прийняттям Кримінального процесуального кодексу України" " 4652-V1 від 13.04.2012 р. - Х.: Право,2012. - 392 с.

8. Кримінатьно-процесуальний кодекс України: за станом на 1 травня 2012 р. - К.: CD-вид-во "Інфодиск", 2012 - 1 електрон, опт. диск (CD-ROM): кольор.; 12 см - Систем, вимоги: Pentium-226; 32 Mb RAM; CD-ROM Windows 98/2000/NT/XP. - Назва з титул, екрану.

9. Петру хин И. Л. Экспертиза как средство доказывания в советском уголовном процессе / И. Л. Петрухин. - М., 1984. - 97 с.

10. Постанова Пленуму Верховного Суду України від ЗО травня 1997 р. № 8 "Про судову експертизу в кримінальних і цивільних справах". - К.: CD-вид-во "Інфодиск", 2012. - 1 електрон, опт. диск (CD-ROM): кольор.; 12 см - Систем, вимоги: Реппшп-226; 32 Mb RAM; CD-ROM Windows 98/2000/NT/XP. - Назва з титул, екрану.

11. Торбин Ю. Г. Уголовно-процессуальные и криминалисгичекие проблемы освидетельствования / Ю. Г. Торбин [Електроннийресурс]. - Режим доступу: www.k-press.ru/bh/2002/4/torbin/torbin.asp.

**Н.А. Савінова***

## КІБЕРНЕТИЧНА ІНТЕРВЕНЦІЯ, ЯК СУСПІЛЬНО-НЕБЕЗПЕЧНЕ ДІЯННЯ, ЩО ПОТРЕБУЄ КРИМІНАЛІЗАЦІЇ

***Стаття Н.А.Савінової присвячена проблемі загроз кібернетичної інтерве нції у інформаційному суспільстві та потребі кримінально-правової протидії її проявам.***

Ключові слова: ***кібернетична інтервенція, безпека у інформаційному суспільстві, безпека кібернетичного простору, посягання на інфраструктуру держави.***

***Статья Н.А.Савиновой "Кибернетическая интервенция, как общественно опасное деяние, нуждающееся в криминализации" посвящена проблеме угроз кибернетической интервенции в информационном обществе и потребности уголовно-правового противодействия ее проявлениям.***

Ключевые слова: ***кибернетическая интервенция, безопасность в информационном обществе, безопасность кибернетического пространства, посягательства на инфраструктуру государства.***

*** Кандидат юридичних наук, доцент кафедри кримінально-правових дисциплін ННІПП НАВС.**

*The article of N. Savinova" Cybernetic intervention, as a socially dangerous act that needs to criminalize" is devoted to cyberthreats to intervene in the information society and the needs of the criminal law countering its manifestations.*

Key words: *cyber intervention, security in the information society, cyberspace security, attacks on the infrastructure of the state.*

Значна низка суспільно-небезпечних діянь, спрямованих на заподіяння шкоди державним інтересам сьогодні може вчинюватися як у інформаційному просторі, так і у суто кіберпросторі. З розвитком інформаційного суспільства спрямування збільшилася кількість злочинних дій спрямованих на заподіяння шкоди віддаленим предметам і посягання на об'єкти, які раніше були фактично недосяжні для такої значної кількості осіб. Вчинення посягань на державні політичні та економічні інтереси шляхом втручання в функціонування їх учасників та інститутів у межах яких вони діють, містять ознаки інтервенції: насильницького втручання у інтереси держав та органів влади держав з боку інших суб'єктів. Оскільки вчинюються подібні дії з використанням комп'ютерних систем і вчинюються у кіберпросторі, вказаний вид інтервенції доцільно розуміти як ***"кібернетична інтервенція", характеризуючи її як окрему групу суспільно небезпечних діянь, спрямованих на завдання шкоди інформаційній інфраструктурі держав, життєво важливим сферам існування суспільства.***

Під інтервенцією, в загальному розумінні, звично сприймати насильницьке втручання одного чи декількох держав у внутрішні справи іншої держави з метою подавлення революції, захоплення території, встановлення свого панування, отримання особливих привілеїв та ін. [1, с. 278]. Особлива актуальність кримінальної інтервенції, яка вчинюється всупереч правилам ведення війни, була проаналізована і підкреслена А.Н.Трайніним, який характеризував її як втручанням у державні справи саме злочинністю [2, с. 414-417].

У глобальному відкритому суспільстві, яким є ІС, кібернетична інтервенція може мати не лише глобальні наслідки, як і безпосередньо полягати у діях, що характеризуватимуться глобальними ознаками: можливості спільної участі у інтервенції необмеженої кількості суб'єктів, які значно віддалені як один від одного щодо одного об'єкту, або щодо необмеженої кількості об'єктів одночасно. Аналогічно, можливе одночасне вчинення кіберзлочинів з метою інтервенції до великої кількості об'єктів, або одного над важливого, у т.ч. страте-

гічного об'єкту. З урахуванням можливостей робити це поза межами кордонів на будь якій відстані, підвищення суспільна небезпечність кібернетичної інтервенції стає безперечною. На жаль, існують прямі докази наявних фактів вчинення кібернетичної інтервенції, що дозволяють констатувати факт існування такої.

Таким чином під ***кібернетичною інтервенцією слід розуміти агресивні дії у інформаційному просторі, які містять ознаки втручання у сфери, що забезпечують життєдіяльність окремих держав та міждержавних об'єднань, а також у порядок функціонування основних життєзабезпечуючих структур таких держав та об'єднань та їх вищих органів влади та управління.***

Найпростішим прикладом кібернетичної інтервенції є 3-денна безперервна кібернетична атака на сайт Президента **України** В.А.Ющенко, яка розпочалася 30 жовтня 2007 р., і нараховувала близько 18000 точкових атак, які вчинювалися з території РФ, Казахстану, **України,** США, Ізраїлю і Великобританії. [3] Поте у служб безпеки такі дії не викликають особливе здивування, адже сайти президентів різних **країн** світу постійно відчувають на собі подібні хакерські атаки [4, 5].

Кібернетичні атаки на офіційні сайти вищих керівних органів держав не обмежуються прикладами стосовно атак на сайти президентів, наведеш вище [3. 4. 5]. Атакуються комп'ютерні системи всіх гілок влади по всьому світу: атаки здійснюються з метою перешкоджання діяльності прокуратури [7]; з метою фальсифікації списків виборців і фальсифікації підрахунку голосів на виборах [8. 9], посягаючи, відповідно, на функції державного обвинувачення, або на волевиявлення народу, яке є складовою суверенітету держави. Доречно навести оцінку ступеню суспільної небезпечності кібернетичної інтервенції Республікою Польща, президентом якої у червні 2011 р. було внесено пропозицію щодо військового стану у разі вчинення кібернетичних атак на інфраструктуру держави [10].

Проте, не лише втручання злочинності у діяльність органів державної влади є ознакою кримінальної інтервенції. Таке визначення, на погляд автора, на сьогодні не повною мірою відповідає сучасним вимогам в частинах суб'єкту і об'єкту посягання - втручання у внутрішні справи власної держави може здійснювати і громадянин цієї державі - у описаних прикладах це очевидно, а оскільки в умовах можливості дистанційного вчинення злочинів інтереси суспільства не

обмежуються державними кордонами[1], то поняття „внутрішні справи" з часом втрачатиме сенс, за виключенням питань, що охоплюються поняттям суверенітету.

Також, визначення А.Н.Трайніна не враховує можливості вчинення агресивних дій стосовно міждержавних об'єднань та їх керівних органів, оскільки у той час це, по-перше, не було актуальним, а, по-друге, вчинення інтервенції злочинності могло розглядатися виключно з урахуванням можливостей необхідності фізичної присутності агресора, у той час, як зараз, завдяки можливостям ІТ та ІКТ, фізична присутність не обов'язкова.

Короткий огляд найбільш відомих прикладів кібернетичних атак на інформаційну інфраструктуру держав, демонструють сучасний стан і можливості кібернетичної інтервенції.

Історія кібернетичної інтервенції бере початок з перших спроб дистанційованого втручання при посередництві ІКТ з 80-х років XX сторіччя. Фактично, на початку це відбувалося з незначним відставанням трансформації загальнокримінальної злочинності у кіберзлочинність - приблизно на 10 років, адже саме кіберзлочини слугували базою навичок та знань, необхідних для вчинення діянь, що належать до кібернетичної інтервенції.

У 80-х роках XX сторіччя найгучнішою спробою вчинити кібернетичну інтервенцію сталі злочинні дії так званої "банда 414", яка

[1] **В умовах глобального відкритого інформаційного суспільства, розуміння кібернетичої інтервенції потребує нового підходу, який враховуватиме особливості здійснення транскордонного злочинного втручання в умовах постійного розвитку** ІКТ. **А.С.Гальчинський зазначає: "/.../ми акцентуємо увагу на розвитку самовідтворювальних технологічних структур, де автоматизовані системи відтворюватимуться за рахунок автоматизованих систем" [11, с. 123]. Така думка наводить на роздуми, що у разі досягнення бажаної мети на створювання само відтворювальних структур, а також подальших розробок штучного інтелекту, ідея створення якого була озвучена у 50-х роках XX століття Н.Віннером [12, р. 17-22.1- у разі втрати контролю людини над такими над такими новаціями, людство повною мірою підпаде під загрозу повної залежності від технологій. Слід також враховувати факти дійсного використання певних часткових компонентів штучного інтелекту, що поки функціонують під контролем людини, наприклад у банківській та біржовій сферах, адже такі можуть потрапити і під управління злочинців, а загроза наслідків управління біржовими торгами злочинцями навіть потенційно здається жахливою, адже у системі геополітичних центрів біржі є центрами акумуляції коштів фінансових гігантів.**

протягом дев'яти днів встигла втрутитись у роботу шістдесяти комп'ютерів, у тому числі "зламати" системи доступу Лос-Аламоської лабораторії ядерних досліджень. Важким ударом для державних і освітянських структур США були наслідки запровадження у студентом Р.Морісом шкідливої комп'ютерної програма, яка вивела з ладу близько 6 000 урядових та університетських комп'ютерів у США наприкінці 80-х років [13].

У 1989 р. хакерською групою "Chaos Computer Club" з території ФРН були зламані урядові комп'ютери деяких федеральних органів США, а вилучена інформація продана агентам КДБ СРСР [13]. У 1995 р. підданий Бразилії Х.С.Ардіта був засуджений до трьох років тюремного ув'язнення за вчинену ним атаку на військової мережі США, внаслідок якої він заволодів паролями кількох реєстраційних записів військової мережі Navy та отримав доступ до секретних розробок в галузі супутникової, авіаційної та радарної технологій [14]. У 1998 р. ізраїльтянин Е.Тененбаум проник у комп'ютерні мережі Пентагона. У 1999 р. розроблений громадянином США Д.Смітом комп'ютерний вірус Mellissa зруйнував більше трьохсот комп'ютерних мереж [15], заподіявши багатомільйонну шкоду користувачам Internet по всьому світу. У 2001 р. А.Дікман проник у мережу JPL NASA, а також комп'ютерну мережу Стенфордського університету (США), отримавши доступ до комп'ютерів, які відповідали за розробку програмного забезпечення для супутників [16].

У 2001-2002 рр. англієць Г.Маккіннон несанкціоновано втрутився у роботу 72 комп'ютерних систем Міністерства оборони США і NASA та вивів такі системи з ладу, заподіявши шкоду на загальну суму більше мільйона доларів США. Серед атак, вчинених злочинцем на комп'ютерні системи державних органів США, виділяється атака, що її вчинив Г.Маккіннан одразу після подій 11 вересня 2001 р. у Нью-Йорку, порушивши комп'ютерні системи "Єрл" ВМФ США у Колдс-Неку, внаслідок чого отримав доступ до закритої інформації Атлантичного флоту США [17],

Ці приклади яскраво демонструють можливості втручання у внутрішні та зовнішні справи за використанням кібернетичних, навіть, індивідуальних атак. У глобальному суспільстві такі індивідуальні дії набувають іншого сенсу, адже вони можуть вчинюватися з будь-якої території у відношенні ресурсів, які перебувають на іншій території. У т.ч. транзитом через низку територій інших держав.

**Удосконалення взаємодії оперативних підрозділів органів внутрішніх справ України з відповідними підрозділами та установами Державної пенітенціарної служби України щодо виконання завдань ОРД**

Не можна не приділити окремої уваги можливості спрямування кібернетичної інтервенції у мілітаристичну сферу. Сучасна мілітаристична війна неможлива без використання ГКТ. М.Тетчер стосовно характеру зміни можливостей ведення сучасних мілітаристичних війн зазначає: „сьогоднішній світ досяг однієї з тих неповоротних точок у історії військової справи, коли роль технологій у веденні військових дій набула іншого значення, а революція у військовій справі абсолютно реальна, оскільки вона пов'язана головним чином з миттєвим доступом до мережевої інформації та крупно масштабним використанням високоточної зброї [18, с. 70].

Слід наголосити на тому, що у разі цілеспрямованої кібернетичної інтервенції з метою захоплення керування подібним арсеналом, а це в умовах динаміки розвитку ІКТ та ГТ не виключено, подібна атака, або певні її елементи, зможуть бути використана злочинцями за їх волевиявленням проти внутрішніх та зовнішніх інтересів держави або міждержавного об'єднання за розсудом злочинців[1]. Окремі злочини, що можуть бути вчинені у складі кібернетичної інтервенції, можуть призвести, якнайменше, до втрати високоточною зброєю орієнтації або втратити зв'язок з пунктами керування.

Також важливим є той факт, що незважаючи на те, що у наведених вище прикладах кібернетичної інтервенції не акцентувалося увагу на виконанні певних агресивних дій за власною ідеєю, або на замовлення, з точки зору оцінки небезпечності вказаних діянь значення не має, адже кожна атака з одного терміналу здійснюється безпосередньо певною особою, незалежно від того, на замовлення така особа вчинює атаку, чи генерує ідею стосовно атаки самостійно. Важливим є те, яка саме шкода може бути заподіяна або заподіюється державним та суспільним інтересам.

Внаслідок вищевикладеного під ***кібернетичною інтервенцією*** слід розуміти ***сукупність агресивних дій у кіберпросторі, направлених на втру-***

**[1] З метою повного усвідомлення наслідків отримання злочинцями можливостей керування мілітаристичним арсеналом у разі вдалої кібернетичної інтервенції, необхідно навести описання сучасної професором Е.Коеном: "Супутники миттєво передають зображення виявлених цілей пілотам літака-перехоплювача, танки повідомляють про своє місцезнаходження на комп'ютеризовані командні пункти, генерали ведуть спостереження за діями молодших командирів на полі бою через камери на безпілотному літаючому апараті - все це реалії сьогоднішнього дня". [19, p.5].**

***чання шляхом застосування ІКТ у внутрішні та зовнішні справи держав з метою заподіяння шкоди їх суверенітету або належному функціонуванню її керівних органів або основних сфер життєдіяльності, а рівно аналогічні дії відносно впорядкованої діяльності міждержавних об'єднань та їх керівних органів.***

Таке визначення повною мірою охоплює всі сфери дійсного і потенційного негативного впливу кіберзлочинності на цінності суспільства, адже кожна визнана цінність перебуває у сфері впорядкованого функціонування міжнародних організацій, міждержавних об'єднань та держав, які повною мірою охоплюють також і інтереси суспільств відповідного обсягу.

Стид звернути увагу на те, що якщо кримінальна інтервенція у попередніх формаціях могла відбуватися лише за умови посягання з перетином фізичних державних кордонів, кібернетична інтервенція - ***інтервенція у ІС,*** яке не має фізичних кордонів, що відокремлюють держави одну від одної, ***може бути як зовнішня, і здійснюватися з території іншої держави чи міждержавного об'єднання, так і внутрішня, і, відповідно, здійснюватися з території власної держави чи міждержавного об'єднання. При умові вчинення кібернетичної інтервенції у співучасті з різних держав, вона має характеризуватися як змішана.***

Можливість здійснення кібернетичної інтервенції обумовлюється станом розвитку саме ІКТ, і запровадженням ІКТ у всі сфери життєдіяльності сучасного суспільства, як на цьому вже неодноразово наголошувалося. Відповідно, кібернетична інтервенція спрямовується саме на ІКТ, які забезпечують діяльність відповідних сфер суспільства, з наміром втручання у керування такими сферами.

***Кібернетична інтервенція першочергово спрямовується на ІКТ, що забезпечують належне функціонування систем життєзабезпечення суспільства, і це, структурно, є визначальною ознакою кібернетичної інтервенції, як специфічної групи злочинів, що створюють загрози розвитку інформаційному суспільству.***

**У** той же час, у широкому сенсі, ідеологія кібернетичної інтервенції у інформаційному суспільстві характеризується іншою ідеєю, виокремленою від ідеї звичайної кіберзочинності, яка направлена, як і загальнокримінальна злочинність на, переважно, отримання певної матеріальної вигоди. Явище кібернетичної інтервенції утворюється внаслідок виникнення у суспільстві групи суспільно-небезпечних діянь, відмінною рисою яких є:

1) мета вчинення - заподіяння шкоди суверенітету держав або належному функціонуванню її керівних органів, чи основних сфер

життєдіяльності, а рівно заподіяння шкоди впорядкованій діяльності міждержавних об'єднань, їх керівних органів та сфер життєдіяльності у такому об'єднання;

2) першочергове спрямування таких злочинів на ІКТ, які забезпечують функціонування основних сфер життєдіяльності відповідних держав або міждержавних об'єднань або їх керівних органів.

Виходячи з наведеного вище, ***очевидна обумовленість криміналізації в Україні суспільно-небезпечних діянь, що мають ознаки кібернетичної інтервенції.***

## Використана література:

1. Словарь иностранных слов / Под И.В.Лехина и проф. Ф.Н.Петрова. - М: Государственное издательство иностранных и национальных словарей, 1954. - 856 с.

2. Трайнин А.Н. Уголовная интервенция / Избранные труды / Составление, вступительная часть докт. юрид. наук, профессора Н.Ф.Кузнецовой. - СПб.: Издательство "Юридический центр Пресс", 2004. - 898 с.

3. Зафиксировано 18 000 атак на сайт президента/ Інформаційна агенція MediaUa, 30.10.2007/ http://mediaua.com.ua/detail/29228

4. Левашова Ю. Сайт президента России подвергся хакерской атаке // Центр Исследования компьютерной преступности / http://www.crime-research. ru/news/18.05.2007/3474/

5. Предвыборный сайт Буша вышел из строя по неизвестной причине /Інформаційна агенція Набережные челны // http://lenta.chelni. ru/?id=8664

6. Зафиксировано 18 000 атак на сайт президента/ Інформаційна агенція MediaUa, 30.10.2007/ http://mediaua.com.ua/detail/29228

7. Хакер ограбил прокуратуру Санкт-Петербурга // CyberSecurity.m/ailMe/hacker_ograbil_prokmehiru_ sankt_ peterburga/

8. СБу розслідує справу про "транзитний сервер"/ РБК. Україна. 07.03.2006//ht^://www.rbc.ua/top/2006/ro/07/11673.shtml

9. ГПУ передає до суду справу про транзитний сервер ЦВК / Політична партія "Молода Україна" 14 вересня 2005 року / http://mu.org. иа/news.asp?IdType=l&Id=3604

10. Ambroziak F. Prezident zaproponowal nowelizacje ustawy o stanie wojennym. Gry wojenne w cyberprzestrzeni / Nash Dziennik / Czwartek, 14 lipca 2011, Nr 162 (4093) / http://www.iiaszdzieimik.pl/index. php?dat=20110714&typ=po&id=po27.txt

11. Гальчинський А.С. Глобальні трансформації: концептуальні альтернативи. Методологічні аспекти: Наук. вид. - К, Либідь, 2006. - 312 с.

12. Norbert Wiener. Cybernetics Second Edition: or the Control and Communications in the Animal and Machines/ - The МГГ Press? 1965/ - 212 p. - P. 17-22

13. Балда Т. Коротка історя гакерства// http://www/universum. org.ua/sp/2002/haker_3.html

14. Аргентинський хакер и американские компьютерные сети //http//:www.rol.ra/news/97/12/12_15.htm

15. Сетевые террористы. 10 самых опасных хакеров планеты / Корреспондент. - 2007. - № 15 (254). - С. 68-69. - С. 68.

16. Неугомонному хакеру предстоит провести 21 месяц в тюрьме/ Компьютер-сервис // http://www.csruk.ra/news/mdex.php3?begin=1755 &orrset=10

17. Н.Сорокша. Пентагон мстит зажерам / "Российская газета" - Федеральный выпуск № 3791. - 9.062005 // http//: www.rg.ru/2005/06 /09/hacker.html

18. Тэтчер М. Искусство управления государством. Стратегии для меняющегося мира / Пер. с англ. - М.: Алыгина Паблишер, 2003. - 504 с.

19. Eliot A. Cohen "War at Arms" // National Review, 24 Januery 2000. - P.5-7. - P.5].

**А.М. Кислий***

## ОСОБЛИВОСТІ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ УЧАСНИКІВ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ

***Стаття присвячена проблемним питанням нормативно-правового регулювання забезпечення безпеки осіб, які є учасниками оперативно-розшукових заходів.***

Ключові слова: ***оперативно-розшукова діяльність, учасник оперативно-розшукової діяльності, соціально-правовий, захист.***

***Статья посвящена проблемным вопросам нормативно-правового регулирования обеспечения безопасности лиц, являющихся участниками оперативно-розыскных мероприятий.***

Ключевые слова: ***оперативно-розыскная деятельность, участник оперативно-розыскной деятельности, социально-правовая защита.***

*** Доктор юридичних наук, старший науковий співробітник, заступник начальника ГУ МВС України в Київській області.**

ВІСНИК
Луганського державного університету
внутрішніх справ імені Е.О. Дідоренка

# УДОСКОНАЛЕННЯ ВЗАЄМОДІЇ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ З ВІДПОВІДНИМИ ПІДРОЗДІЛАМИ ТА УСТАНОВАМИ ДЕРЖАВНОЇ ПЕНІТЕНЦІАРНОЇ СЛУЖБИ УКРАЇНИ ЩОДО ВИКОНАННЯ ЗАВДАНЬ ОРД

Спеціальний випуск № 3

**Луганськ**
**2012**

УДК 351.74/.76(063)
У31

# ВІСНИК

*СПЕЦІАЛЬНИЙ ВИПУСК № 3-2012*

**Луганського державного університету внутрішніх справ імені Е.О. Дідоренка**

***Науково-теоретичний журнал * Виходить щоквартально * Заснований 1997 року * Засновник і видавець: Луганський державний університет внутрішніх справ * Реєстраційне свідоцтво КВ № 15990-4462 ПР, видане Міністерством юстиції України 20.11.2009 р. * Включений до переліку фахових видань ВАК України з юридичних наук ***



*Рекомендовано до друку вченою радою Луганського державного університету внутрішніх справ імені Е.О. Дідоренка (протокол № 13 від 25 травня 2012 року)*

**У даному спеціальному випуску публікуються наукові статті, доповіді й повідомлення вчених-юристів, ад'юнктів (аспірантів), здобувачів, курсантів, студентів і практиків з питань наукового забезпечення вдосконалення та розвитку оперативно-розшукової діяльності в Україні.**

**Статті публікуються в авторській редакції.**

**ЕЗ Україна, 91493, Луганськ, сел. Ювілейне, вул. Генерала Дідоренка, 4. Луганський державний університет внутрішніх справ імені Е.О. Дідоренка т. 35-11-57, 35-11-40, факс 93-50-77.**