Урок №5. **Тема.** **Об'єкти захисту. Види заходів протидії загрозам безпеки. Переваги та недоліки різних видів заходів захисту.**

*3.*У якості об'єктів інформаційної безпеки (information security object) необхідно розглядати: інформацію та інформаційні ресурси, носії інформації, процеси обробки інформації.

*4.* **Концепція захисту інформації**

Розробку *концепції захисту* рекомендується проводити в три етапи:

* І етап – визначення цінності об’єкта захисту інформації.
* ІІ етап – аналіз потенційних дій зловмисників.
* ІІІ етап – оцінка надійності встановлених засобів захисту інформації на об’єкті.

На основі концепції безпеки інформації розробляються стратегія безпеки інформації та архітектура системи захисту інформації, а далі – політика безпеки інформації.

*5.*Для запобігання загрозам інформаційній безпеці та їх усунення використовують правові, морально-етичні, програмно-технічні та організаційно-економічні методи.

* **Морально-етичні засоби** реалізуються у вигляді норм поведінки особи в інформаційному просторі.
* **Правові засоби** встановлюють правила користування інформацією та відповідальність користувачів за їх порушення.
* **Адміністративні (організаційні) засоби** регламентують порядок взаємодії користувачів з інформаційними системами.
* **Технічні (фізичні) засоби** забезпечують захист від несанкціонованого доступу, пошкодження інформаційної системи тощо.
* **Програмні засоби** забезпечують захист інформаційної системи від комп’ютерних вірусів, ідентифікацію користувачів тощо.

*6.* **Правові методи** передбачають розроблення комплексу нормативно-правових актів і положень, що регламентують інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо гарантування інформаційної безпеки.

*7.* **Програмно-технічні методи - це сукупність засобів:**

* запобігання витоку інформації;
* усунення можливості несанкціонованого доступу до інформації;
* запобігання впливам, які призводять до знищення, руйнування, переключення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації;
* виявлення вмонтованих пристроїв;
* запобігання перехопленню інформації технічними засобами;
* використання криптографічних засобів захисту інформації під час передачі каналами зв'язку.

*8.* **Організаційно-економічні методи передбачають:**

* формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації;
* сертифікацію цих систем відповідно до вимог інформаційної безпеки;
* ліцензування діяльності у сфері інформаційної безпеки;
* стандартизацію способів і засобів захисту інформації;
* контроль за діями персоналу в захищених інформаційних системах.

*9.* **Методи і засоби забезпечення безпеки інформації:**

**Перешкода** - метод фізичного втручання на шляху зловмисника до захищеної інформації (до документів, апаратури, носіїв інформації тощо).

**Управління доступом** - методи захисту інформації регулюванням всіх ресурсів ІС і ІТ. Ці методи протистоять можливим способам несанкціонованого доступу до інформації. Управління доступом виконує такі функції захисту:

* ідентифікацію користувачів, персоналу й ресурсів системи (закріплення за кожним об'єктом персонального ідентифікатора);
* пізнання (визначення достовірності) об'єкта або суб'єкта за пред'явленим ним ідентифікатором;
* перевірка повноважень (перевірка відповідності дня тижня, часу доби запрошуваних ресурсів і процедур у межах установленого регламенту);
* дозвіл і створення умов роботи в межах установленого регламенту;
* реєстрація звернень до конфіденційних ресурсів;
* реагування (сигналізація, відключення, затримка робіт, відмова в запиті) у разі спроб несанкціонованих дій.

**Механізми шифрування** - криптографічне закриття інформації. Цей метод захисту дедалі ширше застосовується під час опрацювання та при зберіганні інформації на магнітних носіях. У разі передавання інформації каналами зв'язку великої протяжності цей метод є єдино надійним.

**Протидія атакам шкідливих програм** припускає комплекс різних організаційних заходів і використання антивірусних програм. Мета протидії атакам:

* зменшення вірогідності інфікування АІС;
* виявлення фактів зараження системи;
* зменшення наслідків інформаційних інфекцій;
* локалізація або знищення вірусів;
* відновлення пошкодженої інформації в ІС.

**Регламентація** - створення таких умов автоматизованого опрацювання, зберігання і передавання інформації, що підлягає захисту, за яких норми і стандарти захисту найбільш ефективні.

**Приму**с - метод захисту, за якого користувачі і персонал ІС змушені дотримуватися правил опрацювання, передавання і використання конфіденційної інформації через загрозу матеріальної, адміністративної або кримінальної відповідальності.

**Спонука** - метод захисту, що спонукає користувачів і персонал ІС не порушувати встановлених порядків за рахунок дотримання моральних і етичних норм, що склалися.

*10.* **Система захисту інформації** – це організована сукупність спеціальних установ, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

*11****. Вимоги до системи безпеки інформації***

* чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;
* надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;
* зведення до мінімуму кількості спільних для декількох користувачів засобів захисту;
* облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;
* забезпечення оцінювання ступеня конфіденційної інформації;
* забезпечення контролю цілісності засобів захисту і негайне реагування на вихід їх із ладу.

*12.***Принципи побудови системи захисту інформації:**

* **безперервність захисту інформації.** Характеризується постійною готовністю системи захисту до відбиття загроз інформаційній безпеці в будь-який час;
* **активність,** яка передбачає прогнозування дій зловмисника, розробку і реалізацію випереджаючих захисних заходів;
* **скритність**, що виключає ознайомлення сторонніх осіб із засобами і технологією захисту інформації;
* **цілеспрямованість**, яка передбачає зосередження зусиль щодо запобігання загроз найбільш цінної інформації;
* **комплексне використання різних способів і засобів захисту інформації,** що дозволяє компенсувати недоліки одних перевагами інших;
* **мінімізація** додаткових завдань і вимог до співробітників організації, викликаних заходами щодо захисту інформації;
* **надійність** в роботі технічних засобів системи, що виключає як не реагування на погрози (пропуски загроз) інформаційної безпеки, так і помилкові реакції при їх відсутності;
* **обмежений і контрольований доступ**до елементів системи забезпечення інформаційної безпеки;
* **безперервність роботи системи**в будь-яких умовах функціонування обʼєкта захисту, в тому числі, наприклад, короткочасному відключенні електроенергії;
* **адаптованість** (пристосовність) системи до змін навколишнього середовища.

*13.* Шляхи захисту даних:

* захист доступу до комп’ютера;
* захист даних на носіях інформації;
* захист даних в Інтернеті.

*14*. Для вирішення питання щодо захисту інформації на мобільному пристрої існує кілька варіантів, а саме:

**Використовуйте «хмари».** Практично кожен виробник смартфона пропонує власний хмарний сервіс – потрібно в ньому зареєструватися й користуватися. Крім того, існує і ряд «незалежних» служб, на кштальт Dropbox або сервіси Google. Можна налаштувати їх таким чином, щоб дані, отримані за допомогою смартфона, автоматично відправлятися в «хмари». У разі втрати смартфона, досить одразу змінити пароль свого облікового запису і зловмисник не зможе скористатися вашою інформацією. Існує й ряд платних сервісів, які надає компанія SL Global Service консорціуму Intecracy Group – персональне «хмарне сховище», захищена електронна пошта тощо.

**Зверніть увагу на програмне забезпечення**. Перше, що повинен зробити користувач після покупки смартфона – встановити антивірус. Існують як платні системи, постачальником яких є такі компанії консорціуму Intecracy Group як IQusion і Global Intecraty (вони є партнерами світових лідерів із розробки антивірусів), так і безкоштовні антивіруси. Можливості безкоштовних антивірусів обмежені, але це набагато краще, ніж взагалі без них. Відзначимо, що сучасний антивірус ефективно блокує програми, які займаються перехопленням смс-повідомлень й прослуховуванням телефонних розмов.

Також дуже важливо завантажувати програмне забезпечення лише з перевірених джерел – це магазини додатків, які перевіряє компанія-розробник операційної системи (наприклад, Google або Apple). В жодному разі не можна відповідати згодою на пропозицію завантажити файл через Bluetooth від незнайомого пристрою. Також небезпечно переходити по невідомих посиланнях й відповідати на рекламні SMS.

Відзначимо, що на смартфонах Android кожен додаток перед встановлення запрошує права для себе. Звертайте увагу на те, що саме хоче робити програма. Наскільки ці вимоги відповідають її призначенню? Наприклад, якщо ви хочете встановити програму для читання новин, а та вимагає для себе права відправляти контакти з вашої адресної книги третім особам, є сенс пошукати інші, альтернативні програми.

**Відключайте Bluetooth, WiFi і GPS**. Бездротовий зв’язок на вашому смартфоні потрібно відключати кожного разу, коли ви закінчили ним користуватися. Модулі бездротового зв’язку краще включати з обережністю і в надійних, перевірених місцях. Потрібно знати, що Bluetooth досить легко піддається контролю з боку третіх осіб. Краще використовувати для зв’язку кабель.

Окремої уваги заслуговує GPS-модуль. Потрібно розуміти, що він дозволяє відстежити користувача з точністю до 3-5 метрів (GSM-передавач дозволяє визначити лише з точністю до декількох кілометрів). Якщо ви цього не хочете, краще його вимикати і знову вмикати, у разі потреби.

**Не зберігайте на смартфоні банківські дані.** Експерт із безпеки Symantec Скотт Райт (Scott Wright) провів експеримент: «загубив» смартфони у людних місцях. Майже кожна людина, що знайшла його, намагалася отримати доступ до особистої інформації користувача. І лише половина людей, що знайшли смартфон, спробували повернути пристрій його власнику. Однак навіть вони намагалися подивитися на персональну інформацію: отримати доступ до соціальних мереж, пошти, банківських даних власника.

Цієї інформації на смартфоні не повинно бути. Найкраще зберігати її в «хмарі», причому, не повинно бути ніякої синхронізації з пристроєм. Дуже важливо, щоб пароль до папки з фінансової інформацією не зберігався в кеші браузера або іншої програми – його щоразу краще набирати вручну.

**Слідкуйте за смартфоном**. У тому випадку, якщо смартфон загублений або його вкрали, ви повинні почати з заміни паролів у всіх акаунтах соцмереж та сервісів, до яких був підключений смартфон. Крім того, важливо знати, що загублений пристрій можна розшукати – існують спеціальні програми, які дозволяють відстежити місце розташування втраченого або вкраденого телефону. До речі, якщо смартфон вам подарували або він не новий, найкраще перед використанням скинути його до заводських настройок – хто знає, а раптом він вже заражений?

**Завантажуйте додатки з обережністю.** Будь-які додатки можуть зробити ваш смартфон вразливим. Завантажуйте лише ті додатки, що дійсно вам потрібні та з надійних джерел (офіційних магазинів додатків для вашої платформи) таких, як Google Play маркет, Marketplace, ITunes. При цьому завжди потрібно звертати увагу на те, які саме дані цей додаток потребує при встановленні. Дуже часто користувачі погоджуються та без питань надають свою інформацію для встановлення додатків, яка по суті в дійсності там не потрібна, таким чином надаючи її третій особі.

**Створення резервних копій даних**. Більшість смартфонів мають функцію синхронізації даних із їх хмарними сервісами. Зазвичай це робиться вручну або автоматично. Синхронізуйте дані зі своїм домашнім комп'ютером або ноутбуком з періодичністю 1 раз на тиждень чи навіть частіше, залежно від того, наскільки важливою є інформація та контент на вашому телефоні. **Синхронізація** необхідна для того, щоб на всіх ваших пристроях були необхідні дані і, у випадку втрати або блокування телефону, ви змогли швидко відновити їх. Витративши один раз час, у подальшому ви будете його економити. Налаштувавши синхронізацію, можна миттєво налаштувати пристрій, щоби на вашому телефоні відразу були всі ваші контакти і налаштування. Дана процедура є на всіх сучасних смартфонах: Iphone, Android 4.4, Windows Phone.

* ***Практичне завдання*** *( 17)*

Організувати дослідницьку роботу на тему «Біометричні засоби захисту даних».

1 група – ідентифікація за голосом;

2 група – ідентифікація за відбитками пальців;

3 група – ідентифікація за малюнком райдужної оболонки ока.

Підготувати коротке повідомлення про вид біометричного захисту даних.

Повідомлення повинно супроводжуватися Google-презентацією.

**VII. Підведення підсумків уроку**

* ***Бесіда за питаннями*** *( 19)*

1. Що відносимо до об’єктів інформаційної безпеки?

2. З яких частин складається концепція захисту інформації?

3. Назвіть види заходів протидії загрозам безпеки.

4. Що передбачають правові методи захисту інформації?

5. Система захисту інформації - це…

6. Назвіть принципи побудови системи безпеки інформації.

**VIII. Домашнє завдання**

*20.* Складіть перелік правил «Забезпечення власної інформаційної безпеки в смартфоні».