3. Средство криптографической защиты информации. URL: https://www.cryptopro.ru/sites/default/files/docs/.../admin_guide_general_r3pdf. (Дата звернення 14.09.2018).
4. Депонирование ключей. URL: http://samoychiteli.ru/document34285.html. (Дата звернення 14.09.2018).

***Чанишев Рашид Ібрагімович***

Національний університет «Одеська юридична академія»,
кандидат юридичних наук, доцент,
доцент кафедри інформаційних технологій

## ПРОБЛЕМИ, ПОВ'ЯЗАНІ З БЛОКУВАННЯМ ДОСТУПУ ДО РЕСУРСІВ МЕРЕЖІ ІНТЕРНЕТ

Поява глобальної мережі Інтернет призвела до глобальних змін в житті людства. Ще ніколи в його історії доступ до інформації не був таким легким і доступним для кожного. Однак, через кілька десятиліть його успішного використання, з'явилася необхідність введення обмежень на доступ до певних видів інформації.

Офіційно обмеження на доступ до інформації вводяться за такими основними причинами:

1. Для забезпечення інформаційної безпеки держави;
2. Для протидії тероризму та організованій злочинності;
3. Для захисту моральності;
4. Для захисту авторських прав.

Доступ до інформації за допомогою Інтернет обмежується за допомогою організаційних, технічних заходів або комплексу організаційно-технічних заходів.

Організаційні заходи зазвичай використовуються в наступних випадках:

1. При необхідності введення розмежування доступу в установах (наприклад, в навчальних закладах, на підприємствах).

2. При необхідності введення обмежень за віком (блокування доступу до сайтів для дорослих).

3. Для недопущення публікації на ресурсах, доступ до яких відкритий через мережу Інтернет, інформації, що порушує авторські права або ганьбить честь і гідність людей, інших подібних відомостей (здійснюється особами, які відповідають за контент, розміщений на даному ресурсі).

Організаційні заходи передбачають використання відповідних можливостей застосовуваного програмного забезпечення (парольний захист, установка дозволів для доступу до ресурсів та інші заходи).

Технічні (апаратно-програмні) заходи зазвичай використовуються для автоматичного блокування доступу до певних ресурсів для певних категорій користувачів (використання брандмауерів, т. зв. нейтральних зон (DMZ) і та інших заходів).

Технічні заходи обмеження доступу до інформації зазвичай використовуються для захисту інформації всередині підприємств та організацій, іноді і в глобальному масштабі (хмарні технології). Рішення щодо їх впровадження приймаються керівництвом конкретного підприємства та відділом інформаційної безпеки підприємства. Технічні заходи можуть використовувати і прості громадяни (фізичні особи) для захисту своїх домашніх мереж від несанкціонованого доступу ззовні (апаратні маршрутизатори (роутери), точки доступу та ін.).

Організаційно-технічні заходи обмеження доступу до інформації використовуються в масштабах держави і підкріплені відповідною законодавчою базою. При цьому масштаб вирішуваних завдань вимагає застосування спеціальних технічних засобів, які постачальникам послуг доступу до мережі Інтернет (суб'єктам господарювання, що надають телекомунікаційні послуги) необхідно буде придбати додатково.

Так, до Верховної Ради України було внесено проект Закону України № 6688 від 12.07.2017 р «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері» [1]. Цей законопроект викликав неоднозначну реакцію в суспільстві, як в середовищі юристів і політиків, так і в середовищі фахівців у сфері інформаційних технологій.

В першу чергу увагу критиків законопроекту було звернуто на передбачене в частині третій проекту статті 213-1 положення про надання СБУ і прокуратурі права позасудового блокування сайтів на термін до 48 годин: «У виняткових невідкладних випадках, пов'язаних із врятуванням життя людей та запобіганням вчиненню тяжкого або особливо тяжкого злочину, тимчасове блокування (обмеження) доступу до визначеного (ідентифікованого) інформаційного ресурсу (сервісу) може бути розпочате до постановлення ухвали слідчого судді, суду за постановою прокурора або постановою слідчого, погодженою прокурором, і застосовується на строк не більше 48 годин».

Якщо подібне блокування буде використане для запобігання хакерських атак на інформаційну структуру держави або підприємства (наприклад, часто застосовуваних зловмисниками DDoS-атак), то подібна міра виявиться повністю неефективною, так як при подібних атаках хакери одночасно використовують до кількох мільйонів скомпрометованих ними комп'ютерних пристроїв (хостів). При цьому більшість таких пристроїв в принципі не має доменного імені, а спроба їх блокування по IP- адресах призведе

до блокування сотень тисяч комп'ютерів, які не беруть участі в атаці (в тому числі, можливо, і комп'ютерів, що входять в інформаційну систему держави).

Так, при скандальній спробі блокування Роскомнаглядом месенджера Telegram, останній перейшов до використання ресурсів найбільших хмарних сервісів Amazon Web Services, Google Cloud і Microsoft Azure, що призвело до автоматичного блокування і IP-адрес даних сервісів. Тим самим під блокуванням виявилися й всі інші користувачі даних сервісів [2].

Критики законопроекту зазначають, що в ньому дана принципова можливість блокування ресурсів мережі Інтернет без рішення суду, що чудово підходить для цензури і навіть корупційних дій [3].

Для організації ефективного блокування доступу до мережевих ресурсів необхідно використовувати апаратно-програмні комплекси, спеціально розроблені для цієї мети.

Вони повинні виконувати наступні функції:

1. Блокувати доступ за IP-адресою, доменному імені або конкретному URL (блокування окремої сторінки на сайті);

2. Мати можливість оперативного (ручного) додавання IP-адрес та доменних імен сайтів в список блокування, із зазначенням причин блокування (посиланнями на рішення судів та ін.);

3. Мати можливість використання автоматичного поповнення списку знову виявлених небезпечних сайтів (використовувати т. зв. «чорні списки»). Подібні списки повинні бути розміщені в єдиному державному реєстрі (необхідність створення такого реєстру − «Єдиного реєстру виконання судових рішень і застосування санкцій у сфері телекомунікацій» передбачена в цьому законопроекті).

Для безпосереднього здійснення функції блокування необхідно використовувати спеціальні апаратно-програмні комплекси. Такі пристрої зазвичай включаються в розрив між маршрутизатором, безпосередньо підключеним до мережі Інтернет, і вхідним маршрутизатором користувача або підприємства. Ці пристрої повинні бути встановлені у кожного суб'єкта господарювання, який надає телекомунікаційні послуги (провайдера Інтернет). При цьому, за попередніми оцінками, кожному провайдеру потрібно буде придбати спеціального обладнання на приблизно $1,2-1,5 млн. [4].

Подібні пристрої повинні мати можливість використання технології Deep Packet Inspection (DPI). Ця технологія, на відміну від технології, що використовується в брандмауерах, дозволяє здійснювати перевірку вмісту мережевих пакетів і по виявленому вмісту здійснювати фільтрацію (пропуск або блокування) інформації.

У таких пристроях передбачені механізми виявлення URL, прихованих в запитах HTTP (у тих випадках, коли використовуються програмні засоби обходу блокування). Крім іншого, подібні пристрої здатні збирати і накопичувати дані про сайти, що відвідуються кожним абонентом, підключеним до такої системи.

Подібні можливості можуть привести не тільки до блокування небажаних сайтів, а й до повного контролю дій користувачів мережі Інтернет в масштабах цілої держави.

У зв'язку з цим цікава позиція, яку займають окремі держави в питанні допущення або недопущення можливості блокування доступу до інформації в Інтернет.

Так, в авторитарних державах подібним системам приділяється підвищена увага, і цей процес, одного разу почавшись, не має ніяких тенденцій до зупинки. Навпаки, список ресурсів, що потрапляють під блокування, зростає не тільки кількісно, але якісно (постійно додаються нові категорії інформації, які підлягають забороні) [5].

Протилежний підхід демонструють демократичні країни. Так, в США 14 липня 2016 року Федеральний апеляційний суд заборонив провайдерам, які забезпечують фізичний доступ до мережі, блокувати сайти або застосовувати дискримінаційні заходи проти будь-якого інтернет-трафіку. Цей принцип заборони блокування отримав найменування «принцип мережевого нейтралітету».

***Список використаної літератури:***


1. Проект Закону про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері [Електронний ресурс]. − URL: https://bit.ly/2JGBqjE. − Дата звернення: 09.09.2018 р.
2. Роскомнадзор снимает блокаду. Пострадавшие могут подавать в суд [Електронний ресурс]. − URL: https://habr.com/post/356288/. − Дата звернення: 09.09.2018 р.
3. Законопроект № 6688 и что в нём плохого [Електронний ресурс]. − URL: https://bit.ly/2NzASkm. − Дата звернення: 09.09.2018 р.
4. ВРУ может обязать провайдеров иметь дополнительное оборудование для отключения запрещенных сайтов [Електронний ресурс]. − URL: https://bit.ly/2wXM40W. − Дата звернення: 09.09.2018 р.
5. Роскомнадзор наделил себя правом самостоятельно блокировать любые ресурсы в Сети [Електронний ресурс]. − URL: https://bit.ly/2CDlX4y. − Дата звернення: 09.09.2018 р.