3. Україна отримає понад 700 млн дол. США від Світового банку. Урядовий портал. URL : https://www.kmu.gov.ua/news/ukrayina-otrimaye-ponad-700-mln-dol-ssha-vid-svitovogo-banku

Лаган В.В.
ст. гр. ПД-11
Формігей О.
ст. гр. ПДЕБм-11
Науковий керівник: к. е. н., доцент,
доцент кафедри безпеки та правоохоронної діяльності,
Західноукраїнський національний університет
Колесніков А.П.

ОСНОВИ ПОВЕДІНКИ В КІБЕРПРОСТОРІ

Протидія загрозам національній безпеці, що надходять з кіберпростору, на сьогодні є для України дуже актуальною, у тому числі з огляду на російську агресію.

Під час реалізації Стратегії кібербезпеки України (2016-2020) за цей період, у країні було зроблено чимало для нарощення потенціалу щодо протидії кіберзагрозам – і саме це дає можливість здійснювати подальшу розбудову національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії.

Одним з головних завдань нової Стратегії, як було затверджено в серпні цього року та яка розрахована на період до 2025-го року, є створення максимально відкритого, вільного, стабільного і безпечного кіберпростору де серед інших завдань нацбезпеки враховуються права і свободи людини.

Важливо те, що Україна постійно піддається кібератакам з боку РФ. На долю РФ та хакерів, яких фінансує російська влада приходиться до 90% всіх кібератак. А взагалі, майже 20% кібератак у світі спрямовані проти

України. Тому дуже важливо, що Стратегія передбачає створення в Україні кібервійськ. За думкою експертів, це є вдалою асиметричною відповіддю України російській агресії. Також до завдань новостворюваних військ будуть належати не лише забезпечення захисту критичної та іншої інфраструктури, а й проведення превентивних наступальних операцій у кіберпросторі.

У 2018 році НАТО віднесло кіберпростір до сфери військових операцій, тому зараз у багатьох країн світу є відповідні військові структури, вони пов'язані з наступальними операціями, а також з обороною у кіберпросторі. Вважаються найбільш потужними та просунутими в цих питаннях є Сполучені Штати та Велика Британія. Також Україна, як країна – партнер Альянсу має необхідний потенціал для нарощування у сфері кібербезпеки для адекватної протидії сучасним викликам і загрозам.

Для підвищення рівня захисту персональних даних, рекомендується застосовувати правила безпеки в кіберпросторі. Їх розробили в державному центрі кіберзахисту Держспецзв'язку:

- використоввати ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно й систематично їх оновлювати;

- користуватися антивірусним програмним забезпеченням з технологією евристичного аналізу;

- використовувати програмний міжмережевий екран (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення;

- здійснювати регулярне резервне копіювання даних, зберігати резервні копії на зовнішніх носіях інформації (SDD, HDD тощо) та налаштвати функцію «відновлення системи»;

- не підключати флешки та зовнішні диски, не вставляти CD та DVD тощо у комп'ютер, якщо ви не довіряєте повністю їх джерелу.

- Довіряти лише власним пристроям та бути обережними з пристроями які отримуєте від інших людей по роботі або в інших цілях;
- При підключені пристроїв забезпечити їх автоматичну перевірку на наявність шкідливого програмного забезпечення;
- Включати автоматичний запуск змінних носіїв інформації (захист від autorun.snf).

- регулярно змінювати паролі, не зберігти автентифікаційні дані в легкодоступних місцях (на робочому столі). Використовувати для зберігання паролів спеціальні програмні засоби (наприклад, KeePass). Використовувати стійкі паролі, зокрема такі що:

- містять не менше 8 символів;
- містять літери, цифри та спеціальні символи;
- не містять персоніфікованої інформації (дати народження, номерів телефонів, автотранспорту, банківської карти, адреси реєстрації тощо);
- не використовуються в будь – яких інших акаунтах.

- бути особливо обережними з відкриттям вкладень до електронної пошти від невідомих осіб;

- не переходити за невідомими посиланнями та не завантажувати файли, що мають потенційно небезпечне розширення (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js тощо) та навіть безпечне (наприклад: .docx, .zip, .pdf), адже можуть використовуватися вразливості, макроси та інші небезпеки;

- бути обережні щодо випливаючих вікон та повідомлень у вашому браузері, програмах, операційній системі та мобільному пристрої. Завжди читати вміст цих вікон та не «схвалювати» і не «приймати» нічого похапцем;

- установити обмеження кількості введення помилкових логінів/паролей. Регулярно провіряти журнали логування, планувальник завдань та автозавантаження на предмет несанкціонованих дій.

Отже, основними причинами, що провокують ріст мережної злочинності є недосконалі методи та засоби мережного захисту, а також різні уразливості у програмному забезпеченню елементів, що складають мережну інфраструктуру. Велике значення також має дотримання користувачами правил безпеки під час роботи в інтернеті. Дотримання простих правил спілкування через інтернет, дозволить захиститися від недобрих намірів зловмисників.

Список використаних джерел

1. Безпека у кіберпросторі. URL: http://defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1126-bezpeka-u-kiberprostori (дата звернення 19.04.2022)

2. Державний центр з кіберзахисту та кіберзвязку. URL: https://cert.gov.ua/recommendations/21 (дата звернення 19.04.2022)

Малайна В.В.
ст. гр. ПДЕБ-21
Науковий керівник: к. е. н., доцент,
доцент кафедри безпеки та правоохоронної діяльності,
Західноукраїнський національний університет
Муравська Ю.Є.

ОХОРОНА ТА ЗАХИСТ АВТОРСЬКОГО ПРАВА В СОЦІАЛЬНИХ МЕРЕЖАХ

На сьогодні досить актуальною є проблема порушення авторських прав у соціальних мережах і, водночас, доволі специфічною є система захисту права на недоторканність репутації, честі та гідності в мережі.