

ПИТАННЯ КРИМІНАЛЬНОГО ПРАВА, КРИМІНОЛОГІЇ ТА КРИМІНАЛЬНО-ВИКОНАВЧОГО ПРАВА

ГАРКУША Ю. О.,
аспірант кафедри кримінології
та кримінально-виконавчого права
(Національний університет
«Одеська юридична академія»)

УДК 343.983:004.056.5

ІНФОРМАЦІЙНА БЕЗПЕКА СУЧАСНОГО УКРАЇНСЬКОГО СУСПІЛЬСТВА

У статті розглядається проблема зростаючого впливу соціальних мереж на національну безпеку країни, акцентується увага на інформаційну безпеку особистості, держави, суспільства; пропонується бачення дій української влади щодо захисту вітчизняного сегмента інформаційного простору.

Ключові слова: соціальні інтернет-мережі, інформаційна безпека, інформаційне суспільство, інформаційно-психологічний вплив, державна інформаційна політика.

В статье рассматривается проблема растущего влияния социальных сетей на национальную безопасность страны, акцентируется внимание на информационной безопасности личности, государства, общества; предлагается введение действий украинской власти по защите отечественного сегмента информационного пространства.

Ключевые слова: социальные интернет-сети, информационная безопасность, информационное общество, информационно-психологическое воздействие, государственная информационная политика.

The problem of growing influence of social networks on national security of country, focus is on information security of individual, state, society; it proposes introduction of Ukrainian government action to protect domestic segment of information space.

Key words: social online networks, information security, information society, information and psychological impact, state information policy.

Вступ. Сучасне суспільство не може існувати без безперервного обміну інформацією та використання інформаційних технологій. Більш того, підвищення важливості інформації в житті суспільства і зростання числа людей, зайнятих у сфері інформаційної індустрії, стають не просто черговим етапом науково-технічного прогресу, а новою ерою в розвитку людства. У зв'язку з цим не може не змінюватися ситуація щодо дослідження ціннісної орієнтації особистості, її інформаційного обґрунтування та інформаційної безпеки. Багато країн світу почали співвідносити свої державні інтереси з розвитком інформаційної інфраструктури, активною інформаційною взаємодією з громадянським суспільством і засобами масової інформації. Але в той же час на державному рівні прийшло і розуміння того, що зловживання свободою масової інформації в сучасних умовах може представляти загрозу для національної безпеки країни. Будучи важливим фактором життя суспільства, інформа-



ційна сфера має суттєвий вплив на стан політичної, оборонної та економічної складових безпеки України. Від забезпечення інформаційної безпеки істотно залежить національна безпека України, і ця залежність буде значно зростати в ході технічного прогресу і проникнення інформаційних технологій в усі сфери діяльності сучасного суспільства. У зв'язку з цим інформаційна безпека стає найважливішим базовим елементом всієї системи безпеки Української держави.

Так, найбільш популярним прикладом комунікації в мережі Інтернет є соціальні мережі, які донедавна стали засобом вираження активної громадянської позиції, формування суспільної думки, впливу на політичні рішення влади. З одного боку, вони є одним із небезпечних інструментів інформаційно-психологічного впливу й маніпулювання масовою свідомістю, що становлять загрозу стабільності та національній безпеці будь-якої країни, у тому числі України. З іншого боку, не можна забувати про свободу слова, без якої не може існувати громадянське суспільство. Однак, незважаючи на позитивні сторони цього явища, прикладом є інформаційно-експансіоністська кампанія, що була розв'язана між Росією та Україною під час незаконної анексії АР Крим та агресії на південному сході України, яка досягла своїх певних цілей, перш за все, завдяки активному використанню соціальних інтернет-мереж.

Проведений аналіз вивчення проблеми інформаційної безпеки показав, що, незважаючи на величезний інтерес до проблеми, її вивчення має переважно техніко-прикладний характер і орієнтоване на рішення конкретних науково-технічних завдань. Лише в небагатьох роботах актуалізується кримінологічний аспект проблеми інформаційної безпеки. Інформаційна безпека в контексті кримінології лише починає досліджуватися, і цілі галузі знання, пов'язані з функціонуванням різних соціальних інститутів, залишаються мало вивченими. Здебільшого у роботах аналізуються в основному причини виникнення інформаційних загроз, їх характерні особливості, розглядаються окремі технічні питання [1–3]. Окремі автори аналізують зміст і сутність інформаційного протистояння, вибудовують моделі протидії інформаційним операціям, деструктивним інформаційним впливам та інформаційним потокам [4]. Низку робіт присвячено уточненню існуючих та наведенню нових визначень форм інформаційної боротьби в рамках запровадження єдиної термінології [5], досліджується еволюція інформаційно-психологічного протистояння, спеціальних інформаційних операцій та акцій інформаційного впливу [6].

Постановка завдання. Метою статті є розгляд проблеми активного поширення і розвитку соціальних мереж у контексті їх використання для диференційованого впливу на суспільство, розкриття технологій та механізмів їх маніпулятивного застосування, визначення заходів для захисту національного інформаційного простору.

Результати дослідження. Однією з умов формування інформаційного суспільства є розгортання єдиного для України інформаційного простору. В рамках інформаційного суспільства створюється інформаційна економіка, пов'язана з автоматизованою обробкою, обміном по каналах зв'язку і практичним використанням, насамперед, формалізованої інформації. Наступною умовою формування інформаційного суспільства є впровадження та підтримання в актуальному стані єдиного інформаційного простору формалізованих даних України. Третьою умовою розвитку інформаційного суспільства є наявність інформаційно-комунікаційних технологій, що реалізують інформаційний обмін між усіма елементами інформаційного суспільства, основою яких в сучасних умовах служить глобальна інформаційна мережа Інтернет.

Фактори безпеки держави завжди безпосередньо співвідносилися зі стійкістю його внутрішнього і зовнішнього становища. У суспільних науках стійкість країни пов'язувалася, насамперед, з економічним зростанням або стабільністю. Питання інформаційного благополуччя суспільства привернули пильну увагу вітчизняних учених тільки в останні роки, і викликаний цей відсоток саме зростанням ролі інформаційних технологій. Однак усвідомлення того факту, що інформаційне благополуччя означає безпеку, прийшло не відразу.

У зв'язку з цим політичні і наукові кола в Україні довгий час не розглядали проблеми економічної та інформаційної безпеки, як такої. Сама постановка питань, що стосуються да-



ної теми, що не була актуальна в теорії і практиці аж до 1991 року, коли стало очевидно, що соціально-економічна система українського суспільства не може ефективно чинити опір зовнішнім загрозам. Такі терміни, як «безпека» [7, с.90-98], «державна безпека» [8, с. 7–9] вживалися лише в сенсі «громадська безпека» і тільки в службових та офіційних документах.

Термін же «інформаційна безпека» взагалі стає актуальним тільки останнім часом, що вимагає глибокого наукового аналізу та криминологічного опрацювання основних елементів даного явища. Інформаційна безпека входить у структуру загальної національної безпеки держави. Під інформаційною безпекою України, як частиною системи загальної безпеки держави, розуміється стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства і держави [9].

Разом із тим у науковій літературі термін «інформаційна безпека» визначається аж ніяк не однозначно. Наприклад, ряд дослідників відзначає, що інформаційна безпека – це стан захищеності особистості, суспільства і держави в інформаційній сфері від можливих внутрішніх і зовнішніх загроз. Існують також й інші точки зору на саме поняття «інформаційна безпека» [10–12].

Сьогодні популярним явищем, що стрімко розвивається в системі інформаційних технологій, є соціальні мережі. І хоча для більшості нинішніх «споживачів» їх благ це, в основному, лише засіб спілкування, для частини особливо «просунутих» користувачів – це не тільки пристойний заробіток, але і майданчик для досягнення конкретних економічних, соціальних і політичних завдань. Соціальні мережі з наявним ресурсом соціальної довіри наразі досить успішно використовуються для просування власних інтересів, для введення в суспільний обіг тенденційної та відверто шкідливої для суспільної свідомості інформації, а також для організації і керівництва соціальними заворушеннями в інших країнах шляхом:

- розпалювання протестних настроїв серед населення з використанням блогів, форумів та розсиланням повідомлень користувачам соціальних мереж;
- визначення часу початку акцій протесту, що приурочуються до знакових подій, зокрема: оголошення результатів виборів; резонансних інцидентів; світських і релігійних свят тощо;
- розсилання (анонімно або від імені відомих осіб, опозиційних організацій) закликів вийти на мітинги та демонстрації з визначенням точного місця і дати їх проведення. Залежно від ситуації заклики можуть надсилатись на адресу визначених груп осіб (певної національності або віросповідання, молоді тощо);
- керівництва ходом проведення протестних акцій через розсилання повідомлень про зміну місць і часу проведення мітингів та напрямів зосередження зусиль.

Існує справедлива думка, що надлишок інформації та простота її поширення призводять до того, що цінністю стає зовсім не отримання нами інформації, а її доведення до нас тими, хто в цьому зацікавлений. Тому змінюється економічна модель роботи з інформацією. За інформацію платить той, хто хоче її поширювати, а не той, хто хоче її отримувати [13]. І в цьому полягає загроза. Той, хто володіє засобами, володіє і шляхами поширення «своєї» інформації, а значить і можливостями впливати на рішення людей. Так, сьогодні соціальні мережі активно використовуються провідними країнами світу, у першу чергу такими, як США, Росія, Китай та іншими для просування власної ідеології та посилення свого впливу на ситуацію в певних країнах.

Серед великої кількості існуючих на сьогодні соціальних мереж необхідно відмітити такі, які завдяки накопиченому інтелектуальному потенціалу, високому професіоналізму команди розробників, створеним ними технологіям та можливості швидко розв'язувати складні проблеми є інформаційними ресурсами, що мають значний вплив на суспільство. Найбільш відомими мережами, в яких спілкується більшість населення, у тому числі українців, є Facebook, Twitter, «В контакте», Live Journal, You Tube та «Однокласники». Багато вже пророкують, що протягом останніх п'яти років соціальні мережі в корені змінять роль і місце звичних інформаційних агентств та інтернет-ресурсів. Адже соціальна мережа – це не просто клуб віртуальних друзів, це – нове інформаційне поле, простір нових протистоянь і конфліктів, які вже почалися.



Сьогодні в багатьох країнах місце вираження протесту перенесено з «вулиці» у віртуальний простір. Соціальні мережі стають не тільки «притулком» людей, які активно виступають із конкретними політичними вимогами, але і майданчиком для підготовки державних переворотів. Практично з 2010 року на тлі хвилювань у цілому ряді країн Північної Африки і Близького Сходу тривають події, які отримали назву «арабської весни» [14]. Під впливом цих подій було повалено кілька правлячих режимів, а у випадку з Лівією – навіть убитий керівник держави. Всі ці події об'єднувала одна важлива риса – в їх підготовці активно був задіяний Інтернет, а точніше – соціальні мережі. Група активістів опозиційного руху (як правило, представники молоді), створювали віртуальні спільноти незадоволених політикою чинної влади, де за підтримки ззовні поширювали заклики до зміни політичного ладу і організовували акції опозиції. Зокрема, в організації революцій в арабському світі широко використовувалися можливості таких соціальних мереж, як Twitter і Facebook. Взагалі аналіз останніх «інтернет– революцій» у Північній Африці і на Близькому Сході дає вражаючі результати. Можна сказати, що вперше соціальні мережі були не просто постачальниками кібер-послуг, а основними розповсюджувачами «революційної» іскри.

У період єгипетських подій влади країни з введенням спеціальних поліцейських підрозділів і армії в місто, прагнучи придушити виступи ще в зародку, відключали доступ до Інтернету і мобільний зв'язок. Однак учасники протесту за допомогою все тих же соціальних мереж, а вірніше їх власників, «зуміли» обійти обмеження, введені єгипетським урядом, і отримати доступ до соціальних мереж [15]. На сторінках користувачів цих соціальних мереж стали з'являтися інструкції для протестуючих, що пояснювали, як скористатися модемним доступом до Інтернету в обхід обмежень, введених урядом. «Перейшовши» на бік воюючої опозиції, Google і Twitter об'єднали зусилля і відкрили три телефонні лінії – в США, Італії та Бахреїні, зателефонувавши на які люди могли записати свої твітти, як голосові повідомлення. Фактично вперше провідні пошукові системи і соціальні мережі об'єдналися, щоб підтримати інформаційний потік під час масових заворушень усупереч зусиллям уряду сформувати «потрібну» громадську думку.

Практично такий же сценарій зараз розвивається і в Сирії, де за повідомленнями «проурядових» сирійських блогерів в інтернет-просторі була організована антисирійська кампанія шляхом викиду великої кількості брехливих статей та інформаційних бюлетенів, аналітичних матеріалів і повідомлень «Твіттер», які тут же з'являлися в «Google-пошуковик». На їхню думку, соціальні мережі активно використовували аудіозаписи невідомих свідків із місць подій, відеозаписи, зняті в інших країнах регіону і при інших обставинах. Ці голосові повідомлення і відео видавалися за «сирійські» і масштабно розсилалися по мережі через Facebook, Youtube і мікроблоги в Twitter з метою нагнітання страху, створюючи певну світову громадську думку.

Після 2010 року хвиля акцій, підготовлених у соціальних мережах, пройшла і по страдянському простору. Несанкціоновані пікети і мітинги в Азербайджані, Вірменії, Білорусі, Росії, Україні та інших країнах. Практично в кожному випадку в підготовці до цих акцій були використані соціальні мережі.

Останнім вагомим прикладом агресивного інформаційного впливу з активним залученням соціальних мереж слід вважати їх використання Російською Федерацією в ході підготовки та здійснення агресії в Криму. Адже дестабілізація обстановки на півострові почалася із зовнішньої інформаційної агресії в соціальних мережах. Це була особлива форма ведення інформаційної війни з використанням заздалегідь заготовленого дезінформаційного контенту, спеціально підготовлених інформаційних груп у соціальних мережах, що використовували методи масової психологічної обробки інтернет-користувачів і населення АР Крим. Соціальні мережі використовувалися як інформаційна зброя, як засіб для проведення акцій дезінформації. Ще до подій березня 2014 року пропаганда з боку Росії велася із залученням усіх інформаційних систем: ЗМІ (телеканали НТВ, Россия-24, РТР та інші), різноманітні портали новин (Итар-ТАСС, РИА Новости), онлайн-додатки для мобільних пристроїв («Становление империи», «Мировое господство»), соціальні мережі («В Контакте», «Одноклассники», Facebook, Twitter) [16]. Нинішньою особливістю політики РФ у контексті



використання соціальних мереж є те, що російська влада активно вживає заходів, щоб узяти їх під повний контроль та зробити інструментом впливу як на внутрішнє, так і на зовнішнє інформаційне середовище. Протягом останнього року Держдумою та урядом РФ було прийнято низку законів і постанов щодо контролю за ресурсами, які поширюють інформацію в мережі Інтернет (пошукові системи, блоги, соціальні мережі, форуми).

На сьогодні уряди багатьох країн уже усвідомили, що неконтрольоване використання соціальних мереж становить безпосередню загрозу національній безпеці та стабільності держави, тому владні структури вживають дієвих заходів із забезпечення безпеки власного інформаційного простору. Суспільна небезпека, яку несуть деструктивні дії з використанням соціальних мереж, вимагає ефективної організації протидії цим процесам та явищам. З огляду на це створюються та впроваджуються національні комплексні системи кібербезпеки, що дозволяють оперативно відстежувати процеси зростання соціальної напруженості, провокування безладу, протестні й електоральні настрої в соціальних медіа щодо основних політичних партій, діяльність екстремістських і терористичних угруповань, прояви комп'ютерної злочинності та злочинів проти суспільної моралі тощо, оперативно реагувати на них. Окремі країни захищають свій національний інформаційний простір шляхом постійного моніторингу соціальних мереж та їх негайного блокування у разі виявлення загроз національній безпеці від цих сервісів.

Показовим прикладом у цьому плані є державна політика сучасної КНР стосовно національної стратегії у забезпеченні інформаційної безпеки країни. Китай, як і інші провідні країни світу, намагається протистояти противнику безкровними методами, замість зброї використовувати сучасні інформаційні ресурси й технології, дотримуючись відомого вислову китайського великого стратега і мислителя Сунь Цзи: «Воювати без зброї, перемагати без бою» [17]. Китай на сьогодні впевнено зберігає пальму першості в інформаційній війні. За оцінками американських експертів у китайській армії є спеціальні підрозділи, що спеціалізуються на кібервійнах, які навіть здатні в разі потреби вивести з ладу більшість об'єктів інформаційної інфраструктури США.

Також необхідно підкреслити ту важливу роль, яка відводиться соціальним мережам у діяльності іноземних розвідувальних структур. З урахуванням того, що Інтернет у свій час створювався на замовлення Міністерства оборони США, не виключено, що і створення соціальних мереж із самого початку передбачало їх використання з розвідувальною метою. Ні для кого не є таємницею, що спецслужби деяких країн давно і цілеспрямовано використовують соціальні мережі, як специфічні розвідувальні канали. Підтвердженням цього є вислів Джозефа Фістанакіса з IntelNews.org, співавтора доповіді Intelligence Studies Yearbook у 2012 році, підготовленої Середземноморською Радою з досліджень у галузі розвідки: «Ми пояснюємо, що Facebook, Twitter, YouTube і ціла низка інших соціальних мереж все більше розглядаються спецслужбами як безцінні канали отримання інформації» [18].

Висновки. Проаналізувавши фактично всі події, що відбулися за останній рік, слід говорити про «перехід» соціальних мереж від інформаційного поля в бік політичного лобіювання, а іноді – і просто політичної перебудови конкретно взятого суспільства. Проблеми інформаційної безпеки сучасного українського суспільства, держави, особистості, їх захисту від різного виду погроз як зовнішніх, так і внутрішніх мають сьогодні безсумнівно теоретичну і практичну актуальність. Однак сьогодні можна запропонувати такі пропозиції щодо вирішення даного питання:

- розвиток власних ефективних засобів інформаційного впливу на громадську думку за кордоном;
- формування основ державної системи протидії акціям інформаційно-психологічного тиску в блогосфері і соціальних мережах проти керівництва та населення України;
- вироблення нормативно-правових механізмів захисту інформаційного простору України від негативного інформаційного впливу в блогосфері і соціальних мережах;
- вдосконалення національного законодавства, спрямованого на підвищення рівня комунікаційного суверенітету, правових заходів щодо захисту громадян країни від негативного інформаційно-психологічного впливу;



- моніторинг діяльності та виявлення негативних комунікаторів, які прагнуть підірвати інформаційний суверенітет держави;
- моніторинг соціальних мереж із метою блокування поширення в інформаційному просторі негативної інформації, спрямованої на підрив національного суверенітету та територіальної цілісності України;
- поширення в соціальних мережах повної і точної інформації про зовнішньополітичні ініціативи і дії, внутрішній соціально-економічний розвиток країни, досягнення культури і науки;
- активізація інформаційного обміну та міжнародного співробітництва в інформаційній сфері.

Метою подальших наукових досліджень має бути розроблення сучасних методів захисту національного інформаційного простору в українському сегменті мережі Інтернет із метою контролю та управління діяльністю соціальних мереж, механізмів їх використання для просування внутрішньої та зовнішньої політики України.

Список використаних джерел:

1. Почепцов Г.Г. Контроль над разумом / Г.Г. Почепцов. – Київ: Києво-Могилянська академія, 2012. – 350 с.
2. Супрунов Ю.М. Напрями та окремі проблеми використання соціальних сервісів Інтернету в контексті інформаційної безпеки держави / Ю.М. Супрунов // ЖВІ НАУ. – 2013. – № 7. – С. 145–159.
3. Петрик В.М. Сугестивні технології маніпулятивного впливу / В.М. Петрик, М.М. Присажнюк, Л.Ф. Компанцева. – Київ: ВІПОЛ, 2011. – 248 с.
4. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В.П. Горбулін, О.Г. Додонов, Л.Ф. Присажнюк. – Київ: Інтертехнологія, 2009. – 163 с.
5. Левченко О.В. Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату / О.В. Левченко. – Київ: МО. – Наука і оборона : зб. наук. праць, 2013. – 21 с.
6. Жарков Я.М. Інформаційно-психологічне протиборство (еволюція та сучасність) / Я.М. Жарков, В.М. Петрик, М.М. Присажнюк. – Київ: ПАТ Віпол, 2013. – 201 с.
7. Заплатинський В.М. Логіко-детермінантні підходи до розуміння поняття «Безпека» / В.М. Заплатинський // Вісник Кам'янець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоров'я людини. – Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2012. – № 5. – 248 с.
8. Труды Высшей школы КГБ СССР. – 1975. – № 9.
9. Князев А.А. Информационная война // Энциклопедический словарь СМИ / А.А. Князев. – Бишкек: Издательство КРСУ, 2002.
10. Кисляковский А.В. Административно-правовое обеспечение информационной безопасности : дис. канд. юр. наук / А.В. Кисляковский. – Москва, 2003.
11. Курушин В.Д. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев. – Москва, 1998.
12. Мартиросян Т.А. Правовое обеспечение информационной безопасности РФ: автореф. дис. на доб. науч. степени канд. юр. наук / Т.А. Мартиросян. – Москва, 2005.
13. Мирошниченко А. Почему устарели СМИ? Потому что новость нельзя не узнать. [Электронный ресурс] / А. Мирошниченко. – 2011. – Режим доступа до ресурсу: www.slon.ru/1Шsia/pochemu_ustareli_smi_potomu_chno_novost_nelzya_ne_uznat-693227.xhtml.
14. Гуменюк Н. Майдан Тахрір. У пошуках втраченої революції / Н. Гуменюк. – Київ: Політична критика, 2015.
15. Бочаров Ю. Киберпреступность и кибертерроризм. Новая глобальная угроза государственному строю. [Электронный ресурс] / Ю. Бочаров. – 2011. – Режим доступа до ресурсу: www.elections-ices.org/russian/publications/textid:12835.
16. Спільнота MDK на ВКонтатті заробляє до \$1 млн на рік. [Електронний ресурс]. – 2014. – Режим доступа до ресурсу: <http://watcher.com.ua/spilnota-mdk-na-vkontakti-zaroblyaye-do-1-mln-na-rik>.



17. Tzu S. The Art of War. [Електронний ресурс] / Sun Tzu. – Режим доступу до ресурсу: <http://classics.mit.edu/Tzu/a>.

18. Fitsanakis J. US cybersecurity posture is not purely defensive. [Електронний ресурс] / Joseph Fitsanakis // Comment. – 2012. – Режим доступу до ресурсу: <http://intelnews.org/2012/05/28/01-999>.

ДИКА Є. О.,
аспірант кафедри кримінології та
кримінально-виконавчого права
(Національний університет
«Одеська юридична академія»)

УДК 343.9.01.001.33

ДОКТРИНАЛЬНІ ПІДХОДИ ДО КЛАСИФІКАЦІЇ КРИМІНОГЕННИХ СИТУАЦІЙ ТА ЇХ ЗНАЧЕННЯ ДЛЯ СУЧАСНОЇ КРИМІНОЛОГІЧНОЇ НАУКИ

Стаття присвячена аналізу існуючих в кримінологічній науці класифікацій криміногенних ситуацій і дослідженню їх теоретичного та практичного значення.

Ключові слова: ситуація, криміногенна ситуація, класифікація, копінг-поведінка, профілактика злочинів.

Статья посвящена анализу существующих в криминологической науке классификаций криминогенных ситуаций и исследованию их теоретического и практического значения.

Ключевые слова: ситуация, криминогенная ситуация, классификация, копинг-поведение, профилактика преступлений.

The article analyzes existing criminological science classifications crime situation and investigation of their theoretical and practical importance.

Key words: situation, crime situation, classification, coping behavior, crime prevention.

Вступ. Складні життєві ситуації, негативні соціально-політичні події, негаразди у професійній діяльності призводять до дисфункцій у процесі розвитку конкретної особистості. Вміле та правильне використання відповідних стратегій, які можуть надавати особі кваліфіковані відповіді на те, як поводити себе в тих чи інших ситуаціях, визначить подальший процес саморегуляції відносин між особою та злочинцем. Тому існуючі класифікації ситуацій можуть набути більшого значення та допомогти при розв'язанні деяких конфліктів.

У кримінологічній науці вивченням криміногенної ситуації, а також її впливом на суб'єкт злочину займалося чимало вітчизняних та зарубіжних вчених. Безпосередньо багатокритеріальні та одиничні класифікації криміногенних ситуацій, які можливо інтерпретувати в прикладне вираження та використати при спробі профілактики правопорушень вивчали такі вчені, як Є.М. Блажівський, П.М. Бузало, Л.А. Волкова, В.В. Голіна, С.Ф. Денисов, О.М. Джужа, А.П. Закалюк, С.М. Іншаков, О.В. Кириченко, В.М. Кудрявцев, Н.Ф. Кузнєцова, В.В. Лунєєв, В.Д. Малков, І.Г. Малкіна-Пих, В.І. Полубінський, С.О. Степанчикова, Є.В. Черних та інші.

