Далее обозначим наиболее распространенные источники киберугроз современного предприятия:

- электронная почта (письма, во вложениях которых исполняемые файлы вирусного программного обеспечения);
- получение исполняемых и замаскированных под данные различного типа файлов, содержащих вредоносный код с ресурсов глобальной сети;
- запуск вирусного программного обеспечения непосредственно с внешних накопителей данных (flash-накопители, внешние HDD, смартфоны и т.п.);
- направленное внешнее подключение злоумышленников и запуск вирусного программного обеспечения непосредственно в системе.
- попадание вирусного ПО в систему через специализированные каналы связи с внешними предприятиями (судоходные линии, стивидорные компании и т.п.)

Проанализировав основные источники и виды угроз заражения информационно-компьютерных систем вредоносным программным обеспечением, целесообразны следующие методы обеспечения кибербезопасности:

1. Обучение персонала (общие понятия компьютерной безопасности: права доступа,макрос, автозапуск, исполняемый файл, и. т.п.). В 99 процентахслучаев заражений, источником является пользователь, который запустил на исполнение вирусное ПО).
2. Антивирусное программное обеспечение (поддержание антивирусных баз в актуальном состоянии, а также защита от автозапуска с внешних носителей).
3. Использование ранжирования доступа пользователей к внутренним ресурсам предприятия (позволяет локализовать очаг заражения в пределах доступа данного пользователя к данным) и внедрение двухфакторной авторизации.
4. Ограничение доступа пользователей к внешним ресурсам в сети интернет (позволяет предотвратить угрозы, связанные с закачкой вирусного ПО с небезопасных ресурсов).
5. Административный запрет на использование неучтенных внешних накопителей информации.
6. Обмен данными с внешними организациями в строго обговоренном формате (позволяет предотвратить попадание вредоносного ПО через специализированные программные продукты).
7. Резервное копирование данных (многоуровневое бекапирование позволяет восстановить данные с минимальными потерями с момента среза резервной копии).
8. Мониторинг нагрузок оборудования системы (позволяет определить угрозы, направленные на серверное и сетевое оборудование).
9. Наличие формализованных протоколов действий пользователей и администраторов ресурсов при возникновении угроз и различных внештатных ситуаций.

Выводы и предложения. Проведен анализ угроз и защищённости портовых компьютерных систем от различного вида заражения вирусным ПО. Отмечается значительная зависимость уровня безопасности информационно-компьютерных систем от квалификации пользователей. Для обеспечения максимальной защищённости портовых и других предприятий морской отрасли систем от различных видов киберугроз рекомендуется одновременное комбинационное использование всех методов защиты.

Литература

1. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.
2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: Форум, 2010. – 594 с.

Ісмайлов К.Ю., к.ю.н.,
Сіфоров О.І., к.т.н., доцент,
Одеський державний університет внутрішніх справ

ПРАВОВИЙ МЕХАНІЗМ БЛОКУВАННЯ ІНТЕРНЕТ-РЕСУРСУ В УКРАЇНІ

Сучасний період розвитку суспільства характеризується сильним впливом на нього комп'ютерних технологій, які проникають в усі сфери людської діяльності, забезпечують поширення інформаційних потоків в суспільстві, утворюючи глобальний інформаційний простір.

Разом з стрімкою інформатизацією суспільства цей процес супроводжується ростом кількості прямих та прихованих незаконних дій правопорушників у кіберпросторі. Наприклад, як то втручання в виборчий процес (США, Франції, Німеччині), розповсюдження комп'ютерних вірусів (Wanna Cry, MiniDuke, BlackEnergy та інших) або комп'ютерного шахрайства (вішинг,смішинг, скіминг,траппінг,фантом,шаттер,шиммінг,трешинг, фішинг).

Відповідно ст. 17 Конституції України інформаційна безпека є найважливішою функцією держави нарівні з захистом суверенітету і територіальної цілісності та забезпеченням економічної безпеки країни [1].

Тому, виходячи із загроз виконавчі органи Україна повинні мати належний організаційно-правовий механізм обмеження поширення незаконної інформації на теренах всесвітньої мережі Інтернет, а законодавчий орган відповідно створити належну правову базу для цього.

Для більш комплексного розкриття правового механізму блокіровки Інтернет-ресурсу розглянемо, який саме контент на сьогодні заборонений в Україні.

Отже, згідно ст. 28 закону України «Про інформацію». *Інформація не може бути використана для:*

- повалення конституційного ладу;
- пропаганди війни, насильства, жорстокості;
- розпалювання міжетнічної, расової, релігійної ворожнечі;
- вчинення терористичних актів;
- посягання на права і свободи людини [2].

Відповідно до ст. 6 закону України «Про телебачення і радіомовлення». *Не допускається використання телерадіоорганізацій для:*

- поширення відомостей, що становлять державну таємницю;
- закликів до насильницької зміни конституційного ладу України;
- трансляції програм або їх відеосюжетів, які можуть завдати шкоди фізичному, психічному чи моральному розвитку дітей та підлітків;
- трансляції телепередач що містять популяризацію або пропаганду органів держави-агресора;
- трансляції аудіовізуальних творів (фільмів, телепередач), одним із учасників яких є особа, внесена до Переліку осіб, які створюють загрозу національній безпеці;
- розповсюдження і реклами порнографічних матеріалів та предметів;
- пропаганди наркотичних засобів, з метою їх застосування [3].

Ст. 3 закону України «Про друковані засоби масової інформації (пресу) в Україні». *Забороняє використання друкованих засобів масової інформації для:*

- закликів до захоплення влади або територіальної цілісності України;
- розпалювання расової, національної, релігійної ворожнечі;
- пропаганди війни, насильства та жорстокості;
- розповсюдження порнографії;
- втручання в особисте і сімейне життя особи;
- пропаганди війни, насильства та жорстокості [4].

Ст. 2 закону України «Про захист суспільної моралі». Забороняє виробництво та обіг у будь-якій формі продукції еротичного характеру та продукції, що містить елементи насильства та жорстокості, дозволяються виключно за умови дотримання обмежень, встановлених законодавством. *Забороняються виробництво та розповсюдження продукції, яка:*

- принижує або ображає націю чи особистість за національною ознакою;
- пропагує війну, національну та релігійну ворожнечу;
- пропагує фашизм та неофашизм;
- пропагує бузувірство, блюзнірство, неповагу до національних і релігійних святинь;
- пропагує невігластво, неповагу до батьків;
- пропагує наркоманію, токсикоманію, алкоголізм, тютюнопаління та інші шкідливі звички [5].

Ст. 2 закону України «Про інформаційні агентства». Забороняється цензура інформації, поширюваної інформаційними агентствами. Інформаційні агентства не мають права у своїх матеріалах розголошувати дані, що становлять державну таємницю, або іншу інформацію з обмеженим доступом. Інформаційні агентства не мають права у своїх матеріалах пропагувати комуністичний або націонал-соціалістичний тоталітарні режими та їхню символіку [6].

Ст. 17 закону України «Про боротьбу з тероризмом». *Забороняється поширення через засоби масової інформації або в інший спосіб інформації, яка:*

- розкриває спеціальні технічні прийоми і тактику проведення антитерористичної операції;
- може утруднити проведення антитерористичної операції і створити загрозу життю та здоров'ю заручників та інших людей які знаходяться в районі проведення зазначеної операції;
- має на меті пропаганду або виправдання тероризму;
- містить дані про предмети та речовини, можуть бути використані для вчинення актів технологічного тероризму;
- розкриває дані про склад співробітників підрозділів оперативного штабу, які беруть участь у проведенні антитерористичної операції [7].

Ст. 50 закону України «Про авторське право і суміжні права». *Порушенням авторського права і суміжних прав, що дає підстави для захисту таких прав, у тому числі судового, є:*

- вчинення будь-якою особою дій, які порушують особисті немайнові права суб'єктів авторського права і (або) суміжних прав;
- піратство - опублікування, відтворення, ввезення, вивезення з території України і розповсюдження контрафактних примірників творів (комп'ютерних програм, фонограм, відеограм) тобто вчинення дій, які визнаються порушенням авторського права;
- плагіат - оприлюднення повністю або частково, чужого твору під іменем особи, яка не є автором цього твору;
- ввезення на територію України без дозволу осіб примірники творів (комп'ютерні програми, фонограми, програм мовлення);
- підроблення, зміна чи вилучення інформації, зокрема в електронній формі;
- вчинення дій, що створюють загрозу порушення авторського права і (або) суміжних прав [8].

У зв'язку з тим, що метою написання статті не є аналіз міжнародного правого досвіду з моніторингу та блокіровки незаконного контенту, але так як на українські правовідносини з міжнародними інституціями впливає міжнародна практика, приведемо лише категорії забороненого контенту в інших державах:

- *соціально-небезпечна інформація*: порнографія, методи самогубств, статевий просвітництво, ЛГБТ-тематика, алкоголь, наркотики, онлайн-казино і букмекерські контори, образа релігії;
- *економічна безпека*: недотримання авторських прав, файлообмінні сайти, торент-трекери, сервіси передачі голосу в Інтернеті (Skype, Viber та інші);
- *загроза національній безпеці*: тероризм, екстремізм, сепаратизм, відкриття секретних даних, шкідливе програмне забезпечення
- *політичний контент*: опозиційний рух, критика влади
- *спеціальні інструменти та соціальні сервіси*: анонімайзери, проксі-сервера, хакерські сайти, пошукові системи, соціальні мережі, майданчики для блогів, хостинги відео і зображень.

При виявленні вищевказаного контенту необхідно притягувати винних до кримінальної або адміністративної відповідальності. Це питання набуває сьогодні неабияку актуальність особливо після підписання Президентом України Указу № 133/2017 від 15.05.2017 «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», який покликаний захистити інформаційний простір країни і зменшити можливості кібератак на бізнес [9]. Саме для цього необхідний чіткий правовий механізм дій уповноважених на це осіб (рис. 1).

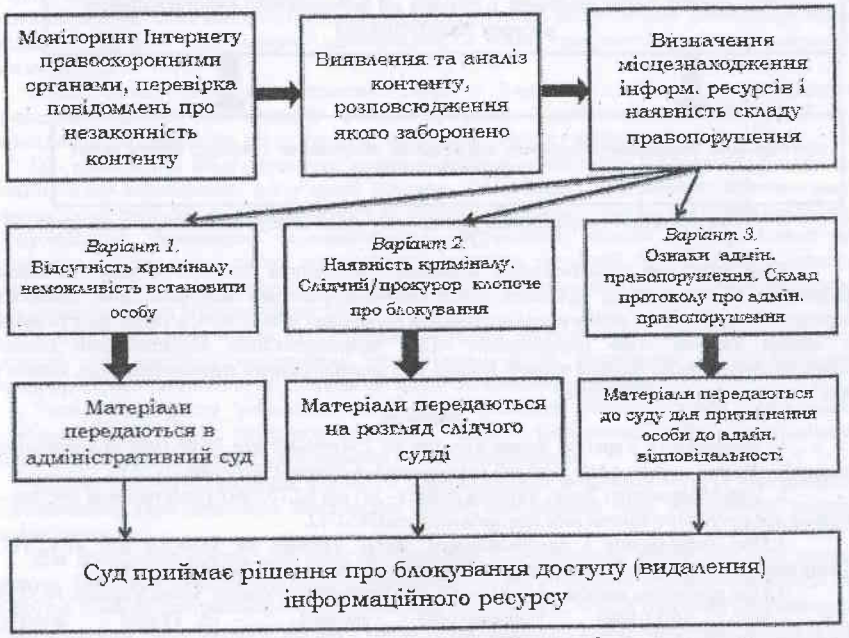

Рис. 1. Механізм блокування забороненого Інтернет-ресурсу

Після того як Суд прийме рішення про блокування доступу або видалення інформаційного ресурсу для його виконання необхідно виконати рішення суду щодо блокування Інтернет-ресурсу (рис. 2).

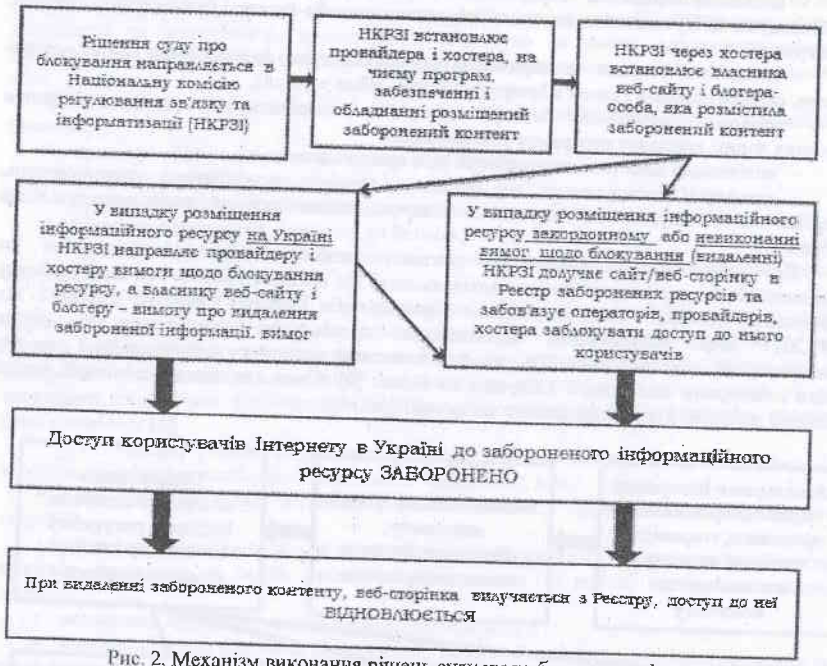

Рис. 2. Механізм виконання рішень суду щодо блокування Інтернет-ресурсу

Крім того, для удосконалення механізму блокування Інтернет-ресурсу необхідно розробити та законодавчо прийняти понятійно-категоріальний інструментарій, обов'язки юридичних та фізичних осіб у сфері поширення інформації в Інтернеті, а також внести зміни в закони України «Про інформацію», «Про телекомунікації», Кримінальний кодекс, Кримінальний процесуальний кодекс, Кодекс про адміністративні правопорушення, Кодексу адміністративного судочинства.

Джерела

1. Конституція України: Закон України № 254к/96-ВР від 28.06.1996 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/254к/96-вр

2. Про інформацію: Закон України №2658- XII від 02.10.1992 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12.

3. Про телебачення і радіомовлення: Закон України № 3759-XII від 21.12.1993 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3759-12.

4. Про друковані засоби масової інформації (пресу) в Україні: Закон України №3759-XII від 16.11.1992 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2782-12.

5. Про захист суспільної моралі: Закон України № 1296-IV від 20.11.2003 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1296-15.

6. Про інформаційні агентства: Закон України № 74/95-XII від 28.02.1995 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/74/95-вр.

7. Про боротьбу з тероризмом: Закон України № 638-IV від 20.03.2003 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/638-15.

8. Про авторське право і суміжні права: Закон України № 3792-XII від 23.12.1993 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3792-12.

9. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України № 133/2017 від 15.05.2017 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/1332017-21850.

Кінзерявий В.М., к.т.н., доцент,
Степаненко І.В., студентка,
Лозінський І.Л., студент,
Національний авіаційний університет, Київ

ОБФУСКАЦІЙНИЙ МЕХАНІЗМ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Дослідження надійності та захищеності комп'ютерних систем проводиться за рахунок аналізу безпеки використовуваного у них програмного забезпечення. Однією з основних проблем забезпечення надійності таких систем є відсутність розробленого та впровадженого механізму захисту програмного забезпечення, а саме програмного коду від реверс-інжинірингу.

Даний аспект безпеки є порівняно новим в Україні і пов'язаний з можливістю проведення аналізу виконуючих файлів програми, відновлення алгоритму роботи, знаходження незахищених місць у коді та проведення процесу модифікацію.

Був проведений аналіз сучасних наукових робіт у даній галузі. Відповідно до даного аналізу було встановлено, що у праці Каплуна В.А. «Захист програмного забезпечення» велику увагу звернено на основні вимоги до процесу обфускації, описані категорій розподілу обфускаційних перетворень та представлені обфускаційні методи захисту. Однак не зважаючи на те, що у роботі представлені приклади реалізації обфускаційних заходів захисту, відсутній комплексний механізм захисту програмного коду з використанням більшості описаних обфускаційних перетворень.

У роботі іноземних вчених також наведені загальні поняття та принципи роботи окремих методів обфускаційних перетворень, представлені схеми проведення деобфускаційних процесів. Проте також відсутній загальний механізм забезпечення захисту.

Таким чином, для зменшення ймовірності реалізації загроз безпеки *актуальним завданням* є розробка надійного механізму захисту виконавчих файлів програмного забезпечення від процесів декомпілювання та деассемблювання.

Метою роботи є створення надійного обфускаційного механізму захисту програмного забезпечення, який дозволить забезпечити захист програмного коду від процесу реверс-інжинірингу.

Для досягнення поставленої мети використаний обфускаційний метод StiK. Для даного методу проведені експериментальні дослідження, щодо швидкості процесу обфускації та відсотка відмінності трансформованого коду від початкового. Хоча у результаті дослідження була показана ефективність методу, проте було виявлено певні недоліки, які можуть негативно впливати на забезпечення надійності та цілісності вихідного коду програмного забезпечення.

У результаті цього запропоновано удосконалення розглянутого методу StiK. До обфускаційного процесу в використанням методу StiK висувалися наступні вимоги:

1. Трансформований код програми повинен суттєво відрізнятися від його початкового коду, проте залишатися дієздатним і виконуватиме ті самі функції.
2. Алгоритм роботи початкового коду та трансформованого коду повинен буди різним.