тому актуальність аналізу загроз інформаційному простору країни стає важливим питанням державного рівня, інтерес до якого викликаний на усій міжнародній арені.

Проблемами інформаційної безпеки займалися багато науковців, серед яких: А. Марущак, Б. Кармич, В. Ліпкан, В. Петрик, Г. Почепцов, І. Арістова, І. Громико, О. Гончаренко, Є. Лисицин.

Інформаційна безпека, будучи важливою складовою національної безпеки, забезпечує цілісність суспільства, інформаційного суверенітету країни.

У Доктрині інформаційної безпеки України визначено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ, а також мережу Інтернет; деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками [1].

До загроз національній безпеці України в інформаційній сфері також варто зарахувати: прояви обмеження свободи слова та доступу громадян до інформації; викривлення, спотворення, блокування, замовчування, упереджене та тенденційне висвітлення інформації; несанкціоноване її поширення; відкриту дезінформацію; інформаційну експансію з боку інших держав та руйнівне інформаційне вторгнення у національний інформаційний простір, коли країни з потужнішим інформаційним потенціалом отримали можливість розширити свій вплив через ЗМІ на населення і громадськість менш потужної держави; виникнення і функціонування у національному інформаційному просторі держави непідконтрольних інформаційних потоків; поширення засобами масової інформації культу насильства, жорстокості; повільність входження України у світовий інформаційний простір; невиваженість державної інформаційної політики та відсутність необхідної інфраструктури в інформаційній сфері; розміщення дезінформації в Інтернеті [2, с. 27–32].

Для попередження руйнівного стану інформаційної безпеки в країні цілком доцільно забезпечити належний захист інформаційного простору, забезпечивши активність інформаційних служб, закцентувати увагу на міжпартійних відносинах, конфесійних конфліктах, належній компетентності працівників державних органів і установ, поглибити розробку ефективних механізмів захисту інформаційного простору України й пам'ятати, що головним носієм інформації є людина, свобода пересування якої належить до природних прав усіх демократичних державах світу, і тому методи захисту інформації повинні виходити саме з цієї парадигми.

Перспективним вирішенням проблеми інформаційної безпеки буде аналіз та запровадження зарубіжного досвіду технологій протидії загрозам інформаційному простору українського суспільства.

1. Доктрина інформаційної безпеки України. URL: http://www.zakon3.rada.gov.ua/laws/show/514/2009.
2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. №1. 2016. С. 27–32.
3. Інформаційна безпека держави у контексті протидії інформаційним війнам: навч. посібник / В.Б. Толубка. Київ: НАОУ. 2004. 315 с.
4. Почепцов Г. Сучасні інформаційні війни. Київ. Києво-Могилянська академія. 2015. 497 с.
5. Медвідь Ф. Інформаційна безпека України: виклики та загрози. URL: http://www.nato.ru.if.ua/journal/2009-2-28.pdf.

Ігнатов Сергій Олександрович
викладач кафедри адміністративного права,
процесу та адміністративної діяльності
Дніпропетровського державного
університету внутрішніх справ

КІБЕРТЕРОРИЗМ ЯК НОВА ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Стрімкий розвиток цивілізації вимагає належного правового регулювання нових груп суспільних відносин, що донедавна взагалі не розглядалися як об'єкти правового регулювання. До новітніх сфер можна віднести ядерну енергетику, генні технології, космос. Однією з таких складових суспільного життя став кіберпростір, що протягом останніх десятиліть перетворився у самостійну сферу суспільного життя, яка стрімко розвивається і сьогодні.

Нагадаємо, що згідно зі статтею 1 Закону України «Про основні засади забезпечення

кібербезпеки України», кіберпростір являє собою середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [1].

Кіберпростір є не лише місцем, яке спрощує ведення бізнесу, спілкування та обміну інформацією. У віртуальній реальності поряд із реальним життям мають місце численні випадки вчинення кримінальних та адміністративних правопорушень, незаконних операцій, кібернетичних атак, погроз, пранку, кібербулінгу та кібертероризму. Все це у сукупності становить групу деструктивних факторів, які справляють негативний вплив на стан національної безпеки України і ускладнюють правове регулювання в цій сфері.

Вбачається, що сьогодні особливу загрозу для національної безпеки становить кібертероризм. Саме це явище поступово приходить на заміну традиційним формам терористичної діяльності.

Акцентуємо увагу, що відповідно до Закону України «Про національну безпеку України», загрозами національній безпеці України слід вважати явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [2].

Разом із тим, відповідно до частини 4 статті 3 вищезгаданого Закону, державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо [2].

Як випливає з викладеного, сфера кіберпростору вбачається Законодавцем надзвичайно важливою, що закріплено окремим напрямком державної політики у сферах національної безпеки і оборони.

Що стосується визначення поняття кібертероризму (інформаційного тероризму), то відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кібертероризм являє собою терористичну діяльність, що здійснюється у кіберпросторі або з його використанням.

Якщо тероризм в узагальненому вигляді має на меті залякування, то сучасні кібертехнології дають широкі можливості для реалізації відповідної протиправної діяльності. Наприклад, для виведення з ладу системи водопостачання або освітлення достатньо провести успішну атаку на центральний сервер, який забезпечує життєдіяльність відповідної системи. При цьому зловмисник вчиняє протиправні дії віддалено, використовуючи телекомунікаційні технології. Також віддалено можуть бути висунуті політичні або ідеологічні вимоги, взята відповідальність за такі дії тощо.

Гриник Р.О., Пилипенко В.М. слушно зазначають, що головне у тактиці кібертероризму полягає в тому, щоб кіберзлочин мав досить небезпечні наслідки, став широко відомий населенню, отримав великий суспільний резонанс і створював атмосферу загрози повторення акту без вказівки конкретного об'єкта. Так, керівники ряду радикальних мусульманських організацій Близького Сходу надають дедалі більшого значення використанню у своїй діяльності саме сучасних інформаційних технологій, розглядаючи їх як ефективний різновид зброї у боротьбі з режимами Ізраїлю, Саудівської Аравії і підтримуючих їх західними країнами. Це, по-перше, досить недорогий засіб здійснення терористичного акту (тому до кібертероризму вдаються переважно країни з нерозвиненою економікою), а по-друге, складнощі з виявленням кіберзлочинця [3, с. 62].

У цілому підтримуючи тезу про загрозу кібертероризму, не можна погодитись із думкою, що кібертероризм є притаманним для держав із нерозвиненою економікою. До відповідних дій все частіше вдаються радикальні групи фактично з усіх держав світу і масштаби поширення кібертероризму збільшуються.

Не вдаючись до розлогих дискусій щодо небезпеки кібертероризму та необхідності запровадження заходів з протидії цьому явищу, наведемо слушну думку Топчія В.В. про те, що питання профілактики та протидії кібертероризму на нормативному рівні взагалі не врегульовано та потребує детального вивчення та опрацювання. Головною прогалиною, яка є на даний час, цієї проблеми є недосконаліть національного та міжнародного законодавства [4, с. 68]. Дійсно, початком протидії кібертероризму має бути нормативний рівень вітчизняного законодавства. Тільки після створення ефективного правового механізму можна вести мову про практичні заходи щодо запобігання і протидії кібертероризму.

У підсумку зазначимо, що характер змін і доповнень до національного законодавства щодо протидії кібертероризму має враховувати сучасний стан справ та не має обмежуватись одним-двома законами. Звичайно, такі зміни мають бути комплексними та враховувати сучасні

тактики і методи використання кіберпростору зі злочинною метою. Лише своєчасне оновлення національного правового масиву та урахування світових тенденцій у розглядуваній сфері може створити підґрунтя для розробки і впровадження антитерористичних заходів у кіберпросторі.

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
2. Про Національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
3. Гриник Р.О., Пилипенко В.М. Кібертероризм як нова форма міжнародного тероризму // Актуальні задачі та досягнення у галузі кібербезпеки: матеріали Всеукраїнської наук.-практ. конф. 23–25 листопада 2016 року. м. Кропивницький. С. 61–62.
4. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. *Науковий вісник Херсонського державного університету. Юридичні науки*. Вип. 6. Т. 3. 2015. С. 65–68.

Марченко Олеся Денисівна
викладач кафедри
загальноправових дисциплін
Дніпропетровського державного
університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ПРАВОВИХ РЕЖИМІВ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

На сучасному етапі розвитку інформаційного суспільства особливої актуальності набувають питання доступу громадян до різних видів інформації. Після прийняття Окінавської хартії 2000 року і введення її в дію на території країн-підписантів постала потреба привести українське законодавство до основних положень цього документа. Верховна Рада прийняла низку законів, спрямованих на це, і, зокрема, визначила види інформації, що належать до публічної інформації, а також встановила правові режими доступу до публічної інформації в цілому та до публічної інформації зокрема. З огляду на сучасну ситуацію в Україні та підвищення ролі Служби безпеки України (далі – СБУ) в забезпеченні національної безпеки в державі, питання правового режиму доступу до публічної інформації СБУ набувають особливої актуальності.

Питання правових режимів доступу до публічної інформації СБУ були предметом дослідження таких науковців: Андрусів В., Бєляков К., Гущин О., Демкова М., Коропатник І., Марущак А., Нестеренко О., Нікітчук І., Таран В., Тацишин І., Тищенко М., Фурман І. та ін.

Метою даної роботи є визначити правові режими доступу до публічної інформації СБУ.

Перш ніж розглядати правові режими публічної інформації, вважаємо за доцільне надати визначення терміна «публічна інформація». За загальним правилом, встановленим частиною 2 статті 20 Закону «Про інформацію» [1], будь-яка інформація є відкритою, окрім випадків, прямо передбачених законодавством. А отже, громадяни можуть вільно та безперешкодно реалізовувати своє право на інформацію, обмеження якого допускається тільки за наявності умов та підстав, прямо визначених нормами чинних нормативно-правових актів.

За своєю сутністю, правові режими визначають режими доступу до публічної інформації, які виражаються у тому, що доступ до одних відомостей (подій, даних) запитувач може отримати вільно – не докладаючи особливих зусиль, а до іншої інформації – лише через проходження визначеного законодавством порядку.

Термін «режим», у загальному розумінні, тлумачиться як певні умови, необхідні для забезпечення роботи, функціонування, існування чого-небудь [2, с. 1921]. Законодавець встановлює, що режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення й зберігання інформації [3]. Ми вважаємо, що визначена законодавцем дефініція «режим доступу до інформації» включає цілий комплекс прав, які передбачені Конституцією, але які не стосуються самого права на доступ. Тому під режимом доступу до інформації ми пропонуємо розуміти визначені та врегульовані законодавством вимоги (умови) отримання потрібної інформації від розпорядника для реалізації конституційних прав в усній, письмовій, електронній формах чи на звуко-, відео- та будь-яких інших носіях тощо.

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. У законодавстві зазначено, що будь-яка інформація є відкритою,