АКТУАЛЬНІ ПИТАННЯ ВПРОВАДЖЕННЯ ПРОЦЕСУАЛЬНИХ МЕХАНІЗМІВ З ПРОТИДІЇ РОЗПОВСЮДЖЕННЮ ІНФОРМАЦІЇ З ПРОТИПРАВНИМ ЗМІСТОМ В МЕРЕЖІ ІНТЕРНЕТ

Демедюк С.В., начальник Департаменту кіберполіції Національної поліції України, кандидат юридичних наук.

Протидія кіберзлочинам наразі є вкрай актуальним питанням. В сучасних умовах зросла активність атак на комп`ютерні системи об'єктів критичної інфраструктури, розповсюдження контенту з протиправним змістом, пов`язаного з порушенням авторських і суміжних прав, розповсюдження дитячої порнографії, незаконий обіг зброї та наркотичних засобівв мережі Інтернет.

Під час досудового розслідування кримінальних правопорушень, виникають непоодинокі випадки, які вимагають від органів досудового розслідування вжиття невідкладних заходів із обмеження (блокування) визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) на якому розміщено інформацію, що містить ознаки діяння, передбаченого законом України про кримінальну відповідальність.

У вітчизняному законодавстві цьому питанню увага не приділялося взагалі, тоді як його актуальність давно назріла.

У той же час, в багатьох країнах Європи усвідомили наскільки важливим є захист суспільства від інформації з незаконним змістом, що розповсюджується мережею Інтернет. Блокування ресурсів з протиправним контентом запроваджено в Великобританії, Франції, Канаді, Німеччині.

Наприклад, у Франції фільтрація трафіку внутрі країни та закордоного контенту по законодавству перебуває під юрисдикцією правоохоронних та судових органів. Створено так названі «чорні списки» ресурсів з протиправним контентом. Таким чином, країни з

давніми демократичними традиціями не цураються таких заходів, а навпаки широко їх використовують для захисту своїх громадян.

Розв`язання цієї проблеми вбачається у необхідності на законодавчому рівні передбачити можливістьобмеження (блокування) визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) з протиправним контентом. До речі, відповідні положення знайшли своє відображення також в Стратегії кібербезпеки України, що затверджена Указом Президента від 15.03.2016 № 96/2016 (далі – Стратегія). Наразі одне із першочергових завдань з реалізації положень Стратегії - це приведення у відповідність до її норм вітчизняного законодавства.

Відповідно до Стратегії серед пріоритетів та напрямів забезпечення кібербезпеки України визначено ряд завдань, серед іншого, запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду[1].

При вирішенні цього питання необхідно дотримуватися балансу між потребами забезпечення правопорядку і захисту прав та інтересів громадян та постачальників телекомунікаційних послуг. Такий захід повинен детально регулюватися, щоб мати змогу вживати ефективних заходів у протидії розповсюдженню протиправного контенту.

Саме тому, обмеження (блокування) визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) пропонується приймати на підставі рішення слідчого судді у рамках кримінального провадженняз метою попередження та припинення кримінального правопорушення, з дотриманням процедури, у тому числі вивчення підстав, які послугували для прийняття такого рішення.

Вбачається доцільним визначити обмеження (блокування) визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) як різновид заходів забезпечення кримінального провадження, виключно за рішенням слідчого судді.

Разом з тим, у невідкладних випадках, пов’язаних із врятуванням життя людей та запобіганням вчиненню тяжкого або

особливо тяжкого злочину тимчасове обмеження (блокування) доступу до визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу), адреси мережі Інтернет, домену, може бути розпочато до постановлення ухвали слідчого судді, суду за постановою прокурора або постановою слідчого, погодженою прокурором, на конкретно визначений строк.У такому випадку, прокурор, слідчий за погодженням із прокурором, зобов'язаний невідкладно після здійснення таких дій, звернутися з відповідним клопотанням до слідчого судді.

Дії постачальників телекомунікаційних послуг щодо обмеження (блокування) доступу до визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу), адреси мережі Інтернет, домену, негайно припиняються, якщо слідчий суддя, суд постановить ухвалу про відмову в наданні дозволу на проведення цих дій або після закінчення строку, на який було обмежено (блоковано) доступ до інформаційного ресурсу (інформаційного сервісу), адреси мережі Інтернет, домену.

Одночасно, необхідно передбачити процесуальні важелі для унеможливлення зловживань під час застосування названого заходу забезпечення кримінального провадження. Тому, доцільним є визначення процедури оскарження рішення щодо обмеження (блокування) доступу до визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу).

Торкаючись тематики злочинів, які вчиняються в мережі Інтернет не можливо оминути особливості здійснення тимчасового доступу до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку. З метою забезпечення ефективного проведення такої слідчої дії, яка є вкрай специфічною та потребує особливих знань доцільним є залучення до її проведення спеціаліста та/або представника уповноваженого (спеціалізованого) оперативного підрозділу Національної поліції чи Служби безпеки України, який діє з дотриманням вимог статті 41 КПК України [2]. Одночасно необхідно передбачити те, що копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем

зв'язку, без їх вилучення з використанням програмно-апаратних комплексів, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації.

Фактичні дані, отримані шляхом копіювання з використанням зазначених комплексів слід вважати допустимим доказом у кримінальному провадженні.

У разі неможливості здійснення копіювання інформації з технічних причин, у тому числі зашифрованої, вилучення інформаційних систем або їх частин, мобільних терміналів систем зв'язку проводиться у межах граничного строку, передбаченого цим Кодексом, та має бути таким, що дає достатньо часу для дешифровки та/або огляду інформації, після чого вони повинні бути якнайшвидше повернуті володільцю, окрім випадків, визначених у частині І статті 100 КПК України.

Тимчасовий доступ до речей і документів здійснюється на підставі ухвали слідчого судді, суду.

Разом з тим, необхідно передбачити можливість у невідкладних випадках, пов'язаних із врятуванням життя людей та запобіганням тяжкого або особливо тяжкого злочину тимчасовий доступ до інформації, що міститься в електронних інформаційних системах або їх частинах, мобільних терміналів систем зв'язку, може бути розпочато до постановлення ухвали слідчого судді, суду за постановою прокурора або постановою слідчого, погодженою прокурором. У такому випадку прокурор, слідчий за погодженням із прокурором, зобов'язаний невідкладно після здійснення таких дій звернутися з відповідним клопотанням до слідчого судді.

На наш погляд запровадження таких новел у вітчизняне кримінальне процесуальне законодавство, буде сприяти ефективному досудовому розслідуваню кримінальних правопорушень, що вчиняються в мережі Інтернет.Одночасно ці правові норми слугуватимуть розвитку регуляторної нормативно-правової бази для впровадження процесуальних повноважень ізврахуванням публічних і

приватних інтересів.

Список використаних джерел

1.Прорішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.2016 № 96/2016[Електронний ресурс].– Режим доступу:http://www.president.gov.ua/documents/.

2. Кримінальний процесуальний кодекс України [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua.