УДК 658.11

Міроничева Д.С., магістрант гр. ЕК-17-1мд,

Комазов П.В., доц., к.е.н. – науковий керівник

АНАЛІЗ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Запорізька державна інженерна академія, кафедра ЕІТ

За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень та боротьби різновекторних національних інтересів держав стає інформаційний простір. Науково технічний прогрес стрімко розвивається і входить в усі сфери: бізнес, журналістику, політику, освіту. Таким чином, інформаційна безпека є невід'ємною складовою частиною кожної з сфер національної безпеки. Інформаційні технології принципово змінили обсяг і важливість інформації, яка обертається в технічних засобах її збереження, обробки та передачі. Загальна комп'ютеризація основних сфер діяльності призвела до появи широкого спектру внутрішніх і зовнішніх загроз, нетрадиційних каналів втрати інформації і несанкціонованого доступу до неї [2].

Так, наприклад, 27 червня 2017 року сталась масштабна атака останнім представником шкідливої програми Petya [1]. Перші представники були виявлені в 2016 році та були звичайними зразками здирницьких вірусів.

У жовтні 2017 року сталась чергова епідемія ураження інформаційних систем вірусом-хробаком для здирництва через шифрування файлів Bad Rabbit (Win32/Diskcoder.D, Ransom.BadRabbit). Спочатку зловмисники отримали несанкційований доступ до низки веб-сайтів, де вставили власні сценарії JavaScript у сторінки. Ці сценарії звертались на сервер управління зловмисників, звідки отримували основну частину подальшого сценарію. Всього відомо про 15 підприємств, що постраждали від цієї атаки.

Реальністю сьогодення стало застосування інформаційної зброї і ведення інформаційних війн. Окрім військової галузі, інформаційна зброя також може використовуватися в економічній, банківській, соціальній та інших сферах з метою: 1) дезорганізації діяльності управлінських структур, транспортних потоків і засобів комунікації; 2) блокування діяльності окремих підприємств та банків, а також цілих галузей промисловості шляхом порушення багатоланкових технологічних зв'язків і системи взаєморозрахунків, проведення валютно-фінансових махінацій тощо; 3) ініціювання великих техногенних катастроф на території супротивника внаслідок порушення штатного управління технологічними процесами та об'єктами, що мають справу з великими об'ємами небезпечних речовин і високих концентрацій енергії; 4) масового поширення і впровадження у свідомість людей визначених уявлень, звичок і поведінкових стереотипів; 5) викликання невдоволення чи паніки серед населення, а також провокування деструктивних дій різних соціальних груп.

Отже, з вищезазначеного можна зробити такі висновки:

– інформаційна безпека набуває дедалі більшої актуальності в системі національної безпеки України;

– актуальними є питання пов`язані з комп`ютерними злочинами, та співпраця з іншими країнами, особливо в контексті реагування на кіберзлочини;

– є нагальна потреба визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Список використаних джерел

1. Вікіпедія – вільна енциклопедія. Petya [Електронний ресурс]. Спосіб доступу: https://uk.wikipedia.org/wiki/Petya

2. Марков В.В. Актуальні проблеми інформаційної безпеки України в системі міжнародної координації. Право і безпека №1(48), 2013. – С. 78, 80.