3. Блищенко И.П. Международный уголовный суд. Москва : Закон и право, «ЮНИТИ», 1998. 240 с.

4. Военные преступления : Это надо знать всем / под ред. Р. Гутмена, Д. Риффа ; юрид. ред. К. Андерсон; пер. с англ. О. А. Варшавер. Москва : 2001. 486 с.

Страшко Олександр Павлович,
курсант взводу ФЕБ - 841,
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник: к.е.н., доцент кафедри
фінансово-економічної безпеки Г.В. Соломіна

АКТУАЛЬНІ ПИТАННЯ БОРОТЬБИ ІЗ КІБЕРЗЛОЧИНАМИ

Розвиток сучасної цивілізації характеризується переходом від індустріального суспільства до інформаційного. Широке впровадження сучасних інформаційних технологій створює нові можливості для активного і ефективного розвитку економіки, політики, держави, суспільства, соціальної свідомості і громадянина. Однак вдосконалення технологій призводить не тільки до зміцнення індустріального суспільства, а й до появи нових джерел небезпеки для нього. Таким чином, актуальність дослідження обумовлена наступними проблемами: брак даних, втрата місця розташування і правові обмеження кібер-діяльності.

Брак даних. Інтернет-провайдери мають змогу зберігати інформацію для комерційних чи бухгалтерських цілей, до яких не мають доступу правоохоронні органи. Такі невідповідності перешкоджають роботі компетентних органів з кібернетики та призводять до гальмування слідства, і в кінцевому рахунку, можуть вплинути на можливість ефективного переслідування злочинної діяльності в Інтернеті. Крім того, ситуація, що склалася, може створити несправедливий тиск на слідчі органи щодо надання пріоритетності їх діяльності відповідно до існуючих в даний час різних систем зберігання даних, а не зосередження уваги на триваючому слідстві [1]. Все більша кількість постачальників електронних послуг реалізує шифрування за замовчуванням у наданні своїх послуг. У той же час широко доступні інструменти, що дають можливість особистого шифрування комунікаційних та інших даних. Це означає, що традиційні методи комунікації, такі як прослуховування, стають менш ефективними. Як результат, злочинці можуть ефективно приховувати критичні докази та діяльність (наприклад, пряму трансляцію сексуальної експлуатації дітей) від правоохоронних органів. Крім того, використання децентралізованих віртуальних валют та збільшення використання сервісів, ефективно перешкоджають правоохоронним органам «слідкувати за грошима» та значно ускладнюють можливості відновлення активів та запобігання шахрайським операціям [2].

Втрата місця розташування. Останні тенденції, такі як збільшення кримінального використання шифрування, інструментів анонімізації, віртуальних валют та «темних» мереж призвели до ситуації, коли правоохоронні органи вже не можуть (достатньо точно) встановлювати фізичне місцезнаходження підозрюваного, кримінальні схеми чи електронні докази. У таких ситуаціях часто незрозуміло, яка країна має юрисдикцію та яка законодавча база регулює збір доказів (у режимі реального часу) або використання спеціальних слідчих повноважень, таких як моніторинг злочинної діяльності в Інтернеті та різні оперативні заходи. Більше того, зростаюче використання, так званих, хмарних систем зберігання означає, що інформація, яка зберігається у «Хмарі» та бути фізично розташована в юрисдикціях різних держав, які можуть мати несумісні законодавчі рамки. Втрата місця розташування також може спричинити конкурентні позови у притягненні до кримінальної відповідальності, підкреслюючи необхідність якнайшвидшого залучення судових органів, прямих каналів поліції для співпраці, комунікації та постійному обміну інноваціями у процесі оперативного співробітництва із іншими країнами [3].

Правові обмеження кібер-діяльності. Незважаючи на існування міжнародних законодавчих актів, розбіжності у вітчизняній законодавчій системі часто є серйозною перешкодою міжнародному кримінальному розслідуванню та переслідуванню кіберзлочинності. Частково це пов'язано з неповним імплементуванням міжнародних правових механізмів до внутрішнього законодавства. Основні відмінності стосуються рівня девіантної поведінки, а також положень щодо розслідування кіберзлочинності та збору електронних доказів. Адаптація та узгодження цих законодавчих обмежень часто забирає багато часу. Застосування чинного законодавства, і можливо його розширення шляхом пошуку судової практики щодо нових розробок (наприклад, віртуальних валют, засобів анонімізації та різних кримінальних способів функціонування), а також впорядкування існуючих операційних процесів (стандарти збирання та передачі електронних доказів). Тим не менш, розповсюдження Інтернету та зростаюча складність кіберзлочинних організацій вимагають спеціального законодавства, яке регулює присутність та дії правоохоронних органів в онлайн-середовищі (включаючи таємну діяльність та усунення цифрової кримінальної інфраструктури). У міжнародному практиці не існує спільної правової бази для прискореного обміну доказами (як це існує для збереження доказів). Це означає, що на практиці, докази зберігаються, але знадобитися багато часу, перш ніж вони стануть доступними для розслідування кримінальної справи або судового розгляду в країні, яка здійснює запит [4].

Рівень кіберзлочинності має тенденцію до зростання. Показники динаміки кіберзлочинності в цілому відповідають показникам загальної злочинності в країні, що свідчить про відставання можливостей правоохоронних органів від сучасного рівня технологічного та програмного забезпечення кримінальної активності. Найбільш ефективними заходами, безпосередньо спрямованими на протидію кіберзлочинності, є такі:

збільшення кількості планових і позапланових перевірок; установлення жорсткого контролю за обігом технічних засобів, заборонених або обмежених у вільному цивільному обігу; перейняття досвіду діяльності правоохоронних органів інших країн у цій сфері; співробітництво з відповідними органами інших країн щодо розкриття, розслідування та запобігання злочинам в аналізованій сфері, обмін досвідом правозастосування; виявлення осіб, схильних до вчинення злочинів в аналізованій сфері.

Список використаних джерел:

1. Іванченко О.Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. Актуальні проблеми вітчизняної юриспруденції. 2016. Вип. 3. С. 172–177.
2. Конвенція про кіберзлочинність: міжнародний документ від 23.11.2001//База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.11.2019).
3. Кравцова М.О., Литвинов О.М. Запобігання кіберзлочинності в Україні: монографія. Харків: Панов, 2016. 212 с.
4. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. Право і Безпека. 2009. № 4. С. 215–219.

Тарасенко Володимир Володимирович,
курсант 3 курсу, спеціальність 081 «Право»
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник: д.е.н., доцент, Паршин Юрій Іванович
професор кафедри фінансово-економічної безпеки ДДУВС

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ПОПЕРЕДЖЕННЯ ЕКОНОМІЧНОЇ ЗЛОЧИННОСТІ

Своєчасне здійснення діяльності з попередження злочинності в державі дозволить забезпечити вирішення багатьох інших проблем, серед яких економічні, політичні, ідеологічні, соціальні, моральні, організаційні тощо.

Попередження злочинності – це багаторівнева система заходів (державних, громадських, спеціальних), спрямованих на виявлення, усунення, обмеження, ослаблення або нейтралізацію причин і умов злочинності, окремих видів злочинів і конкретних злочинів, а також на утримання від переходу або повернення на злочинний шлях людей, умови життя і поведінка яких вказують на реальну можливість вчинення ними злочинів у майбутньому.

Забезпечення економічної безпеки держави є надзвичайно важливою передумовою формування стійкого збалансованого розвитку країни та зростання її конкурентоспроможності на міжнародному ринку. На сучасному етапі розвитку економіки гостро постає питання організації ефективної системи попередження та протидії економічній злочинності, як однієї із