СЕКЦІЯ 2
КРИМІНАЛЬНО-ПРАВОВІ, ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 343.9.01

Дмитро Володимирович ШВЕЦЬ,
кандидат педагогічних наук, доцент,
перший проректор
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-1999-9956

ПІДХОДИ ДО ВИЗНАЧЕННЯ ПСИХОЛОГІЧНОГО ПОРТРЕТУ КІБЕРЗЛОЧИНЦЯ

У сучасному світі з кожним роком кіберзлочинність стає все більш серйозною загрозою для суспільства. Безумовним пріоритетом у боротьбі з кіберзлочинами є вдосконалення технічного захисту інформації, проте цей напрямок не висвітлює суб'єктивну сторону правопорушення, вивчення якої є основою для профілактики злочинів. Це, разом із надвисоким рівнем латентності кіберзлочинів, зумовлює необхідність дослідження особи кіберзлочинця. Наслідком такого вивчення є більш глибоке уявлення про соціальні, фізичні, емоційно-психологічні прояви цього суб'єкта, що полегшуватиме його наступну ідентифікацію та розкриття злочинів, учинених у кіберпросторі. Знання основ психології кіберзлочинців допоможе в розробці засобів протидії їм, оскільки зловмисники досить часто використовують психологічні прийоми у своїй діяльності.

Сьогодні поняття «кіберзлочин» тлумачать як у вузькому сенсі – 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 договорами України (Закон України «Про основні засади забезпечення кібербезпеки України»), так і в широкому – будь-які злочини, вчинені за допомогою електронних пристроїв.

У загальному вигляді під кіберзлочинами міжнародна спільнота розуміє: незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями, пов'язані з комп'ютерами, підробки та шахрайство, всі види забезпечення обігу та використання дитячої порнографії за допомогою комп'ютерної мережі, а також порушення авторських та суміжних прав.

Основною особливістю кіберзлочинів є середовище їх здійснення – утворений електронними пристроями та їх мережами кіберпростір (або віртуальний простір). При цьому «віртуальні» предмети

психологічно здаються більш доступними, в тому числі для незаконного заволодіння ними.

Суттєвим криміногенним фактором психологічного характеру, властивим кіберпростору, є можливість збереження повної анонімності користувача пристрою або мережі (за винятком технічної інформації про підключення до мережі, способи приховування якої також існують). Анонімність дозволяє не тільки не бути ідентифікованим у певний момент часу, але також, як наслідок, надавати про себе неправдиву інформацію, вступати в соціальну взаємодію, представляючись іншою особою. Очевидно, що в умовах анонімності будь-яка людина відчуває можливість безкарно здійснювати вчинки негативного характеру, при цьому відсутність ефективних механізмів осуду тільки посилює бажання здійснювати негативні дії, особливо якщо першопричина таких дій лежить у реальному світі.

У той же час подібне відчуття безкарності впливає не тільки на окремих осіб, а й створює атмосферу вседозволеності, яка сприяє подальшому поширенню й розвитку суспільно небезпечних ідей.

Саме анонімність робить кіберпростір «паралельним» нашому звичайному життю і дозволяє створювати новий образ власної особистості або водночас кілька образів, що відрізняються від реального і не обтяжених психологічним обов'язком слідувати реальному образу, як це було б у разі ідентифікації користувача. Особливо яскраво це виражено в онлайн-іграх, де анонімність пов'язана з вигаданим світом. Тому цілком можливо, що у кіберзлочинців можуть зустрічатися психічні відхилення, які фіксують у звичайних користувачів Інтернету: інтернет-залежність, тривожні розлади, диссоціативні розлади особистості.

Можна припустити, що на кількість злочинів негативно може впливати зростання потенційних і діючих факторів соціальної взаємодії, швидкість протікання зв'язків і можливість установлення одночасно декількох зв'язків. Завдяки перерахованим факторам у кіберпросторі навіть більшою мірою, ніж у реальному світі, можливе виникнення перевантаження соціальними контактами, буває «втрата здатності та можливості зосереджувати увагу на конкретній людині», що веде не стільки до озлоблення й агресії, як у реальному світі, скільки до «знецінення» кожного з контактів на тлі «тріумфу» власного «Я», забезпеченого суб'єктивним сприйняттям кіберпростору.

Значне місце займають психологічні процеси, що протікають при безпосередньому вчиненні кіберзлочину. На відміну від переважної більшості звичайних злочинів, вчинення кіберзлочину не вимагає, як правило, будь-яких пересувань або вчинення будь-яких активних фізичних дій. Кіберзлочинець під час реалізації свого злого умислу перебуває вдома, в комп'ютерному клубі, місці з безкоштовним доступом до мережі Інтернет, будь-якому іншому місці, яке для нього

є комфортним або знайомим. 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 обмежена технічними рамками, що дозволяє передбачувати наслідки своїх дій. Це, у свою чергу, дозволяє зловмисникові не відчувати невизначеності ситуації, планувати свої дії навіть за несприятливих для нього обставин, а значить – відчувати себе більш впевнено і спокійно під час вчинення злочину.

Якщо після вчинення звичайного злочину на злочинця, як правило, більшою мірою починає впливати фактор невизначеності свого положення, обумовлений, з одного боку, свідомістю винності та страхом покарання, а з іншого – браком інформації про заходи, які проводяться правоохоронними органами для розслідування злочину і викриття винного, то в разі вчинення кіберзлочину дія цього чинника може зменшуватися або виключатися з двох причин. По-перше, при здійсненні кіберзлочинів злочинці, впевнені у високому рівні своїх знань і можливостей, а часом і у своїй геніальності, припускають, що не залишили жодного сліду, який міг би допомогти викрити їх. По-друге, в наш час органи, які ведуть боротьбу з кіберзлочинністю, не завжди володіють достатнім інтелектуальним і кадровим потенціалом, що веде до недооцінки їх кіберзлочинцями.

Важливим моментом для юридичної практики є встановлення мотивів та цілей вчинення злочину. Складність полягає в тому, що мотивація кіберзлочинців формується одразу в двох просторах – реальному та кіберпросторі. При цьому на формування мотивації більший вплив може чинити і той, і інший простір. У кіберпросторі, як у фактично паралельній реальному світу соціальній системі, разом зі змішанням національних культур і зародженням власної кіберкультури відбуваються ті ж процеси з соціальними нормами. Деякі з соціальних норм в кіберпросторі відмирають, оскільки є непридатними, але при цьому під впливом низки негативних факторів, притаманних кіберпростору, формуються нові норми. Можна припустити, що оскільки кіберпростір відіграє чималу роль у житті молоді, то у свідомості молодих активних користувачів Інтернету відбувається заміщення соціальних норм нормами кіберпростору, точно так само можуть нівелюватися соціальні норми реального життя, непридатні у мережі.

При спробі класифікувати кіберзлочинців за їхньою психологічною характеристикою можна, взявши за основу вид злочину та рівень комп'ютерних навичок, навести наступні групи:

– злочинці «спеціального» кіберзлочинного типу, які володіють професійними технічними знаннями, що фактично означає належність такого злочинця до субкультури хакерів (крекерів);

– злочинці «загальнокримінального» типу, які за допомогою електронних пристроїв здійснюють злочинні дії (шахрайство, крадіжки, відмивання грошових коштів, незаконне розповсюдження

порнографічних матеріалів тощо), не застосовуючи при цьому спеціальні технічні знання або використовуючи тільки поверхневі знання й набуті програмні засоби.

Залежно від мотивації злочинної поведінки можна виділити такі типи кіберзлочинців:

– корисливого типу (дії спрямовані на здобуття матеріальних цінностей у будь-якій формі);

– насильницького типу (незважаючи на відсутність фізичного контакту з особою, дії спрямовані на доведення до самогубства, залякування, погрози вбивством, психологічний тиск тощо);

– сексуального типу (дії спрямовані на незаконне розповсюдження порнографічних матеріалів або предметів, без мети наживи, спонука до дій сексуального характеру, розпусні дії тощо);

– ідеологічно або політично вмотивований тип (дії особи є формою протесту і політичної або ідеологічної боротьби у кіберпросторі);

– соціально дезорганізуючий тип (основною метою є саме порушення соціальних норм і надання деструктивного впливу на соціум і суспільні відносини);

– статусний тип (дії спрямовані на отримання/підвищення неформального соціального статусу, найчастіше в спільнотах кіберсоціуму);

– дослідницький тип (дії спрямовані на вивчення програмних і апаратних складових електронних пристроїв і їх мереж, пошук вразливостей, можливості їх використання та усунення).

До портрета особистості кіберзлочинця слід додати наступні загальні для всіх їх характеристики: філософський склад розуму; дезорганізуючий тип злочинця; особливе ставлення до жертви; особливий тип мотивації; специфічна взаємодія з особами свого роду діяльності; обумовленість місця проживання певною місцевістю; необхідна наявність матеріально-технічної забезпеченості; галузі переважної зайнятості для відвернення уваги.

Отже, кіберзлочинець – це особа, що має надвисокі інтелектуальні здібності, ультрависокий рівень спланованості й підготовки злочину, великі знання у галузі комп'ютерної безпеки та бере участь у вчиненні злочину з великим рівнем суспільної небезпеки. Найбільш серйозні атаки вчиняються групами кіберзлочинців, тому слід відстежувати їхню комунікацію. Чітке уявлення внутрішніх та зовнішніх характеристик суб'єкта злочину дає можливість прогнозувати його дії, мислити, як він, та усвідомлювати наперед його кроки. Це полегшує його ідентифікацію, дає можливість припиняти та попереджувати плановані кіберзлочини.

Подальше вивчення психології кіберзлочинців вимагає великого обсягу емпіричних даних, які можуть бути отримані при роботі зі злочинцями в ході слідства. Велике значення в таких дослідженнях має обмін отриманою інформацією між правоохоронними органами різних країн.

Одержано 02.11.2018