Задерейко Олександр Владиславович

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

КОНЦЕПТУАЛЬНІ ОСНОВИ ЗАХИСТУ ЦИФРОВОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ

Будь-який громадянин, що володіє достовірною інформацією, має велику перевагу з точки зору ухвалення правильних рішень, що часто суперечать політиці, яка проводиться владними елітами держави. Цей факт є ключовим і визначає зовнішню та внутрішню політику провідних держав світу в області регулювання інформаційних потоків, циркулюючих в усіх сферах життя контролюємого суспільства.

Саме ця обставина робить офіційний контроль за регулюванням потоків інформації важливим пріоритетом для будь-якої держави, яка хоче зберегти свій інформаційний суверенітет та проводити незалежну політику [1]. Цей безперечний факт диктує необхідність детального розгляду тенденцій регулювання в інформаційній сфері держав з розвиненою мережевою інфраструктурою.

У сфері регулювання інформаційних потоків в мережі Інтернет існують такі способи:

- чинення впливу на джерела розміщуваного контенту (інформаційні компанії, блогерів, власників інформаційних ресурсів);
- здійснення вибіркової фільтрації контенту інтернет-ресурсів або блокування доступу до них;
- контроль трафіку користувачів та його наступна фільтрація, згідно з встановленими законодавчими нормами забезпечення інформаційного суверенітету держави.

Існують узагальнені принципи регулювання інформаційних потоків у національних сегментах Інтернет-середовища, які мають бути реалізовані в провідних країнах Євразійського і Латиноамериканського континентів.

Інформаційний «щит» держави

Інформаційний щит держави повинен складатися з наступних складових:

- система законодавчого обмеження на поширення інформації в Інтернет-просторі держави;
- система моніторингу Інтернет-простору держави;
- система фільтрації Інтернет-простору держави;
- планомірне створення кібервійск держави.

Засоби контролю «інформаційного щита»

Засоби контролю інформаційного щита держави повинні утворюватися з наступних складових:

- моніторинг інформаційного простору держави;
- законодавство про відповідальність за контент різних категорій операторів (хостер, провайдер доступу, медійний провайдер, ЗМІ);
- законодавство про фільтрацію інтернет-трафіку та його публічне правозастосування;
- державний фільтр на усіх рівнях (школи, університети, магістралі).

Засоби впливу «інформаційного щита»

Засоби впливу інформаційного щита держави повинні складатися з наступних складових:

- ринок ідеологічних послуг і технологій, робота над власною державною ідеологією;
- використання кіберпростіру як середовища та інструменту для поширення певної політичної культури;
- система впливу та ведення інформаційних воєн (кадри і інструменти);
- своя інформаційна інфраструктура (пошукові системи, контентні проекти, блоги, соцмережі).

Впровадження СОРЗ

Для захисту цифрової інфраструктури держави необхідно здійснювати постійний контроль метаданих, що циркулюють у каналах передачі даних. Найбільш відповідним рішенням, що дозволяє вирішити це завдання, є система СОРЗ, яка може ставити користувачів на контроль по імені облікового запису, номеру телефону, адресі електронної пошти, IP-адресі, номеру ICQ та забезпечує виявлення і перехоплення: поштових повідомлень за адресою електронної пошти, файлів, що передаються по протоколу FTP, IP – телефонії та тому подібне (див. рис. 1) [2].

Контроль зашифрованих метаданих

Будь-який користувач мережі Інтернет є генератором трафіку, в якому неухильно росте доля криптозахищених потоків інформації. Це обумовлює додаткову складність роботи СОРЗ. При перехопленні інформації, зашифрованої тим або іншим способом, практично неможливо розшифрувати її без використання ключів та спеціалізованих дешифраторів. Ця обставина спонукає спецслужби та правоохоронні органи будь-якої держави завжди обмежувати «чужу» криптографію та стимулювати впровадження «власної» такими шляхами:

- розробкою власних систем кріптозахисту інформації;
- використанням власних систем криптографії на території держави;

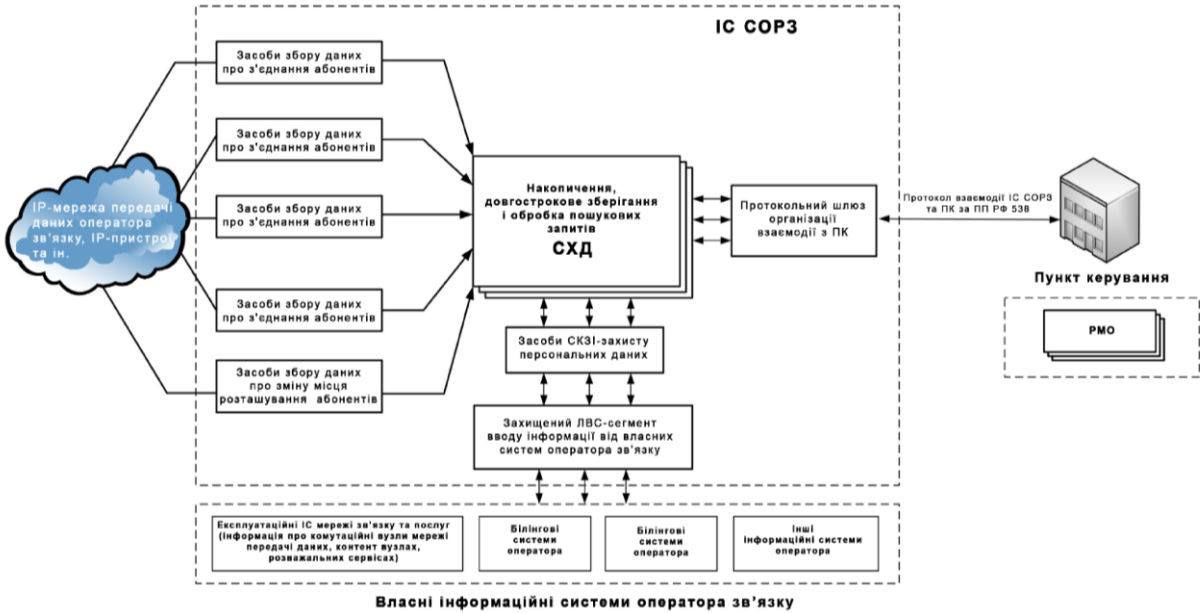

Рис. 1. Інформаційна система СОРЗ. Структурна схема

Неухильне зростання долі шифрованого трафіку (більше 50%) в Інтернет-просторі робить його фактично недосяжним для аналізу спецслужбами. Тому їм залишається тільки в законодавчому порядку примушувати усіх виробників криптографічного устаткування та криптографічного ПЗ депонувати ключі шифрування (ділитися сертифікатами відкритих ключів) для «законодавчього» вклинення в потік даних [3].

Депонування криптографічних ключів

У спрощеному виді державний стандарт шифрування даних з депонуванням ключа реалізується за допомогою криптографічного протоколу:

1) розробник генерує пару ключів, що складається з відкритого та закритого ключів;

2) розробник передає закритий ключ та відповідну йому частину відкритого ключа уповноваженій державою структурі;

3) уповноважена структура перевіряє отримані частини відкритого та закритого ключів та приймає їх на зберігання;

4) якщо виникає необхідність ознайомитися із зашифрованим контентом користувача або уклинитися в його зашифрований трафік, уповноважена структура використовує отриману пару ключів.

Багато держав замість депонування ключів впровадили спосіб законного отримання ключів шифрування від самих користувачів по запиту правоохоронних органів. У разі відмови їм загрожує карна відповідальність і/або штраф за ненадання допомоги в розслідуванні злочинів [4].

Таким чином, багато країн, не маючи можливості зобов'язати депонувати ключі і не маючи власних розробників засобів шифрування, які могли б вбудовувати системи відновлення ключів або програмні закладки, вимагають від громадян надавати ключі шифрування по мотивованих запитах з боку держави.

Вище викладене показує, що більшість провідних держав, реалізують заходи щодо захисту власного інформаційного суверенітету. Практична реалізація цих заходів стає одним з найважливіших елементів забезпечення національної безпеки держави яка грунтується на захисті цифрового суверенітету.

Список використаної літератури:

1. Проблемные аспекты защиты информационного суверенитета государства и перспективы его защиты в Украине / Задерейко А.В., Троянский А.В., Чечельницкий В.Я. // Юридичний науковий електронний журнал. – 2017. – № 2. – С. 10–13.
2. СОРМ-3: формальное закрепление реализованного. URL: http://www.securitylab.ru/analytics/446852.php. (Дата звернення 14.09.2018).

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).