Маковський І. Ю., аспірант
Державний університет «Житомирська політехніка»

ЕТАПИ СТАНОВЛЕННЯ ТА ЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ ПІДПРИЄМСТВ

Поняття «інформаційна безпека» з'явилось із появою засобів інформаційної комунікації між окремими людьми чи цілими соціумами. Це пов'язано з обміном тією інформацією, заволодіння якою може завдати збитків особі чи суспільству, що їх стосується та чи інша інформація.

Єдиного визначення поняття «інформаційна безпека» не існує, втім деякі дослідники подають такі визначення:

Р. Л. Кіссель визначає «інформаційну безпеку» як практику попередження несанкціонованого доступу, використання, розкриття, перекручення, зміни, дослідження, запису чи знищення інформації [1]. Таке універсальне визначення застосовується незалежно від форми, що її можуть набувати дані (електронна чи, наприклад, фізична).

Більш практичне визначення можна знайти у Танцюри М. Ю., який трактує його як відношення рівня інформаційного захисту до рівня інформаційних загроз [2]. Застосування такого визначення надає змогу обчислити ефективність вжитих заходів щодо забезпечення інформаційної безпеки в окремо взятій організації або на підприємстві.

Основним завданням інформаційної безпеки є збалансований захист конфіденційності, цілісності й доступності даних.

Якщо розглядати історичні аспекти розвитку інформаційних відносин, можна виділити такі основні етапи становлення інформаційного захисту [3]:

I етап — до початку XIX століття. В той період використовувались природно утворювані засоби інформаційних комунікацій. У той період основним завданням інформаційної безпеки був захист відомостей про події, факти, майно, місцезнаходження й інші дані, що мали для людини особисто або соціуму, до якого вона належала, життєве значення. В широкому сенсі заходи захисту інформації було спрямовано на запобігання перехопленню фізичних повідомлень, особливо під час ведення бойових дій. Разом із тим, важливим було збереження особистої інформації, в тому числі про проведення торгових операцій, виготовлення чи винайдення нових товарів, інновації у промисловому виробництві тощо.

II етап — від 1816 до 1935 року. Цей етап був пов'язаний із початком використання технічних засобів електро- та радіозв'язку. Після того, як інформація перемістилась з фізичних носіїв до електромагнітного поля, постала необхідність її захисту в принципово новій площині. Таким чином, з розвитком технологій передачі інформації, почали розвиватись технології її захисту. На даному етапі потрібно було забезпечити скритність і завадостійкість радіозв'язку шляхом застосування завадостійкого кодування повідомлення з подальшим декодуванням прийнятого сигналу.

III етап — від 1935 до 1946 року. Той період пов'язаний з появою засобів радіолокації і гідроакустики. Основним способом забезпечення інформаційної безпеки в ті роки було поєднання організаційних і технічних заходів, спрямованих на підвищення захищеності засобів радіолокації від дії на їхні приймальні пристрої активними маскувальними і пасивними імітувальними радіоелектронними перешкодами. Особливо бурхливо на тому етапі засоби захисту інформації розвивались під час Другої світової війни, оскільки від реалізації політики інформаційної безпеки прямо залежав успіх тієї чи іншої операції, а також живучість своїх військ. В економічному сенсі засоби захисту інформації в той період були спрямовані на забезпечення інформаційної безпеки нових технологій, передусім військового призначення, втім не слід забувати й про ті технології, що розвивались у мирних країнах та на які націлювались усі сторони конфлікту, що не мали можливості в силу умов розвивати власне виробництво.

IV етап — середина XX століття. Винайдення та впровадження в практику електронно-обчислювальних машин (комп'ютерів) зумовило народження нової проблеми – забезпечення захисту інформації, представленої в електронному вигляді. На тому етапі завдання інформаційної безпеки вирішувались, в основному, методами і способами обмеження фізичного доступу до устаткування засобів добування, перероблення й передачі інформації. Фактично в ті роки інформацію в електронному вигляді можна було добути лише отримавши фізичний доступ до устаткування, втім під час передачі інформації захисту підлягали її фізичні носії або все ті ж радіо-, електро-, електромагнітні сигнали тощо.

V етап — 1960-ті – 1970-ті роки. З появою та розвитком локальних інформаційно-комунікаційних мереж завдання інформаційної безпеки майже не змінились, вони полягали у фізичному захисті елементів локальних мереж. Разом з тим, з'явились і нові завдання, зокрема необхідність адміністрування й управління доступом до мережевих ресурсів, які на той момент поки не могли зазнати зовнішнього впливу. Інформаційно-комунікаційні системи на промислових підприємствах також потребували захисту інформації, що в них циркулювала, оскільки втрата чи пошкодження даних могли призвести до зриву виробництва та, відповідно, збитків.

VI етап — до середини 1980-их років. Цей етап пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. Загрози інформаційній безпеці стали набагато серйознішими. Для забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах з бездротовими мережами передачі даних потрібно було розробити нові критерії безпеки. Більше того, з'явились цілі співтовариства людей — хакерів, що ставлять собі за мету завдання збитків інформаційній безпеці окремих користувачів, підприємств, організацій і цілих країн. Інформація стала найважливішим ресурсом держави, а забезпечення його безпеки —

найважливішою й обов'язковою складовою національної безпеки. З’явилась навіть нова галузь міжнародної правової системи – інформаційне право. В економічній царині відбувалось те ж саме, кожне підприємство почало формувати власну політику безпеки й визначати шляхи її реалізації.

VII етап — від 1985 року. Стрімкий розвиток глобальних інформаційно-телекомунікаційних систем, а також широке застосування космічних засобів зв’язку, спонукає до пошуку нових високотехнологічних засобів захисту інформації. Всеосяжна автоматизація виробничих процесів на підприємствах також вимагає розширення заходів інформаційної безпеки, що потребує постійного оновлення політики безпеки.

Як зазначала професор Г. Я. Аніловська, на сучасному етапі з бурхливим розвитком інформаційних технологій і їх широким впровадженням в облікові процеси виникає проблема взаємодії цих облікових систем з іншими системами та між собою, а також проблема конфіденційності. До того ж, ці проблеми існують на технічному, програмному та інформаційному рівнях. Вирішити їх можна шляхом розроблення і впровадження єдиних, загальних і обов'язкових правил побудови і використання облікових інформаційних систем [4]. У світлі розвитку нових IT-технологій, поняття інформаційної безпеки значно розширилося. Сьогодні від захисту процесів, інформації та діяльності в кіберпросторі залежить значно більше, ніж просто втрата інформації. Тобто, втрата інформації тягне за собою низку інших комплексних ускладнень. Нині комплекс заходів із захисту інформації повинен враховувати, в тому числі, антивірусний захист, захист від хакерських атак, підробки даних тощо. Наприклад, враження комп’ютерними вірусами може не лише видалити чи викрасти дані, але й вплинути на роботу та продуктивність співробітників чи навіть зупинити виробництво.

Таким чином інформаційна безпека є чи не найважливішим аспектом ефективності бізнесу будь-якого підприємства. Головним завданням заходів забезпечення захисту інформації на підприємстві є формування такої політики безпеки, що передбачала б усебічний захист інформації на кожному етапі виробництва, а також у кожному з бізнес-процесів підприємства.

Список використаних джерел:

1. NIST Interagency or Internal Report 7298 : Glossary of Key Information Security Terms : [англ.] / Richard L. Kissel, editor, Computer Security Division, Information Technology Laboratory. — Revision 2. — Gaithersburg, MD, USA : National Institute of Standards and Technology, 2013. — 222

2. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим): автореф. дис.на здобуття наук ступеня канд. екон. наук: 08.00.04//М.Ю. Танцюра.- Сімферополь, 2012.-21

3. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009 [рос.]

4. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій: Науковий вісник НЛТУ України. – 2008, вип. 18.9. С. 270