Пашнєв Дмитро Валентинович,
кандидат юридичних наук, доцент
(Харківський національний університет внутрішніх справ)

УДК 343.85

СТРАТЕГІЯ ЗАБЕЗПЕЧЕННЯ КРИМІНОЛОГІЧНОЇ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ОРГАНАМИ ВНУТРІШНІХ СПРАВ

В статті запропоновано стратегію забезпечення кримінологічної кібербезпеки на основі застосування кримінологічних наукових розробок до сфери кіберзлочинності. Обґрунтована необхідність забезпечення кібернетичної безпеки органами внутрішніх справ за певними напрямками в рамках науково обґрунтованої стратегії. Проаналізовані окремі напрямки стратегії забезпечення кримінологічної кібернетичної безпеки органами внутрішніх справ та внесені пропозиції щодо їх удосконалення.

Ключові слова: *кримінологічна безпека, кібернетична безпека, кіберзлочинність*

В часи переходу до інформаційного суспільства особливої актуальності набуває забезпечення безпеки людини, суспільства, держави від потужних можливостей нових комп'ютерних технологій, які можуть використовуватися не тільки для підвищення якості життя, але й для порушення прав, свобод та інтересів особи, нанесення шкоди суспільству та державі. З точки зору кримінології, виникає необхідність застосування до цієї сфери концепції кримінологічної безпеки, що в останні часи набуває все більшої підтримки серед науковців [1–3].

Певні аспекти теорії кримінологічної безпеки, основи якої були вперше сформульовані професорами М. М. Бабаєвим і В. О. Плешаковим [4; 5], були предметом досліджень багатьох українських та закордонних вчених, зокрема: О. М. Бандурки, В. А. Бодренкова, Г. Г. Горшенкова, В. М. Дрьоміна, О. М. Костенка, О. О. Лапіна, С. Я. Лебедєва, О. М. Литвинова, Т. В. Мельничук, Д. О. Симоненка, А. А. Тер-Акопова, М. Л. Шелухіна, О. Ю. Шумилова та інших. Проблеми кримінологічної безпеки від кіберзлочинності розглядалися В. М. Бутузовим, В. Д. Гавловським, К. В. Тітуніною, В. П. Шеломенцевим.

Розробка теорії кримінологічної безпеки покликана сприяти перенесенню значеннєвого акценту з об'єкта нападу (злочинність) на об'єкт захисту (особа, суспільство, держава), тобто на ті цінності, яким, власне, і повинна бути гарантована

кримінологічна безпека. А тому необхідна переорієнтація на оборонну доктрину кримінологічної безпеки, забезпечення якої повинне перевершувати характер і спрямованість криміногенних і кримінальних загроз. Тому в ієрархії форм діяльності по забезпеченню кримінологічної безпеки на першому місці стоїть захист від джерела загрози безпеці, а вже потім – вплив на саме джерело, звичайно, не виключаючи паралельності в здійсненні названих форм діяльності.

В світлі такого принципово нового теоретичного й практичного значення для здійснення державної політики в сфері контролю над кіберзлочинністю виникає низка проблем в забезпеченні кримінологічної безпеки в цій сфері.

Відповідно до Проекту Закону України «Про кібернетичну безпеку України» кібернетична безпека (кібербезпека) – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [6]. Цей Закон повинен визначити основні засади державної політики, спрямованої на захист життєво важливих інтересів особи, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, та, відповідно, забезпечити правову базу для досягнення вказаного стану захищеності.

Така політика, звичайно не буде ефективною без кримінологічної стратегії, значення та необхідність якої слушно обґрунтовує О. М. Литвинов: «Кримінологічна стратегія надає функціонуванню механізму протидії злочинності стабільності, планомірності, спрямованості, забезпечує безпосередність і послідовність розробки завдань діяльності та їх диференціацію за рівнями та сферами застосування. Вона служить своєрідною платформою для довгострокових і перспективних планів діяльності окремих суб'єктів, вбирає в себе фундаментальні надбання науки та новітні форми організації практичної сторони справи, чітко визначає засоби, у тому числі обумовлені специфікою дії механізмів реалізації довгострокової кримінологічної політики» [7].

Діяльність органів внутрішніх справ із забезпечення кримінологічної безпеки, зокрема і в кіберсфері, оскільки саме в їх складі сформовані підрозділи боротьби з кіберзлочинами, також потребує розроблення відповідної стратегії.

Отже метою даної статті є формування стратегії забезпе-

чення кримінологічної кібербезпеки органами внутрішніх справ на основі застосування кримінологічних наукових розробок до сфери кіберзлочинності.

Для досягнення цієї мети застосуємо підхід, запропонований О. О. Лапіним [8, с. 24], виходячи з його комплексності, охоплення всіх напрямків діяльності та простоти для розуміння і реалізації. Отже стратегія забезпечення кримінологічної безпеки містить у собі шість видів стратегій:

1. Стратегія стримування загроз кримінологічній безпеці.
2. Стратегія впливу на особу злочинця як носія, суб'єкта кримінальної загрози.
3. Стратегія впливу на джерела загроз кримінологічній безпеці.
4. Стратегія попередження злочинів.
5. Стратегія кримінологічного захисту об'єктів злочинного посягання.
6. Стратегія віктимологічної профілактики.

Застосовуючи ці напрями до сфери кіберзлочинності, отримаємо наступні напрями стратегії забезпечення кримінологічної кібербезпеки органами внутрішніх справ:

1. Стратегія стримування загроз кримінологічній кібербезпеці, у якості яких виступає в кіберзлочинність, а також її види, відповідно до Конвенції [9] та Додаткового протоколу до неї [10]. Основним критерієм стратегії стримування кіберзлочинності є критерій домірності якості й масштабу кримінальних загроз і відповідних заходів. У Декларації принципів і програми дій ООН в області попередження злочинності й кримінального правосуддя, прийнятою Резолюцією 46/152 Генеральної Асамблеї від 18 грудня 1991 р., прямо говориться: «Будь-якому розширенню можливостей і здатностей правопорушників вчиняти злочини повинне відповідати аналогічне розширення можливостей і здатностей правоохоронних органів і органів кримінального правосуддя».

Розглянута стратегія не має потреби в особливому поясненні, оскільки вона практично збігається із традиційною стратегією боротьби зі злочинністю в її класичному варіанті, тобто націленістю на: зниження рівня кіберзлочинності, зокрема тяжкої й особливо тяжкої; призупинення зрощування загальнокримінальних структур з кіберзлочинцями, подальшого поширення

й консолідації тих або інших найнебезпечніших форм злочинності; недопущення втягування в злочинну діяльність нових соціальних груп, особливо неповнолітніх; витиснення злочинності з окремих сфер кіберпростору; зменшення тиску кіберзлочинності на економічні відносини в кіберпросторі; обмеження незаконного обігу шкідливих програмних та технічних засобів, пропаганди в кіберпросторі пияцтва й алкоголізму, проституції та інших супутніх злочинності явищ.

Реалізацією цієї стратегії в МВС України займаються відповідні підрозділи боротьби з кіберзлочинністю.

2. Стратегія впливу на кіберзлочинця як носія, суб'єкта кримінальної загрози. Дана стратегія в основному спрямована на вдосконалення системи виявлення й покарання кіберзлочинців, виконання покарання й ресоціалізацію раніше судимих осіб з метою зниження рецидиву злочинів. Ця стратегія в цей час реалізується шляхом істотної корекції кримінально-правових норм, підвищення відповідальності й об'єктивності рішень судових органів, проведення реформи кримінально-виконавчої системи, спрямованої на поліпшення умов утримання засуджених, зниження кримінального впливу в місцях позбавлення волі, а також поширення заходів покарання, не пов'язаних з позбавленням волі. Істотний вплив на умови виправлення та ресоціалізації раніше судимих осіб має Закон України «Про адміністративний нагляд за особами, звільненими з місць позбавлення волі» [11]. На наш погляд, враховуючи специфіку протиправної діяльності в кіберсфері до ст. 10 цього Закону слід додати ще одне обмеження для піднаглядних, а саме: заборону користування інформаційними, комунікаційними та інформаційно-телекомунікаційними системами.

3. Стратегія впливу на джерела загроз кримінологічній кібербезпеці, а саме на криміногенні фактори. Ця стратегія багато в чому пов'язана з реалізацією соціальної політики держави. Багато аспектів соціальної політики можуть впливати на злочинність. У зв'язку з цим найбільш часто, у тому числі й у міжнародних документах, приводяться шість напрямків соціальної політики [12]:

– політика планування міських і сільських районів, і зокрема політика ліквідації нетрів, керування розміщенням, проблема бездомності, проектування й передбачення місць суспіль-

ного користування й торгівлі, взаємозв'язок між наданням житла й іншими службами, особливо транспорт і місце роботи;

– політика зайнятості, і зокрема політика, пов'язана з ліквідацією безробіття й створенням робочих місць;

– політика в галузі освіти, включаючи дітей дошкільного віку;

– сімейна політика;

– молодіжна політика, включаючи створення умов для відпочинку, проведення дозвілля й заняття культурою;

– політика в області охорони здоров'я, і зокрема боротьби з наркоманією й алкоголізмом.

Діяльність в цих напрямках цілком ефективно може впливати і на загрози кібербезпеці, якщо в їх рамках підвищиться увага до сфери інформаційних технологій, зокрема до виховання культури поводження із комп'ютерними системами, що створює в особи психологічний бар'єр щодо вчинення кіберзлочинів.

Органи внутрішніх справ повинні приймати активну участь у всіх цих заходах, виявляти слабкі місця у цих напрямках та виходити з пропозиціями до інших органів влади щодо їх укріплення.

4. Стратегія попередження кіберзлочинів, яка стосовно до теорії кримінологічної безпеки розглядається як стратегія попередження кримінальних загроз. Ця стратегія передбачає розробку заходів щодо надання стримуючого, нейтралізуючого, а головне – попереджувального впливу на кримінальні загрози.

Стратегія запобігання кіберзлочинам передбачає вирішення наступних завдань:

1) виявлення осіб, що замишляють або підготовляють кіберзлочини;

2) примушування особи до відмови від вчинення кіберзлочину;

3) вжиття до особи примусових заходів, що виключають, відтягують строки або створюють додаткові труднощі для вчинення особою кіберзлочину;

4) усунення або нейтралізація умов, що штовхають особу на кіберзлочин;

5) вжиття заходів до захисту об'єкта можливого посягання;

6) захист можливої жертви від злочинного посягання;

7) надання впливу на ситуацію, що склалася в місці можливого вчинення кіберзлочину і сприяє його вчиненню.

Реалізація стратегії припинення кіберзлочинів у діяльності органів внутрішніх справ повинна здійснюватися виходячи із двох основних факторів, що впливають уже на тактику припинення:

1) виявлення місць можливого вчинення кіберзлочинів, потенційних жертв;

2) виявлення осіб, які від готування переходять до вчинення кіберзлочинів.

Основними завданнями припинення кіберзлочину, на який замахується встановлена органами міліції особа, є наступні:

1) затримання особи (осіб) і притягнення її (їх) до кримінальної відповідальності за замах на кіберзлочин;

2) захист осіб, на яких може бути вчинений замах;

3) превентивний інструктаж населення про тактику поведінки при злочинному замаху на їх інформацію чи комп'ютерну систему.

Реалізація стратегії попередження загроз кібербезпеці, таким чином, припускає реалізацію стратегії запобігання кіберзлочинам і стратегії припинення кіберзлочинів.

5. Стратегія кримінологічного захисту об'єктів злочинного кіберпосягання виступає стрижневою стратегією в рамках забезпечення кримінологічної безпеки, оскільки саме ця стратегія припускає перенесення центру ваги із впливу на кіберзлочинність, особу кіберзлочинця й криміногенні фактори на захист особи, суспільства, держави від злочинних кіберпосягань.

Такі заходи в кримінології вже досліджувалися як заходи кримінологічного захисту об'єктів злочинного посягання, у тому числі й у рамках забезпечення кримінологічної безпеки [5, с. 31–33, 44; 13, с. 387–389; 14, с. 168, 169].

Проте в рамках цього напрямку стратегії стосовно протидії кіберзлочинності виникає найбільше труднощів. Якщо інформаційно-телекомунікаційні системи, що належать державі доступні для захисту, і саме їх захисту присвячено більшість заходів, що передбачені Законом «Про кібернетичну безпеку»; то захист приватних систем лежить повністю на приватному секторі. Це виходить хоча з того, що одним з принципів забезпе-

чення кібернетичної безпеки є принцип особистої відповідальності громадян про власну безпеку, неухильного дотримання ними правил безпечної поведінки у кіберпросторі.

Перенесення ж акцентів впливу із суб'єкта загрози (злочинця) на об'єкт захисту (в даному випадку – особу) передбачає, звичайно, проведення більшості заходів захисту саме з об'єктом. В цьому вся суть цієї концепції: не більше затримати злочинців, а більше небезпеки відвернути від особи – об'єкту захисту. З цією метою змінюється спосіб діяльності правоохоронних органів – вони, звичайно, не перестають демонструвати можливість викрити злочинця, розкрити злочин тощо, але основною діяльністю стає саме створення в особи впевненості в тому, що вони можуть її захистити від цього посягання. В цьому плані найбільш ефективним є заходи з виключення контакту зловмисника із особою та іншими об'єктами, що представляють її інтерес (майном, речами, тваринами тощо), і недопущення нанесення їм шкоди.

Але стосовно кібербезпеки нарощування таких традиційних заходів безпеки не може принести користі, з очевидних причин: об'єкти, що представляють інтерес особи, і сам зловмисник, що отримує контакт и наносить їм шкоду, – все це знаходиться у кіберпросторі, засоби доступу до якого знаходяться у виключному володінні особи. Більше того, держава сама забезпечує охорону і захист такого виключного володіння. Навіть в ході кримінального провадження всі дії, що стосуються речей і документів, які містять охоронювану законом таємницю, в тому числі «інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо» (ст. 162 КПК України), можуть бути вчинені тільки за рішенням суду за особливих умов (ч. 6 ст. 163 КПК України).

Таким чином, забезпечення кримінологічної кібербезпеки особи є справою тільки її рук. І в цьому плані рівень такого забезпечення залишає бажати кращого, оскільки некомпетентність в цій сфері більшості громадян призводить до незахищеності їх від кіберзагроз.

Але, з іншого боку, нам бачиться, що забезпечити кіберзахист приватного сектору правоохоронними органами можли-

во шляхом використання можливостей, які закладені в самих комп'ютерних технологіях. Пропонуємо створити в структурі МВС України служби кіберохорони по типу Державної служби охорони (ДСО). Такий підрозділ, умовно назвемо його ДСК – Державна служба кіберохорони, на умовах договору із об'єктом охорони на платній основі може здійснювати забезпечення кібербезпеки об'єкту, починаючи із встановлення та обслуговування відповідних програмних та технічних засобів і закінчуючи реагуванням на потенційні та реальні загрози безпеці інформаційно-телекомунікаційній системі об'єкта. При чому ця робота може здійснюватися без безпосереднього виїзді та контакту службовців із клієнтом, як того потребує діяльність ДСО, що забезпечується можливостями комп'ютерних технологій, які полягають у віддаленому управлінні комп'ютером за допомогою спеціальних програм. Найбільш популярним таким засобом є програма TeamViewer, яка дає можливість «адміністрування віддалених комп'ютерів або серверів в будь-якому місці і в будь-який час, так, наче Ви сидите прямо перед ними» [15].

Перевага такої служби над приватними уявляється в тому, що реагування на реалізацію загроз системі об'єкта, по-перше, буде швидким, а по-друге, буде включати не тільки відвернення їх шкоди, але й весь спектр кримінально-процесуальних заходів, що дозволить ефективно зібрати докази та швидко виявити зловмисника. В результаті діяльність ДСК забезпечить не тільки захист прав приватних осіб в інформаційній сфері, але й кібернетичну безпеку держави, оскільки вона і складається із, так би мовити, «безпек» окремих інформаційно-телекомунікаційних систем.

6. Стратегія віктимологічної профілактики кіберзлочинності спрямована на зниження ризику потенційних жертв стати об'єктом злочинного кіберпосягання й активізацію захисних властивостей таких осіб. У цьому випадку, як і при кримінологічному захисті, дії по забезпеченню кібербезпеки в основному йдуть не від реальної загрози злочинного кіберпосягання, а від можливості й імовірності її внаслідок провокуючих, сприяючих поведінки, статусу, стану й т. П. можливої жертви.

Комплексне застосування заходів в цих напрямках повинне суттєво знизити рівень зростання кіберзлочинності. Але ефективність стратегії безпосередньо залежить від її наукового

забезпечення та впровадження результатів досліджень в практику. Взагалі, ці напрямки діяльності вже знайшли досить широке відображення в науковій і навчальній літературі, але вони потребують доповнення та корекції відповідно до сфери інформаційних технологій та протидії кіберзлочинності в рамках окремих досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Гавловський В. Д. Протидія організованій злочинності у сфері інформаційних технологій як окремий аспект кримінологічної безпеки / В. Д. Гавловський, В. М. Бутузов // Боротьба з організованою злочинністю і корупцією (теорія і практика) . – 2010. – Вип. 22. – С. 236–246.

2. Шеломенцев В. П. Безпека людини, суспільства і держави в Україні: кримінологічний аспект / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2009. – № 22. – С. 215–222.

3. Шеломенцев В. П. Кримінологічна безпека у кіберпросторі: система понять / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2010. – № 23. – С. 342–348.

4. Бабаев М. М. Теоретические и прикладные проблемы обеспечения криминологической безопасности / Бабаев М. М., Плешаков В. А. // Уголовная политика и проблемы безопасности государства : труды Академии управления МВД России. – М., 1998. – С. 25–32.

5. Плешаков В. А. Криминологическая безопасность и ее обеспечение в сфере взаимовлияния организованной преступности и преступности несовершеннолетних : дис. ... докт. юр. наук : 12.00.08 / Плешаков Владимир Алексеевич. – Москва, 1998. – 323 с.

6. Проект Закону України «Про кібернетичну безпеку України» № 2207а від 04.06.2013 р. [Електронний ресурс] // Верховна Рада України : Законопроекти. – 14.11.2014 р. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=47240&pf35401=264705.

7. Литвинов, О. М. Кримінологічна стратегія як компонент стратегії національної безпеки України / О. М. Литвинов // Право і безпека : Науковий журнал. – 2010. – № 3. – С. 137–141.

8. Лапин А. А. Стратегия обеспечения криминологической безопасности личности, общества, государства и ее реализация органами внутренних дел : монография / А. А. Лапин; под ред. С. Я. Лебедева. – М. : ЮНИТИ-ДАНА: Закон и право, 2012. – 295 с.

9. Конвенція про кіберзлочинність від 23.11.2001 р. [Електронний ресурс] / Верховна Рада України : Законодавство. – 14.11.2014 р. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/994_575.

10. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру,

вчинених через комп'ютерні системи від 28.01.2003 р. [Електронний ресурс] / Верховна Рада України : Законодавство. – 14.11.2014 р. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/994_687.

11. Закон України «Про адміністративний нагляд за особами, звільненими з місць позбавлення волі» від 01.12.1994 р. № 264/94-ВР [Електронний ресурс] / Верховна Рада України : Законодавство. – 14.11.2014 р. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/264/94-ВР.

12. Руководство по основным направлениям предупреждения преступлений от 7 сентября 1990 г. (СЮ 93-2,3,5,6). Подготовлено для ООН Отделом исследования и планирования Министерства внутренних дел Англии // Советская юстиция. – 1993. – № 2. – С. 28-31; № 3. – С. 24-27; № 5. – С. 25-27; № 6. – С. 25-28.

13. Аванесов Г. А. Криминология : учебник / Аванесов Г. А. – 2-е изд., перераб. и доп. – М. : Акад. МВД СССР, 1984. – 500 с.

14. Жалинский А. Э. Специальное предупреждение преступлений в СССР : (Вопросы теории) / А. Э. Жалинский. – Львов : Вища школа, Львов. ун-т, 1976. – 194 с.

15. TeamViewer – функціонально повне рішення для віддаленого доступу та підтримки за допомогою Інтернет [Електронний ресурс]. – 25.08.2014 р. – Режим доступу: http://www.teamviewer.com/uk/index.aspx. – Назва з екрану.

В статье предложена стратегия обеспечения криминологической кибербезопасности на основе применения криминологических научных разработок к сфере киберпреступности. Обоснована необходимость обеспечения кибернетической безопасности органами внутренних дел по определенным направлениям в рамках научно обоснованной стратегии. Проанализированы отдельные направления стратегии обеспечения криминологической кибернетической безопасности органами внутренних дел и внесены предложения относительно их усовершенствования.

Ключевые слова: *криминологическая безопасность, кибернетическая безопасность, киберпреступность.*

The article proposes the strategy of ensuring criminological cybersecurity through the application of criminological scientific research in the sphere of cybercrimes. The necessity of ensuring cybersecurity by internal affairs authorities in the certain spheres within the frame of scientifically-based policy is grounded. Certain directions of strategy for ensuring criminological cyber security by internal affairs authorities are analyzed and the suggestions for their improvement are proposed.

Keywords: *criminological security, cyber security, cybercrimes.*

Стаття надійшла до редакції 15.11.2014