УДК 004.056

Савченко Т.В., канд. техн. наук, доцент
Шевченко С.В., студентка
Державний торговельно-економічний університет, м. Київ, sv_t@ukr.net

ТЕХНОЛОГІЇ ТА МЕТОДИ ЗАХИСТУ ВІД РОСІЙСЬКОЇ КІБЕРАГРЕСІЇ

З 2014 року Україна стала однією з головних цілей російської кіберагресії. Особливо ситуація загострилася з початком повномасштабного вторгнення. Росія активно веде інформаційну війну проти України, використовуючи кіберзброю та дезінформацію. Україна відчула на собі, як кібератаки можуть завдати серйозної шкоди економіці та інфраструктурі держави. У цей складний час українські спеціалісти з кібербезпеки відіграють надзвичайно важливу роль у захисті країни. Зокрема, ІТ-фахівці допомагають українській армії та правоохоронним органам виявляти та нейтралізувати кіберзагрози і захищати інформаційні ресурси держави від кібератак. Також вони співпрацюють з міжнародними партнерами та обмінюються досвідом у боротьбі з кіберзлочинністю. Кібератаки впливають на роботу урядових відомств, критичну інфраструктуру, бізнес та на приватних осіб. З боку ворога кібератаки спрямовані на погіршення економічного, військового та соціального стану нашої країни.

Захист від кібернападів став надзвичайно важливим завданням для української влади та підприємств, які опинилися на передовій цієї війни. У своїй боротьбі з російською кіберагресією Україна використовує різноманітні технології та методи кіберзахисту. Одним з найважливіших методів є захист від DDoS-атак, що є одним з найбільш поширених видів кібератак у війні з Росією. Українські експерти з кібербезпеки використовують різні засоби для захисту, такі як фільтри трафіку, перехоплення пакетів і використання хмарних сервісів. Україна також використовує шифрування для захисту конфіденційної інформації. Криптографія є одним з найефективніших методів захисту від кібератак, оскільки вона дозволяє захистити дані, що передаються мережею, від перехоплення та зламу. Українські фахівці з кібербезпеки використовують захист від розповсюдження шкідливих програм, які можуть завдати значної шкоди комп’ютерній мережі. Ще одним їхнім завданням є виявлення та нейтралізація дезінформації, яку поширює Росія. Спеціалісти з кібербезпеки аналізують соціальні мережі та мас-медіа, виявляють фейкові новини та російську пропаганду працюють над забезпеченням широкого доступу до правдивої інформації.

Захист від кібератак у війні з Росією є складною задачею, що вимагає використання комплексного підходу та поєднання різних засобів і методів захисту. Деякі з таких методів передбачають [1]:

1. Захист мереж і систем від кібератак. Здійснюється шляхом використання різних захисних технологій, таких як фаєрволи, системи виявлення вторгнень, системи контролю доступу, шифрування даних.
2. Контроль за доступом до інформації. На рівні користувачів важливо встановлювати політику доступу до різних ресурсів та мереж, забезпечувати достатньо складні паролі та обмеження на використання різних пристроїв.
3. Моніторинг та аналіз кіберзагроз. Для ефективного кіберзахисту необхідно вести моніторинг і аналізувати різні види кіберзагроз, щоб оперативно реагувати на них та уникати можливих наслідків.
4. Створення резервних копій та планів відновлення після кібератак. Це важливо, щоб мінімізувати наслідки таких атак.
5. Підвищення кіберсвідомості серед персоналу. Важливо навчати співробітників компаній та державних структур правилам кібербезпеки та навчати їх виявляти можливі кіберзагрози.

Забезпечення кібербезпеки та впровадження ефективних методів та засобів захисту є надзвичайно важливими для забезпечення безпеки та відновлення нормального функціонування країни.

Українські кіберзахисники використовують спеціальні програми для автоматичного виявлення зловмисних кодів та інших кіберзагроз. Після виявлення таких загроз, експерти проводять їх аналіз, визначають характеристики та видають рекомендації щодо захисту. Для розробки та використання захисту від DDoS-атак, фішингу та інших соціально-інженерних загроз використовуються спеціальні програми, що допомагають відстежувати та блокувати небезпечний трафік [2]. Україна використовує такі технології для захисту від кіберагресії, як захист мережі та даних, резервне копіювання, контроль доступу.

Україна активно використовує військово-кібернетичні вправи для тренування своїх кіберзахисників. Учасники вправ використовують реалістичні сценарії, що допомагають краще реагувати на кіберагресію. Такі вправи допомагають розробляти нові методи та технології захисту. Використовуються різноманітні захисні технології, такі як брандмауери, антивірусні програми та системи виявлення вторгнень. Завдяки цим інструментам вдалося знизити кількість кібератак та уникнути значних збитків.

Окрім захисту від кіберагресії, Україна активно працює над розвитком власних кіберзахисних можливостей та розширенням міжнародного співробітництва в цій сфері. Наприклад, створено Національний кіберцентр з метою координації кіберзахисних заходів та взаємодії з іншими країнами у відповіді на кіберзагрози. Україна активно співпрацює з міжнародними партнерами у сфері кібербезпеки, зокрема з Європейським Союзом, НАТО та США. Ця співпраця дозволяє обмінюватись досвідом та найкращими практиками, отримувати фінансову та технічну підтримку для розвитку кіберзахисту.

Важливою складовою заходів з кібербезпеки є підвищення інформаційної грамотності серед населення та бізнесу. Україна проводить кампанії з освіти населення щодо кібербезпеки, надає рекомендації щодо захисту особистих даних та створення складних паролів.

Україна продовжує покращувати свої заходи з кібербезпеки та відповідно реагувати на кіберзагрози, що дозволяє їй захищати не лише себе, а й бути прикладом для інших країн у боротьбі з цими загрозами.

Висновки. Війна України з Росією поставила до кібербезпеки високі вимоги та випробування. Україна використовує передові технології та інновації, щоб захистити себе від російської кіберагресії та забезпечити безпеку своїх громадян. Військові та цивільні спеціалісти працюють над розробкою та впровадженням нових технологій та методів захисту від кібератак. Важливою складовою є співпраця з партнерами з ЄС, НАТО та США, яка дозволяє використовувати досвід та знання від провідних країн у сфері кібербезпеки. Україна активно займається навчанням та тренуванням бійців на передовій у кібербезпеці, що допомагає підвищувати вміння реагувати на кібератаки. Такі заходи дозволяють збільшити рівень кібербезпеки в Україні та зменшити вразливість перед можливими кібератаками.

Список посилань

1. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.

2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – Львів: «Магнолія 2006», 2018. − 320с.