavria Scientific Bulletin. Series: Technical Sciences, (4), 11-22.
14. Kravchenko O. V. Standardization of Software in Ukraine: Current State and Prospects. Bulletin of the Taras Shevchenko National University of Kyiv. Series: Radiophysics and Electronics. 2023. Vol. 28, No. 2. P. 45–52.
15. Bondarenko E.S., Kan'shyn K. V., Stepanchuk V. I., & Lanevsky L. A. (2023). Classification and features of data collection in management decision support systems. Tavria Scientific Bulletin. Series: Technical Sciences, (4), 23-31.

16. Petrenko I.S. Certification of quality systems in ICT: regulatory and legal aspects. Scientific Bulletin of the National University "Lviv Polytechnic". Series: Information Systems and Networks. 2024. No. 1. P. 112–120.
17. Sydorenko A.M. Quality management based on ISO 9000 in the field of information technologies. Economics and management of information systems. 2022. No. 4. P. 67–75.
18. Hrytsenko, L.O. Information support for standardization in ICT: the role of the national fund. Standardization. Certification. Quality. 2024. No. 3. P. 15–22.
19. Bondarenko T.V. Classification of standards in software: analysis of the ISO/IEC series. Proceedings of the International Scientific and Practical Conference "Innovations in ICT". Kyiv, 2023. P. 89–96.
20. Kovalenko, O. D. Structure of state standards in the field of IT means. Technologies and means of communication. 2023. No. 4. P. 34–41.
21. Boyko N.V. IT Services Certification: Schemes and Problems in Ukraine. Electronic Technologies and Information Systems. 2025. No. 1. Pp. 78–85.

Chapter 6.

1. Трояновська Т. І. Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.
2. Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2021. – 188 с.
3. Комп'ютерні мережі: навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2022. – 228 с.
4. Трояновська Т. І. Інформаційна технологія доставки контенту у системах комп’ютеризованої підготовки спеціалістів. // Гороховський О. І., Трояновська Т. І., Азаров О. Д. Монографія. Вінниця : ВНТУ, 2016.–160 с.
5. Маліновський, В. І., Куперштейн, Л. М., Лукічов, В. В., & Дудатьєв, А. В. (2024). Проблематика і підходи підвищення рівня захисту в каналах передачі

даних систем і пристроїв Інтернету речей. Вісник Вінницького політехнічного інституту.№ 4: 105-115.

6. Лужецький, В., Савицька, Л. (2024). Механізми забезпечення захисту даних у піринговых мережах. Herald of khmelnytskyi national university. Technical sciences, 339(4), 503-508.
7. Чинчик Д. М. Методи та засоби комплексного захисту корпоративної мережі / Д. М. Чинчик, Т. І. Коробейнікова, С. М. Захаченко // Scientific Collection «InterConf», (84): with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021). Rome, Italy: Dana, 2021. 478 p. – С. 433-450.
8. Методи та засоби комплексного захисту корпоративної мережі. / Чинчик Д. М., Коробейнікова Т. І. // Стратегічні напрямки розвитку науки: фактори впливу та взаємодії: матеріали II Міжнародної наукової конференції, м. Рівне, 7 квітня, 2023р. Міжнародний центр наукових досліджень. – Вінниця: Європейська наукова платформа, 2023. – С. 97-102.
9. Чинчик Д. Метод комплексного захисту корпоративної мережі / Д. Чинчик, Т. Коробейнікова, Н. Лужецька // Захист інформації і безпека інформаційних систем: матеріали IX Міжнар. наук.-техн. конф. – Львів : Видавництво Львівської політехніки, 2023. – Режим доступу: https://drive.google.com/drive/folders/1z5BLogqaxwh4xgGk2eMLI8WcVNOXCFX6, вільний – Заголовок з екрана. – С. 29-30.
10. Chynchyk D. Specialized mechanisms for protecting the corporate network in terms of network security / D. Chynchyk, T. Korobeinikova // “Information protection and information systems security” : Materials of VIII-th International Scientific and Technical Conference, November 11 – 12, 2021. – Lviv: NULP, 2021 – С. 51-53.
11. Таченко І. А. Огляд сучасного стану питання в галузі оцінювання ризиків мережевої безпеки / І. А. Таченко, Т. І. Коробейнікова, С. М. Захаченко // Scientific Collection «InterConf», (84): with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science:

Key Aspects» (November 7-8, 2021). Rome, Italy: Dana, 2021. 478 p. – C. 417-432.

12. T. Korobeinikova, I. Tachenko, O. Romanyuk, S. Romanyuk, O. Stakhov and O. Reyda, "Assessing Network Security Risks: a Technological Chain Perspective," 2024 14th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2024, pp. 565-570, doi: 10.1109/ACIT62333.2024.10712586.
13. T. Korobeinikova, I. Tachenko, R. Chekhmestruk, P. Mykhaylov, O. Romanyuk and S. Romanyuk, "A General Method of Risk Estimation," 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland, 2023, pp. 410-413, doi: 10.1109/ACIT58437.2023.10275626. (Scopus)

SCIENTIFIC EDITION

MONOGRAPH

DER STAND DER ENTWICKLUNG VON WISSENSCHAFT UND TECHNIK IM XXI JAHRHUNDERTS

INFORMATIK, KYBERNETIK UND AUTOMATISIERUNG; SICHERHEITSSYSTEME IN DER MODERNEN WELT

THE LEVEL OF DEVELOPMENT OF SCIENCE AND TECHNOLOGY IN THE XXI CENTURY

COMPUTER SCIENCE, CYBERNETICS, AND AUTOMATION; SECURITY SYSTEMS IN THE MODERN WORLD

MONOGRAPHIC SERIES «EUROPEAN SCIENCE»

BOOK 42. PART 4

Authors:

Kuklin V.M. (1), Babchuk S. (2), Pavlenko V.D. (3), Lukashuk D.K. (3), Pozniak O.V. (4), Kharakhash N.M. (4), Antonenko A.V. (5), Tolok G.A. (5), Brovenko T.V. (5), Vostrikov S.O. (5), Chechyk S.V. (5), Tkachenko O.V. (5), Didovets V.M. (5), Kozhemiakin O.V. (5), Borodavko M.I. (5), Nazarenko D.O. (5), Korobeinikova T.I. (6), Zhuravel I.M. (6)

The scientific achievements of the authors of the monograph were also reviewed and recommended for publication at the international scientific symposium
«Der Stand der Entwicklung von Wissenschaft und Technik im XXI Jahrhunderts/
The level of development of science and technology in the XXI century '2025»
(September 30, 2025)

Monograph published in the author's edition

The monograph is included in
International scientometric databases

500 copies
September, 2025

Published:
ScientificWorld -NetAkhatAV
Lußstr 13,
Karlsruhe, Germany

e-mail: editor@promonograph.org
https://desymp.promonograph.org

ISBN 978-3-989241-14-5

https://desymp.promonograph.org

e-mail: editor@promonograph.org