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,

крім тієї, що віднесена законом до інформації з обмеженим доступом [4, с. 20].

Відповідно до ст. 12 Закону України «Про доступ до публічної інформації», суб'єктами відносин у сфері доступу до публічної інформації є такі:

1) запитувачі інформації – фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень;

2) розпорядники інформації – суб'єкти, визначені у ст.13 Закону України «Про доступ до публічної інформації»;

3) структурний підрозділ або відповідальна особа з питань запитів на інформацію розпорядників інформації [5].

Таким чином, можна визначити, що право на отримання інформації може реалізовуватися у двох формах: пасивній і активній.

Пасивна форма: розпорядник інформації у випадках, передбачених законодавством, зобов'язаний на тих чи інших носіях поширити інформацію так, щоб будь-яка особа могла з нею ознайомитися, відкривши веб-сайт чи інформаційний бюлетень. Якщо розпорядник інформації не виконує такого зобов'язання, це порушує конституційне право кожного на отримання інформації. Звідси фізичні та юридичні особи можуть оскаржувати бездіяльність такого розпорядника інформації та вимагати відновлення порушеного права, тобто розміщення інформації.

Активна форма: запитувач інформації звертається із запитом на інформацію і розпорядник зобов'язаний її надати у формі, про яку просить запитувач (усно, письмово, факсом тощо).

У той же час необхідно зазначити, що законодавець, передбачивши обов'язки розпорядника щодо оприлюднення публічної інформації, не закріпив у жодному нормативно-правовому акті відповідальність осіб, які порушують встановлені обов'язки, фактично нівелювавши значущість даної норми.

Запити на інформацію, оформлені відповідно до вимог статті 19 Закону України «Про доступ до публічної інформації», підлягають обов'язковому прийняттю та розгляду в системі СБУ.

Публічна інформація про діяльність СБУ надається у формі, визначеній законодавством.

У разі, якщо частина запитуваної інформації належить до інформації з обмеженим доступом, а інша частина є відкритою інформацією, надається відкрита запитувана інформація.

Отримання запитів на інформацію на особистому прийомі здійснюється через приймальні громадян посадовими особами, що здійснюють особистий прийом громадян.

Згідно з чинним законодавством України, обмеження доступу до інформації можливе лише на підставі закону та з відповідною метою. Вичерпний перелік цілей наведено в ч. 2 ст. 32 та ч. 3 ст. 34 Конституції України [6]. Він цілком відповідає європейським стандартам у цій сфері. Відповідно до ч. 3 ст. 34 Конституції України, право на доступ до інформації може бути обмежено законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [6]. Згідно зі ст. 32 Конституції, не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [6]. Але слід зазначити, що Конституція не закріплює безпосередніх умов застосування таких обмежень.

Таким чином, здебільшого обмеження прав і свобод людини і громадянина може бути здійснено виключно «в інтересах національної безпеки». Дослідження законодавства в цій сфері дозволяє стверджувати, що в українському законодавстві правове та легітимне визначення даного поняття відсутнє. А тому відсутні критерії віднесення тих чи інших явищ або подій до «інтересів національної безпеки».

Згідно з нормативно-правовими документами, які регулюють питання доступу до публічної інформації та визначають режими доступу, пропонуємо таку класифікацію режимів доступу в органах СБУ:

- закритий доступ – містить інформацію, віднесену до конфіденційної інформації, зокрема: дані, розголошення яких може загрожувати національній безпеці; завдати шкоди життю і здоров'ю та безпеці громадян; які стосуються охорони державної, комерційної або банківської таємниці тощо;
- обмежений доступ – містить інформацію, яка належить до службової інформації (відповідно до законодавства);
- процесуальний доступ – містить інформацію, яка отримується за запитом;
- повний (загальний) доступ – містить інформацію, яка підлягає обов'язковому

оприлюдненню на офіційному веб-порталі СБУ; опублікуванню у друкованих виданнях; поширенню в електронній формі тощо.

Таким чином, підсумовуючи, можна визначити, що українське законодавство встановлює два правових режими доступу до публічної інформації. Право на отримання інформації може реалізовуватися у двох формах: пасивній і активній. Але, з огляду на специфіку таа мету і завдання діяльності СБУ, ми вважаємо за доцільне розширити перелік правових режимів доступу до публічної інформації в органах СБУ з двох до чотирьох, а саме закритий, обмежений, процесуальний, повний.

1. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

2. Великий тлумачний словник сучасної української мови: 170000 слів / уклад. і гол. ред. В. Т. Бусел; Київ; Ірпінь: Перун, 2003. 1427 с.

3. Рекомендація Ради Європи Комітету Міністрів державам-членам № R (2002) 2 про доступ до офіційних документів, схвалена 02.02.2002 // Доступ до інформації та електронне урядування / авт.-упоряд. М.С. Демкова, М.В. Фігель. Київ: Факт, 2004. 336 с.

4. Коломоєць Т.О. Адміністративне судочинство України: підручник. Київ: Істина, 2008. 256 с.

5. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17.

6. Конституція України від 28.06.1998 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

Махницький Олександр Васильович
старший викладач кафедри

Гавриш Олег Степанович
викладач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

АНАЛІЗ КІБЕРЗАГРОЗ. НАЙБЛИЖЧІ ПЕРСПЕКТИВИ

На 26-й найбільшій у світі конференції хакерів DefCon працівник компанії Endgame, що займається системами безпеки, показав програму, яку можна було налаштувати так, щоб вона самостійно створювала шкідливе ПЗ.

Вивчивши середу OpenAl Gym – платформу для тренування ШІ (штучний інтелект), програма навчилася ховати вірус від систем захисту. Система вносила зміни в коректний код, «проводила» його повз антивірус, збирала дані і випускала нову шкідливу версію. Виявити вірус не вдалося.

А якщо шкідлива програма, використовуючи ШІ, зможе автономно визначати, як імітувати нормальну поведінку або рух (наприклад, за допомогою локальних облікових даних), зловмисникам не буде потрібно спеціальний сервер, а шкідливе ПО буде в рази важче ідентифікувати.

У дослідженні компанії Darktrace йдеться про перші зразки програм, які здатні аналізувати оточення. Це дозволяє їм розуміти, де вони перебувають, і знаходити відмінності між віртуалізованим і «голим» середовищем (bare metal), а також знаходити вади в операційній системі.

Така програма зможе підібрати відповідний набір дій для кожного середовища. Коли ІБ-фахівці аналізуватимуть вірус, він буде маскуватися і може залишитися непоміченим. А за справу шкідливий код візьметься вже в руках кінцевого користувача і буде, наприклад, красти коди доступу до банківських рахунків або персональні дані.

Крім цього, використовуючи штучний інтелект, хакери зможуть діяти швидше, ніж фахівці з ІБ, що блокують атаку.

Проаналізувавши ситуацію, ШІ зможе скористатися іншою вразливістю або, не чекаючи на людину, почати пошук альтернативних шляхів злому. В результаті ІБ-шники можуть банально не встигати відображати атаки.

У тому, що штучний інтелект може стати хакерською кіберзброєю, впевнені 62% опитаних ІБ-фахівців. Механізми захисту в найближчі роки теж повинні будуватися із застосуванням ШІ – про це варто замислитися вже зараз, адже з кожною новою адаптацією машинне навчання буде все більш гнучким і легко зможе використовувати знайдені лазівки і уразливості на шкоду сумлінним користувачам.

Розумний фішинг і діпфейки.