аналітикою / ILP: навчальний посібник / за заг. ред. Вербенського М.Г. Київ, 2019. 120 с.

8. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник / А.В. Мовчан. Львів ЛьвДУВС, 2017. 244 с.

9. Кримінальний кодекс України від 30.06.2022 р. Відомості Верховної Ради України (ВВР), 2001, № 25–26, ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#top.

Свистонюк Владислав Андрійович,
здобувач ступеня вищої освіти бакалавра
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник: **Неклеса О. В.,**
викладач кафедри кримінального процесу
та стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ

МІСЦЕ ТА РОЛЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ В ПРОТИДІЇ КІБЕРТЕРОРИЗМУ ПІД ЧАС ВОЄННОГО СТАНУ

Стрімкий розвиток інформаційних технологій, які мають вплив на всі сфери нашої життєдіяльності становлять собою певні загрози. За рахунок глобальної інтеграції, міжнародної конкуренції і феномену інформаційного простору головною ареною розподілу сфер впливу і контролю за масами є інформаційний простір. Головним негативним аспектом постійного прогресу інформаційних технологій є виникнення злочинної поведінки. Електронно обчислювальні машини надають можливість скоєння злочинів нетрадиційними правовими засобами. Тому закономірно, що використання інформаційних технологій породжує нові види злочинів, одним з яких є кібертероризм [1].

Як кримінально-правовий феномен, тероризм носить міжнародний характер та відповідно до низки міжнародних документів належить до числу міжнародних злочинів. Повною мірою це поширюється і на нові форми його прояву – кібертероризм або, як його часто ще називають комп'ютерний тероризм. Аналіз світових тенденцій розвитку кібертероризму з великою часткою ймовірності дозволяє прогнозувати, що його загроза з кожним роком зростатиме.

Для ефективної боротьби з кібертероризмом необхідно розробити державну програму розвитку інформаційно-комунікаційних технологій, що забезпечують підключення корпоративних мереж до мережі Інтернет при дотримання вимог безпеки інформаційних ресурсів.

Також необхідно вжити заходів щодо вдосконалення технологій своєчасного виявлення та припинення спроб несанкціонований доступ до інформації. Крім цього, важливо законодавчо встановити вичерпний перелік видів відомостей, що підлягають передачі по

відкритих мережах, та забезпечити контроль за дотриманням встановленого статусу конфіденційної інформації.

При цьому необхідно продовжувати роботу з попереджувального виявлення нових факторів ризику, по створенню і використання випереджаючих технологій боротьби з кібертероризмом [2].

Велике значення має організація системи підготовки та підвищення кваліфікації спеціалістів з інформаційної безпеки.

Крім того, необхідно підвищувати правосвідомість людей, що дозволить їм, маючи чітке розуміння розумності подібних норм, надавати всіляку допомогу правоохоронним органам у виявленні випадків кібертероризму вже на стадії підготовки злочинів, що здійснюються з використанням інформаційних систем.

Особливу роль у боротьбі з кіберзлочинцями відіграє здійснення перепідготовки та регулярне підвищення кваліфікації кадрів, що спеціалізуються на боротьбі з кібертероризмом, їх пошук з числа професіоналів тільки на конкурсній та контрактній основі. Таке навчання спонукатиме їх постійно самовдосконалюватися, щоб ефективно протистояти новим видам мережевих атак та комп'ютерних злочинів.

При цьому постійне технічне та програмне переоснащення служб та підрозділів, що займаються протидією кібертероризму, має стати регулярним, що стане однією з дійових гарантій інформаційної безпеки держави.

Ще одним важливим напрямком боротьби із використанням інформаційних технологій у терористичних цілях є їх профілактика. Особливо важливо проводити таку профілактичну роботу серед молоді, оскільки саме молодь через ряд психологічних і інших факторів є найбільш вразливою у плані схильності негативний вплив різноманітних кримінальних груп [3].

Отже, визначено місце та роль Національної поліції у протидії кібертероризму під час воєнного стану. Соціальна та матеріальна незахищеність молоді, частий максималізм в оцінках та судженнях, психологічна незрілість, значна залежність від чужої думки, загальне захоплення інформаційно-комунікаційними технологіями, прагнення підвищити свою самооцінку будь-якими способами, у тому числі протизаконними, такими, як хакерські атаки – це лише деякі з причин, що дозволяють говорити про можливості легкого поширення радикальних ідей серед молоді та привабливості кібертероризму.

Список використаних джерел

1. Анатолій Грабовий Не «M.E.Doc»ом єдиним. Закон і Бізнес: юридична газета. URL: https://zib.com.ua/ua/129461-dlya_styagnennya_zbitkiv_vid_petya_varto_pidtverditi_fakt_at.html.

2. Віктор Мороз Кібератака. Як захистити власний бізнес?, Юридична газета онлайн. URL: https://yur-gazeta.com/dumka-eksperta/kiberataka-yak-zahistiti-vlasniy-biznes.html.

3. Вільна енциклопедія «Вікіпедія». URL: https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%B.