УДК 004.89:355.0

Я. О. Оболонська, А. Г. Стаднік

КІБЕРРОЗВІДКА, МЕТОДИ ЗБОРУ ДАНИХ І АНАЛІЗ ІНФОРМАЦІЇ В КІБЕРВІЙСЬКАХ

Анотація: *розглянуто кібернетична розвідка як підхід до збору та аналізу інформації в кіберпросторі, що охоплює телекомунікаційну і комп'ютерну розвідку, етапи операцій та пріоритети кібербезпеки України.*

Ключові слова: *кібернетична розвідка, телекомунікаційні системи, комп'ютерна розвідка, кібербезпека, етапи розвідки, законодавство, захист інформації, європейська інтеграція, права громадян.*

Abstract: *The article analyzes cyber intelligence as an approach to gathering and analyzing information in cyberspace, covering telecommunications and computer intelligence, stages of operations and priorities of Ukraine's cyber security.*

Keywords: *Cyber intelligence, telecommunications systems, computer intelligence, cyber security, stages of intelligence, legislation, information protection, European integration, citizens' rights.*

Вступ

У сучасному світі, де технології стрімко розвиваються, кібернетична розвідка стає критично важливою для забезпечення інформаційної безпеки. Актуальність цієї теми зумовлена зростаючими кіберзагрозами, які вимагають ефективних механізмів збору та аналізу інформації. Основною метою дослідження є вивчення основних цілей кіберрозвідки, зокрема підвищення ефективності розвідувальних операцій, захисту інформаційних систем та реагування на загрози. Завдання включають аналіз методів збору даних, визначення основних напрямків кіберрозвідки таоцінку їхнього впливу на безпеку.

Результати дослідження

Кібернетична розвідка охоплює комплексний підхід до збору, аналізу та використання інформації для забезпечення ефективності розвідувальних операцій у кіберпросторі. Вона поділяється на два основні напрями: розвідку телекомунікаційних систем і комп'ютерну розвідку. Розвідка телекомунікаційних систем включає перехоплення повідомлень, прослуховування телефонних розмов у мобільних та провідних мережах, визначення географічного розташування власників мобільних телефонів і розшифровку закодованих повідомлень. Комп'ютерна розвідка спрямована на добування інформації, що обробляється, зберігається та передається в інформаційній системі, отримання відомостей про характеристики програмних, апаратних і програмно-апаратних комплексів, аналіз методів і механізмів захисту інформації, виявлення персональних даних користувачів та вразливостей інформаційно-управляючих систем.

Етапи проведення кібернетичної розвідки складаються з шести основних фаз: рекогносцировка, сканування мережі, отримання доступу, підтримка доступу, приховування слідів присутності та аналітичний звіт. На етапі рекогносцировки здійснюється початковий збір інформації та визначення потенційних цілей для подальшого дослідження. Сканування мережі дозволяє аналізувати мережеву інфраструктуру, виявляючи відкриті порти, служби і потенційні точки входу. На етапі отримання доступу здійснюється проникнення в систему через знайдені вразливості, а на етапі підтримки доступу забезпечується збереження доступу до системи без виявлення. Приховування слідів присутності передбачає маскування слідів для уникнення виявлення і збереження непомітності дій. Останнім етапом є аналітичний звіт, який включає узагальнення зібраної інформації та її обробку для формування висновків і рекомендацій. Кібернетична розвідка забезпечує всебічний аналіз інформаційних систем та мереж супротивника[1].

Сучасні технології збору даних для кіберрозвідки включають інструменти OSINT (Open-Source Intelligence) [2], системи автоматизації, машинне навчання, аналіз, обробку великих даних. Інструменти OSINT, забезпечують збір інформації з відкритих джерел, таких як соціальні мережі та новинні сайти.

Системи автоматизації моніторингу кіберпростору в реальному часі допомагають відслідковувати потенційні загрози та реагувати на інциденти. Алгоритми машинного навчання дозволяють ефективно виявляти аномалії у великих обсягах даних, що допомагає виявляти кіберзагрози. Інструменти для аналізу, допомагають швидко реагувати на підозрілу активність у мережах. Технології великих даних , дозволяють обробляти великі масиви інформації для виявлення загроз. Threat Intelligence, забезпечує обмін інформацією про загрози, що підвищує ефективність розвідувальних операцій [3]. Усі ці технології суттєво покращують здатність до виявлення, аналізу та запобігання кіберзагрозам.

Пріоритети кібербезпеки України охоплюють три основні напрямки [4]. Кожен із цих напрямівє критично важливим для створення ефективної системи захисту країни від кіберзагроз та забезпечення стійкості в умовах глобальних цифрових викликів.

Убезпечення кіберпростору для захисту суверенітету держави та розвитку суспільства. Цей пріоритет спрямований на створення надійної системи кіберзахисту, яка буде здатна відбивати кібератаки, що становлять загрозу національному суверенітету. Це включає побудову інфраструктури для моніторингу та реагування на загрози в реальному часі, а також вдосконалення кібероборони, яка може ефективно протидіяти втручанню в державні та суспільні процеси. Забезпечення кібербезпеки на рівні держави також сприятиме розвитку цифрових технологій, інновацій та зміцненню економіки, що, в свою чергу, посилить загальну стійкість суспільства до кіберризиків.

Захист прав, свобод і законних інтересів громадян України у кіберпросторі. Цей аспект передбачає забезпечення приватності та безпеки персональних даних громадян, захист їхньої інформації від несанкціонованого доступу та протидію кіберзлочинності. Пріоритетом є також підтримка прав на свободу слова і захист громадян від цифрових загроз, таких як фішинг, кібершахрайство, кіберпереслідування та інші форми зловживання у кіберпросторі. Для цього необхідно зміцнити правові та технічні механізми захисту, що дозволить кожному громадянину відчувати себе безпечно у цифровому середовищі та користуватися його перевагами без страху перед кібератаками.

Європейська і євроатлантична інтеграція у сфері кібербезпеки. Враховуючи геополітичну ситуацію та стратегічні інтереси України, інтеграція до європейської і євроатлантичної систем кібербезпеки є важливим пріоритетом. Це передбачає поглиблення співпраці з країнами ЄС та НАТО, обмін досвідом, участь у спільних кібернавчаннях та отримання доступу до новітніх технологій і стандартів захисту. Завдяки тіснішій інтеграції з європейськими партнерами, Україна зможе ефективніше запроваджувати передові практики кібербезпеки, а також оперативно реагувати на спільні загрози у рамках міжнародних партнерських програм.

На сьогоднішній день існує проблема недосконалості законодавства в галузі кібербезпеки, зокрема застарілість інформаційно-правових норм, низький рівень санкцій за правопорушення та повільне впровадження європейського законодавства.Це викликає занепокоєння, оскільки стрімкий розвиток технологій і зростання кіберзагроз вимагають термінового вдосконалення норм. Застарілі положення не можуть адекватно реагувати на нові виклики, а недостатні стягнення не стримують потенційних правопорушників. Повільна імплементація європейських норм у національне законодавство також ускладнює забезпечення ефективного кіберзахисту. Важливо зосередити зусилля на актуалізації законодавства, підвищенні відповідальності та пришвидшенні впровадження європейських стандартів [5].

Висновки

Кібернетична розвідка та забезпечення кібербезпеки є критично важливими аспектами сучасного світу, в якому технології стрімко розвиваються, а кіберзагрози стають все більш складними і різноманітними. Дослідження показало, що основними цілями кіберрозвідки є підвищення ефективності розвідувальних операцій, захист інформаційних систем та швидка реакція на загрози. Основні етапи кіберрозвідки, від рекогносцировки до аналітичного звіту,

забезпечують системний підхід до збору та аналізу інформації, що сприяє виявленню та нейтралізації загроз. Сучасні технології збору даних, такі як OSINT, автоматизація, машинне навчання і аналітика великих даних, значно покращують здатність організацій реагувати на кіберзагрози, а також підвищують ефективність їхніх розвідувальних операцій. Пріоритети кібербезпеки України, зосереджені на захисті державного суверенітету, забезпеченні прав і свобод громадян у кіберпросторі, а також на інтеграції в європейську систему кібербезпеки, є ключовими для формування ефективної системи захисту в умовах глобальних цифрових викликів. Однак, існуючі недоліки в законодавстві, такі як застарілість норм і недостатня відповідальність за правопорушення, створюють серйозні виклики для кіберзахисту. Тому, для забезпечення надійної кібербезпеки необхідно терміново вдосконалити законодавчу базу, адаптувати її до сучасних реалій та підвищити відповідальність за кіберзлочини. Це дозволить Україні не тільки ефективніше захищати свої інформаційні ресурси, але й сприятиме розвитку цифрових технологій.

Список використаних джерел:

1. В.Кива, Є.Судніков, О.Войтко. МЕТОДИ РОЗВІДКИ КІБЕРПРОСТОРУ. URL: https://www.researchgate.net/publication/346114187_Metodi_rozvidki_kiberprostoru.
2. Козицька О. Г. КІБЕРРОЗВІДКА ЯК НОВІТНІЙ НАПРЯМ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ. Хмельницький Університет Управління та Права. URL: http://old.univer.km.ua/statti/Kozytska,%20O.H.%20Kiberrozvidka%20yak%20novitnii%20napriam%20operatyvn o-rozshukovoi%20diialnosti.pdf.
3. IBM. What is Threat Intelligence? , IBM. IBM - United States. URL: https://www.ibm.com/topics/threat-intelligence.
4. Стратегія кібербезпеки України: цілі та пріоритети. АрміяInform – Інформаційне агентство АрміяInform. URL: https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/.
5. Зуй В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. Правове забезпечення адміністративної реформи. URL: http://www.sulj.oduvs.od.ua/archive/2022/4/part_1/35.pdf.

Оболонська Яна Олександрівна – студентка групи 1БС-22б, факультету інформаційних технологій та комп'ютерної інженерії, громадянка кафедри Військової підготовки, Вінницький національний технічний університет, Вінниця, e-mail: vn.oyana@gmail.com

Стаднік Анна Григорівна - громадянка кафедри Військової підготовки, Вінницький національний технічний університет, м.Вінниця,e-mail:stadnikanna2909@gmail.com

Obolonska Yana Oleksandrivna - student of group 1BS-22b, faculty of information technologies and computer engineering, citizen of the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: vn.oyana@gmail.com

Stadnik Anna Hryhorivna - a citizen of the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: stadnikanna2909@gmail.com