**Література**

1. Норенков И. П. Основы автоматизированного проектирования: учеб. для вузов. — 4-е изд., перераб. и доп. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2009. — 430 с.

2. Малюх В. Н. Введение в современные САПР: Курс лекций. — М.: ДМК Пресс, 2010. — 192 с.

3. Воротников С. А. Информационные устройства робототехнических систем: учебное пособие. - М.: Изд-во МГТУ им. Н. Э. Баумана, 2005. - 384 с.

4. Чубукова О.Ю. Економіка інформації: ринок продуктів та послуг: монографія / О.Ю.Чубукова – К.: Нора-Принт, 2005.- 344 с.

УДК 334

Мігус І.П., д.е.н., професор
Український науково-дослідний
інститут цивільного захисту

## ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

Інформація є активом, який подібно іншим важливим діловим активам, є суттєвим для бізнесу організації і тому потребує відповідного захисту. Це суттєво важливо у все більш взаємопов’язаному діловому середовищі. Внаслідок цієї зростаючої взаємопов’язаності інформація тепер наражається на зростаючу кількість і більшу різноманітність загроз та вразливостей.

Інформація може існувати у багатьох формах. Вона може бути надрукована або написана на папері, збережена в електронному вигляді, переслана поштою або з використанням електронних засобів, показана на

плівці або сповіщена у бесіді. Незалежно від набутого виду інформації або засобів, за допомогою яких вона поширюється або зберігається, вона повинна завжди бути відповідно захищена.

Інформаційна безпека - це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес ризику і максимізації рентабельності інвестицій і бізнес можливостей [1].

Інформаційна безпека досягається впровадженням відповідного набору контролів, який охоплює політику, процеси, процедури, організаційні структури і програмні та апаратні функції. Ці контролі необхідно розробити, впровадити, моніторити, переглядати та, за необхідності, вдосконалювати для гарантування того, що певні безпека та бізнес-цілі організації будуть досягнуті. Це треба виконувати узгоджено з іншими процесами управління бізнесом.

***Основними каналами витоку інформації є:*** візуально-оптичні (спостереження, відео-, фотозйомка), акустичні та акустоперероблювальні, електромагнітні (в тому числі й магнітні та електричні), матеріально-речові (магнітні носії, папір, фотографії тощо).

**Візуально-оптичні канали** створюються як оптичний шлях від об’єкта інформації до її отримувача. Для цього необхідні енергетичні, часові та просторові умови і відповідні технічні засоби. Особлива цінність інформації, отриманої через такий канал, полягає в тому, що вона є максимально достовірною, оперативною і може бути документальним підтвердженням отриманих відомостей.

**Джерелом створення акустичного каналу** є тіла та механізми, які здійснюють вібрацію або коливання, наприклад голосові зв’язки людини, елементи машин, що рухаються, телефонні апарати, звукопідсилювальні системи, гучномовні засоби, засоби звукозапису та звуковідновлення та ін.

Звукові коливання від голосу людини, інших звуків створюють акустичні хвилі, які, поширюючись у просторі і взаємодіючи з відповідними перешкодами, викликають у них перемінний тиск (двері, вікна, стіни, підлога,

різноманітні прилади), приводячи їх у коливальний режим. Впливаючи на спеціальні прилади (мікрофони), звукові коливання створюють у них відповідні електромагнітні хвилі, які передаються на відстань і несуть в собі створену звуковими коливаннями інформацію.

*Акустичні канали створюються:* завдяки поширенню акустичних (механічних) коливань у вільному повітряному просторі (переговори на відкритому просторі, у приміщенні при відкритих вікнах, квартирках, дверях, виток через вентиляційні канали); через вплив звукових коливань на елементи і конструкції будівель, викликаючи їх вібрацію (стіни, стеля, підлога, вікна, двері тощо); через дію звукових коливань на технічні засоби обробки інформації (мікрофонний ефект, акустична модуляція та ін.).

**Електромагнітні канали** за своєю фізичною природою та експлуатаційними особливостями технічних засобів, які забезпечують виробничу діяльність, є найнебезпечнішими і досить поширеними каналами отримання інформації [2]. Такі канали створюються через наявність у технічних засобах, які використовуються у виробництві, джерел небезпечних сигналів. Насамперед до таких джерел відносять перероблювачів, якими є прилади, що трансформують зміни однієї фізичної величини в зміни іншої. Хороші знання роботи перероблювачів дають змогу визначати можливі неконтрольовані прояви фізичних полів, які й створюють електромагнітні канали витоку (передавання) інформації. Водночас, ураховуючи ідентичність технічних та конструктивних рішень, електронних схем технічних засобів обробки інформації і забезпечення виробничої діяльності підприємств і банків, усім їм потенційно властиві ті чи інші канали витоку (передавання) інформації. Тому в будь-якому випадку використання технічних засобів обробки та передання інформації створює загрозу її безконтрольного витоку (передавання).

**Матеріально-речові канали** отримання інформації створюються через вивчення відходів виробничої діяльності (зіпсовані документи або їх фрагменти, чернетки різних поміток, записів, листів тощо), викрадення,

несанкціоноване ознайомлення, копіювання, фотографування, відеозапис документів, креслень, планів, зразків технічних або програмних засобів.

Поряд із зазначеними вище загрозами інформації існують інші, які не передбачають отримання інформації, але, у свою чергу, не менш небезпечні. Серед них такі, як знищення і модифікація (зміна змісту) інформації.

На підставі викладеного можна зробити висновок, що отримання інформації спецслужбами, конкурентами та зловмисниками здебільшого здійснюється через технічні засоби, які використовуються на фірмах, підприємствах, у банках, та через їх співробітників. Тобто в основу інформаційної безпеки має бути покладено заходи захисту інформації в засобах і мережах її передавання й обробки, а також створення відповідної нормативної бази, яка б регулювала порядок доступу, зберігання і використання інформації фірми, банку, підприємства.

**Література**

1. Зеркалов Д.В. Экономическия безопастность — К.: Основа, 2011. — 586 с. Зубок М.І. Безпека банківської діяльності. — К.: КНЕУ, 2011. — 586 с.