

СЕКЦІЯ «БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ»

УДК 331.45 331.46

Шмирко В.І.¹, Середа О.А.²

¹ канд. техн. наук, доц. ЗНТУ

² студ. гр. М-214м ЗНТУ

АНАЛІЗ ІНФОРМАЦІЙНИХ ЗАГРОЗ

З середини 80-х років ХХ століття, коли виникли «комп'ютерні» технології, відбувається швидка еволюція інформаційного середовища. Нова інформаційна реальність, з одного боку, розширює спектр можливостей людини як користувача інформації, з іншого – впливає на формування (або зміну) її світогляду особистісних цінностей. Перенасиченість та неупорядкованість інформаційного простору потребує від людини фізичного та психічного напруження. Значний вплив на людей чинять ЗМІ, оскільки вони користуються інформацією повсякденно в усіх кутках світу. Проте, переглядаючи фото- та відеоматеріали, статті, слухаючи радіопередачі, людина несвідомо стає заручником системи, котра піддає її значній інформаційній небезпеці.

Фактори інформаційної загрози дуже різноманітні, тому для більш наглядного їх представлення та ефективної візуалізації можливого негативного впливу на особистість, класифікуємо їх у вигляді таблиці 1.

1. Джерела загроз – поділяються на зовнішні (загрозами можуть бути фактори природного походження, неконтрольовані людиною – це ураження блискавкою антен радіопередач, ліній електропередач, підвищена вологість (туманність), переохолодження електрообладнання (напр. серверів з даними) та виділення конденсату; стихійні лиха та катастрофи; злочинна навмисна діяльність компаній та фірм у бік конкурентів) та внутрішні (недотримання норм та правил техніки безпеки персоналом, непередбачені збої у роботі обладнання, навмисне пошкодження носіїв інформації тощо).

2. Напрямки загроз – розкриті (ознайомлення та користування інформацією попри заборону); порушення цілісності (знищення інформації без дозволу та відома власника); порушення готовності (пошкодження інформації у зв'язку з відмовою обслуговування обладнання).

3. Види загроз – програмно-математичні (системні та програмні віруси, програмний «фішинг», використання дефектів та багів); інформаційні (найчастіше викрадення інформації); радіо-електронні (перехоплення або подавлення сигналів); фізичні (викрадення та копіювання ключів доступу, вплив на персонал заради користі).

4. Типи загроз – технологічні (впровадження зайвої та псування інформації на етапі розробки); експлуатаційні (впровадження зайвих «лівих» інформаційних систем (наприклад, шпигунських,) на етапі користування).

Таблиця 1 – Загальна характеристика загроз інформаційній безпеці

Джерела загроз	Зовнішні: атмосферні явища, стихійні лиха, катастрофи, аварії; діяльність конкуруючих економічних структур; діяльність злочинних угруповань. Внутрішні: порушення персоналом режимів безпеки; відмови та збої апаратних засобів і носіїв інформації; помилки програмного забезпечення; діяльність злочинних угруповань тощо.
Напрямки загроз	Розкриті: нелегальне ознайомлення (читання). Порушення цілісності: несанкціоноване знищення або модифікація. Порушення готовності (доступності): відмова в обслуговуванні.
Види загроз	Програмно-математичні: впровадження комп'ютерних вірусів; впровадження програмних закладок; використання операційних і функціональних дефектів; дешифрування тощо. Інформаційні: несанкціоноване проникнення; порушення регламенту інформаційного обміну; розкрадання баз даних тощо. Радіоелектронні: перехоплення інформації в каналах зв'язку; радіоелектронне придушення тощо. Фізичні: знищення та руйнування засобів обробки інформації; розкрадання апаратних та програмних ключів, добування зразків; вплив на персонал.
Типи загроз	Технологічні, які впроваджуються на етапі розробки інформаційних систем та програм. Експлуатаційні, що впроваджуються на етапі експлуатації інформаційних систем.
Види збитків	Явні: порушення безпеки інформації або її втрата. Непрямі: руйнування апаратно-програмного забезпечення. Неявні: промислове шпигунство, розкрадання апаратно-програмного забезпечення та документації, моральний збиток.

5. Види збитків. Будь-яка заподіяна шкода інформації призводить до збитків, їх можна поділити на: явні (пряме порушення інфо-безпеки, втрата цінності інформації); непрямі (пошкодження обладнання та програмного забезпечення); неявні (промислове шпигунство, викрадення документації, апаратно-програмної частини часто призводить, окрім матеріальної шкоди, ще й до моральної)).

Таким чином, інформаційні загрози часто залишаються недооціненими. Подача класифікатора безпеки саме у вигляді таблиці дозволить користувачеві краще орієнтуватись серед значної кількості загроз, їх швидко аналізувати, та розробляти ефективні методи профілактики.