Глава 19. Кримінологічна характеристика та запобігання кіберзлочинам

(Савченко А. В., Литвинов О. М., Орлов Ю. Ю.)

План

§ 1. Поняття кіберзлочинності та кіберзлочинів.

§ 2. Класифікація кіберзлочинів.

§ 3. Причини та умови кіберзлочинності.

§ 4. Характеристика осіб, які вчиняють кіберзлочини.

§ 5. Запобігання кіберзлочинності.

§ 1. Поняття кіберзлочинності та кіберзлочинів

У кримінологічній літературі наголошується, що концепція кіберзлочинності була сформульована завдяки діяльності правоохоронних органів розвинутих країн Європи та світу і стосується злочинів у сфері комп'ютерної інформації та телекомунікацій, незаконного обігу радіоелектронних і спеціальних технічних засобів, поширення не ліцензованого програмного забезпечення для комп'ютерів, а також деяких інших видів злочинів [589]. Щодо терміну «кіберзлочинність», то у міжнародно-правових документах його не визначено. Навіть у Конвенції (Ради Європи) про кіберзлочинність від 23 листопада 2001 року дефініція цього терміну відсутня, хоча ця Конвенція і розтлумачує у ст. 1 «Визначення», що є «комп'ютерною системою», «комп'ютерними даними», «постачальником послуг» і «даними про рух інформації» [590].

Уявляється, що термін «кіберзлочинність» (англ. «cybercrime») ширше, ніж «комп'ютерна злочинність» («computer crime»), оскільки більш точно відображає природу злочинності в інформаційному просторі. Приставка «cyber-» вважається компонентом складного слова та означає щось таке, яке відноситься до мережі Інтернет, віртуальної реальності, інформаційних технологій, комп'ютерної системи тощо. Відповідно «кіберзлочинність» є злочинною (протиправною) діяльністю чи злочинністю, що пов'язана з використанням комп'ютерів, інформаційних технологій і глобальних мереж. Практично так само її описують електронний словник «Dictionary», Оксфордський і Кембриджський словники. В електронному словнику «Techopedia» зазначено про таке: «Кіберзлочинність визначається як злочинність, де комп'ютер є об'єктом злочину (хакерство, фішинг, спам) або використовується як інструмент для вчинення злочину (дитяча порнографія, злочини з ненависті). Кіберзлочинці можуть використовувати комп'ютерні технології для доступу до особистої інформації, комерційної таємниці або використовувати Інтернет для експлуатаційних або шкідливих цілей. Злочинці можуть також використовувати комп'ютери для зв'язку та зберігання документів або даних. Злочинців, які здійснюють ці незаконні дії, часто називають хакерами» [591]. У той же час термін «комп'ютерна злочинність» («computer crime») переважно описує злочини, вчинені щодо комп'ютерів або комп'ютерних даних.

У національному законодавстві термін «кіберзлочинність» визначено лаконічно – «сукупність кіберзлочинів» (п. 9 ст. 1 «Визначення» Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року) [592]. Сьогодні кіберзлочинність для нашої держави є більш небезпечною, ніж навіть п'ять років тому, і, незважаючи на всі заходи правоохоронних органів, які спрямовані на боротьбу з кіберзлочинами, їх перелік не

[589] Голіна В., Головкін Б. Кримінологія: Загальна та Особлива частини: навч. посіб. Харків: Право, 2014. 513 с. С. 332.

[590] Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року (Конвенцію ратифіковано Україною із застереженнями і заявами Законом № 2824-IV від 7 вересня 2005 року). URL: http://zakon2.rada.gov.ua/laws/show/994_575 (дата звернення: 02.05.2019).

[591] Cybercrime. Techopedia. URL: https://www.techopedia.com/definition/2387/cybercrime (дата звернення: 03.05.2019).

[592] Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 03.05.2019).

зменшується, а, навпаки, зростає, при цьому боротьба з кіберзлочинністю неможлива без глибокого розуміння правових питань регулювання інформаційних мереж [593].

У свою чергу термін «кіберзлочин (комп'ютерний злочин)» означає «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорамиУкраїни» (п. 8 ст. 1 «Визначення» Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року) [594].

З цього визначення випливають такі ознаки кіберзлочину:

1) суспільна небезпечність (наприклад, щороку кількість виявлених кіберзлочинів збільшується в середньому на 2,5 тисячі) [595];

2) винність (цей злочин може бути вчинено умисно або необережно);

3) діяння, вчинене у кіберпросторі та/або з його використанням (під терміном «кіберпростір», згідно п. 11 ст. 1 «Визначення» Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, розуміють «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних») [596];

4) протиправність (відповідальність за його вчинення передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України).

У ст. 12 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року законодавець уточнює, що кримінальна відповідальність настає за умови, якщо кіберпростір є місцем та/або способом вчинення злочину. Поняття «місце вчинення злочину» та «способу вчинення злочину» чітко не визначені в українському законодавстві, що, в свою чергу, тягне різне розуміння цих термінів науковцями-юристами.

Місце вчинення злочину – це певна територія (межі, сфера), де було розпочато і закінчено діяння або настав злочинний результат. Як місце злочину кіберпростір може виступати, наприклад, в якості середовища обігу інформації, наслідки несанкціонованих дій з якою визначені статтями Розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України (зокрема, якщо йдеться про дії, що призвели до витоку інформації, що становить державну таємницю, яка містилася на захищеному комп'ютері, розташованому у приміщенні відповідного правоохоронного органу).

Спосіб вчинення злочину – це певний метод, порядок і послідовність рухів, прийомів, що застосовуються особою для вчинення злочину. Спосіб завжди притаманний дії, утворює її зміст, а в деяких випадках може ставати окремою дією стосовно основної. Як спосіб вчинення злочину кіберпростір може бути, наприклад, прийомом чи методом вчинення злочинів у сфері національної безпеки, електронних комунікацій та захисту інформації (зокрема, несанкціоноване втручання в роботу сайту адміністративних послуг, що призвело до його блокування та неможливості подальшого надання послуг).

Проблема запобігання та протидії кіберзлочинам була сформована ще у 80-ті роки XX ст., однак перші норми відповідного характеру було внесено до законодавства про кримінальну відповідальність лише у 1994 р. на підставі Закону України «Про внесення змін і доповнень до Кримінального та Кримінально-процесуального кодексу України», який передбачав доповнення тоді ще глави IX «Злочини проти порядку управління» КК України 1960 р. новою ст. 198-1:

Стаття 198-1. Порушення роботи автоматизованих систем.

Умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації, чи розповсюдження програмних і технічних

---

[593] Бондаренко О. С., Рєпін Д. А. Кіберзлочинність в Україні: причини, ознаки та заходи протидії. *Порівняльно-аналітичне право*. 2018. № 1. С. 246–248. С. 246.

[594] Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 03.05.2019).

[595] Кількість кіберзлочинів збільшується на 2,5 тисячі в рік – голова Кіберполіції (Понеділок, 15 січня 2018, 16:05). URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 03.05.2019).

[596] Кількість кіберзлочинів збільшується на 2,5 тисячі в рік – голова Кіберполіції (Понеділок, 15 січня 2018, 16:05). URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 03.05.2019).

засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи то носіїв інформації, –

карається позбавленням волі на строк до двох років або виправними роботами на той же строк, або штрафом у розмірі від ста до двохсот мінімальних розмірів заробітної плати.

Ті ж дії, якщо ними спричинено шкоду у великих розмірах, або вчинені повторно чи за попереднім зговором групою осіб, –

караються позбавленням волі на строк від двох до п'яти років.

(Кодекс доповнено статтею 198-1 згідно з Законом № 218/94-ВР від 20.10.94) [597].

У подальшому появу в Особливій частині КК України 2001 р. розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» слід визнати об'єктивною необхідністю. На момент ухвалення нового КК України в межах згаданого розділу було криміналізовано три суспільно небезпечні діяння: 1) незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (ст. 361); 2) викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем (ст. 362); 3) порушення правил експлуатації автоматизованих електронно-обчислювальних систем (ст. 363).

У період з 2003 по 2015 рр. законодавець вдався до таких нормативних змін і доповнень до розділу XVI Особливої частини КК України:

– по-перше, Законом України № 908-IV від 5 червня 2003 р. до назву розділу XVI Особливої частини цього Кодексу доповнено словами «і мереж електрозв'язку», а також змінена назва і редакція ст. 361;

– по-друге, Законом України № 2289-IV від 23 грудня 2004 р. у розділі XVI Особливої частини цього Кодексу ст.ст. 361, 362 і 363 були викладені в новій редакції, а також Кодекс доповнено новими статтями – 361-1, 361-2 і 363-1;

– по-третє, на підставі Закону України № 721-VII від 16 січня 2004 р. розділ XVI Особливої частини цього Кодексу був доповнений ст.ст. 361-3, 361-4, 362-1, які незабаром були виключені на підставі Закону України № 767-VII від 23 лютого 2014 року;

– по-четверте, Законом України № 770-VIII від 10 листопада 2015 р. вдосконалено інституту спеціальної конфіскації з метою усунення корупційних ризиків при її застосуванні, відтак у ст.ст. 361, 361-1, 361-2, 362, 363-1 цього Кодексу була виключена вказівка на відповідні види спеціальної конфіскації.

Таким чином, на даний момент розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України містить шість статей:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК);

4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК);

5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК);

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК).

[597] Про внесення змін і доповнень до Кримінального та Кримінально-процесуального кодексу України: Закон України № 218/94-ВР від 20 жовтня 1994 року. URL: http://zakon3.rada.gov.ua/laws /show/218/94-вр (дата звернення: 03.05.2019).

§ 2. Класифікація кіберзлочинів

Слід наголосити, що на сьогодні ні у національному законодавстві, ні у теорії кримінального права немає одностайної (усталеної) позиції щодо класифікації кіберзлочинів. Більше того, відсутня єдність з приводу того, які саме конкретні злочини слід відносити до посягань у сфері кібербезпеки. У принципі з використанням кіберпростору в наш час можна вчинити широке коло злочинів: від умисного вбивства (наприклад, через відключення системи штучного дихання у хворого або зупинку «штучного серця», або втручання в комп'ютерну систему транспортних засобів з людьми, що рухаються) до крадіжки грошових коштів чи шахрайства з іншим майном; від кібершпигунства та кібертероризму до збуту заборонених у вільному обігу предметів (вогнепальної зброї, наркотичних засобів і психотропних речовин, порнографічних предметів тощо); від несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку до пропаганди війни тощо.

В юридичній літературі комп'ютерні злочини (правопорушення) класифікуються науковцями по-різному.

Наприклад, Б. В. Романюк та М. В. Гуцалюк комп'ютерні правопорушення поділяють на три групи:

1) правопорушення, де сам комп'ютер чи інформація у ньому є предметом вчинення протиправних дій;

2) правопорушення, де комп'ютер виступає як знаряддя вчинення злочину;

3) правопорушення, доказом яких є інформація, що міститься в комп'ютерних системах [598].

М. В. Плугатир стверджує, що:

– по-перше, чинний КК України містить норми, які спрямовані на захист суспільних відносин у сфері використання сучасних комп'ютерних технологій від злочинних посягань;

– по-друге, ці посягання можливо визначити як «комп'ютерні злочини (кіберзлочини)» та розділити їх на дві групи:

а) злочини у сфері комп'ютерної інформації (їх об'єктом є суспільні відносини у сфері комп'ютерної інформації);

б) злочини, пов'язані з використанням комп'ютерної техніки та обробкою комп'ютерної інформації (суспільні відносини у сфері комп'ютерної інформації в таких злочинах виступають додатковим обов'язковим або додатковим факультативним об'єктом) [599].

М. В. Карчевський визначив таку систему злочинів у сфері інформаційної безпеки, яка включає три групи посягань:

1) злочини у сфері використання інформаційних технологій (ч.ч. 11, 12 ст. 158, ст.ст. 361–363-1, 376-1 КК України);

2) злочини у сфері забезпечення доступу до інформації (ст.ст. 111, 114, 132, 145, ч.ч. 11, 12 ст. 158, ст.ст. 159, 163, 168, 182, ч. 2 ст. 209-1, 231, 232, 328, 330, 361-2, 361, 362, 376-1, 381, 387, 422 КК України – злочини у сфері обмеженого доступу до інформації; ст. 136, ч. 1 ст. 209-1, ст.ст. 232-2, 238, ч. 3 ст. 243, ст. 285, ст. 298-1, 385 КК України – злочини у сфері отримання доступу до інформації);

3) злочини у сфері формування інформаційного ресурсу (ч.ч. 2, 3 ст. 109, ст.ст. 110, 161, 171, 258-2, 295, 300, 301; ч. 2 ст. 442 КК України) [600].

Н. А. Савінова виділяє:

1) суспільно небезпечні діяння, що трансформувалися під впливом розвитку інформаційного суспільства, до якої належать безпосередньо діяння, які охоплюються окремими складами раніше відомих злочинів, а також злочини терористичної спрямованості, що вчиняються у спосіб використання дистанційних комунікацій;

---

[598] Романюк Б. Гуцалюк М. Координація боротьби з комп'ютерною злочинністю – нагальна вимога сьогодення. *Міліція України.* 2001. № 11. С. 22.

[599] Плугатир М. В. Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації: автореф. дис. … канд. юрид. наук: спец. 12.00.08. Київ, 2010. С. 6–7.

[600] Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: автореф. дис. … д-ра юрид. наук: спец. 12.00.08. Київ, 2013. С. 10.

2) новітні суспільно небезпечні діяння, що виникли в умовах розвитку інформаційного суспільства, за ознаками спільних характеристик – «кібернетичні злочини» («кіберзлочинність»), «кібернетична інтервенція», «інформаційна експансія», «впливи на свідомість населення» [601].

Зважаючи на сучасні завдання кіберполіції, усі кіберзлочини можна поділити на такі види:

1) у сфері використання платіжних систем:

а) скімінг (шимінг) – незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток;

б) кеш-трепінг – викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки;

в) кардінг – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем;

г) несанкціоноване списанням коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування;

2) у сфері електронної комерції та господарської діяльності:

а) фішинг – виманювання у користувачів Інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти, тощо;

б) онлайншахрайство – заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

3) у сфері інтелектуальної власності:

а) піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті;

б) кардшарінг – надання незаконного доступу до перегляду супутникового та кабельного TV;

4) у сфері інформаційної безпеки:

а) соціальна інженерія – технологія управління людьми в Інтернет просторі;

б) мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення;

в) протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;

г) рефайлінг – незаконна підміна телефонного трафіку [602].

Однак проблемним моментом у класифікації кіберзлочинів кіберполіцією є те, що про більшість із них КК України текстуально (буквально) не згадує взагалі. За суттю, такі суспільно небезпечні прояви можуть бути формами або способами вчинення конкретних злочинів. Наприклад, «онлайншахрайство» є формою вчинення шахрайства як злочину проти власності, що здійснюється шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК України), а «рефайлінг» – лише способом вчинення несанкціонованого втручання в роботу мереж електрозв'язку (телекомунікаційних мереж), тобто злочину, передбаченого ст. 361 КК України [603].

У нормативному плані відомо, що з 1985 по 1989 рр. Комітет експертів Ради Європи з проблем злочинності, пов'язаної з комп'ютерами, виробив Рекомендацію № (89) 9, затверджену Комітетом Міністрів ЄС 13 вересня 1989 р., в якій містився список правопорушень, рекомендований країнам – учасницям ЄС для розробки єдиної карної стратегії, пов'язаної з комп'ютерними злочинами. Також в документі відмічена необхідність досягнення міжнародного консенсусу з питань криміналізації деяких злочинів, пов'язаних з комп'ютерами. Згадана Рекомендація містить два списки злочинів – «мінімальний» і «факультативний (додатковий)». До «мінімального» списку потрапили діяння, які обов'язково мають бути заборонені міжнародним законодавством і підлягають переслідуванню в судовому порядку. «Додатковий» список містив ті правопорушення, по яких досягнення міжнародної згоди уявляється складним завданням [604].

---

[601] Савінова Н. А. Кримінально-правова політика забезпечення інформаційного суспільства в Україні: автореф. дис. … д-ра юрид. наук: спец. 12.00.08. Львів, 2013. С. 19–23.

[602] Аваков Арсен. Кіберполіція (крок реформі): 11 жовт. 2015 р. URL: http://blogs.pravda.com.ua /authors/avakov/561a92c183c27/ (дата звернення: 02.05.2019).

[603] Савченко А. В. Воробей П. А., Бельський Ю. А. Рефайлінг (ре файл) як спосіб вчинення несанкціонованого втручання в роботу мереж електрозв'язку. *Юридична наука.* 2018. № 1. С. 149–165.

[604] European committee on crime problems (1990) «Computer-related crime. Recommendation No. R (89) 9 on computer-related crime and final report of European committee on crime problems». Stasbourg 1990. 60 p.

У Конвенції (Ради Європи) про кіберзлочинність від 23 листопада 2001 року (розділ ІІ – Заходи, які мають здійснюватися на національному рівні, частина 1 – Матеріальне кримінальне право) розрізняються такі кримінальні правопорушення, що спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ (ст. 2); нелегальне перехоплення (ст. 3); втручання у дані (ст. 4); втручання у систему (ст. 5); зловживання пристроями (ст. 6);

2) правопорушення, пов'язані з комп'ютерами: підробка, пов'язана з комп'ютерами (ст. 7); шахрайство, пов'язане з комп'ютерами (ст. 8);

3) правопорушення, пов'язані зі змістом: правопорушення, пов'язані з дитячою порнографією (ст. 9);

4) правопорушення, пов'язані з порушенням авторських та суміжних прав: правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10).

Крім того, в межах додаткової відповідальності та санкцій у ст. 11 «Спроба і допомога або співучасть» зазначено, що держави-члени Ради Європи та інші держави, що підписали цю Конвенцію, мають вжити такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за:

1) умисну допомогу чи співучасть у вчиненні будь-якого зі злочинів, перерахованих у ст.ст. 2–10 цієї Конвенції, з метою вчинення такого злочину (ст. 11);

2) умисну спробу вчинити будь-який зі злочинів, перерахованих у ст.ст. 3–5, 7, 8, 9.1.a та 9.1.c цієї Конвенції (проте вимога у п. 2 не є обов'язковою для підписантів). Також ця Конвенція встановлює вимоги щодо корпоративної відповідальності (ст. 12) та санкцій і заходів (ст. 13) [605].

Крім того, 28 січня 2003 р. до цієї Конвенції було ухвалено Додатковий протокол, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, в якому положення Частини ІІ «Заходи, які мають вживатися на національному рівні» передбачають криміналізацію таких дій: поширення расистського та ксенофобного матеріалу через комп'ютерні системи (ст. 3); погроза з расистських та ксенофобних мотивів (ст. 4); образа з расистських та ксенофобних мотивів (ст. 5); заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства (ст. 6); пособництво та підбурювання у згаданих злочинах (ст. 7) [606].

Слід зазначити, що Україна ратифікувала цей Додатковий протокол з таким застереженням: «Україна заявляє, що відповідно до підпункту «а» пункту 2 ст. 6 Додаткового протоколу вона вимагатиме, щоб заперечення чи значна мінімізація, про які йдеться в пункті 1 цієї статті, були вчинені з наміром підбурити до ненависті, дискримінації чи насильства проти будь-якої особи чи групи осіб на підставі ознак раси, кольору шкіри, національного чи етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій» [607].

Порівняльний аналіз Конвенції про кіберзлочинність та КК України дає підстави стверджувати, що переважна кількість діянь, передбачених нею, визнається злочинами в українському законодавстві, зокрема: нелегальне перехоплення (ст.ст. 163, 361, 362 КК України); втручання в дані (ст.ст. 361, 362 КК України); втручання в систему (ст. 361 КК України); злочини, пов'язані з дитячою порнографією (ст. 301 КК України); підробка, пов'язана з комп'ютерами (ст.ст. 358, 366 КК України), шахрайство, пов'язане з комп'ютерами (ч. 3 ст. 190 КК України).

---

[605] Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року (Конвенцію ратифіковано Україною із застереженнями і заявами Законом № 2824-IV від 7 верес. 2005 р.). URL: http://zakon2.rada.gov.ua/laws/show/994_575 (дата звернення: 05.05.2019).

[606] Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (Протокол ратифіковано Україною із застереженнями Законом № 23-V від 21 лип. 2006 р.). URL: http://zakon2.rada.gov.ua/laws/show/994_687 (дата звернення: 05.05.2019).

[607] Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: Закон України № 23-V від 21 лип. 2006 р. URL: http://zakon2.rada.gov.ua/laws/show/23-16 (дата звернення: 06.05.2019).

Діяння, передбачені Додатковим протоколом до Конвенції про кіберзлочинність, охоплюються ст. 161 КК України, де встановлена відповідальність за порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками, та нормами, що передбачають відповідальність за злочини проти свободи совісті (ст.ст. 178–181 КК України) та злочини проти миру, безпеки людства та міжнародного правопорядку (ст. 442 КК України).

Водночас сьогодні наявна ситуація, за якої національне законодавство про кримінальну відповідальність за незаконний доступ не повною мірою відповідає ратифікованій Україною Конвенції про кіберзлочинність. Так, незаконний доступ за цією Конвенцією (ст. 2) вважається закінченим з моменту вчинення діяння, тобто є формальним складом злочину, та полягає в умисному доступі до цілої комп'ютерної системи або її частини без права на це. У КК України відповідальність за незаконний (несанкціонований) доступ (ст. 361) може наставати лише тоді, коли він призвів до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, а отже виходить, що несанкціонований доступ сам по собі, без настання вказаних наслідків, не є злочином (зазначимо, що терміни «несанкціонований» та «незаконний» не є тотожними, відтак поняття «несанкціонований доступ» є ширшим за поняття «незаконний доступ» та повністю його охоплює). Такі дії не є настільки суспільно небезпечними, щоб їх слід було б криміналізувати, а тому їх доречно розглядати в межах адміністративної відповідальності.

Проте Конвенцією про кіберзлочинність передбачена можливість криміналізації замість простого несанкціонованого доступу іншого діяння – «незаконного (несанкціонованого) доступу, вчиненого шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою». Вказане діяння, без сумніву, вже є достатньо суспільно небезпечним і може підлягати криміналізації, оскільки: по-перше, для подолання заходів інформаційної безпеки, технічного або програмного характеру необхідні спеціальні знання, навички, вміння й досвід, що свідчить про підвищену суспільну небезпечність суб'єкта даного злочину; по-друге, шкода від цього діяння полягатиме в істотних матеріальних збитках, зумовлених необхідністю відновлення або заміни системи комп'ютерного захисту.

Аналогічний підхід має бути застосований і до положень ст. 362 КК України. Зокрема доцільно було б склад несанкціонованого перехоплення або копіювання комп'ютерної інформації (ч. 2 ст. 362 КК України) визначити як формальний та визнавати несанкціоноване перехоплення або копіювання злочинними з моменту вчинення самих дій, що забезпечить імплементацію зобов'язань з приводу криміналізації нелегального перехоплення відповідно до ст. 3 Конвенції про кіберзлочинність, де склад цього злочину визначено як формальний. Крім цього, доречно у ст. 362 КК України визначити суб'єкта злочину в якості загального, що усуне суперечність між цією нормою та ст.ст. 3 і 4 Конвенції про кіберзлочинність. Вчинення цього злочину спеціальним суб'єктом можна було б розглядати як кваліфікуючу ознаку у ст. 362 КК України.

Найбільш типовими кіберзлочинами є злочини, передбачені ст.ст. 361–363-3 розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України, при цьому їх ретельний аналіз дається в юридичній літературі [608].

Разом з тим, перелік кіберзлочинів не вичерпується діяннями, зазначеними у розділі XVI Кримінального кодексу. Певні злочини, які існували задовго до створення комп'ютерів, також можуть бути вчинені із застосуванням сучасних інформаційних технологій. При цьому використання комп'ютерів зазвичай спрощує вчинення злочину або уможливлює його вчинення в нових формах. Отже, ці злочини можна розглядати як такі, що підпадають під дію Конвенції про кіберзлочинність. Зокрема, йдеться про наступні злочинні діяння:

– різні види підробки: грошей, цінних паперів, платіжних карток, знаків поштової оплати, марок акцизного збору, контрольних марок, номерів вузлів та агрегатів

[608] Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України». Станом на 1 січня 2019 року / М. В. Гуцалюк та ін.; за ред. М. В. Гребенюка. Київ: Нац. акад. прокуратури України, 2019. 220 с.

транспортних засобів, документів на отримання наркотиків, інших документів тощо (ст.ст. 199, 200, 215, 216, 224, 290, 318, 358, 366 КК України);

– шахрайство з різними предметами (ст.ст. 190, 192, 222, 262, 308, 312, 313, 357, 410 КК України);

– ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України);

– порушення авторського права і суміжних прав (ст. 176 КК України).

Відповідність між статтями Конвенції про кіберзлочинність та статтями Кримінального кодексу України на семантичному рівні надано в таблиці 19.1.

Таблиця 19.1

Номер статті Конвенції	**Зміст статті Конвенції**	**Відповідність статтям КК України**
Злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем		
2	Протизаконний доступ	Статті 361, 363
3	Протизаконне перехоплення	Статті 362, 363
4	Вплив на дані	Статті 361, 362, 3631
5	Вплив на функціонування системи	Статті 361, 3611, 362, 363, 3631
6	Протизаконне використання пристроїв та комп'ютерних програм	Статті 3611, 362, 363
Злочини, пов'язані з використанням комп'ютерних засобів		
7	Підробка з використанням комп'ютерних технологій	Статті 199, 200, 215, 216, 224, 290, 318, 358, 366
8	Шахрайство з використанням комп'ютерних технологій	Статті 190, 192, 222, 262, 308, 312, 313, 357, 410
Злочини, пов'язані зі змістом даних		
9	Злочини, пов'язані з дитячою порнографією	Стаття 301
Злочини, пов'язані з порушенням авторського права та суміжних прав		
10	Злочини, пов'язані з порушенням авторського права та суміжних прав	Стаття 176

Водночас в Україні передбачено кримінальну відповідальність й за інші діяння, що можуть бути вчинені шляхом застосування інформаційних технологій, проте відсутні в тексті Конвенції про кіберзлочинність.

Можна виділити три групи цих діянь. До першої слід віднести злочини, які полягають у незаконному придбанні та (або) збуті предметів, заборонених для вільного обігу, і можуть бути вчинені із використанням мережі Інтернет:

– незаконне придбання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307 КК України);

– незаконне придбання чи збут вогнепальної зброї, бойових припасів, вибухових речовин; збут холодної зброї (ст. 263 КК України);

– придбання радіоактивних матеріалів (ст. 265 КК України).

До другої групи діянь належать злочини, пов'язані зі змістом даних (контентом). Конвенція розуміє під незаконним контентом дитячу порнографію.[609] Разом з тим, законодавство України дозволяє вважати злочином розміщення в Інтернеті також інформації іншого характеру, а саме:

– відомостей, що становлять державну або іншу таємницю, яка охороняється законом: незаконне розголошення лікарської таємниці (ст. 145 КК України), порушення таємниці голосування (ст. 159), розголошення таємниці усиновлення (удочеріння) (ст. 168), розголошення комерційної таємниці (ст. 232), розголошення державної таємниці (ст. 328), несанкціоноване розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 3612), розголошення відомостей про заходи безпеки щодо

[609] Окремим протоколом до конвенції охоплюється також расизм та ксенофобія.

особи, взятої під захист (ст. 381), розголошення даних досудового слідства та дізнання (ст. 387), розголошення відомостей військового характеру, що становлять державну таємницю (ст. 422);

– завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259 КК України);

– закликів до вчинення дій, що загрожують громадському порядку (ст. 295 КК України);

– пропаганди расової, національної, релігійної нетерпимості (ст. 161), культу насильства і жорстокості (ст. 300) або війни (ст. 436 КК України).

До третьої групи діянь слід віднести легалізацію (відмивання) грошових коштів, здобутих злочинним шляхом (ст. 209 КК України). Для цього злочинці застосовують послуги електронних банків, надають рахунки на завищені або занижені суми, беруть участь у кібераукціонах тощо.

Слід зауважити, що деякі положення Конвенції про кіберзлочинність не знайшли відображення у вітчизняному законодавстві про кримінальну відповідальність. Так, КК Україні не передбачає кримінальної відповідальності за:

– придбання шкідливих комп'ютерних програм та пристроїв, створених чи адаптованих для вчинення комп'ютерних злочинів (п. «a I» ч. 1 ст. 6);

– виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми надання у користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому чи будь-якої її частини з наміром використати їх з метою вчинення комп'ютерних злочинів (п. «a II» ч. 1 ст. 6);

– володіння вище зазначеними шкідливими комп'ютерними програмами, пристроями, комп'ютерними паролями, кодами доступу чи іншими аналогічними даними (п. «b» ч. 1 ст. 6);

– придбання дитячої порнографії через комп'ютерну систему (п. «d» ч. 1 ст. 9);

– володіння дитячою порнографією, що перебуває в комп'ютерній системі чи на носіях комп'ютерних даних (п. «e» ч. 1 ст. 9).

Запровадження кримінальної відповідальності за більшість з вказаних діянь кожна держава – учасник Конвенції про кіберзлочинність має право визначати самостійно. Тому питання щодо необхідності криміналізації цих діянь має визначатися ступенем їхньої суспільної небезпеки в умовах України та кримінологічними характеристиками: рівнем, динамікою тощо. Водночас, питання щодо криміналізації діянь, передбачених пунктом «a II» ч. 1 ст. 6 конвенції, має вирішуватися із урахуванням змісту ч. 3 ст. 6 цього міжнародного документу, що контекстуально зобов'язує всіх держав-учасників ввести кримінальну відповідальність за продаж, оптовий продаж чи інші форми надання у користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути вчинений комп'ютерний злочин.

На X Конгресі ООН по боротьбі із транснаціональною організованою злочинністю (Відень, 2000) було запропоновано класифікацію кіберзлочинів за ознакою насильства. Згідно з цим критерієм кіберзлочини поділяють на:

– насильницькі або інші потенційно небезпечні (загроза фізичної розправи, кіберпереслідування, дитяча порнографія, кібертероризм);

– ненасильницькі (протиправне порушення володіння в кіберпросторі, кіберзлодійство, кібершахрайство, реклама послуг проституції в мережі інтернет, незаконний обіг наркотиків із використанням мережі інтернет, азартні ігри у мережі інтернет, відмивання грошей за допомогою їх електронного переміщення, деструктивні кіберзлочини, інші кіберзлочини).

За класифікатором Інтерполу кіберзлочини поділяють на такі групи:

– несанкціонований доступ та перехоплення (QA);

– зміна комп'ютерних даних (QD);

– комп'ютерне шахрайство (QF);

– незаконне копіювання (QR);

– комп'ютерний саботаж (QS);

– інші комп'ютерні злочини (QZ).

Швидкий розвиток інформаційних технологій призводить до появи нових видів послуг у сфері зв'язку, торгівлі, фінансів, розваг тощо. Відповідно, злочинці винаходять нові способи вчинення соціально небезпечних діянь із застосуванням інформаційних мереж та систем. Тому перелік кіберзлочинів не є вичерпним і постійно поповнюється. Останніми роками як в Україні, так і в світі з'являються нові види злочинів, вчинення яких передбачає застосування новітніх інформаційних технологій.

§ 3. Причини та умови кіберзлочинності

В останнє десятиліття XX – на початку XXI ст. на світовій арені відбулися суттєві зміни, які протягом тривалого часу визначатимуть головні напрями розвитку людства. Внаслідок глобальних трансформацій формуються принципово нові риси світового порядку, а міжнародні процеси проявляються у вигляді суперечливих тенденцій, постійно виникають нові виклики і загрози міжнародній безпеці [610]. Інтенсивна інтеграція України в світові соціально-політичні та економічні інституції обумовлює її не менш інтенсивну інтеграцію у світовий інформаційний простір. Активне використання країнами інформаційних систем та користування інформаційними ресурсами (як спільними так й власними), запровадження та користування відповідними технологіями в умовах глобалізації обумовлює необхідність активної участі у політико-правовому регулюванні даних процесів з боку кожної країни.

З точки зору політичних процесів і політичних чинників поява кіберзлочинності та її зростання обумовлені відсутністю адміністративно-територіальних й інших меж в глобальних інформаційних мережах, неузгодженістю позицій урядів різних держав з питань вільного розповсюдження інформації і дотримання прав і інтересів особи, комерціалізація політичної діяльності. Також процес досягнення політичної згоди в питаннях, що стосуються кіберзлочинності ускладнюється різними уявленнями держав про те, які дії є кіберзлочинами і потребують кримінально-правової заборони, у тому числі і уявленнями про морально-етичну сторону діянь [611]. Сьогодні кіберпростір, як п'ятий загальний простір, після наземного, морського, повітряного і космічного, вимагає координації, співпраці і особливих правових заходів на міжнародному рівні. Проте, на жаль, ефективні заходи міжнародного масштабу з боротьби з кі-берзлочинцями відсутні, що створює певний вакуум в правовому регулюванні відповідальності і порядку кримінального переслідування осіб, що вчинили транснаціональні злочини, і, відповідно, викликає у кіберзлочинців уявлення про можливість уникнути кримінальної відповідальності [612].

Необхідною умовою розвитку інформаційного суспільства є забезпечення належного рівня кібернетичної безпеки. На відміну від провідних країн світу, у яких вже сформовані загальнодержавні системи кібернетичної безпеки, в Україні сьогодні відбувається процес формування такої системи. Слід зазначити, що вказане положення справ значною мірою обумовлене й самим станом розвитку інформаційного суспільства. Так, як зауважують фахівці, якщо у світі вже замислюються про наслідки, визначають тенденції та прогнозують перспективи, то в Україні переважно доводиться надавати аргументи на захист існування та визнання кібервіртуальної компоненти соціального простору, її специфіки та соціальних особливостей [613]. Як свідчить сучасний стан інформаційної складової життя нашого суспільства, за останні роки ситуація суттєво не змінилася.

Кібернетична ж безпека країни забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих з установленому порядку доктрин, концепцій, стратегій і програм.

В Україні сьогодні, на жаль, відсутня єдина державна стратегія кібернетичної безпеки, немає відповідної розвиненої нормативно-правової бази та заточеної на її створення політичної волі. Ця стратегія, як слушно вказують фахівці, повинна бути вбудована у розвиток Доктрини інформаційної безпеки України. Вона має визначати мету і головні пріоритети діяльності держави у цій сфері, а також коротко-, середньо– і довгострокові цілі, методи їх досягнення; стратегічні завдання та засоби зменшення уразливості об'єктів

---

[610] Мала енциклопедія міжнародної безпеки / Нац. акад. наук України, Київ, ун-т права ; за заг. ред. проф., засл. юриста України Ю. Л. Бошицького, д-ра іст. наук О. В. Потєхіна. Київ: Європ. ун-т, 2012. С. 10.

[611] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08 / Тропина Татьяна Львовна; Дальневосточный государственный университет. Владивосток, 2005. С. 111.

[612] Косенков А. Н., Черный Г. А. Общая характеристика психологии кибер-преступника. *Криминологический журнал Байкальского государственного университета экономики и права.* 2012. № 3. С. 87–94 URL: http://cj.isea.ru/pdf.asp?id= 13288.

[613] Петренко-Лисак А. О. Соціальні детермінанти кібервіртуального простору: автореф. дис. ... канд. соц. наук. Київ, 2007. 24 с. С. 3.

критичної інфраструктури у національному кібернетичному просторі; основні напрями, підходи та методи забезпечення кібернетичної безпеки України.

Саме у Стратегії кібернетичної безпеки України доцільно передбачити основні напрями державної політики з питань кібернетичної безпеки України, а саме: забезпечення суверенітету України у кіберпросторі, наповнення кіберпростору достовірною інформацією про Україну; створення сприятливих зовнішньополітичних умов для прогресивного розвитку національного сегменту кіберпростору; запобігання втручанню у внутрішні справи України і відвернення посягань на її Інтернет-ресурси з боку інших держав; забезпечення повноправної участі України в загальноєвропейській та регіональних системах кібернетичної безпеки; участь України в міжнародному співробітництві у сфері боротьби з кіберзлочинністю та кібертероризмом; зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби у кіберпросторі з проявами організованої злочинності та кібертероризму; боротьба з організованими злочинними угрупованнями, в тому числі міжнародними, які намагаються діяти у національному сегменті кіберпростору; забезпечення максимальної ефективності Збройних Сил України у кіберпросторі та їх здатності давати адекватну відповідь реальним і потенційним кібернетичним загрозам Україні; запобігання проявам екстремізму в національному сегменті кіберпростору; посилення державної підтримки розвитку пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій; забезпечення необхідних умов для реалізації прав інтелектуальної власності у національному сегменті кіберпростору; створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури і ресурсів. Ідеї Стратегії кібернетичної безпеки України повинні отримати розвиток у положеннях базового закону в цій сфері, а також змінах і доповненнях до інших законів України, що регулюють відносини у сфері кібернетичної безпеки [614].

Недостатня політична воля керівництва країни щодо регулювання інформаційних відносин та запобігання кіберзагрозам, в тому числі кіберзлочинності, інтенсивність розвитку інформаційного простору (усіх його складових: інформаційних систем, ресурсів, технологій тощо) та транскордонний характер відповідних відносин обумовлюють відставання правової бази протидії кіберзлочинності як на національному, так й на міжнаціональному рівні. При цьому це стосується правових норм, що визначають міжнародні засади протидії кіберзлочинності, так й правового регулювання процесу виявлення, розкриття та розслідування (від збору і фіксації доказів до судового переслідування, екстрадиції підозрюваних, засуджених осіб) кіберзлочинів.

Відсутність належного кримінально-правового регулювання в результаті недосягнення згоди на міжнародному рівні є одним з суттєвих чинників зростання кіберзлочинності. Оскільки електронні посягання є проблемою транскордонною за своєю природою, правові основи боротьби з цим явищем повинні розроблятися на міждержавному рівні. Тим часом, наразі, законодавство різних країн світу є суперечливим: відсутній одноманітний понятійний апарат, зокрема у визначенні кіберзлочинів, не закріплено на міжнародному рівні, які діяння повинні переслідуватися відповідно до кримінального законодавства [615]. Хоча чинне у більшості країн кримінальне законодавство є достатньо гнучким, щоб кваліфікувати правопорушення цього типу, соціальні і технічні зміни створюють все нові і нові проблеми. Тому деякі з відомих світовій практиці комп'ютерних посягань не підпадають під дію кримінального законодавства і в юридичному сенсі не можуть вважатися злочинними [616].

---

[614] Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. № 1 (27). С 314–315.

[615] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08 / Тропина Татьяна Львовна; Дальневосточ. гос. ун-т. Владивосток, 2005. С. 112–113.

[616] Криминальная психология: учеб. пособие / авт.-сост.: А. И. Ушатиков, О. Г. Ковалев ; Российская акад. образования, Московский психолого-социальный ин-т. Москва: Моск. психолого-социальный ин-т; Воронеж: МОДЭК, 2007. С. 375.

Також відчувається відсутність належного цивільно-правового регулювання відносин у сфері високих технологій, що також; створює прогалини в законодавстві, що дозволяють злочинцям уникати відповідальності, а безкарність, у свою чергу, провокує зростання посягань [617].

Щодо вад національного законодавства, то поширенню кіберзлочинності та ускладненню запобігання їй сприяють проблеми правового забезпечення системи кібернетичної безпеки України, обумовлені, перш за все, відсутністю чітко розробленого та нормативно закріпленого понятійного апарата у сфері кібернетичної безпеки.

Так, недоліки понятійного апарата у сфері забезпечення кібернетичної безпеки не дозволяють: визначити ознаки та об'єктивно оцінити основні загрози у національному сегменті кіберпростору; визначити найбільш ефективні заходи забезпечення кібернетичної безпеки; чітко сформулювати завдання та функції суб'єктів кібернетичної безпеки тощо. У законодавстві відсутнє визначення не тільки поняття «кібернетична безпека (кібербезпека)», але й таких ключових понять як «кібернетичний простір (кіберпростір)», «кібернетична загроза (кіберзагроза)», «кібернетична атака (кібератака)», «кібернетичний захист (кіберзахист)», «кібернетичний злочин (кіберзлочин)», «кіберзлочинність» тощо. Визначення зазначених термінів передбачає їх широкого розуміння, враховуючи вже наявні напрацювати у таких галузях науки як кібернетика, інформатика, безпекознавство, кримінальне право тощо [618].

Отже, сьогодні Українській державі бракує ефективних системних заходів щодо протидії кіберзлочинам. Відсутність належної теоретичної основи та законодавчої бази не сприяє ефективній боротьбі з цими посяганнями. Разом з тим низка розвинених країни світу проблемі комп'ютерних злочинів приділяють значну увагу. Ними розроблені пакети відповідних законодавчих актів, діють національні програми боротьби із зазначеними посяганнями. Брак належного нормативно-правового забезпечення протидії комп'ютерним злочинам обтяжується відсутністю системності у законотворенні. Відсутність належного теоретико-правового забезпечення у зазначеній сфері суттєво ускладнює застосування відповідних кримінально-правових норм, нерідко призводить до прийняття суперечливих рішень у слідчій та судовій практиці [619].

У механізмі детермінації кіберзлочинності можна умовно виділити такі групи чинників: соціальні, політичні, економічні, технологічні, психологічні, а також чинники, пов'язані з діяльністю правоохоронних органів та віктимною поведінкою потерпілих.

Соціальні чинники виступають своєрідними передумовами функціонування та розвитку кіберзлочинності. Передусім це зміни в соціальному житті, породжені сучасним науково-технічним прогресом, пов'язані з усебічною комп'ютеризацією суспільства, а також формуванням інформаційного простору, заснованого на використанні комп'ютерної техніки, та зумовленого цим створенням і розвитком нових суспільних відносин у сфері комп'ютерної інформації. У зв'язку з цим багато сфер суспільної активності переходить у віртуальний простір, що не залишилось без уваги кримінального середовища та створило нові можливості для вчинення різноманітних злочинів за допомогою комп'ютерної техніки. Отже, кіберзлочинність виступає побічним продуктом так званої «техноревалюції».

Політичні чинники виявляються у недостатньому усвідомленні урядом можливих соціальних наслідків кіберзлочинності. У зв'язку з цим обмежуються бюджетні фінансування робіт зі створення правової, організаційної, технічної бази інформаційної безпеки держави та захисту прав і свобод громадян у віртуальному просторі. Фактично не виділяються кошти на фундаментальні та прикладні вітчизняні дослідження у сфері запобігання кіберзлочинності. Недостатня увага також приділяється правовому регулюванню комп'ютерної сфери, що на фоні її бурхливого неконтрольованого розвитку призводить до відставання правових норм від потреб суспільства в кіберпросторі.

---

[617] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08 / Тропина Татьяна Львовна; Дальневосточ. гос. ун-т. Владивосток, 2005. С. 113.

[618] Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. № 1 (27). С. 313.

[619] Музика А. А., Азаров Д. С. Законодавство України про кримінальну відповідальність за «комп'ютерні» злочини: наук.-практ. комент. і шляхи вдосконалення. Київ: Вид-во «Паливода А. В.», 2005. С. 8.

Економічні чинники проявляються у значній прибутковості кіберзлочинів. Повідомлення зарубіжних науковців свідчать, що кіберзлочинність за рівнем кримінального збагачення займає третє місце після торгівлі зброєю та наркотиками. За оцінками Рахункової палати уряду США, щорічний дохід злочинців тільки від розкрадань та шахрайств, вчинених із використанням комп'ютерних технологій через Інтернет, досягає 5 млрд дол. Ці показники щорічно збільшуються пропорційно зростанню у структурі національної та міжнародної економіки сектору торгівлі та надання послуг через електронні (комп'ютерні) засоби телекомунікації.

Технологічні чинники проявляються у технічній простоті вчинення кіберзлочинів. Навіть при наявності загальних знань у галузі системного адміністрування чи програмування можна отримати доступ до слабкозахищеної комп'ютерної мережі. Високопрофесійні ж хакери можуть оминути будь-який захист та замаскувати сліди вторгнення чи модифікації інформації. Негативною тенденцією є також поширення в мережі Інтернет ринку програм-вірусів, що надає можливості для вчинення кіберзлочинів зловмисникам, які не володіють комп'ютерними знаннями.

Психологічні чинники зумовлені особливостями функціонування віртуального простору. У реальному світі існують певні стримувальні засоби, а у віртуальному – злочинці не можуть бачити своїх жертв, яких вони вибрали для атаки. Красти у тих, кого ти не бачиш, до кого не можеш доторкнутися рукою, набагато легше. Немає фізичної шкоди, кровопролиття та інших атрибутів небезпеки. Злочини у мережі – це злочини на відстані. У зв'язку з цим у винних осіб є певне усвідомлення анонімності та відсутності безпосереднього ризику бути виявленим та притягнутим до кримінальної відповідальності.

Чинники, пов'язані з діяльністю правоохоронних органів, суттєво впливають на функціонування та розвиток кіберзлочинності. Назвемо деякі з них:

– відсутність спеціалізації при навчанні працівників правоохоронних органів, що призводить до їх непідготовленості до ефективного виявлення та розслідування кіберзлочинів;

– недосконаліть чинного законодавства про кримінальну відповідальність та кримінального процесуального законодавства;

– недостатня забезпеченість правоохоронних органів спеціальними технічними засобами виявлення та розслідування кіберзлочинів;

– технічна складність відстеження інформаційних загроз;

– слабкість координації дій у боротьбі з кіберзлочинністю правоохоронних органів та інших органів державної влади, а також відсутність ефективного міжнародного співробітництва з протидії кіберзлочинності;

– відсутність належної взаємодії між правоохоронними органами та приватним бізнесом із питань захисту комп'ютених мереж, надання необхідної інформації стосовно правопорушень у віртуальному просторі.

Чинники, пов'язані з віктимною поведінкою потерпілих, виявляються у відсутності в більшості населення належної культури безпечної поведінки у поводженні з комп'ютерною технікою. Зокрема, це економія жертвами на системах програмного і технічного захисту інформації (відсутність антивірусних програм, брандмауерів; недооцінка оновлення програм захисту; використання неліцензійного програмного забезпечення), порушення загальних правил роботи з інформацією в мережі (відсутність резервних копій важливої Інформації, порушення своєї анонімності, застосування виробничого комп'ютера для невідповідних цілей), ігнорування вимог, спрямованих на збереження конфіденційної інформації (відсутність локальних нормативних актів поводження з комп'ютерною технікою на підприємстві, відсутність нагляду за персоналом, що має доступ до важливої інформації, недосконаліть парольної системи захисту від несанкціонованого доступу до робочої станції та її програмного забезпечення, яка не передбачає достовірної ідентифікації користувача за індивідуальними біометричними параметрами), порушення інших правил (ведення публічного особистого життя), а також неповідомлення потерпілими про вчинення кіберзлочинів.

Характеризуючи дану групу детермінант, важливо звернути увагу на те, що специфічне середовище вчинення кіберзлочинів обумовлює також специфіку взаємозв'язків на рівні кібер-злочинець – жертва злочину.

Дистанційованість і «віртуалізація» шкоди, що заподіюється діями, що реалізовуються в кіберпросторі, обумовлює його специфічне уявлення жертвою злочину. З одного боку, жертва злочину, яка виявляє заподіяну їй «нематеріалізовану» шкоду, не в повній мірі усвідомлює її

характер і масштаби, відповідно, характер і ступінь суспільної небезпеки вчиненого відносно неї діяння. З іншого боку, жертва злочину часто нездатна в своїй свідомості адекватно сприйняти зв'язок заподіяної шкоди з конкретним (хай неперсоніфікованим) злочинцем. Отже, вчинений відносно неї злочин і заподіяна ним шкода, жертвою часто сприймається як абстрактне «зло», що не має перспективи бути виправленим.

У разі ж усвідомлення як кіберзлочинцем, так і жертвою злочину протиправності та суспільної небезпеки вчиненого діяння і його наслідків, специфіка взаємозв'язків на рівні кіберзлочинець – жертва злочину обумовлюється наступним. Як указують фахівці, парадоксальна особливість комп'ютерних злочинів полягає і в тому, що важко знайти інший вид злочину, після вчинення якого його жертва не виявляє особливої зацікавленості в пійманні злочинця, а сам злочинець, будучи спійманим, всіляко рекламує свою діяльність на терені комп'ютерного злому, мало що втаюючи від представників правоохоронних органів. Психологічно цей парадокс цілком пояснимий. По-перше, жертва комп'ютерного злочину абсолютно переконана, що витрати на його розкриття (включаючи втрати, понесені в результаті втрати своєї репутації) істотно перевершують вже заподіяний збиток. І по-друге, злочинець набуває широкої популярності в ділових і кримінальних колах, що надалі дозволяє йому з вигодою використовувати придбаний досвід [620].

Зазначимо, що це не вичерпний перелік причин та умов (детермінантів, факторів, чинників) кіберзлочинності, зважаючи на комплексність відповідних суспільних відносин. Доречно зауважити, що у спеціальній літературі окремі дослідники виділяють також організаційно-управлінські фактори (дана група факторів пов'язана, перш за все, з недоліками соціального контролю й управлінського процесу загалом, що в підсумку також зумовлює самодетермінацію кіберзлочинності як наслідок неможливості контролю над інформацією, що розміщується в глобальних інформаційних мережах) [621], культурно-психологічні фактори (за якими вчинення кіберзлочинів, як і злочинів інших видів, пов'язане з негативними наслідками зниження загального рівня культури та моральних критеріїв у суспільстві) [622] тощо.

Отже, інтенсивна інформатизація і глобалізація світу при відсутності ефективних механізмів економічного, політичного та правового регулювання (як на рівні окремих держав, так й на міжнаціональному рівні) цих процесів призводить до криміналізації значної частини їх складових. При цьому, чим нижче рівень економічного розвитку країни, політичного та правового забезпечення її інформаційної безпеки, тим вище рівень кіберзлочинності й кіберзагроз в цілому.

Слід також погодитися з фахівцями, що значне місце в детермінації кіберзлочинності займають психологічні процеси, що протікають при безпосередньому вчиненні кіберзлочину. На відміну від переважної більшості звичайних злочинів, вчинення кіберзлочину не вимагає, як правило, яких-небудь пересувань або здійснення яких-небудь активних фізичних дій. Кіберзлочинець при реалізації свого злого наміру знаходиться удома, в комп'ютерному клубі, місці з безкоштовним доступом в Інтернет, будь-якому іншому місці, яке для нього є комфортним або, принаймні, знайомим і звичним. Тому кіберзлочинці можуть не відчувати, або відчувати в значно меншому ступені, дискомфорт, страх бути випадково виявленим і затриманим. Хоча кіберпростір і є багатогранним соціальним простором, в той же час він залишається штучно створеним програмно-апаратним середовищем, діяльність в якому все-таки обмежена технічними рамками, що робить передбаченими наслідки дій. Це, у свою чергу, дозволяє зловмисникові не відчувати невизначеності ситуації, планувати свої дії навіть при несприятливих для нього обставинах,

---

[620] Криминальная психология: учебное пособие / авт.-сост.: А. И. Ушатиков, О. Г. Ковалев ; Российская акад. образования, Московский психолого-социальный ин-т. Москва: Моск. психолого-социальный ин-т; Воронеж: МОДЭК, 2007. С. 375.

[621] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук: 12.00.08 / Тропина Татьяна Львовна; Дальневосточ. гос. ун-т. Владивосток, 2005. С. 113.

[622] Кудрявцев В. Н. Генезис преступления: опыт криминол. моделирования: учеб. пособие для вузов. Москва: ИНФРА-М, 1998; Кудрявцев В. Н., Эминов В. Е. Причины преступности в России: криминологический аналіз. Москва: Норма, 2006.

а отже, відчувати себе впевненіше і спокійно під час вчинення злочину [623]. Саме ці особливості обумовлюють умисний характер кіберзлочинів. У свою чергу, дані особливості обстановки вчинення кіберзлочинів повинні враховуватися правоохоронними органами при розробці відповідних методик і практичної реалізації заходів по виявленню, припиненню, розслідуванню злочинних діянь даної категорії, запобігання їх поширенню.

§ 4. Характеристика осіб, які вчиняють кіберзлочини

Перейдемо тепер до класифікації осіб, які вчиняють кіберзлочини. Сучасний рівень технологій сприяє тому, що хакери спеціалізувалися у окремих напрямах. Така спеціалізація дає можливість виділити в загальній масі хакерів «групи за інтересами», наприклад «крекеров» (cracker) – спеціалістів по обминанню механізмів безпеки; «кранчеров» (cruncher) – спеціалістів по знаттю з програмного забезпечення захисту від копіювання; «крешеров» (crasher) – любителі активно експериментувати з комп'ютерною системою з метою дослідження можливостей управління нею.

Залежно від предмету діяльності, хакерів можна поділити на три групи:

Software hackers, чи софтверні хакери, займаються тим, що «ламають» («зламують») програмне забезпечення. Це навіть сам багато численна група хакерів, і шкода від діяльності цих людей вимірюється мільйонами доларів.

Phreks. По визначенню фрікер – це особа, що надає перевагу «альтернативним» способам оплати теле – та інших комунікаційних послуг (наприклад, заставить заплати за телефон сусіда замість себе, якщо на телефоні стоїть блокіратор). В останній час серед фрікерів з'явився новий прошарок – carders. Кардери – це особи, які перепраграмовують телефонні чіпи таким чином, що на карті відкривається практично безмежний кредит на телефонні розмови. Це, мабуть, найбільш небезпечна частина фрікерів. Вони мають глибокі знання у галузі радіоелектроніки та програмування мікросхем. Оскільки кардери потенційно можуть принести велику шкоду, за їх діями уважно слідкують спеціальні служби.

Net hackers. Ця група осіб відділилася від фрікерів, коли почали активно розвиватися технології у мережах. Мережевий хакер повинен дуже добре розбиратися у мережах зв'язку та способах їх захисту. Мережеві хакери зламують захист серверів Інтернет, атакують державні та корпоративні інформаційні системи. Мета атак може бути різною, навіть до промислового шпіонажу за замовленням конкуруючих кампаній.

Зломщики програмного забезпечення. Найбільш численна категорія. Основними видами діяльності є: зняття захисту з комерційних версій програмних продуктів, виготовлення регістраційних ключів для умовно-безкоштовних програм тощо.

Розробники комп'ютерних вірусів. Найбільш небезпечна категорія хакерів. Постраждати від їх діяльності може будь-який користувач комп'ютерних систем. Розповсюджують віруси різноманітними способами. В останні роки частіше за все розповсюдження проходить через електронну пошту.

Особистість є об'єктом дослідження багатьох, у тому числі юридичних наук – філософії, соціології, психології, кримінології тощо. У кримінології вивчення про особистість злочинця підпорядковано виявленню закономірностей злочинної поведінки, індивідуального рівня її детермінації та розробці науково обґрунтованих превентивних рекомендацій [624]. Отже, кримінологічне дослідження особистості злочинця має виключне значення для забезпечення повноти пізнання феномену злочинності та, відповідно, розробки заходів запобігання.

З огляду на те, що особистість людини, яка вчиняє злочин, є центральною віссю у механізмі злочинної поведінки, без врахування особистості злочинця не можуть бути встановлені і зрозумілі як причини окремого злочину, так і причини злочинності в

---

[623] Косенков А. Н., Черный Г. А. Общая характеристика психологии кибер-преступника. *Криминологический журнал Байкальского государственного университета экономики и права*. 2012. № 3. С. 87–94. URL: http://cj.isea.ru/pdf.asp?id= 13288.

[624] Криминология: учеб. для вузов / авт. кол.: А. И. Алексеев, Ю. Н. Аргунова, С. В. Ванюшкин и др.; под общ. ред. А. И. Долговой. Москва: Норма – Инфра-М, 2001. С. 274.

цілому [625]. Для кримінології головне в особистості – джерела, шляхи, форми і механізми формування її антисуспільних рис, ті особливості, які у взаємодії із середовищем або злочинною ситуацією, породжують злочинну поведінку, іншими словами все те в злочинці, що входить у причинний комплекс злочину [626]. Крім того, саме досліджуючи особистість злочинця, можна визначити ті кримінологічно значущі характеристики середовища, які іноді важко (або неможливо) виявити іншим шляхом [627].

Складність досліджуваного питання обумовлює численність та різноманіття поглядів як щодо визначення самого поняття особистості злочинця, так і щодо його змісту, тобто структури особистості злочинця, її елементів. Ми приєднуємося до погляду на визначення особистості злочинця як сукупності істотних і стійких суспільно значущих біосоціальних ознак, особливостей індивіда, які, реалізуючись у прийнятті рішення про вчинення злочину, його реалізації, наділяють винну особу властивістю суспільної небезпечності, у зв'язку з чим вона притягується до відповідальності, передбаченої законом про кримінальну відповідальність [628] та становить об'єкт запобіжного впливу на індивідуальному та спеціально-кримінологічному (щодо групи осіб з типовими антисуспільними рисами) рівнях. В свою чергу особистість злочинця є цілісним утворенням, що складається з декількох елементів (складових частин), сукупність яких, через певні зв'язки, знаходячись у взаємодії між; собою, формує її структуру. Відповідні складові групуються, утворюючи самостійні блоки-групи ознак і властивостей: соціально-демографічні ознаки; особистісно-рольові особливості; соціально-психологічні якості; риси правової і моральної свідомості; психологічні відхилення і аномалії; кримінально-правові ознаки; загальнозначущі позитивні людські якості [629].

Сьогодні кіберзлочинцям вченими надаються неоднозначні соціально-психологічні характеристики, які засноваш на узагальнених емпіричних даних, оскільки сам предмет розгляду недостатньо вивчений з причин специфічності й складності цих злочинів [630]. Як зазначає Д. С. Азаров, на жаль, вітчизняна кримінологія не має у своєму арсеналі даних узагальнюючого характеру щодо особи цих злочинців, майже відсутні публікації з цього приводу. А окремі характеристики «комп'ютерного злочинця» (як то: вік – 24–25 років (середній вік – 30 років); за освітою – інженер в галузі електроніки і математики, займає відповідальну посаду (віце-президент компанії, фінансові керівники, скарбники, вкладники капіталів тощо); можуть не мати ніякої технічної освіти; не мають кримінального минулого; більшість становлять чоловіки, але можуть зустрічатися й жінки; у цілому це яскрава, думаюча, творча особа, професіонал своєї справи, готовий прийняти технічний виклик, бажаний працівник [631]), як справедливо зауважує вчений, є поверхневими, суперечливими та емпірично необґрунтованими [632].

Враховуючи те, що індивідуальний підхід в пізнанні особистості злочинця повинен поєднуватись із дослідженням сукупності всіх осіб, які вчинили злочин, на статистичному рівні [633], з метою виявлення специфічних особливостей та статистичних закономірностей

---

[625] Сахаров А. Б. О личности преступника и причинах преступности в СССР. Москва: Госюриздат, 1961. С. 10.

[626] Антонян Ю. М. Изучение личности преступника: учеб. пособие. Москва: ВНИИ МВД СССР, 1982. С. 11.

[627] Кваша О. О. Організатор злочину кримінально-правове та кримінологічне дослідження: монографія. Київ: Ін-т держави і права ім. В. М. Корецького, 2003. С. 121.

[628] Даньшин И. Н. К вопросу о личности пре ступника. *Проблемы социалистической законности.* 1980. Вып. 6. С. 125.

[629] Кримінологія: Загальна та Особлива частини / І. М. Даньшин, В. В. Голіна, О. Г. Кальман, О. В. Лисодєд; за ред. І. М. Даныпина ; Нац. юрид. акад. України ім. Ярослава Мудрого. Харків: Право, 2003. С. 166.

[630] Борисова Л. В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права.* 2008. Вип. 44. С. 78.

[631] Біленчук П. Д. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: навч. посіб. / П. Д. Біленчук, М. А. Зубань ; Українська академія внутрішніх справ. Київ, 1994. С. 15–16.

[632] Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: дис. ... канд. юрид. наук: 12.00.08. НАН України; Інститут держави і права ім. В. М. Корецького. Київ, 2002. С. 134–135.

[633] Антонян Ю. М. Изучение личности преступника: учеб. пособие. Москва: ВНИИ МВД СССР, 1982. С. 53; Яковлев С. В., Гнусов Ю. В. Математические методы оценки состояния и прогнозирования преступности. Харків: Ун-т внутр. дел, 1998. С. 18.

щодо відповідних кримінологічно значущих ознак особистості кіберзлочинців, нами проаналізовані статистичні дані Державної судової адміністрації України про осіб (у кількості 359), засуджених за злочини досліджуваного виду. Ці дані відображають результати розгляду судами України кримінальних справ та проваджень за статтями 361–363-1 КК України за 2004–2015 роки, за якими судові вироки набрали законної сили.

Так, загальна кількість вивчених нами осіб, вироки (постанови) щодо яких вступили в законну силу в 2004–2015 роках, становить 559. Неосудних осіб виявлено не було. Відносно 199 осіб (35,6 %) справу або провадження було закрито. Підставами для цього у 29,6 % випадків слугував акт амністії. У 26,1 % випадків справу або провадження було закрито у зв'язку зі зміною обстановки. У 23,1 % випадків – зв'язку з передачею особи на поруки. Враховуючи той факт, що переважна більшість (43,7 %) засуджених кіберзлочинців – працездатні особи, які на момент вчинення злочину не працювали і не навчалися, безробітні, виявлені обставини викликають певне здивування. У 12,5 % випадків справи або провадження закривалися у зв'язку з дійовим каяттям. Також; зафіксовані випадки закриття справ і проваджень у зв'язку з примиренням винного з потерпілим (2 %) та з інших підстав.

Розглянемо основні соціально-демографічні, кримінально-правові та морально-психологічні ознаки особистості кіберзлочинця.

1. Соціально-демографічні ознаки. Соціально-демографічні ознаки (стать, вік, національність, сімейний стан, освітній рівень, професія тощо) не тільки дають інтегроване уявлення про особу злочинця, але й розкривають її функціональний зв'язок із вчиненим злочином [634]. Відтак, вони формують характеристику соціального статусу і свідчать про його вплив на злочинця. Соціально-демографічні ознаки особистості злочинця також дають можливість визначити місце особистості у різних сферах суспільного життя, а разом з цим, виявити обставини, що сприяють формуванню злочинної поведінки. Аналіз зазначених відомостей на статистичному рівні дозволить встановити особливості демографічних показників, соціального походження й статусу, освітнього і культурного рівня злочинця та визначити їх вплив на спрямованість злочинної поведінки [635].

Аналіз статистичних даних дозволив зробити певні висновки щодо наявності деяких характерних закономірностей щодо соціально-демографічних характеристик осіб, що вчиняють кіберзлочини.

До соціально-демографічних ознак, перш за все, відносять стать злочинця. Встановлення статевих особливостей злочинців окремого виду дозволяє виявити їх фізіологічні і психологічні особливості.

Аналіз даних щодо засуджених осіб в Україні показав, що кіберзлочини вчиняються переважно чоловіками (90,8 %), на долю жінок припадає лише 9,2 % злочинів.

Розподіл засуджених за вчинення кіберзлочинів осіб в Україні за 2004–2015 рр. за статтю.

Такий статевий розподіл кіберзлочинців обумовлений не лише традиційно низькою у порівнянні з чоловіками кримінальною активністю жінок, але й з специфікою даного виду злочинів. Професійне з технічної точки зору вчинення кіберзлочинів жінками практично не спостерігається, оскільки вони менш представлені серед технічних спеціальностей. Вчинення професійних кіберзлочинів особами жіночої статі обумовлене їх соціальним статусом, пов'язаним з професійною діяльністю, здійснення якої пов'язане з комп'ютерними технологіями. Зокрема, результати дослідження матеріалів кримінальних проваджень засвідчили, що всі злочини, вчинені жінками, кваліфіковано у сукупності з іншими статтями КК України, які не відносяться до розділу XVI. Це підтверджує тенденції зростання жіночої злочинності в сфері раніше невідомих економічних злочинів, таких, як розкрадання в кредитно-банківській сфері, шахрайські дії шляхом створення фінансових організацій [636]. Однак, беручи до уваги тенденції у світовій практиці, відповідно до яких третина

---

[634] Коган В. М. Значение социально-демографических факторов для изучения причин преступности. *Вопросы борьбы с преступностью.* 1975. Вып. 22. С. 92.

[635] Головкін Б. М. Кримінологічні проблеми умисних вбивств і тяжких тілесних ушкоджень, що вчиняються у сімейно-побутовій сфері: монографія. Харків: ППВ «Нове слово», 2004. С. 41.

[636] Явчунская Т. М., Степанова И. Б. Феминизация современной преступности и ее причины. Закономерности преступности, стратегия борьбы и закон / Рос. криминол. ас-соц. Науч.-исслед. ин-т проблем укрепления и правопорядка; ред-кол.: А. И. Долгова (отв. ред.) и др. Москва: Рос. криминол. ассоц., 2001. С. 280.

арештованих за злочини хакерів в США були жінками [637], можна припустити, що частка жінок серед кіберзлочинців буде збільшуватися.

Вік злочинця вказує не лише на рівень біологічного, а й соціального розвитку людини, на відповідний стан і зміни особистості людини. Здійснюючи перехід з одного вікового ступеня на інший, людина постійно взаємодіє з соціальним середовищем, отримує і накопичує життєвий досвід [638]. Аналіз віку злочинця дозволяє в свою чергу виявити найбільш кримінально активні вікові групи населення.

Статистичні дані щодо засуджених за кіберзлочини осіб (Форма 7 статистичної звітності Державної судової адміністрації України) свідчить про наявність певної специфіки розподілу кримінальної активності у кіберпросторі окремих груп населення (табл. 19.2).

Таблиця 19.2

Градація засуджених за вчинення кіберзлочинів в Україні за віковим критерієм (2004–2015 рр.)

Роки	Вік засуджених на момент вчинення злочину				
	від 16 до 18 років	від 18 до 25 років	від 25 до 30 років	від 30 до 50 років	від 50 до 65 років
2004	1	4	0	3	0
2005	0	5	3	5	1
2006	2	15	14	11	2
2007	0	31	7	20	2
2008	0	18	11	23	5
2009	0	22	10	19	0
2010	1	17	20	25	6
2011	0	11	18	24	3
2012	0	12	24	40	4
2013	0	7	11	29	2
2014	0	7	9	20	1
2015	0	8	10	27	1

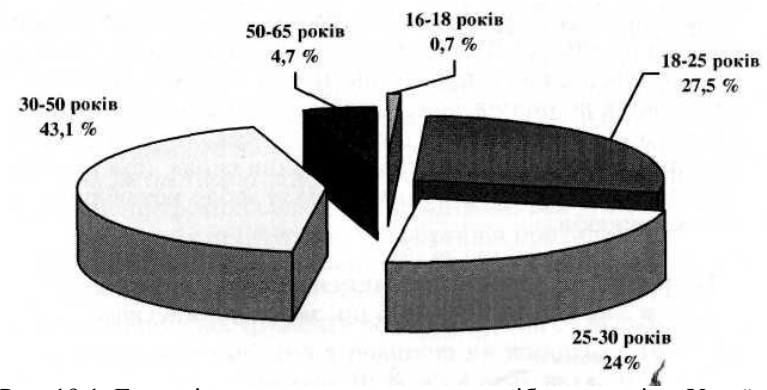

Рис. 19.1. Градація засуджених за вчинення кіберзлочинів в Україні за віковим критерієм (2004–2015 рр.)

Так, на відміну від загальнокримінальної злочинності при вчиненні кіберзлочинів, дуже низькою є кримінальна активність населення віком від 16 до 18 років, на долю якого припадає усього 0,7 % осіб, засуджених за вчинення кіберзлочинів. Слід зазначити, що це певною мірою може обумовлюватися позицією слідства та суду щодо уникнення за

[637] Кузнецов А. В. Пираты в Интернете. *Милиция.* 2000. № 2. С. 27.

[638] Шеремет А. П. Злочини проти статевої свободи: монографія; Закарпатський держ. ун-т. Чернівці: Наші книги, 2008. С. 54.

можливості засудження неповнолітніх осіб та застосування до них інститутів звільнення від кримінальної відповідальності та покарання. Однак зазначені дані та розподіл за рівнем кримінальної активності інших вікових груп в цілому спростовують поширене уявлення щодо омолодження кіберзлочинності та вкрай високу кримінальну активність у кіберпросторі саме осіб молодого віку [639].

Характерним на відміну від загальнокримінальної злочинності є відсутність серед засуджених осіб вікової групи від 65 років і старше. Це обумовлене, перш за все, відсутністю у більшості осіб даної вікової групи відповідних навичок роботи з комп'ютерною технікою, а також більшим життєвим досвідом та вищими моральними цінностями.

Аналіз розподілу вікових груп за рівнем кримінальної активності (рис. 19.1) показав, що найбільш активною є група осіб віком від 30 до 50 років на долю якої припадає 43,1 % засуджених за кіберзлочини осіб. На другому місці знаходиться група осіб віком від 18 до 25 років (27,5 %), на третьому місці особи віком від 25 до 30 років (24 %), на четвертому місці особи віком від 50 до 65 років (4,7 %), а на останньому місці, як вже зазначалося, знаходиться група осіб віком від 16 до 18 років (0,7 %).

Таким чином, хоча більше половини (51,5 %) кіберзлочинів вчиняються особами віком від 18 до 30 років, кримінальна активність відносно даного виду злочинів корелює з соціальною активністю населення. Також необхідно відмітити поступове падіння кримінальної активності вікових груп 18–25 років та 50-65 років: якщо у 2010 році частка перших складала 24 %, а других – 8,7 %, то у 2015 році – 17,4 % та 2,2 % відповідно. Як видається, така тенденція може бути пояснене інтенсивним розвиток комп'ютерних технологій, що зумовлює, по-перше, необхідність отримання попереднього досвіду мережевої і/або програмістської роботи, та, по-друге, відомі труднощі для осіб поважного віку щодо освоєння вказаних технологій.

Слід зазначити, що отримані дані щодо найбільш кримінальної активної групи населення в цілому співпадають зі світовою практикою. Так, результати соціологічних і кримінолого-криміналістичних досліджень проведених в Австралії, Канаді, Німеччині та США свідчать, що найбільш активний віковий період в якому вчиняються комп'ютерні злочини дорівнює саме віку від 15 до 35 років [640]; половина всіх комп'ютерних злочинців мають вік від 20 до 40 років [641].

Громадянство злочинця. Відповідно до даних Державної судової адміністрації України 95,5 % засуджених кіберзлочинців – громадяни України. На долю громадян інших держав припадає лише 4,5 % засуджених (див. діаграму 10).

Як зазначають фахівці, сучасне розширення інформаційного простору створює нові можливості для організованої злочинності, яка рухається у структурному плані до домінування гнучких мереж і, відповідно, стає можливим використання Інтернету не тільки для правопорушень, але й для створення злочинних груп, що може втілитися в перехід існуючих груп хакерів і кракерів, які координують свої операції, до формування кримінальних організацій, членам яких не має потреби зустрічатися або знаходитися в одній державі [642].

Отже, на наш погляд, з урахуванням транскордонності кіберзлочинів (яка обумовлена як глобальністю кіберпростору, так й міжнародним рівнем діяльності організованих угруповань кіберзлочинців), така картина в більшій мірі відповідає недосконалості слідчої та судової практики щодо розслідування кіберзлочинів та притягнення винних до відповідальності. Також: це свідчить про дуже високий ступень латентності відповідних злочинів, обумовлений як високим професіоналізмом їх вчинення, так й неготовністю вітчизняних правоохоронних органів протидіяти їм.

---

[639] Баранов О. А. Проблеми законодавчого забезпечення боротьби з комп'ютерними злочинами. Інформаційні технології та захист інформації: зб. наук, праць. Запоріжжя: Юрид. ін-т МВС України, 1998. Вип. 2. С 8–9; Мазуров В. А. Компьютерные преступления. Классификация и способы противодействия: учеб.-практ. пособие. Москва: Палеотип: Логос, 2002. С. 120; Окинавская Хартия Глобального Информационного Общества / Институт развития информационного общества URL: http://www.iis.ru/events/okinawa/charter.ru.html.

[640] Біленчук П. Д., Котляревський О. І. Портрет комп'ютерного злочинця: навч. посіб. Київ: B&B, 1997. С. 9; Кузнецов А. В. Пираты в Интернете. *Милиция.* 2000. № 2. С. 27.

[641] Комп'ютерна злочинність: навч.посіб. / П. Д. Біленчук та ін. Київ: Атіка, 2002. С. 10.

[642] Борисова Л. В. Суб'єкт (особа) комп'ютерного злочину транснаціонального криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права.* 2008. Вип. 44. С. 77.

Сімейний стан злочинця. Здійснений нами аналіз кримінальних справ та проваджень виявив, що більшість кіберзлочинців неодружені – 58 %. Розлучені складають 14 %, а одружені але такі, що з родиною не живуть, – 16 %. На долю одружених припадає 10 %, а на осіб, що перебувають у цивільному шлюбі, – 12 %. Таким чином, переважна більшість кіберзлочинців – особи, які не мають дружини/чоловіка. Це може бути обумовлено значною частиною серед кіберзлочинців осіб молодого віку, які не встигли завести сім'ю, а також характерною для кіберзлочинців нестабільністю особистості, жагою ризику, авантюризмом тощо, тобто властивостями характеру, які не сприяють зміцненню сімейних відносин.

Освітній рівень злочинця. Освітній рівень є важливою ознакою соціально-демографічної характеристики злочинця, оскільки багато в чому визначає соціальний статус особи, вид та кваліфікацію праці, а в цілому свідчить про рівень її інтелектуального розвитку та культури.

Рівень освіти людини впливає на формування її життєвих настановлень, ціннісних орієнтацій, потреб і інтересів людини, мотивів і цілей діяльності, правил поведінки, способів реагування на конкретні життєві ситуації. Чим вище рівень освіти індивіда, тим менше можливості для формування в нього антисуспільних поглядів, звичок і їх злочинного прояву зовні [643]. Низький освітній рівень сприяє спрощенню вибору засобів та шляхів реалізації потреб та бажань людини, вибору злочинних форм поведінки.

Якщо зіставити цей показник зі статистикою вчинення кіберзлочинів у співучасті: у групі діяли лише 13,1 % засуджених кіберзлочинців, з них у складі організованої групи лише 1,7 %, а засуджених за вчинення кіберзлочинів у складі злочинної організації взагалі не виявлено, – то очевидною є практично повна відсутність виявлених фактів вчинення кіберзлочинів громадянами України у групі з іноземними громадянами. Це було підтверджено і дослідженням матеріалів кримінальних справ та проваджень, при виборці яких не виявлено ні одного матеріалу щодо розслідування таких випадків.

В ході дослідження встановлено, що для кіберзлочинців в цілому на відміну від злочинців, що вчиняють злочини загальнокримінальної спрямованості, характерний високий освітній рівень, вищій рівня освіти населення в цілому (табл. 19.3). Так, переважна кількість кіберзлочинців (48,1 % засуджених осіб) – це особи з вищою освітою (з них з повною вищою освітою – 33,9 %, з базовою вищою освітою – 14,2 %). Другою за поширеністю є група осіб з загальною середньою освітою (30,3 %), з яких повну загальну середню освіту мають 25,3 % осіб, а базову загальну середню освіту – 5 % осіб. Частка осіб з професійно-технічною освітою складає 21,1 %. Виявлений один випадок (0,3 %) засудження за вчинення кіберзлочину особи з початковою загальною освітою. Осіб без освіти не виявлено (табл. 19.3).

Таблиця 19.3

Структура засуджених за вчинення кіберзлочинів в Україні за рівнем освіти (2004–2015 рр.)

Роки	Освіта на час вчинення злочину						
	повна вища	базова вища	професійно-технічна	повна загальна середня	базова загальна середня	початкова загальна	без освіти
2004	1	0	3	4	0	0	0
2005	5	1	1	5	2	0	0
2006	17	10	7	7	3	0	0
2007	20	9	10	17	4	0	0
2008	21	9	11	14	2	0	0
2009	11	10	12	16	2	0	0
2010	26	6	19	13	4	1	0
2011	21	6	13	15	1	0	0
2012	33	5	17	21	4	0	0

[643] Ветров Н. И. Криминологическая характеристика правонарушителей молодежного возраста: учеб. пособие. Москва: Юрид. лит., 1981. С. 43–44.

Закінчення табл. 19.3

2013	25	11	7	4	2	0	0
2014	13	1	11	7	5	0	0
2015	19	2	14	6	5	0	0

Таким чином, половина (48,1 %) кіберзлочинців мають вищу (в тому числі технічну) освіту, однак факт, що кожен третій злочинець (30,3 %) має загальну середню освіту вказує на наступне. З розвитком комп'ютерних технологій та систем комунікації, їх агресивною ескалацією в усі сфери нашої життєдіяльності, все більш поширеним стає вчинення кіберзлочинів не фахівцями-комп'ютерщиками, а звичайними користувачами кібертехнологій. Досягнення у цій сфері уможливили вчинення кіберзлочинів не за допомогою відповідної освіти, багажу знань та навичок, а за допомогою відповідних керівництв та посібників.

Соціальний статус злочинця. Будучи значною мірою пов'язаним з освітнім рівнем, соціальний статус людини визначається, перш за все, її професією і родом заняття.

Аналіз даних Державної судової адміністрації України дозволив виявити певні специфічні особливості щодо соціального статусу кіберзлочинця.

Встановлено, що переважна більшість засуджених кіберзлочинців – працездатні особи, які на момент вчинення злочину не працювали і не навчалися (43,7 %) та безробітні (2,5 %). При цьому слід відзначити тенденцію зростання останніми роками частки саме вказаної категорії осіб.

Взагалі той факт, що працездатна людина не залучена до праці, навчання або іншої соціально корисної діяльності має відоме криміногенне значення – людина позбавлена легальних прибутків та засобів існування, оточена, як правило, негативним мікросередовищем, легко та природно встає на злочинний шлях. Кіберзлочини ж, як свідчить практика, з огляду на освітній рівень злочинця та інші соціально-демографічні ознаки, вчиняються далеко не маргінальними, примітивно-кримінально орієнтованими представниками нашого соціуму. Більше того, вчинення кіберзлочину обумовлює наявність необхідного технічного (комп'ютерного) обладнання чи, принаймні, доступу до нього. Отже, на наш погляд, відповідні статистичні дані свідчать про недосконалість вітчизняного трудового, податкового та іншого законодавства та практики його застосування, що дозволяє відповідній категорії осіб «влаштовуватися» у суспільстві, офіційно маючи при цьому статус «безробітного» тощо.

В цілому розподіл засуджених за вчинення кіберзлочинів осіб за родом їх занять вказує, що другою за поширеністю є група службовців, на частку яких припадає 17 % (з них 1,7 % державні службовці). Третьою – робітники (16,1 %) та приватні підприємці (11,4 %). На п'ятому місці за поширеністю знаходиться група осіб, що навчаються – 7,4 % (6,9 % складають студенти навчальних закладів, а 0,5 % – учні шкіл, ліцеїв, коледжів, гімназій). На шостому місці за поширеністю серед осіб, засуджених за вчинення кіберзлочинів йдуть працівники господарських товариств (3,3 %), а на сьомому – пенсіонери (у т.ч. інваліди) (1,1 %). Також зустрічаються поодинокі випадки засудження за вчинення кіберзлочинів військовослужбовців, лікарів, фармацевтів тощо.

Отже, в цілому, аналіз соціального статусу кіберзлочинця дозволяє підтвердити справедливість висновку, що усі кіберзлочини, які вчиняються в нашій країні (відповідно до судової практики) доцільно поділити на три основні умовні групи: 1) злочини, що вчиняються у зв'язку з професійною (службовою) діяльністю особи; 2) злочини, що вчиняються особами з низьким офіційним соціальним статусом (безробітні тощо) з метою незаконного збагачення; 3) злочини, що вчиняються з особистих (крім користі) мотивів (самоствердження, помста тощо).

2. Кримінально-правові ознаки. В першу чергу проаналізуймо відомості про судимість. Інформація про наявність кримінального минулого, не кажучи вже про наявність незнятої або непогашеної судимості у злочинця, є кримінологічно значущою, оскільки характеризує ступінь його суспільної небезпечності, вказуючи на глибину та стійкість антисуспільної спрямованості його особистості. Кількість попередніх судимостей й вид злочинних посягань розкривають характер антисуспільної спрямованості особистості злочинця, в тому числі вказуючи й на окремі специфічні морально-психологічні ознаки.

Судимість. Відповідно до даних Державної судової адміністрації України серед осіб, засуджених за вчинення кіберзлочинів 5,1 % фактично раніше вчиняли злочинні діяння.

Однак, кримінально-правового рецидиву не мають, оскільки вони були звільнені від кримінальної відповідальності (0,5 %), визнані такими, що не мають судимості (1,9 %) або судимість погашена чи знята (2,7 %).

Водночас, 5,8 % осіб, засуджених за вчинення кіберзлочинів, мають незняту і непогашену судимість. З них 5 % мають одну, та 0,8 % дві незняті і непогашені судимості. При цьому частка осіб, які мають незняту і непогашену судимість, є відносно стабільною.

Щодо характеру попередньої судимості, то з осіб, які мають незняту і непогашену судимість, більшість була засуджена за вчинення злочинів проти власності (68 %). Далі йдуть особи, що були засуджені за злочини у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів (27 %), за злочини проти життя чи здоров'я особи (3 %), за злочини проти громадського порядку, моральності (2 %) та ін.

Дослідження матеріалів кримінальних справ та проваджень також вказує на корисливий характер кримінальної орієнтації кіберзлочинців з огляду на їх попередню злочинну діяльність. Те, що більшість осіб, які раніше засуджувались – засуджувалися за вчинення злочинів корисливої спрямованості при тому, що переважна більшість засуджених кіберзлочинців – працездатні особи, які на момент вчинення злочину не працювали і не навчалися, свідчить про глибоку та стійку кримінальну спрямованість особистості злочинців цієї групи та характерну деформацію ціннісно-орієнтаційної сфери.

У свою чергу, уникнення кіберзлочинцем реального покарання сприяє вчиненню нового, більш тяжкого злочину, зростанню спеціального рецидиву. А приклади фактичної безкарності такого роду діянь створюють ілюзію вседозволеності, комплекс сваволі та сприяють вчиненню злочинів іншими особами.

3. Морально-психологічні ознаки. Суб'єктивні дані особи, яка вчиняє злочин у сфері комп'ютерних технологій, її психічні та психологічні характеристики визначають спосіб кримінального впливу на інформаційні системи, інформацію та програмне забезпечення, як предмет злочинного посягання, в результаті послідовних у просторі та часі дій цієї особи [644].

Досліджуючи особистість злочинця, не можна не враховувати значення індивідуально-психологічних особливостей особистості у разі вчинення конкретного злочину, оскільки в цьому випадку вони можуть визначати поведінку особистості 645. Пізнання ж особливостей внутрішнього світу злочинців, зокрема їх моральних якостей, потребує знання життєвих позицій осіб, які скоюють злочинні діяння, їх ставлення до оточуючої дійсності, до людей, до суспільства. Це неможливо без вивчення їх потреб, інтересів, ціннісних орієнтацій, мотивів діяльності. Саме з'ясувавши стійкі, переважаючі в духовному житті індивіда інтереси до тих чи інших сфер соціального життя, явищ культури, ідеалів можна отримати уявлення про спрямованість особистості [646].

Світогляд, ціннісні орієнтації, інтелектуальні ознаки, емоційні особливості, вольові ознаки, культурний рівень, психічні аномалії, що не виключають осудність, рівень потреб та інші морально-психологічні ознаки особистості багатьох злочинців досліджені науковцями значно менше, ніж інші ознаки, через труднощі, пов'язані, перш за все, з методикою проведення таких досліджень [647]. Це в повній мірі стосується й такого специфічного (перш за все, через особливості засобів вчинення злочинів) виду злочинності, як кіберзлочинність.

Як відомо, ціннісні орієнтації в цілому визначають ставлення людини до основних сфер життя, а також характеризують спрямованість особистості в цілому. Відповідно до цього критерію, доречним є виділення таких типів злочинців:

1. Соціально дезадаптований тип – особи, характерними рисами яких є аутизація та інтравертність, тобто відхід у себе, відгородженість від навколишніх, спрямованість інтересів

---

[644] Борисова Л. В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права.* 2008. Вип. 44. С 78.

[645] Волков Б. С. Криминологическое исследование личности преступника в советском праве. Теоретические проблемы учения о личности преступника: сб. науч. тр. / ред-кол.: Г. В. Антонов-Романовский, В. К. Звирбуль, К. Е. Игошев, А. Б. Сахаров. Москва: Всесоюз. ин-т по изуч. причин и разраб. мер предупреждения преступности, 1979. С. 22.

[646] Джекебаев У. С. Криминологическое изучение личности преступника и преступного поведения: автореф. дис. ... д-ра юрид. наук. Москва, 1974. С. 13, 17.

[647] Антонин Ю. М. Социальная среда и формирование личности преступника (неблагоприятные влияния на личность в микросреде). Москва: Академия МВД СССР, 1975. С. 30–37.

лише на задоволення своїх власних, в основному інформаційних потреб. Для злочинців даного типу інформативне спілкування й здійснення внаслідок цього кіберзлочину є засобом подолання дезадаптації. Для них досить важливим є прирахування себе до класу «хакерів», тобто ототожнення з однією з невеликих, але все-таки соціальних груп. Тим самим вони внутрішньо прагнуть подолати своє соціальне відчуження, відчути свою значимість, а також; одержати можливість бути упевненим і зрозумілим у цьому соціальному середовищі. Щоб подолати власний психологічний дискомфорт, люди даного типу легко піддаються сторонньому негативному впливу, переймають «навколозлочинний» спосіб життя.

2. Емоційно сприйнятливий тип – особи, які долучилися до вчинення кіберзлочинів для задоволення своїх особистих інтересів і потреб. Цей тип осіб має підвищену сприйнятливість і особливою чутливістю до всього, що стосується інтересів особистості. В основному даний тип злочинців здійснює правопорушення з корисливих мотивів з метою задоволення своїх матеріальних потреб, рідше потреби в знаннях та інших потреб. На відміну від правопорушників першого типу, це особи, що володіють лідерськими схильностями, з досить високим рівнем інтелекту. Вони самолюбні, проявляють завидну енергію й активність у досягненні поставлених цілей, гнучкість і легкість у спілкуванні, установленні соціальних контактів. Однак досягнення своїх цілей «будь-яким шляхом» породжує в них почуття вищості й відповідно презирливе відношення до навколишніх. їм необхідний реальний успіх, щоб задовольнити свої потреби й честолюбство. Характерним для них є мінливість, відсутність прихильностей до кого-небудь, навіть до рідних й близьких, несприйняття й нерозуміння честі, гідності й обов'язку, нігілізм стосовно правових і моральних норм. Більшість кіберзлочинців належать саме до цього типу.

3. Соціально неадекватний тип – представлений в основному молодими людьми з вищою освітою, високим інтелектуальним рівнем, матеріально забезпеченими. Корисливі мотиви й матеріальні потреби для них не відіграють ніякої ролі, на перший план виходить задоволення інших, нематеріальних потреб. Надмірні або незрозумілі з погляду навколишніх, але гадані природніми для особистості запити породжують проблему потреби промотиваційної сфери, яку неможливо дозволити через особисте небажання й неприйняття встановлених правових (соціальних) норм. Психологічний комфорт і зняття напруги досягаються цілеспрямованою діяльністю, що веде до бажаних результатів [648].

Таким чином, оскільки основна маса кіберзлочинців відноситься до другого типу, основним визначальним фактором деформації ціннісно-орієнтаційної сфери кіберзлочинця, тобто негативною рисою особистості, що найбільш сильно проявилася у кіберзлочинця при вчиненні злочину, є корислива спрямованість особистості.

Особливістю кіберзлочинів є їх умисний характер, оскільки саме умисна форма вини є однією з основних ознак злочинів у даній сфері. Виключення може складати лише злочин, передбачений ст. 363 КК України, оскільки особливість суб'єктивної сторони складу цього злочину полягає в тому, що ставлення суб'єкта до суспільно небезпечного діяння може бути як умисне, так і необережне [649].

Як вже зазначалося, переважна більшість засуджених – працездатні особи, які на момент вчинення злочину не працювали і не навчалися, що свідчить про відсутність позитивних настановлень та глибоку і стійку кримінальну спрямованість особистості кіберзлочинців.

Одним з найважливіших показників, що характеризує моральний рівень особистості злочинця, є його відношення до алкоголізму і наркоманії. Аналіз статистичних даних показав, що для кіберзлочинців (на відміну від більшості злочинців) характерним є вчинення злочину виключно в тверезому стані. Зареєстровано лише одиничний випадок засудження особи за вчинення кіберзлочину у стані алкогольного сп'яніння. Це підтверджує висновок щодо кримінальної спрямованості особистості кіберзлочинця, який вчиняє злочин холоднокровно та обачливо, досягаючи передбачуваного результату.

---

[648] Евдокимов К. Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации: по материалам Восточно-Сибирского региона: дис. ... канд. юрид. наук: 12.00.08 / Евдокимов Константин Николаевич; Восточно-Сибирский институт МВД России. Волгоград, 2006. С. 151–153.

[649] Кримінальний кодекс України. Науково-практичний коментар: у 2 т. Т. 2 / за заг. ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна. 5-те вид., допов. Харків: Право, 2013. С. 779.

В результаті аналізу статистичних даних не виявлено жодної особи, що вчинила відповідне діяння в стані неосудності чи обмеженої осудності. Особистісні відхилення, на жаль, практично завжди залишаються поза увагою слідства та суду в силу тяжкості злочинів даного виду і непроведення відповідних експертиз.

Щодо інтелектуальних ознак особистості кіберзлочинця, то природа комп'ютерних злочинів вимагає встановлення певних властивостей особи обвинуваченого в плані технічних пізнань, їх особливостей, інтелектуальної можливості вчинення злочину. Тобто необхідний відповідний інтелектуальний рівень особи, пов'язаний з можливістю правильно розуміти і застосовувати інструкції тощо [650].

Деякі фахівці вказують, що характерною особливістю вчинення комп'ютерних злочинів є достатньо високий інтелектуальний рівень злочинця, оскільки, вчинення складних операцій, і, зокрема, написання комп'ютерних програм, підбирання паролів доступу до систем захисту, наявність можливості підкорити собі електронно-обчислювальну машину потребує не лише наявності спеціальних знань і навичок, а й достатньо високого рівня володіння собою і ситуацією, в якій вчинюється злочин [651].

Дійсно, у деяких випадках вчинення кіберзлочину потребує значних розумових зусиль та серйозної вольової концентрації [652], однак, з нашої точки зору, таке висловлювання не можна сприймати категорично. Хоча на відміну від осіб, що вчиняють злочини загально-кримінальної спрямованості, для кіберзлочинців характерний високий освітній рівень, вищій за рівень освіти населення, проте відповідно до соціального статусу та інших соціально-демографічних ознак кіберзлочинці відображають структуру населення в цілому. Отже, відповідний рівень інтелектуального розвитку кіберзлочинця є не константою, а предметом доказування здатності (можливості) вчинення відповідного діяння конкретною особою.

Мотивація кіберзлочинців. Кримінологічна суть злочину, відповідно й особистість того, хто його вчиняє, найбільш повно виявляється в змісті мотивації злочинної діяльності, оскільки саме у мотивах виражається не будь-яка окрема риса особистості, а у певному сенсі вся людина, всі характерні для неї властивості й особливості. Мотив цементує думку й волю, свідомість і дію й служить тією основною пружиною, що направляє вольовий процес, надаючи йому певний зміст [653]. Отже, мотив – це одне з найбільш суттєвих психологічних понять, за допомогою якого розкривається внутрішня природа людських вчинків, їх суть. Він виступає найважливішим компонентом психологічної структури будь-якої людської діяльності, її рушійною силою, позначає внутрішню (психологічну) причину вчинків конкретної особи [654].

Одним з найбільш розповсюджених мотивів злочинної поведінки є корисливий мотив [655]. Кіберзлочини, як підтверджують фахівці, в цьому плані не становлять виключення [656]. Для переважної більшості комп'ютерних злочинів найбільш характерною метою є заволодіння чужим майном [657]. В цілому більшість дослідників виокремлюють наступну групу мотивів,

---

[650] Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини: дис... канд. юрид. наук: 12.00.09 / Журба Андрій Іванович; Донец. юрид. ін-т Луган. держ. ун-ту внутр.. справ України ім. Е. О.Дідоренка. Донецьк, 2007. С. 111.

[651] Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: дис. ... канд. юрид. наук: 12.00.08 / Розенфельд Наталія Антріївна; НАН України; Інститут держави і права ім. В. М. Корецького. Київ, 2003. С .143.

[652] Баранов О. А. Проблеми законодавчого забезпечення боротьби з комп'ютерними злочинами. Інформаційні технології та захист інформації: зб. наук, праць. Запоріжжя: Юридичний ін-т МВС України, 1998. Вип. 2. С. 10.

[653] Волков Б. С. Мотивы преступлений: уголовно-правовое и социально-психологическое исследование / Б. С. Волков; науч. ред.: М. Д. Лысов. Казань: Казанский ун-т, 1982. С. 132.

[654] Тарарухин С. А. Установление мотива и квалификация преступления. Київ: Вища шк., 1977. С. 6.

[655] Музика А. А., Горбата О. І. Про класифікацію злочинів. Проблеми пенітенціарної теорії і практики: щорічний бюлетень Київського інституту внутрішніх справ. Київ: КІВС, «МП Леся». 2002. С. 45.

[656] Азаров Д. С Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: дис. ... канд. юрид. наук; НАН України ; Інститут держави і права ім. В. М. Корецького. Київ, 2002. С. 147.

[657] Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини: дис... канд. юрид. наук; Донец. юрид. ін-т Луган. держ. ун-ту внутр. справ України ім Е. О. Дідоренка. Донецьк, 2007. С. 111.

типових для вчинення кіберзлочинів: 1) корисливий мотив, 2) хуліганські мотиви, 3) помста, 4) політичні мотиви [658].

Проведений нами аналіз матеріалів кримінальних справ та проваджень також показав, що характерними для кіберзлочинців є наступні мотиви: користь (86 %), помста (6 %), потреба у самоствердженні та ігрові мотиви (3 %), хуліганські мотиви (2 %), кар'єризм (1 %), інша особиста нематеріальна зацікавленість (2 %).

§ 5. Запобігання кіберзлочинності

5.1. Правове регулювання запобігання кіберзлочинності

Надаючи характеристику системі правового регулювання запобігання кіберзлочинності, розпочнемо з міжнародних засад. Варто зазначити, що актуальні проблеми кіберзлочинності обговорювалися на 10, 11, 12-му Конгресах ООН по запобіганню злочинності та кримінальному правосуддю (10-17 квітня 2000 р., 18–25 квітня 2005 р., 12–19 квітня 2010 р, відповідно). Серед пропозицій стосовно протидії цьому різновиду злочинності слід виділити найбільш значущі:

1. Необхідний постійний розвиток внутрішньодержавної правової бази у сфері обігу комп'ютерної інформації, яка повинна відповідати вимогам сучасності та бути адаптованою до норм міжнародного права. Особливу увагу потрібно приділяти удосконаленню та узгодженню кримінального та кримінально-процесуального законодавства, пов'язаного з кваліфікацією, виявленням та розслідуванням кіберзлочинів. Слід також вирішити правові питання з приводу розголошення провайдерами інформації про користувачів па запит правоохоронних органів та можливості використання такої інформації як доказу тощо.

2. Важливе значення має високопрофесійна підготовка відповідних фахівців підрозділів боротьби з кіберзлочинністю, спеціалістів та експертів у галузі комп'ютерних технологій, а також впровадження постійної системи підвищення їх кваліфікації з питань виявлення кіберзлочинів, пошуку та використання фактичних даних, що можуть виступати як докази. Обґрунтованою є пропозиція щодо створення міжнародної мережі експертів для обміну досвідом та знаннями. Це надасть можливість проводити спільні наукові дослідження та порівняльний аналіз проявів кіберзлочинності.

3. Слід удосконалити координацію правоохоронних органів у галузі протидії кіберзлочинності та посилити співробітництво із суб'єктами інформаційного обороту. Налагодження партнерських відносин із приватним сектором допоможе в розробці і здійсненні ефективних заходів боротьби зі злочинністю, пов'язаною з використанням комп'ютерів. Але для цього треба забезпечити спеціальні підрозділи правоохоронних органів відповідною правовою, матеріальною та кадровою підтримкою з боку держави, а також надати сучасне технічне обладнання, що може бути використане в їх професійній діяльності.

4. Необхідно ускладнити або виключити можливості кримінального використання комп'ютерної інформації і техніки. Суб'єктами інформаційного обороту повинна забезпечуватися відповідна система фізичного і технічного захисту комп'ютерної інформації. На державному рівні мають розроблятися спеціальні системи захисту комп'ютерної Інформації загальнонаціонального значення та створюватися правові основи їх функціонування. При цьому передбачається належне державно-правове регулювання систем захисту, з метою недопущення обмеження прав і законних інтересів фізичних та юридичних осіб.

5. Одним із важливих кроків є підвищення обізнаності правоохоронних органів, представників приватного сектору і потенційних жертв про кіберзлочинність та надання

---

[658] Абов А. И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации / А. И. Абов. Москва: Прима-Пресс, 2002. С. 16; Вехов В. Б. Компьютерные преступления: Способы совершения и раскрытия / В. Б. Вехов ; под ред. акад. Б. П. Смагоринского. Москва: *Право и Закон,* 1996. Вехов В. Б. Компьютерные преступления: Способы совершения и раскрытия / В. Б. Вехов ; под ред. акад. Б. П. Смагоринского. Москва: Право и Закон, 1996. С. 42. Абов А. И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации / А. И. Абов. Москва: Прима-Пресс, 2002. С. 16; Косенков А. Н., Черный Г. А. Общая характеристика психологии кибер-преступника. *Криминологический журнал Байкальского государственного университета экономики и права.* 2012. № 3. С. 87–94. URL: http://cj.isea.ru/pdf.asp?id= 13288.

відповідних консультацій щодо зменшення їх віктимності. Для цього треба постійно проводити моніторинг інформаційних загроз, ґрунтовні дослідження функціонування та розвитку кіберзлочинності. Не останнє місце також займає спеціалізоване правове виховання суб'єктів інформаційного обороту та користувачів комп'ютерної техніки.

6. Важливість ефективного міжнародного співробітництва в галузі правоохоронної діяльності. У зв'язку з глобальним характером мережі Інтернет та поширенням електронної торгівлі національні кордони втрачають своє значення при вчиненні кіберзлочинів. Таким чином, для ефективного проведення розслідування надзвичайно важливим стає фактор швидкодії. Для цього необхідні тісні взаємовідносини з державними та правоохоронними органами в інших країнах.

Чільне місце в правовій основі діяльності правоохоронних органів у сфері протидії кіберзлочинності складає Конвенція Ради Європи «Про кіберзлочинність», прийнята 23.11.2001 року та ратифікована Верховною Радою України 07.09.2005 року. Ця Конвенція є комплексним документом, що охоплює такі основні напрями: узгодження національних кримінально-правових норм, що визначають склади кіберзлочинів (у документі надано перелік діянь, що повинні бути криміналізовані державами-учасницями), визначення порядку розслідування вказаних злочинів, вчинених у світових комп'ютерних мережах, створення оперативної та дієвої системи міжнародної співпраці у боротьбі з кіберзлочинністю, а також інші процедурні питання.

Незважаючи на міжнародне визнання того факту, що кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремих держав, а загрожує людству та міжнародному порядку, нині в Україні відсутня концепція стратегії реалізації державної політики щодо протидії кіберзлочинності, у зв'язку з чим наявність цієї проблематики та її розуміння в контексті державної та міжнародної безпеки на загальнодержавному рівні обумовлює необхідність вчинення дійових заходів, з боку вищих органів державної влади, спрямованих на запобігання злочинним проявам у цій сфері. У зв'язку з цим виникає необхідність розроблення відповідних нормативно-правових актів, удосконалення чинного законодавства і, в першу чергу, законодавчого закріплення діяльності правоохоронних органів у цій сфері. Однак виконання вказаного завдання може бути здійснене лише на підставі попередньої оцінки стану правового регулювання, який би окреслив напрями подальшого його реформування.

Так, проблеми кіберзлочинності, у контексті інформаційної безпеки як складової національної безпеки, розглядалися неодноразово Радою національної безпеки і оборони України. Про це, зокрема, свідчать укази Президента України: Про рішення Ради національної безпеки і оборони України від 17 червня 1997 року «Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин» від 21 липня 1997 р. № 663/97; Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної політики та забезпечення інформаційної безпеки України» від 6 грудня 2001 р. № 1193/2001; «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» від 14 липня 2000 р. № 891; «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 р. № 928/2000; «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24 вересня 2001 р. № 891/2001; Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»» від 26 травня 2015 року № 287/2015; Про рішення Ради національної безпеки та оборони від 6 травня 2015 року «Про заходи щодо посилення боротьби зі злочинністю в Україні» від 16 червня 2015 року № 341/2015 та інші.

У вказаних нормативно-правових актах йдеться, по-перше, про визнання серйозного рівня загрози від кіберкримінальної активності, по-друге, формуються пріоритетні напрями, принципи протидії їй. Зокрема, п. 7 Указу Президента України «Про рішення Ради національної безпеки та оборони від 06 травня 2015 року «Про заходи щодо посилення боротьби зі злочинністю в Україні» на МВС України та СБУ, інших заінтересованих державних органів покладено обов'язок розробити та запровадити у місячний строк механізм моніторингу стану транскордонної і транснаціональної організованої злочинності, передбачивши періодичну оцінку її впливу на суспільно-політичні та соціально-економічні

процеси у державі в цілому, її регіонах [659]. Серед іншого йдеться про моніторинг кіберзлочинності як різновиду транскордонної злочинності: її динаміки, структурних трансформацій, змін у детермінаційному комплексі.

Принагідно зауважимо, що вказаний Указ виданий в умовах зовнішньої агресії по відношенню до України, у зв'язку з чим зорієнтований передусім на формування внутрішніх механізмів контрвпливу, обструкції атакуючого потенціалу агресора, в тому числі і його кібернетичних складових. Транскордонна організована кіберзлочинність становить серйозну загрозу національній безпеці нашої держави, у зв'язку з чим існує нагальна потреба у мобілізації максимуму ресурсів спеціалізованих органів протидії злочинності, в тому числі і перш за все МВС та Національної поліції. Разом з тим, маємо констатувати, що закріплені вимоги стосовно розроблення та запровадження моніторингу транскордонної та транснаціональної організованої злочинності й досі не виконані, ані МВС, ані СБУ. Основна причина цього вбачається в організаційних труднощах розмежування компетенцій та обсягів роботи двох зазначених незалежних суб'єктів, а також у недостатньому науковому забезпеченні цього процесу, відсутності налагоджених зв'язків з цього питання із Кримінологічною асоціацією України, іншими дослідницькими організаціями, уставами, можливості та науковий рівень яких здатні забезпечити вироблення схеми, принципів функціонування, механізму моніторингу транскордонної, в тому числі й кіберзлочинності.

Вихід з цієї ситуації вбачається у створенні розпорядженням Президента Україна міжвідомчої (МВС та СБУ) робочої групи із широким представництвом наукової спільноти щодо вироблення основоположних засад, принципів побудови вказаного механізму, змістовного та операційного насичення моніторингових процедур, напрямів та методів здійснення інформаційно-аналітичної роботи в їх межах. Гадаємо, керівна роль в цьому процесі має відводитись саме МВС, яке уповноважене акумулювати та обробляти інформаційні масиви, які формуються в діяльності спеціалізованих підрозділів Національної поліції, зокрема кіберполіції.

Зауважимо, що здійснення заходів протидії злочинності є першочерговим завданням правоохоронних органів, про що зазначено у нормативно-правових актах, які регламентують їх діяльність. У зв'язку з чим здійснюючи заходи протидії кіберзлочинності вони керуються, в першу чергу, всіма нормативно-правовими актами, що регулюють їх діяльність (закони України «Про Національну поліцію» від 02.07.2015 року, «Про прокуратуру» від 14.10.2014 року, «Про Службу безпеки України» від 25.03.1992 року, «Про Службу зовнішньої розвідки України» від 01.12.2005 року тощо).

Важливо акцентувати на тому, що відповідно до положень Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 року № 2824-IV в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України [660]. З цього випливає, що МВС України та органи Національної поліції залишаються в орбіті реалізації запобіжних практик, спрямованих на нейтралізацію (зниження інтенсивності) детермінаційного комплексу кіберзлочинності. Такий же висновок напрошується з аналізу положень згадуваного вище Указу Президента України «Про рішення Ради національної безпеки та оборони від 6 травня 2015 року «Про заходи щодо посилення боротьби зі злочинністю в Україні».

Завдання запобігання та протидії кіберзлочинам покладено на спеціалізований підрозділ Національної поліції України – кіберполіцію, яка виконує свої функції з жовтня 2015 року [661]. Департамент кіберполіції є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції та відповідно

[659] Про рішення Ради національної безпеки та оборони від 6 травня 2015 року «Про заходи щодо посилення боротьби зі злочинністю в Україні»: Указ Президента України від 16 черв. 2015 р. № 341/2015 URL: http://www.president.gov.ua/documents/3412015-19136.

[660] Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 верес. 2005 р. № 2824-IV. URL: http://zakonl.rada.gov.ua/laws/show/2824-15.

[661] Про утворення територіального органу Національної поліції: Постанова Кабінету Міністрів України від 13 жовт. 2015 р. № 831 URL: http://zakon5.rada.gov.ua/laws/show/831-2015-%D0%BF.

до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність [662].

До основних завдань кіберполіції належать:

– реалізація державної політики у сфері протидії кіберзлочинності;

– протидія кіберзлочинам у сферах: використання платіжних систем, електронної комерції та господарської діяльності, інтелектуальної власності та інформаційної безпеки;

– завчасне інформування населення про появу новітніх кіберзлочинів;

– впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини;

– реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів;

– участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності;

– участь у міжнародних операціях та співпраця в режимі реального часу; забезпечення діяльності мережі контактних пунктів між 90 країнами світу [663].

Крім того, кіберполіція має сприяти у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень [664].

Також на підставі аналізу нормативно закріплених положень про структурні підрозділи кримінальної поліції можна зробити висновок, що до суб'єктів запобігання кіберзлочинності, які функціонують в структурі Національної поліції, слід також віднести:

– Департамент протидії наркозлочинності – щодо виявлення, перекриття, запобігання виникненню каналів поширення наркотичних засобів з використанням електронних мереж;

– Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми – щодо виявлення, перекриття та запобігання виявленню мережево-телекомунікаційних комплексів вербування, підшукування жертв торгівлі людьми;

– Робочий апарат Укрбюро Інтерполу (на правах департаменту) – щодо забезпечення взаємодії з Інтерполом у справі протидії кіберзлочинності;

– Департамент захисту економіки (у складі кримінальної поліції) – здійснює протидію злочинам, що вчиняються у економічній сфері за допомогою електронно-обчислювальних машин (комп'ютерів);

– Департамент карного розшуку. Враховуючи, що у багатьох випадках кіберзлочини мають організований характер, відповідне забезпечення, прикриття злочинної діяльності, на вказаний Департамент та його структурні підрозділі покладаються завдання щодо опосередкованого запобігання кіберзлочинності. Крім того працівники цього департаменту виявляють осіб, які займаються виготовленням та розповсюдженням порнографічної продукції, видань, що пропагують насильство, жорстокість, сексуальну розпусту, тобто діянь, що можуть вчинятися за допомогою технічних засобів, в тому числі комп'ютерів;

– Департамент превентивної діяльності – щодо ранньої превенції кіберзлочинів особами, які виявляють первинні ознаки антисуспільної спрямованості, або раніше вчиняли правопорушення, щодо яких встановлено адміністративний нагляд.

Чільне місце в правовій основу діяльності правоохоронних органів у сфері запобігання кіберзлочинності посідає Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 квітня 1994 р. [665]. Зазначений нормативно-правовий акт містить визначення понять, що використовуються у сфері інформаційно-телекомунікаційних систем. Регламентує об'єкти захисту, суб'єктів відносин, що виникають у вказаній сфері та порядок поводження з інформацією, що міститься у цих системах тощо.

Безпосередньо, що стосується діяльності правоохоронних органів, вказаний документ регламентує повноваження спеціально уповноваженого центрального органу виконавчої

---

[662] Орлов Ю. Ю., Кудінов В. А. Підготовка фахівців з протидії кіберзлочинності. *Бюлетень з обміну досвідом роботи.* № 188. Київ: РВВ МВС України, 2011. С. 23–33. URL: https://cyberpolice.gov.ua/contacts.

[663] URL: https://www.facebook.com/arsen.avakov.1/posts/916452195111554.

[664] URL: https://cyberpolice.gov.ua/contacts.

[665] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 лип. 1994 р. № 80/94-ВР. URL: Mtp://zakon4.rada.gov.uaAaws/show/80/94-%D0%B2%Dl%80.

влади з питань організації спеціального зв'язку та захисту інформації та його регіональних органів, який:

– розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

– визначає вимоги та порядок створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

– здійснює контроль за забезпеченням захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

У разі виявлення уповноваженими особами вказаного органу порушень захисту зазначеної інформації, порядку поводження з цією інформацією звертаються до відповідних органів, в тому числі до органів Національної поліції, з метою притягнення винних осіб до відповідальності.

Наступним нормативно-правовим актом, що регламентує діяльність правоохоронних органів у зазначеній сфері є Закон України «Про захист суспільної моралі» від 20 листопада 2003 р.[666] Зазначений нормативно-правовий акт містить визначення понять, що використовуються у сфері суспільної моралі, основні напрями державного регулювання обігу інформаційної продукції, що негативно впливає на суспільну мораль тощо.

Наступним нормативно-правовим актом, що регламентує діяльність правоохоронних органів у сфері протидії кіберзлочинності є Указ Президента «Про невідкладні додаткові заходи щодо зміцнення моральності у суспільстві та утвердження здорового способу життя» від 15 березня 2002 р. № 258/2002. Норми зазначеного документу спрямовані на зміцнення моральних та етичних засад у суспільстві, з метою посилення захисту моралі, а також збереження вікових культурних традицій Українського народу від негативного впливу культу насильства, жорстокості, порнографії насамперед через засоби масової інформації, ліквідації наркоманії та інших ганебних явищ, які продовжують руйнувати суспільну мораль, перешкоджають реалізації конституційних прав і свобод людини, інтеграції України в європейський інформаційний, освітній та культурний простір, утвердженню здорового способу життя громадян, належному вихованню молодого покоління, створюючи все відчутнішу загрозу національній безпеці держави, гідному майбутньому народу. Безпосередньо, що стосується діяльності правоохоронних органів, в тому числі підрозділів протидії кіберзлочинності, вказаний документ визначає їх завдання у зазначеній сфері відносно розвитку міжнародного співробітництва, перейняття зарубіжного досвіду, розроблення пропозицій відносно удосконалення їх діяльності.

Наступним документом, який являє собою правову основу діяльності правоохоронних органів у сфері боротьби з кіберзлочинністю є Указ Президента «Про заходи щодо забезпечення захисту прав і законних інтересів дітей» від 5 травня 2008 р. № 411/2008. Він зобов'язує правоохоронні органи, в тому числі підрозділи протидії кіберзлочинності, підвищувати ефективність роботи щодо виявлення, запобігання та розкриття злочинів проти статевої свободи та статевої недоторканості щодо дітей та посилення і удосконалення профілактичної роботи у цьому напрямі.

На підставі вивчення зазначених нормативних актів, на нашу думку, можна зробити висновок, що правове регулювання діяльності правоохоронних органів у сфері протидії кіберзлочинності має наступні недоліки:

– відсутня чітка регламентація заходів протидії кіберзлочинності, а саме відсутність єдиного нормативно-правового акту Національної поліції щодо запобігання кіберзлочинам;

– неузгодженість завдань і функцій щодо протидії кіберзлочинності серед підрозділів поліції;

– неузгоджений порядок взаємодії органів та підрозділів Національної поліції у вказаній сфері;

---

[666] Про захист суспільної моралі: Закон України від 20 листоп. 2003 р. № 1296-IV URL: http://zakon2.rada.gov.ua/laws/show/1296-15.

– відсутні положення, які б регламентували діяльність новостворених органів та підрозділів Національної поліції, в тому числі й Департаменту кіберполіції;

– наявність прогалин у правовому регулюванні взаємодії МВС та Національної поліції з питань протидії злочинності.

5.2. Система заходів запобігання кіберзлочинності

Необхідно зауважити, що у зарубіжній і вітчизняній законодавчій практиці, науках кримінально-правового циклу, кримінологічній і спеціальній правовій літературі щодо діяльності з впливу на злочинність використовуються різні терміни: «попередження злочинності», «профілактика злочинності», «соціальна профілактика», «боротьба зі злочинністю», «війна зі злочинністю», «протидія злочинності», «протистояння злочинності», «контроль злочинності», «регулювання злочинності», «управління злочинністю», «запобігання злочинності», «превенція злочинності», «припинення злочинів» тощо. Причому кожний з термінів викликає наукові суперечки [667].

На думку більшості авторів узагальнюючим, базовим (родовим) терміном є термін протидія злочинності, яку можна визначити як систему різноманітних видів діяльності та комплексних заходів (які здійснюються суспільством та державою), спрямованих на попередження, усунення, нейтралізацію і обмеження (ослаблення) факторів, детермінуючих злочинність [668]. Ми також; підтримуємо цю позицію. Але слід зауважити, що чимала кількість нормативно-правових актів, які стосуються тих чи інших аспектів кримінально-превентивної діяльності використовує термін «запобігання». На підставі позиції, які ми підтримуємо, відносно використання термінів, ми будемо використовувати поняття «запобігання» та «протидія», як тотожні.

Щодо протидії злочинності у кримінології виокремлюють загальносоціальні, спеціально-кримінологічні та індивідуальні напрями [669], а саме: загальносоціальні – комплекс перспективних соціально-економічних і культурно-виховних заходів, спрямованих на подальший розвиток та вдосконалення суспільних відносин і усунення або нейтралізацію разом з тим причин і умов злочинності; спеціально-кримінологічні – сукупність заходів боротьби зі злочинністю, змістом яких є різноманітна робота державних органів, громадських організацій, соціальних груп і громадян, спрямована на усунення причин та умов, що породжують та сприяють злочинності, а також недопущення вчинення злочинів на різних стадіях злочинної поведінки; індивідуальні – різновид запобігання злочинності щодо конкретної особи [670].

Загальносоціальне запобігання злочинності – це, насамперед, комплекс перспективних соціально-економічних, організаційно-управлінських, ідеологічних, культурно-виховних та інших заходів, спрямованих на вирішення нагальних соціальних проблем і суперечностей в країні. Саме реалізація загальносоціальних заходів запобігання дає змогу усунути чи мінімізувати вплив криміногенних факторів детермінації злочинності, запобігти формуванню особистості злочинця.

Заходи загальносоціального запобігання передбачають проведення комплексу правових, соціально-економічних, сімейно-побутових, ідеологічних, технічних, організаційних заходів [671].

Правові заходи спрямовані на удосконалення законодавчої бази, на основі якої відбувається регулювання суспільних відносин у всіх сферах суспільного життя.

Соціально-економічні заходи загальносоціального запобігання передбачають поступове зростання економічного потенціалу держави та розширення соціальної бази реформ. Перш за все, ці заходи передбачають необхідність сприяння працевлаштування неконкурентоспроможних на ринку праці верств населення (молоді, жінок,

---

[667] Ігнатов О. М. Протидія злочинності: поняття та сутність. *Юридична Україна.* 2009. № 3. С. 93–94.

[668] Литвинов О. М. Поняття та сутність механізму протидії злочинності. *Вісник Академії прокуратури України.* 2007. № 3. С. 65.

[669] Алексеев А. И., Герасимов С. И., Сухарев А. Я. Криминологическая профилактика: теория, опыт, проблемы. Москва: НОРМА, 2001. С. 26.

[670] Кримінологія: Загальна та Особлива частини / І. М. Даньшин, В. В. Голіна, О. Г. Кальман, О. В. Лисодєд; За ред. І. М. Даньшина; Нац. юрид. акад. України ім. Ярослава Мудрого. Харків: Право, 2003. С. 95–100.

[671] Голина В. В. Предупреждение преступности и права человека. *Проблеми законності*. 1998. Вип. 36. С. 165.

військовослужбовців, осіб, які звільнилися із місць позбавлення волі, тощо). Крім того, одним із ключових завдань соціальної політики є вирішення житлової проблеми населення. Ці заходи передбачають необхідне забезпечення належних умов для соціалізації особистості, обмеження негативних наслідків безробіття, розширення соціальної бази реформ, забезпечення мінімально гарантованого рівня медичного, культурного, побутового й соціального обслуговування населення. Молоді необхідна соціальна допомога держави в здобутті освіти, професійній підготовці, працевлаштуванні, забезпеченні житлом.

Запобігання на сімейно-побутовому рівні ґрунтуються на таких заходах, як підвищення авторитету сім'ї, шляхом популяризації історичних традицій української родини, духовних та моральних цінностей сім'ї; формування у свідомості громадян розуміння важливості ролі сім'ї у процесі державотворення, вихованні нового покоління, забезпечення суспільної стабільності та відтворення населення; створення сприятливих умов для повноцінного морально-психологічного, соціально-культурного і духовного розвитку сім'ї; пропаганда здорового способу життя, планування сім'ї; надання гарантованої правової, матеріальної, соціально-психологічної, медичної допомоги сім'ям.

Ідеологічні запобіжні заходи покликані: формувати в членів суспільства моральну свідомість на базі загальнолюдських цінностей; обмежувати негативний вплив на поведінку людей стандартів масової культури за допомогою диференційованого її споживання; виправляти моральні деформації в осіб з девіантною поведінкою за допомогою індивідуально-виховної роботи [672]. Найбільш потужним потенціалом ідеологічного впливу на злочинність поряд з державою володіє церква. Безспірною є позиція фахівців, які зазначають, що церква, релігія з їх основними постулатами ненасильства, милосердя, співчуття, терпіння здатні сформувати такі відносини, які зможуть допомогти в подоланні духовної кризи, вирішенні міжособистісних і групових конфліктів, життєвих проблем, взагалі поступово підточувати кримінальну субкультуру [673].

До технічних заходів відноситься удосконалення технічної оснащеності, в першу чергу, підрозділів органів Національної поліції, впровадження новітніх технологій у їх діяльність, перейняття досвіду діяльності правоохоронних органів інших країн.

До організаційних заходів відносяться вдосконалення організаційної структури правоохоронних органів, укомплектування штатів висококваліфікованими кадрами, забезпечення високої професійної підготовки та перепідготовки кадрів, їх правовий та соціальний захист.

Значну роль у запобіганні злочинності, в тому числі кіберзлочинності, відіграють заходи протидії корупції, як в правоохоронних органах, так і в органах влади в цілому. Запобігання корупції означає прагнення державної влади до самозбереження, бо свавілля та користолюбний службовий нігілізм – це, образно кажучи, прояв смертельно небезпечного вірусу в державному організмі. Вилікуватися від цієї хвороби цілком ще ніде не вдавалося, люди звикли до корупції як до неминучого зла [674]. Як показує міжнародний досвід, найбільших успіхів у протидії корупції досягають ті країни, у яких здійснюються взаємозалежні інституціональні, правові, економічні, культурологічні й політичні заходи, що дають змогу контролювати й впливати на криміногенну ситуацію.

Взагалі, для підвищення та вдосконалення значущості загальносоціальних заходів протидії злочинності, в межах країни, необхідно:

– завершити радикальну реформу економічної, соціальної, політичної та інших сфер суспільства на засадах чесної конкуренції та демократії, подолати глибоку кризу, у якій опинилась Україна при переході від адміністративно-командної системи господарювання до цивілізованої ринкової економіки;

– удосконалити управління державним майном і економічними процесами, зміцнити контроль за мірою праці та споживання, виключити відмивання коштів, отриманих незаконним шляхом;

---

[672] Криминология: учеб. для вузов / В. Н. Бурлаков, В. В. Вандышев, И. В. Волгарева и др. ; под ред. В. Н. Бурлакова, Н. М. Кропачева; С.-Петерб. гос. ун-т. Санкт-Петербург: Питер, 2002. С. 184.

[673] Лукашевич С. Ю. Кримінологічна характеристика та попередження злочинності засуджених в місцях позбавлення волі: дис. ... канд. юрид. наук: 12.00.08 / Лукашевич Сергій Юрійович; Нац. юрид. акад. імені Ярослава Мудрого. Харків, 2001. С. 162.

[674] Багрій-Шахматов Л. В. Корупція як соціальна патологія та її взаємозв'язок з організованою злочинністю. Проблеми боротьби з корупцією та організованою злочинністю. Київ, 1998. Т. VII. С. 45.

– створити ефективну податкову систему, сприятливі умови для підприємницької діяльності, щоб громадяни мали реальну можливість працювати в межах закону;

– запровадити попереднє вивчення банками фінансового стану фізичних та юридичних осіб, які звертаються з проханням про надання кредитів, а також мети, з якою ці кредити отримують, та можливостей їх повернення;

– запровадити обов'язкове прозоре декларування доходів усіма державними службовцями [675].

Отже, задля належної розробки відповідних заходів протидії злочинності, в тому числі кіберзлочинності, необхідна належна організація діяльності, як правоохоронних органів, так і вищих органів держави, яка відповідає вимогам, що ставляться до правової, незалежної та демократичної держави. Крім того, необхідне усунення зазначених вище факторів, що позитивно впливають на існування та розвиток злочинності.

Діяльність правоохоронних органів у сфері протидії злочинності, в тому числі кіберзлочинності, безпосередньо грунтується на реалізації загальних спеціально-кримінологічних та індивідуальних заходах.

На сьогодні серед проблемних питань запобігання злочинам в сфері комп'ютерних та Інтернет-технологій в Україні виділяються наступні:

– недосконаліть законодавства і пов'язані з цим питання кваліфікації й актуальності боротьби з комп'ютерною злочинністю;

– труднощі організації і проведення комп'ютерних експертиз;

– труднощі проведення заходів оперативно-технічного документування злочинних дій осіб;

– відсутність практики й механізмів розкриття «транснаціональних» комп'ютерних злочинів з територіально-розподіленими й нестабільними в часі слідами, а також; проведення надалі слідчих дій відносно осіб, які повинні дати свідчення в якості потерпілого, підозрюваного, свідка [676].

На підставі зазначеного, на нашу думку, доцільним є виокремлення наступних заходів запобігання кіберзлочинності, які повинні реалізовувати МВС та Національна поліція.

В першу чергу йдеться про розроблення та затвердження МВС Стратегії протидії кіберзлочинності. Тут мають спрацювати спільні робочі групи МВС та Національної поліції, яким, на підставі опрацювання кримінологічної інформації про стан, тенденції відтворення кіберзлочинності, відповідних кримінологічних прогнозів, належить виробити концепцію кримінально-превентивої діяльності, науково обґрунтовані стратегічні й тактичні заходи антикримінального впливу, моніторингові механізми забезпечення якості останнього.

Доцільним є збільшення кількості планових та позапланових перевірок відповідними органами поліції підприємств, установ та організацій, діяльність яких прямо пов'язана з використанням комп'ютерних технологій або наданням інформаційних послуг, з метою виявлення випадків використання нелегального (нерегламентованого) програмного забезпечення, так як використання останнього вкрай підвищує можливість вчинення будь-яких злочинних діянь з використанням комп'ютерних технологій. Крім того, доцільним є підвищення відповідальності осіб підприємств, установ або організацій, діяльність яких пов'язана із зазначеною сферою, які за своїми посадовими або функціональними обов'язками відповідають за безпеку функціонування комп'ютерів та комп'ютерних мереж, на законодавчому рівні.

Також з метою протидії вчиненню злочинів в аналізованій сфері, необхідним заходом є збільшення кількості планових та позапланових перевірок поліцією заходів безпеки, які здійснюються, в першу чергу приватними охоронними організаціями, на об'єктах, що призначені для передачі інформації (супутникові вишки, автоматизовані телекомунікаційні мережі, серверні кімнати тощо). Здійснення вказаних заходів повинно бути спрямоване на запобігання незаконного використання зазначених об'єктів та унеможливлення їх захоплення, з метою вчинення будь-яких протиправних діянь у сфері комп'ютерних комунікацій, мереж, інформації тощо. Так само, як і відносно попереднього заходу, на нашу думку, доцільним є підвищення відповідальності осіб підприємств, установ або організацій, діяльність яких

[675] Кримінологія: навч. посіб. / О. М. Джужа, В. В. Василевич, Ю. Ф. Іванов та ін. ; під заг. ред. О. М. Джужи. Київ: Прецедент, 2006. С 21–22.

[676] Буров О. В., Бурова Д. О., Пенська А. М. Кіберзлочинність як загроза інформаційному суспільству. *Теорія і практика інтелектуальної власності.* 2008. № 3. С. 43.

пов'язана із зазначеною сферою, які за своїми посадовими або функціональними обов'язками відповідають за безпеку функціонування комп'ютерів та комп'ютерних мереж або відповідають за забезпечення охорони зазначених об'єктів, на законодавчому рівні.

Необхідною умовою запобіганню вчиненню кіберзлочинів є встановлення жорсткого контролю за обігом будь-яких технічних засобів, що заборонені для використання у вільному обігу (технічні засоби для негласного зняття інформації з каналів зв'язку, для прослуховування, для визначення паролів, тощо). Незаконне використання такого обладнання може досить суттєво спростити незаконне використання комп'ютерів або отримання необхідної інформація, яка знаходиться в них, інформації, необхідної для отримання доступу до комп'ютерів або інформації, передається через комп'ютерні мережі. Так, наприклад, у вільному доступі на відкритих Інтернет сайтах можна придбати пристрій для зняття інформації з мобільних телефонів (до 8 телефонів одночасно) за суму, яка еквівалентна 200 доларам США. Отже, на наш погляд, необхідним заходом протидії кіберзлочинності є проведення правоохоронними органами робіт з відстежування зазначених сайтів з метою їх блокування та виявлення осіб, які займаються незаконним розповсюдження вказаних предметів.

Необхідним заходом протидії кіберзлочинності, на нашу думку, є перейняття досвіду діяльності правоохоронних органів інших країн у цій сфері. В першу чергу, відповідні підрозділи повинні аналізувати стан технічного забезпечення та технології, що використовуються для запобігання вчиненню зазначених злочинів (мається на увазі аналіз того, які саме технічні засоби, програмне забезпечення тощо використовуються у зазначеній сфері). На наш погляд, аналіз, наприклад, таких програм, як «Carnivore», що діє на території США і спрямована на відслідковування та аналіз електронної пошти, системи СОРМ, що діє на території Росії, яка запроваджена з метою запобігання використання мереж електрозв'язку в злочинних цілях, а саме: організації терористичної діяльності, комп'ютерній та організованій злочинності, корупції, наркобізнесу, контрабанді, шпіонажу, розповсюдженню порнографії та іншим протизаконним діям та інших програм, дозволів би суттєво покращити діяльність правоохоронних органів в аналізованій сфері.

Для реалізації зазначених заходів доцільним є прийняття участі відповідних працівників у міжнародних семінарах, круглих столах тощо, що присвячені вказаній проблематиці та ініціювання відповідними органами нашої держави проведення таких заходів на території України.

Крім того, враховуючи міжнародний характер кіберзлочинності важливим елементом запобігання є співпраця з відповідними органами інших країн, що повинно проявлятися не лише в обміні досвідом, а й проведенні спільних операцій, спрямованих на виявлення, попередження та розслідування будь-яких фактів кіберзлочинності, що мають міжнародний характер. Необхідною умовою протидії аналізованому прояву злочинності є приєднання до діяльності міжнародних програм у цій сфері.

Спеціально-кримінологічне запобігання, що, як зазначалося, також відноситься безпосередньо до діяльності Національної поліції, спрямоване головним чином на окремі соціальні групи, які привертають увагу суб'єктів превентивної діяльності: особи, які раніше вчинили злочини, звільнені з місць позбавлення волі, засуджені до покарань, не пов'язаних з позбавленням волі, й особи, від яких можна очікувати кримінальної активності внаслідок їх антисуспільної поведінки тощо. Отже, виявлення та облік осіб, які здійснюють злочинну діяльність (або схильні до неї) у сфері комп'ютерних технологій є однією із центральних організаційних проблем, оскільки специфіка виявлення й наступної роботи з такою категорією осіб залежить від особливостей зазначеної категорії злочинів, на підставі наявності у злочинців певних знань та їх роду діяльності. У зв'язку з цим необхідними умовами для розроблення ефективних заходів протидії кіберзлочинності є постійний моніторинг змін кримінологічно значущих рис особистості кіберзлочинця.

При виявленні зазначених осіб працівники підрозділів кіберполіції, а також інших підрозділів Національної поліції, які є суб'єктами протидії кіберзлочинності, повинні знати та вміти встановлювати певні ознаки, які окремо чи в поєднанні дають підстави підозрювати наявність в особи схильності (імовірність вчинення нею) до вчинення злочинів в аналізованій сфері.

Різноманітність індивідуальних проявів протиправної поведінки обумовлює динамізм відповідних криміногенних особливостей (ознак). Однак можна визначити певні об'єктивні

та суб'єктивні ознаки, що дають змогу з високим ступенем імовірності визначити можливість вчинення злочину конкретною особою [677]. Таким чином, через різноманіття як індивідуальних поведінкових моделей, так і способів вчинення протиправних діянь на сьогодні можна вести мову лише про загальні прогностичні ознаки (соціально-психологічні особливості), які можуть свідчити про ймовірність вчинення окремою особою тих чи інших злочинів у сфері комп'ютерних технологій.

Дослідники визначають наступні типи осіб, які представляють імовірне джерело загрози в глобальній мережі: внутрішні користувачі систем; незалежні хакери; службовці, колишні службовці, консультанти та тимчасові працівники підприємств, установ й організацій, діяльність яких пов'язана з комп'ютерними мережами; комп'ютерні терористи; особи, які займаються, промисловим шпіонажем; працівники іноземних розвідок; постачальники обладнання та програмного забезпечення; аудитори [678].

На нашу думку, встановлення наступних обставин сприяє виявленню осіб, які схильні до вчинення злочинів у сфері комп'ютерних технологій:

– відсутність постійного місця роботи у особи, яка має відповідну технічну освіту або раніше працювала у сфері комп'ютерних технологій;

– наявність судимості за вчинення злочинів у сфері комп'ютерних технологій;

– наявність у членів сім'ї особи судимості за вчинення злочинів у сфері комп'ютерних технологій;

– приналежність особи до кримінальної субкультури, особливо до категорії осіб, які можуть вчиняти злочини із застосуванням комп'ютерних технологій;

– наявність схильності до життя «на широку ногу», марнотратства, азартних ігор, вживання наркотиків тощо;

– наявність безконтрольної можливості підключення будь-якої особи до мережі Інтернет за допомогою бездротових приладів тощо.

У продовження викладеному варто також звернути увагу на віктимологічне запобігання кіберзлочинності. Тому на сьогодні актуальними є наступні рекомендації, як не стати жертвою кіберзлочину:

1. Користуватися лише ліцензійним програмним забезпеченням.

2. Встановити надійну антивірусну програму на комп'ютер, термінал мобільного зв'язку, інші гаджети, що керуються операційною системою й мають вихід до інформаційної мережі.

3. Періодично перевіряти свій гаджет на наявність комп'ютерних вірусів.

4. Не відкривати поштові повідомлення, що надійшли з незнайомих електронних поштових скриньок.

5. Не відповідати на телефонування та SMS-повідомлення з незнайомих телефонних номерів.

6. Тримати в секреті реквізити банківських карток. При виникненні підозри щодо спроб стороннього доступу до банківського рахунку повідомляти безпосередньо відділення банку.

7. Не здійснювати жодних операцій із використанням банківських карток, якщо є найменший сумнів у справжності або доброчесності адресата.

---

[677] Криминология: учеб. для вузов / А. И. Гуров и др.; под. ред. Н. Ф. Кузнецова, В. В. Лунеева. Москва: Волтерс Клувер, 2005. С. 344.

[678] Номоконов В. А. Актуальные проблемы борьбы с киберп-реступностью; Владивостокский центр исследования организованной преступности, Центр исследования компьютерной преступности URL: http://www.crime-research.org/library/Nomokonl.html.