Романюк П.Р., студент
Науковий керівник: Борисюк О.В.,
к.е.н., доцент
Східноєвропейський національний
університет ім. Лесі Українки, м. Луцьк, Україна

ПРИЧИНИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В МОВАХ НЕОІНДУСТРІАЛЬНОГО СУСПІЛЬСТВА

Під інформаційною безпекою розуміють збереження інформації і самого підприємства від непередбачених або заздалегідь обдуманих вчинків, які тягнуть за собою заподіяння шкоди тим людям, які нею користуються або володіють. Захист інформації визначається як сукупність способів, що забезпечують секретність і повноту інформації, з огляду на те, що вона знаходиться у відкритому доступі для фахівців, що володіють доцільними повноваженнями. Єдність характеризується захищеністю особливостей інформації та її якісного змісту. Засекреченість означає гарантію можливості скористатися конкретними даними індивідуальним клієнтам і збереження відомостей в таємниці. Поняття «гласність» складається з ймовірності правильного і надшвидкого виявлення інформації певними клієнтами [1, С. 47].

Основне призначення захисту інформації - зведення до мінімуму шкоди в результаті недотримання умов засекреченості, гласності та єдності.

Можна виділити наступні причини загроз інформаційної безпеки підприємства:

1. Необережність та недбалість працівників. Загрозою інформаційної безпеки підприємства, перш за все, є цілком законослухняні працівники, які й не думають про крадіжку цінних відомостей. Ненавмисний збиток секретних даних наноситься через недбалість або некомпетентність співробітників. У будь-який момент може виникнути такий випадок, що хтось відкриє фішингові листи і запустить вірус з особистого ноутбука на сервер організації. Або, наприклад, скопіює файл з засекреченими даними на смартфон, КПК або флешку для того, щоб працювати у відрядженні. В даному випадку інформацію можна дістати дуже просто [2, С.46].
2. Застосування неліцензійного програмного забезпечення. Загалом, керівники підприємств і раді б дотримуватися закон, і встановлювати тільки ліцензійне програмне забезпечення. Але вартість таких програм і їх установки істотно б'є по бюджету фірми. Настільки істотно, що багато керівників свідомо вважають за краще йти на ризик, скачують 1С:Підприємство з торрентом і потім намагаються вирішити складні питання з інспекторами «на місці», що призводить до додаткових проблем з законом [3, С.270]. Водночас піратські антивіруси не захищають від злочинців, які хочуть вкрасти інформацію за допомогою вірусів. Власнику неліцензійного програмного забезпечення необхідна технічна підтримка, поновлення у визначений термін, які надаються організаціями-розробниками. Поряд з ним він купує також і віруси, які завдають шкоди системі комп'ютерної безпеки. За відомостями дослідження, проведеного Microsoft, в 7%

освоєних неліцензійних програм знайшли спеціальне програмне забезпечення для крадіжки персональних даних і паролів.

3. DDoS-атаки. DDoS (Distributed Denial of Service) - розподілена атака типу «відмова в обслуговуванні». Мережевий ресурс виходить з ладу в результаті безлічі запитів до нього, відправлених з різних точок. Зазвичай атака організовується за допомогою бот-сонетів. Зловмисник заражає комп'ютери ні про що не підозрюють користувачі Інтернету.

Зазвичай подібні атаки використовуються в ході конкурентної боротьби, шантажу компаній або для відвернення уваги системних адміністраторів від деяких протиправних дій на кшталт викрадення грошових коштів з рахунків. На думку фахівців, саме крадіжки є основним мотивом DDoS-атак. Мішенню зловмисників частіше стають сайти банків, в половині випадків (49%) були затронуті саме вони. Наприклад, в 2016 році DDoS-атаки були зафіксовані в кожному четвертому банку (26%). Серед інших фінансових структур шкідливому впливу піддалося 22% компаній [4, С.32].

4. Віруси. Однією з найнебезпечніших на сьогоднішній день загроз інформаційної безпеки є комп'ютерні віруси. Це підтверджується багатомільйонним збитком, який несуть компанії в результаті вірусних атак. В останні роки істотно збільшилася їх частота і рівень шкоди. На думку експертів, це можна пояснити появою нових каналів проникнення вірусів. На першому місці як і раніше залишається пошта, але, як показує практика, віруси здатні проникати і через програми обміну повідомленнями, такі як ICQ та інші [5, С.70]. Збільшилася і кількість об'єктів для можливих вірусних атак. Якщо раніше атакам піддавалися в основному сервери стандартних веб-служб, то сьогодні віруси здатні впливати і на міжмережеві екрани, комутатори, мобільні пристрої, маршрутизатори. Останнім часом особливо активні стали так звані віруси-шифрувальники. Навесні і влітку минулого року мільйони користувачів постраждали від атак вірусів WannaCry, Petya, Misha. Епідемії показали, що жертвою вірусної атаки можна стати, навіть якщо не відкривати підозрілі листи. За інформацією Intel вірусом WannaCry заразилися 530 тисяч комп'ютерів, а загальний збиток компаній склав більше 1 млрд доларів.

Таким чином, у сучасних умовах господарювання, коли інформаційні технології набувають глобального характеру, інформаційна безпека є невід'ємним складником системи економічної безпеки господарюючого суб'єкта й економічної безпеки держави загалом.

Список використаних джерел:

1. Литвиненко О. Інформація і безпека. Нова політика. 1998. № 1. С. 47–49.

2. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. Вісник Київського університету імені Т. Шевченка. 1999. Вип. 14. С. 46–48.

3. Борисюк О. В. Основні загрози фінансової безпеки України. International Scientific-Practical Conference Modern Transformation of Economics and Management in the Era of Globalization: Conference Proceedings. January 29, 2016. Klaipeda: Baltija Publishing. 270-271 p.

4. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи. Вісник Хмельницького національного університету 2010. № 2. Т. 2. С. 32–35.

5. Карлін М. І. Борисюк О. В. Управління державними фінансами: посібник / М.І. Карлін, О. В. Борисюк. Луцьк : ПП Іванюк, 2013. 273 с.