УДК 004.056:351.86]:007.51

Мазур Ю.О. здобувач освіти,
Зелінська О.В., к.т.н, доцент, доцент кафедри інформаційних технологій

ОСОБЛИВОСТІ ЗАХИСТУ СУЧАСНОЇ ІНФОСФЕРИ В УМОВАХ СТОРОННЬОГО КІБЕРНЕТИЧНОГО ВПЛИВУ

Донецький національний університет імені Василя Стуса, м.Вінниця

З розвитком ІТ-технологій, все більшої уваги потребує інформаційне середовище (кіберпростір). Якщо раніше аби нанести шкоди державі використовували збройні війни, то з появою ІТ додалась ще одна небезпека – кібервійна.

За статистикою в Україні упродовж тижня стається близько 40 тисяч кібератак. Найбільше страждають такі сфери як: банківська справа та державні установи. Фахівці пояснюють, що кількість нападів також пов'язана з додатком "Дія", адже саме там зберігається великий обсяг персональної інформації українців. І хоча розробники додатку вказують на те, що "Держава в смартфоні" на високому рівні програмно захищена, це не зменшує кількість спроб злому застосунка.

Розглянути які кібератаки існують на міжнародному рівні та особливості захисту інформаційних систем.

Захист інфосфери (кібербезпека) базується на трьох основних принципах (так званих "китах кібербезпеки"):

- Цілісність
- Доступність
- Конфіденційність

Потрібно зазначити, якщо хоча б один з цих чинників порушено, можна з точністю вказувати на те, що вже відбулась кібератака та систему інфосфери порушено. Якщо ж говорити про те чому відбуваються кібератаки направленні на знешкодження держави, можна виділити наступні чинники [1]:

1. Невідповідність інфраструктури електронних комунікацій держави.
2. Недостатній рівень захищеності інфосфери, державних електронних інформаційних ресурсів, вимог захищеності від кіберзагроз, що встановленні законодавством.
3. Безсистемність заходів кіберзахисту критичної інфосфери.
4. Недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки критичної інфосфери.
5. Недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного характерів.

Особливості захисту інфосфери держави насамперед передбачають знання законодавства. Таким чином, аби визначити яка саме інформація потребує захисту потрібно звернутись до Постанови №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», у котрій вказано що захисту в системі полягає [2]:

- Відкрита інформація, які належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, які оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами.
- Конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації".
- Службова інформація.
- Інформація, яка становить державну або іншу передбачену законом таємницю.
- Інформація, вимога щодо захисту якої встановлена законом.

Якщо після здійснення кібератаки відбуваються дії, що за міжнародним правом класифікуються як кримінальний злочин, тоді це можна з впевненістю назвати кібервійною. Кібервійна – використання Інтернету й пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіянню шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету іншої держави [3]

Список літератури

4. Діордіца І. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України. Підприємництво,господарство і право.10. 2017. С. 206-211.

5. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова від 29.03.2006 р. № 373. Дата оновлення:10.02.202. URL: http://surl.li/aqyyb (дата звернення: 12.11.2021)

6. Кібервійна. URL: http://surl.li/aqvcy (дата звернення: 12.11.2021)