УДК 342:343.346.8

Ольга Михайлівна Головко,
кандидат юридичних наук, старший викладач кафедри публічного права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Кіберзлочини та парадигма Human Rights

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163, кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей:

1) порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів;

2) порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем;

3) використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кібернзахисту.

Перше, що завжди привертає увагу в контексті посягань у кіберпросторі – це питання конфіденційності та збереження приватності. Варто зазначити, що цей аспект корелює зі ст. 12 Загальної декларації прав людини (далі – Декларація), яка виокремлює свободу від втручання в особисте і сімейне життя, від посягання на недоторканність житла, таємницю кореспонденції. Наразі, питання збереження приватності стоїть досить гостро та стосується не тільки технологічної складової забезпечення такої безпеки, однак заключає в собі й елементи особистої гігієни у кіберпросторі. Серед ключових принципів кібербезпеки визначають конфіденційність, цілісність та доступність інформаційної

системи. Якщо один з цих принципів порушується, вірогідність стати жертвою кіберзлочинця підвищується.

Так, в епоху цифрових трансформацій фраза «розумний будинок» перестає бути футурологічною ідеєю. Це цілковита реальність, яка стала можливою завдяки реалізації технологій Інтернету речей (IoT). Втім, досить гостро постала загроза посягання на свободу від втручання в особисте і сімейне життя, від посягання на недоторканність житла, адже інформаційна система, яка керує будинком фактично може стати знаряддям злочину для зловмисників.

У випадку зі ст. 9 Декларації, яка передбачає свободу від безпідставного арешту і вигнання можлива ситуація, в якій через дії злочинців особа, яка не вчиняла нічого протизаконного може бути піддана арешту. Йдеться про ситуації, коли через гаджет сторонньої особи без фізичного доступу до нього було вчинено злочинні дії, наприклад, зламано банківський рахунок. В такому випадку, фактично супутня жертва кіберзлочинця може бути піддана кримінальному переслідуванню. В цьому ж контексті можна розглядати порушення свободи вираження поглядів і переконань. Йдеться про випадки зламу особистої сторінки в соціальних мережах та поширення про певну особу недостовірної інформації, яка принижує її честь та гідність, завдає шкоди діловій репутації. Особа, яка стає жертвою такої кібератаки може бути звинувачена в дифамації.

Зазначені приклади та їх кореляція з деякими основоположними правами людини особливо загострюють увагу на тому, що такі атаки в більшості випадків є результатом недотримання особистої гігієни в кіберпросторі. Найчастіше, особа стає жертвою фітингу або фармінгу, коли особа несвідомо передає зловмиснику свої дані, потрапляючи «на гачок» кіберзлочинця. Тож, перше, на що треба робити акцент в питаннях превенції кіберзлочинів – впровадити освітні процедури, що допоможуть пересічному громадянину виокремити кібератаку чи кіберпастку та діяти таким чином, щоб максимально убезпечити себе від протиправних дій сторонніх осіб.

Одержано 30.10.2019