**Тема 6. Інформаційна гігієна дослідника**

План

1. Безпека збереження даних

2. Безпечне використання інформаційних ресурсів та прикладних програм (спеціалізоване програмне забезпечення та інформаційні системи)

3. Використання інформації з джерел держави-агресора

**Безпека даних –** це практика захисту цифрової інформації від несанкціонованого доступу, порушення цілісності або крадіжки. Ця концепція охоплює всі форми інформаційної безпеки: від фізичного захисту обладнання, контролю доступу, логічної безпеки програмного забезпечення до організаційних політик і процедур.

Заходи безпеки, реалізовані належним чином, допоможуть захистити дані організацій від кіберзлочинів, людських помилок і навіть внутрішніх загроз. Проте також потрібні інструменти й технології для підвищення спроможності організації контролювати використання власних даних. Крім того, ці сервісні програми можуть шифрувати, редагувати та маскувати конфіденційні дані. В ідеалі система інформаційної безпеки також здатна автоматизувати звітність, спростити аудиторські перевірки та допомогти у виконанні нормативних вимог.

У всьому світі організації інвестують у безпеку даних, щоб захистити свої бренди, інтелектуальний капітал, інформацію про клієнтів і забезпечити контроль важливих об’єктів інфраструктури. Нездатність забезпечити відповідні заходи безпеки для даних або відсутність належних заходів контролю можуть призвести до витоку даних. Витоки даних можуть коштувати компаніям багато мільйонів доларів у виді судових витрат, штрафів і втрати бізнесу. За результатами опитувань більшість людей відповіли, що відмовилися б від послуг компанії, в якій стався витік даних, оскільки надійне програмне забезпечення для захисту даних є невід’ємною складовою успіху компанії.

Існує безліч видів захисту даних. Іноді для захисту інформації використовують апаратні засоби, але програмні засоби зустрічаються частіше.

* Шифрування: шифрування файлів і баз даних є останньою лінією захисту конфіденційних даних; може бути як апаратним, так і програмним
* Стирання даних: програмне забезпечення для повного перезапису всіх слідів даних; безпечніше, ніж видалення.
* Маскування даних: приховує персональні ідентифікаційні дані (PII), щоб команди могли розробляти програми або практикуватися на основі реальних даних.
* Виявлення та класифікація даних: автоматизація процесу виявлення конфіденційної інформації та оцінки з подальшим усуненням вразливостей
* Моніторинг активності даних і файлів: ці інструменти аналізують моделі використання даних, щоб служба безпеки могла встановити ризики, виявити аномалії та визначити, хто має доступ до даних; також може бути розгорнуте динамічне блокування й оповіщення.
* Оцінка вразливостей/аналіз ризиків: ці інструменти виявляють і усувають вразливі місця, наприклад, неправильну конфігурацію або слабкі паролі; можуть визначати джерела даних, які створюють загрозу безпеці
* Автоматизована звітність про дотримання нормативних вимог: рішення для захисту даних із можливостями автоматизованої звітності можуть забезпечити централізоване сховище даних для аудиту дотримання нормативних вимог у межах підприємства

Хоча шифрування є одним із найкращих способів захистити свої дані, слід пам’ятати, що програмне шифрування легше обійти або вимкнути, ніж апаратне шифрування. Якщо ви серйозно ставитеся до використання шифрування у вашій стратегії захисту даних організації, вам слід інвестувати в рішення з апаратним шифруванням.

Інструменти й технології захисту даних повинні розуміти, де зберігаються дані, відстежувати, хто ними користується, і блокувати небажані операції, наприклад дії, пов’язані з високим ризиком, або небезпечні переміщення файлів.

Комплексна стратегія захисту даних передбачає відповідний персонал, процеси та технології. Культура та інструментальні засоби мають важливе значення для створення належних механізмів контролю і політик. Тільки цілісний підхід до безпеки даних може зробити її пріоритетним напрямом у всіх сферах діяльності підприємства.

Існує безліч політик, пов’язаних із безпекою даних, які організації можуть впроваджувати, щоб покращити свою діяльність. Однією з таких політик є керування доступом. Здійснюючи жорсткий контроль за доступом до баз даних, мережі та облікових записів адміністраторів, обмежуючи привілейований доступ якомога меншою кількістю осіб, організації можуть захистити свою найважливішу інформацію від загроз, пов’язаних із збільшенням кількості точок відмови. Коли ви чуєте фразу «доступ із найменшими привілеями», це беззаперечна ознака того, що ця організація серйозно ставиться до керування доступом. У безпечному бізнесі-середовищі співробітники повинні мати відповідний доступ, потрібний для виконання своїх робочих завдань, і нічого більше.

Іншою політикою надійного захисту даних є безпека програм. Переконайтеся, що співробітники вашої компанії завжди використовують актуальні версії програмного забезпечення, включно з усіма виправленнями й оновленнями. Так ви можете бути впевнені, що будь-які вразливості системи безпеки, які буде виявлено в програмному забезпеченні, не стануть точками входу в мережу вашого робочого місця.

Програмне забезпечення для моніторингу безпеки мережі й кінцевих точок також є важливою складовою будь-якого плану інформаційної безпеки. Застосування інструментів, наприклад для виявлення загроз або керування ними, а також інструментів і платформ реагування для локальних систем і хмарних середовищ може значно мінімізувати ризики та зменшити ймовірність витоку даних.

Проте жодна з цих політик не буде ефективною, якщо навчання співробітників само собою не є основою стратегії захисту даних організації. Тому навчання правильному використанню програмного забезпечення для захисту даних, а також ширші можливості для освоєння загальних принципів безпеки даних, як-от соціальна інженерія або «гігієна паролів», мають стати основним предметом стурбованості будь-якої організації, особливо якщо більшість співробітників працює з інформацією, що ідентифікує особу.

Установи, які інвестують у безпеку даних, отримують безліч переваг.

* Захист конфіденційної інформації: Установи зазвичай збирають великі обсяги конфіденційних і/або особистих даних. Програмне забезпечення для захисту даних зберігає ці дані у відповідних місцях, і допомагає уникнути ситуацій, пов’язаних із витоком даних.
* Захист репутації організації: надійний план інформаційної безпеки захищає конфіденційність співробітників, а також зовнішніх контрагентів, зміцнюючи довіру до вашої організації.
* Запобігання несанкціонованому доступу до даних: хакери можуть видалити, пошкодити або змінити дані, непомітно встановити зловмисну програми з вимогою викупу тощо. Ефективна система безпеки захищає підприємство від цих небажаних наслідків.
* Перевага над конкурентами: організація з жорстким захистом конфіденційних даних може перевершити своїх конкурентів. Конкурент, в якого станеться витік даних, втратить увесь прогрес і будь-які можливості для розвитку, чим ви можете скористатись із користю для себе.

Програмне забезпечення для захисту даних є невід’ємною складовою ІТ-стратегії будь-якої установи.

#### **Що таке шкідливе програмне забезпечення? Якої шкоди воно може завдати комп’ютеру чи смартфону?**

Шкідливе програмне забезпечення (ШПЗ) – це програмне забезпечення, яке за умови запуску може завдати шкоди пристрою різними способами, зокрема – призвести до:

* блокування пристрою та його непридатності для використання;
* крадіжки, видалення або шифрування даних;
* використання пристрою для атак на інші пристрої;
* отримання кіберзловмисниками інформації щодо облікових даних, які дозволяють дістати доступ до систем або служб, якими ви користуєтесь;
* використання для незаконного майнингу криптовалюти на вашому пристрої;
* використання платних послуг на основі ваших даних (наприклад, телефонні дзвінки на платні номери) тощо.

Серед найвідоміших видів ШПЗ –  віруси, трояни, програми-вимагачі, хробаки та інші. Детальніше про них можна дізнатися на сайті Урядової команди реагування на комп'ютерні надзвичайні події України [CERT-UA](https://cert.gov.ua/recommendation/2502), яка діє при Держспецзв’язку.

##### **Як може поширюватися ШПЗ:**

1. через електронні листи із небезпечними вкладеннями або посиланнями,
2. шляхом експлуатації зловмисником вразливостей систем,
3. через флеш-носії,
4. при використанні неліцензійних копій програмного забезпечення,
5. при завантаженні програмного забезпечення з неофіційних ресурсів тощо.

##### **Щоб убезпечити свій комп’ютер від шкідливого програмного забезпечення:**

* завантажуйте програми лише з офіційних магазинів чи вебсайтів розробника,
* не відкривайте підозрілих посилань і вкладень, надісланих на e-mail від невідомих відправників,
* використовуйте та вчасно оновлюйте антивіруси та програмне забезпечення,
* скануйте антивірусом флеш-носії та завантажені файли перед відкриттям,
* не підключайте периферійних пристроїв невідомого походження тощо.

Розроблено, затверджено та прийнято до виконання рекомендації Комітету з питань етики щодо припинення (обмеження) використання джерел інформації держави-агресора в наукових публікаціях. Рекомендації щодо припинення (обмеження) використання джерел інформації росії та білорусі, яка підтримала державу-агресора (далі – держав-агресорів), в наукових публікаціях (далі – Рекомендації) Комітету з питань етики (далі – Комітет) Національного агентства із забезпечення якості вищої освіти визначають загальні підходи до проведення джерельного пошуку та аналізу при здійсненні досліджень й оприлюдненні їх результатів.

Рекомендації не накладають заборону на використання джерел інформації держави-агресора в наукових публікаціях, а є етичними принципами, які мають застосовувати науковці під час проведення досліджень й оприлюдненні їх результатів.

Війна, яку веде росія проти України, вкотре підтверджує її антигуманну експансіоністську сутність. Інформаційне середовище, освіта, наука держав-агресорів постають одним із засобів реалізації політики злочинного режиму. Інформаційно-літературні й наукові джерела, створені у суспільстві, яке здебільшого підтримує агресивні дії свого уряду, несуть і моральну, і матеріальну шкоду для українського народу, а російська наукова спільнота не становить тут винятку . У зв’язку з цим необґрунтоване використання джерел інформації держав-агресорів є недоцільним для наукової об’єктивності, кругозору дослідників, не кажучи вже про питання національної безпеки в умовах війни та загалом подолання наслідків постколоніального мислення в наукових дослідженнях. Таким чином, нівелюється універсальність поглядів та підходів української науки до світового інформаційного простору. До того ж інформаційно-літературні й наукові джерела держав-агресорів, особливо створені в сфері соціальних, гуманітарних наук, можуть бути продуктом пропаганди та цензури сучасного авторитарного російського режиму. Використання ж інформаційно-літературних і наукових джерел держав-агресорів, а отже посилання на них, підвищує їхню соціальну значущість та наукову вагу, рейтинги їхніх авторів, легітимізує викладене в цих джерелах й російську науку в цілому. Подібний факт у багатьох випадках може не відповідати як юридичній та моральній позиції нашого суспільства й держави, так і міжнародної спільноти, яка підтримує нас у нашій боротьбі. У зв’язку з вищезазначеним пропонуються такі рекомендації:

1. Не використовувати у наукових дослідженнях такі джерела інформації:

– опубліковані на території держав-агресорів;

– опубліковані на територіях, окупованих росією, чи щодо яких вона здійснює контроль, якщо джерело опубліковане з моменту початку окупації чи такого контролю;

– створені та/або опубліковані державними інституціями держав-агресорів;

– автором яких є громадянин держави-агресора, за умови, що публічна позиція цієї особи або саме джерело спрямоване на виправдання російської (у тому числі радянської) імперської політики, містить пропаганду ідеології «русского міра», антиукраїнську пропаганду чи іншу офіційну пропаганду держави-агресора;

– автором яких є юридична особа, зареєстрована на території державагресорів, або кінцевим бенефіціарним власником (контролером) якої є резидент держав-агресорів.

2. Припускаються вмотивовані випадки використання джерел інформації держав-агресорів:

– для ілюстрування, пояснення та критичного аналізу явищ, що відбуваються в державах-агресорах;

– у наукових дослідженнях, зміст яких охоплює вивчення держав-агресорів, їх попередників чи складових політичних утворень, за умови критичного аналізу цих джерел;

– створених громадянином чи громадянкою держави-агресора, юридичною особою, зареєстрованою на території держави-агресора, або кінцевим бенефіціарним власником (контролером) якої є резидент держави-агресора, за умови, що джерела не містять пропаганди, ідеології «русского міра», антиукраїнської пропаганди чи іншої офіційної пропаганди держави-агресора; -за обґрунтованої необхідності, з точки зору досягнення мети дослідження чи які не мають аналогів у відповідній галузі знань та/або містять статистичну інформацію.

**Використані джерела:**

<https://www.kingston.com/ua/blog/data-security/what-is-data-security-software>

<https://naqa.gov.ua/wp-content/uploads/2023/12/%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D1%96%D1%97-%D0%9A%D0%BE%D0%BC%D1%96%D1%82%D0%B5%D1%82%D1%83-%D0%B7-%D0%BF%D0%B8%D1%82%D0%B0%D0%BD%D1%8C-%D0%B5%D1%82%D0%B8%D0%BA%D0%B8-%D0%BF%D1%80%D0%BE-%D0%B2%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F-%D0%B4%D0%B6%D0%B5%D1%80%D0%B5%D0%BB-%D0%B2%D1%96%D0%B4-30.11.2023.pdf?fbclid=IwAR1iBlPyFzlywHA2vsgJtWBU19xY4VM7FmYmH1VUJh1YoQRG3cVq69R2nqA>

<https://www.cip.gov.ua/ua/news/sho-take-shkidlive-programne-zabezpechennya-yakoyi-shkodi-vono-mozhe-zavdati-komp-yuteru-chi-smartfonu>