НОТАРІАЛЬНА
ПАЛАТА УКРАЇНИ

# ПК/ОСНОВИ НАЛАШТУВАНЬ

## ЛЕКТОР

**Костянтин Федосенко,**
приватний нотаріус Запорізького міського нотаріального округу, член комісії Нотаріальної палати України з питань інформатизації, цифрової трансформації та запобігання кіберзлочинності

# Тези:

1. Налаштування операційної системи та ліцензійне програмне забезпечення.
2. Антивірусне програмне забезпечення.
3. Використання окремого комп'ютера, налаштування доступу відвідувачів до локальної мережі інтернет.
4. Запобігання використанню сторонніх носіїв інформації.
5. Надійне збереження особистого ключа ЕЦП, нерозголошення ідентифікаторів доступу та паролів.

# 1. Налаштування операційної системи та використання ліцензійного програмного забезпечення:

Завжди використовуйте ліцензійне програмне забезпечення, оновлюючи його до останніх версій. Ліцензійне програмне забезпечення має більш високий рівень безпеки, оскільки воно підтримується розробниками і включає в себе оновлення з виправленнями вразливостей.

Неліцензійне програмне забезпечення може містити віруси і не мати заходів безпеки, необхідних для їх виявлення. Ви можете піддати свій домашній або робочий комп'ютер серйозним загрозам із боку хакерів та зловмисних програм і навіть не знати про це. Піратство програмного забезпечення є розповсюдженою глобальною проблемою. Кіберзлочинці використовують неліцензійне програмне забезпечення, щоб розповсюджувати зловмисні програми, а користувачі піддаються різним загрозам безпеці.

Наголошуємо Вашу увагу на забезпеченні повного контролювання доступу до системи шляхом використання принципу найменшого доступу. Це означає, що користувачам надається лише необхідний мінімум прав доступу для виконання їхніх обов'язків. Крім того, слід регулярно оновлювати і переглядати список всіх користувачів системи і їхні права доступу. Перевірка здійснюється через налаштування користувачів: перейдіть до налаштувань користувачів у Windows та перегляньте перелік облікових записів. **Якщо буде виявлено користувача з ім'ям odmin – негайно просимо повідомити про це нашу Комісію.**.

Власник системи має особливу відповідальність за забезпечення кібербезпеки інформації, що знаходиться у його власності або під його контролем. Це означає, що він повинен приділяти достатню увагу та ресурси для захисту цієї інформації від потенційних загроз і атак ззовні.

Власник системи має забезпечувати захист конфіденційності, цілісності та доступності даних, що зберігаються у системі. Це включає застосування відповідних заходів безпеки, які гарантують, що дані залишаються конфіденційними, не піддаються маніпуляції та доступні за необхідності.

Власник системи повинен дотримуватися всіх відповідних правових вимог та стандартів щодо зберігання та обробки інформації. Це може включати в себе дотримання законодавства щодо захисту персональних даних, регулятивних вимог щодо кібербезпеки та виконання стандартів безпеки інформації.

Власник системи має забезпечувати належне навчання та інформування свого персоналу щодо правил і процедур з кібербезпеки. Це допомагає підвищити рівень обізнаності персоналу з питань безпеки та зменшити ризик людського фактору у кібербезпеці.

# 2. Встановлення та налаштування антивірусного програмного забезпечення, захист системи та регулярні перевірки комп'ютера:

У сучасному світі важливість антивірусів стає очевидною, і захист від вірусів й інших загроз стає важливим завданням для збереження особистих даних як окремих користувачів, так і глобальних корпорацій в цілому. Антивірусне програмне забезпечення не тільки виявляє і блокує загрози, але також забезпечує спокій і впевненість користувачів в безпеці їхніх даних.

Ви можете обирати найбільш підходящий варіант, встановивши надійне антивірусне програмне забезпечення на ваш комп'ютер і регулярно оновлюйте його бази даних. Виконуйте регулярні сканування системи для виявлення та видалення потенційно шкідливих програм або вірусів. Це допоможе запобігти інфікуванню вашого пристрою шкідливим програмним забезпеченням та зберегти безпеку вашої інформації.

**Що таке брандмауер, та чим він відрізняється від антивірусу? Як налаштувати брандмауер у Windows?** І брандмауер, і антивірус – це програми для захисту ваших пристроїв. Проте їхні функції не тотожні. Брандмауер, фаєрвол чи мережевий екран – один із інструментів для захисту комп'ютера від загроз із інтернету та від кібератак. Це своєрідний "фільтр" (а в дослівному перекладі "пожежна стіна"), який блокує загрозливий контент у мережі та небезпечні з›єднання і запобігає потраплянню шкідливого програмного забезпечення (ШПЗ) у системи комп'ютера. На відміну від брандмауеру, антивіруси виявляють та нейтралізують шкідливе програмне забезпечення (ШПЗ), яке все ж потрапило на ваш пристрій. **Щоб убезпечити свій комп'ютер, використовувати потрібно і фаєрвол, і антивірус.**

У Windows вже є вбудований брандмауер. Щоб його налаштувати:

- відкрийте розділ Безпека у Windows,
- оберіть розділ Брандмауер і захист мережі,
- Встановіть або перевірте значення Увімкнено.

Нашою Комісією НПУ з питань інформатизації, цифрової трансформації та запобігання кіберзлочинності було раніше рекомендовано антивірусне програмне забезпечення Bitdefender, де нотаріуси України отримали на першому етапі безкоштовний (за рахунок сплати членських внесків) інструмент для мінімізації ризиків кібератак.


Для всіх колег, які не впевнені в актуальності та регулярному оновленні свого антивірусного програмного забезпечення або з деяких причин, ще не встигли встановити антивірусне програмне забезпечення Bitdefender та бажають це зробити найближчим часом, нагадуємо та надаємо посилання на завантаження:

https://edu.npu.ua/courses/bitdefender/lessons/videolektsiia-60/

# 3. Використання окремого комп'ютера з фіксованою IP-адресою:

Рекомендується використовувати окремий комп'ютер або ноутбук, призначений виключно для доступу до Єдиних та Державних реєстрів. Це дозволяє уникнути потенційних загроз, які можуть виникнути від використання неперевірених пристроїв чи іншого програмного забезпечення або через мережу інтернет.

Використання окремого комп'ютера з фіксованою IP-адресою та відсутністю доступу до публічних мереж Wi-Fi є ключовим заходом, рекомендованим HAIC, для забезпечення безпеки при проведенні реєстраційних дій у Реєстрах.

Цей підхід має кілька переваг:

- Використання окремого комп'ютера зменшує ризик впливу зовнішніх загроз, таких як хакерські атаки або віруси, на ваші реєстраційні дії. Фіксована IP-адреса може також ускладнити спроби зловмисників зламати вашу систему.
- Використання окремого комп'ютера допомагає уникнути можливих внутрішніх загроз, таких як шкідливі програми або недбале використання інших користувачів.

- Ваша система буде більш захищеною від можливих загроз, що можуть виникнути через використання загально-доступних комп'ютерів або мереж Wi-Fi. Це допоможе забезпечити конфіденційність та цілісність даних, які ви обробляєте у процесі реєстраційних дій.
- Швидкість та надійність вашого комп'ютера можуть бути збережені, оскільки він буде використовуватися виключно для реєстраційних дій і не буде перенавантажений зайвими програмами чи службами.

Також необхідно відмітити про правильні налаштування доступу відвідувачів до локальної мережі інтернет. Відвідувачі офісу не повинні отримувати доступ до локальної мережі інтернет, до якої підключені та мають доступ комп'ютери офісу. Для доступу клієнтів до мережі інтернет (WiFi), необхідно використовуватися іншу мережу WIFI. Особлива увагу треба звернути на налаштування мережевих пристроїв. Обов'язково змінюйте логін і пароль, що встановленні за замовчуванням на мережевих пристроях (маршрутизаторах (роутерах), точках доступу), щоб убезпечити себе від підключення до них за заводськими налаштуваннями (налаштуваннями за замовчуванням). Встановіть надійні паролі на вмикання комп'ютера, на роутері, на wi-fi.

Загальною метою цього заходу є максимізація безпеки та надійності процесу реєстрації за допомогою використання окремого комп'ютера з фіксованою IP-адресою та обмеженим доступом до мереж Wi-Fi. Це допоможе уникнути можливих кіберзагроз та зберегти конфіденційність даних, що обробляються в рамках реєстраційних процесів.

# 4. Запобігання використанню сторонніх носіїв інформації:

Використання сторонніх носіїв інформації (USB-накопичувачі, зовнішні жорсткі диски тощо) створює значні ризики для безпеки даних. Вони можуть бути джерелом зараження шкідливим програмним забезпеченням, а також засобом витоку конфіденційної інформації. Тому впровадження ефективних заходів щодо запобігання їх використанню є критично важливим для будь-якої організації.

Чому використання сторонніх носіїв є небезпечним?

- **Шкідливе програмне забезпечення:** Зловмисники часто використовують флешки для поширення вірусів, троянів та іншого шкідливого програмного забезпечення.
- **Витік даних:** Конфіденційна інформація може бути легко скопійована на сторонній носій та винесена за межі організації.
- **Втрата даних:** Втрата флешки може призвести до втрати важливих даних.
- **Несанкціонований доступ:** Незахищені флешки можуть бути підключені до будь-якого комп'ютера, надаючи зловмисникам доступ до мережі організації.

# Заходи запобігання

## *1. Заборона використання сторонніх носіїв:*

- **Повна заборона:** Найефективніший, але й найжорсткіший метод. Вимагає наявності альтернативних способів обміну даними.
- **Часткова заборона:** Заборона використання сторонніх носіїв для певних категорій працівників або для роботи з конфіденційною інформацією.

## *2. Технічні засоби захисту:*

- **Системи виявлення інцидентів:** Моніторинг мережі на предмет підключення сторонніх пристроїв.
- **Програмні рішення:** Використання програмного забезпечення, яке блокує підключення сторонніх носіїв.
- **Апаратні рішення:** Застосування спеціального обладнання для контролю доступу до портів USB.
- **Шифрування даних:** Захист даних на носіях за допомогою шифрування.

## *3. Політика безпеки:*

- **Розробка чітких правил:** Створення політики, яка регламентує використання сторонніх носіїв.
- **Ознайомлення працівників:** Проведення регулярних тренінгів для підвищення обізнаності працівників про ризики, пов'язані з використанням сторонніх носіїв.
- **Дисциплінарні заходи:** Встановлення чітких санкцій за порушення політики безпеки.

### *4. Альтернативи:*

- **Хмарні сховища:** Забезпечення безпечного зберігання та обміну даними в хмарі.
- **Корпоративні мережеві диски:** Централізоване зберігання даних, до яких працівники мають доступ через мережу.
- **Внутрішні сервери:** Використання внутрішніх серверів для обміну файлами.
-

### *Важливі аспекти реалізації:*

- **Комплексний підхід:** Комбінація технічних, організаційних та правових заходів забезпечить максимальний рівень захисту.
- **Регулярна оцінка ефективності:** Необхідно періодично проводити оцінку ефективності вжитих заходів та вносити необхідні корективи.
- **Співпраця з працівниками:** Залучення працівників до процесу розробки та реалізації політики безпеки підвищить рівень її сприйняття.

Таким чином запобігання використанню сторонніх носіїв інформації є важливим елементом загальної стратегії кібербезпеки організації. Вибір конкретних заходів залежить від багатьох факторів, включаючи розмір організації, специфіку діяльності та фінансової складової. При розробці політики безпеки необхідно враховувати як технічні аспекти, так і людський фактор.

## *5. Надійне збереження особистого ключа ЕЦП. Нерозголошення ідентифікаторів доступу та паролів:*

Особистий ключ ЕЦП – це криптографічний ключ, який використовується для підписання електронних документів. Він є цифровим аналогом особистого підпису і має надзвичайно високу цінність, оскільки забезпечує цілісність та автентичність інформації. Тому його безпечне зберігання є одним з найважливіших аспектів кібербезпеки.

Збереження особистого ключа ЕЦП повинно бути у надійному місці, наприклад сейфі, до якого маєте доступ тільки Ви. Ключ ЕЦП не має потрапляти вільно чи безперешкодно у руки третіх осіб/осіб з якими ви працюєте або знаходитись у свободному доступі. Не допускати сторонніх осіб до особистого ключа ЕЦП, призначеного для роботи Вами з єдиними державними Реєстрами.

Важливо пам'ятати про нерозголошення ідентифікаторів доступу та паролів для входу до Єдиних та Державних реєстрів. Паролі повинні бути складними, унікальними та регулярно оновлюватись, а також ніколи не повинні передаватися третім особам. **Категорично не допускати розголошення особистого ключа ЕЦП, паролів третім особам або співробітникам, не зберігати файл з паролями на робочому столі.** Не допускати сторонніх осіб до комп'ютера, призначеного для роботи з Реєстрами, а також регулярно змінювати паролі для всіх облікових записів, включаючи доступ до Єдиних та Державних реєстрів. Це допомагає уникнути несанкціонованого доступу до вашої інформації та забезпечує безпеку даних.

Ваш цифровий підпис – це ваш цифровий паспорт. Захистіть його надійно!

**Пам'ятайте, що попередження краще за лікування, тому важливо приділяти належну увагу заходам безпеки та практикувати їх регулярно.**

# ПК/ОСНОВИ НАЛАШТУВАНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ:

Використання ліцензійного програмного забезпечення

Антивірусний захист та регулярні перевірки комп’ютера


Зміна паролів з регулярністю

Уникання використання послуг випадкових фахівців


Повне контролювання доступу до системи та паролів


Використання окремого комп’ютера з фіксованою IP-адресою

Запобігання використанню сторонніх носіїв інформації

Нерозголошення ідентифікаторів доступу та паролів