Види інформаційних загроз у системах електронного документообігу

Людмила Чередник
Кафедра УКіД
Полтавський національний технічний університет імені Юрія Кондратюка
Полтава, Україна
ludmila.cherednik@gmail.com

Abstract. The theses address the issue of the types of information threats in the electronic document management system, presents a general classification of information security threats.

Key words: information system, information threat, cyber attack, virus, information security.

Для оптимізації роботи сучасних організацій та підприємств широко впроваджуються системи електронного документообігу. Завдяки цим системам постійно опрацьовується безліч даних, що значно полегшує працю людей. Проте, серед численних переваг сучасні інформаційні технології мають низку досить вагомих недоліків, зокрема виникнення новітніх загроз особистій, національній та міжнародній безпеці. З кожним днем все більше зростає кількість колосальних кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Дана проблема стала першочерговою для усіх країн світу. Важливою вона є й для України.

Особливо гостро проблема інформаційного захисту постали після низки кібератак, що охопили світ упродовж останніх років. Найбільшими серед них були такі: операція «Night Knight» (2011 р.), кібератака на енергетичні компанії України (грудень 2015 р.) та «Укренерго» (17-18 грудня 2016 р.), інтенсивні та цілеспрямовані спроби здобути несакційований доступ до інформаційних систем енергетичних компаній Великої Британії (липень 2017 р.), масштабна кібератака на енергокомпанії під назвою «Berserk Bear», яку розкрила німецька контрозвідка (13 червня 2018 р.) та ін.

Варто наголосити, що жертвами кібератак стають різні інфраструктури: система міського транспорту (м. Сан-Франциско, США, листопад 2018 р.), муніципальні інформаційні системи (м.Атланта, США, 2 березня 2018 р.), урядові організації (хакерська атака на сайти Держказначейства України, 6 грудня 2016 р.).Крім того, 27 червня 2017 р. низка українських банків і компаній, Кабмін, системи електронного документообігу ЧАЕС зазнали хакерських атак від вірусу «Petya». Того ж року атаки хакерів порушили роботу київського метрополітену та інформаційну систему одеського аеропорту. І таких прикладів можна навести безліч.

Поширеним також стає викрадення особистої інформації, кіберкрадіжки,комп'ютерне шпигунство, кібервійни.

Досить часто ця проблема почала підніматися у дослідженнях багатьох науковців, серед яких слід назвати В.Богуша, В. Щербину, І. Маракову, Ю. Васильєва, В. Ліпкана, С. Богатирьова та багатьох інших.

Реалії сучасного життя підтверджують той факт, що нині важливим є не лише питання боротьби з кіберзагрозами, а й ліквідація їх і зведення до мінімуму можливих збитків у випадку реалізації тієї чи іншої загрози.

Зазначимо, що під терміном «загроза» сучасні дослідники розуміють «сукупність факторів і умов, що виникають у процесі взаємодії різних об'єктів чи їхніх елементів, здатних чинити негативний вплив на конкретний об'єкт інформаційної безпеки» [1]. Як правило, загроза є наслідком наявності вразливих місць у захисті інформаційних систем (таких, наприклад, як можливість доступу сторонніх осіб до критично важливого устаткування або помилки у програмному забезпеченні). Загроза інформації, що циркулює в інформаційній системі, багато у чому залежить від її конфігурації й структури, дій персоналу, стану навколишнього фізичного середовища, технології оброблення інформації в ній.

На жаль, на сьогоднішній день не розроблено єдиної класифікації загроз. Хоча більшість

дослідники в основу класифікації кладуть такі чинники:

1. Відповідність до ймовірної реалізації: реальні й потенційні загрози.
2. За характером виникнення. Дані загрози виникають як результат впливів природних сил, так і свідомої діяльності людини.
3. За спрямованістю посягань: загрози інтересам окремої особи (права і свободи), інтересам суспільства, інтересам держави.
4. За характером розташування: внутрішні або зовнішні.
5. За характером засобів застосування: військові й невійськові.
6. За правовою ознакою: протиправні і ті, що відповідають чинному законодавству [3, 63].

На думку вчених, основними джерелами небезпек в Інтернеті є хакери й віруси. До речі, слово «хакер» спочатку мало позитивне значення: так називали достатньо обдарованого програміста. Значно пізніше так почали йменувати зловмисників, які здатні використовувати свої комп'ютерні знання для здійснення шкідливих дій у мережі.

Щодо вірусів, то вони мають досить багато класифікацій. Назвемо деякі з них. У залежності від середовища перебування виділять файлові, завантажувальні, мережні, макровіруси. За функційними можливостями віруси поділяються на нешкідливі, безпечні, небезпечні та дуже небезпечні. Різними є і способи зараження комп'ютера, зокрема виділяють резидентні віруси (вміщуються в оперативну пам'ять і додаються до всіх об'єктів) і нерезидентні (додаються до оперативної пам'яті та є активними лише короткий період часу).

Окрім цього, сайт розробника української антивірусної програми «Zillya!» виділяє такі види вірусів: хробаки, віруси-маскувальники, віруси-шпигуни, зомбі, рекламні віруси, віруси-блокувальники, троянські віруси [2, 125].

Більшість дослідників суголосні у тому, що найнебезпечнішим типом вірусів є так звана «троянська програма». Її загроза полягає у маскуванні в інших нешкідливих програмах, тільки під час запуску якої відбувається активація вірусу і до цього моменту її надзвичайно складно виявити. Троянська програма наносить різні збитки, але зазвичай вона «використовується для крадіжки, зміни або видалення особистих даних користувача» [4, 205].

Короткий аналіз інформації щодо модифікації комп'ютерних вірусів, свідчить про те, що вони поширюються різноманітними способами та несуть загрозу конфіденційності інформації. Саме тому потрібно більше уваги приділити питанню захисту від них. У цьому можуть допомогти антивірусні програми, які розробляють саме для протидії вірусам. Нині існує безліч їхніх видозмін і кожен зможе підібрати оптимальний варіант, зважаючи на рівень захисту та вартість

Важливою проблемою є також питання захисту інформації у системах документообігу. Як показує практичний досвід, до нього слід підходити комплексно. Нині для цього в установах та на підприємствах використовують ідентифікацію, автентифікацію та розмежування прав користувача. Фахівці вважають, що можна виділити три способи ідентифікації, а саме:1)парольну (введення при вході систему логіну і пароля);2) біометричну (ідентифікація відбувається за біометричними даними, тобто відбиток, пальця, сканування сітківки ока, голос); 3) за допомогою унікального предмета або майнову (для підтвердження використовується унікальний носій інформації: USB-ключі, смарт-карти тощо)[2, 303].

Отже, можна зробити деякі узагальнення. У контексті сучасних політичних подій у світі особливого значення набуває питання кібербезпеки як окремої особистості, так і усієї держави. Постійно розробляються й удосконалюються системи інформаційного захисту. Це стосується і систем електронного документообігу сучасних організацій, компаній, підприємств.

ЛІТЕРАТУРА

[1] V.A. Lipkon, Theoretical Foundations and Elements of National Security of Ukraine: K .: Text, 2003.

[2] V.A.Luzhetsky, et al. Fundamentals of Information Security. Vinnitsa: VNTU, 2013.

[3] A.A. Sabanov. Some aspects of electronic document protection. Connect! The world of communication. vol. 7, pp.62-64, July 2010. (references)

[4] O. Shchedrina. New information technology: navch. posib. K.: KNEU, 2005.