

УДК 35.746.1

СЕМЕНЮК О.Г., кандидат юридичних наук

## КРИМІНОЛОГІЧНИЙ АНАЛІЗ ЗАГРОЗ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

**Анотація.** У статті проведено аналіз зовнішніх та внутрішніх загроз у сфері охорони державної таємниці, виокремлено джерела та носії таких загроз, розглянуто мотивацію протиправної діяльності на шкоду Україні та механізми її формування.

**Ключові слова:** державна таємниця, загроза, детермінанти, причинність, механізм злочинної діяльності.

**Аннотация.** В статье проведен анализ внешних и внутренних угроз в сфере охраны государственной тайны, выделены источники и носители таких угроз, рассмотрена мотивация противоправной деятельности во вред Украине и механизмы ее формирования.

**Ключевые слова:** государственная тайна, угроза, детерминанты, причинность, механизм преступной деятельности.

**Summary.** This article presents the analysis of the external and internal threats in the sphere of protection of state secret, distinguishes sources and carriers of such threats, considers motivation of illegal activity to the detriment of Ukraine and mechanisms of its formation.

**Keywords:** state secret, threat, determinants, causality, mechanism of illegal activity.

**Постановка проблеми.** Характерною рисою державної політики у сфері охорони державної таємниці є те, що вона одночасно належить до різних управлінських систем, зокрема, управління діяльністю із забезпечення інформаційної безпеки та управління діяльністю щодо запобігання та протидії злочинності.

Це пояснюється тим, що за своєю предметною спрямованістю охорона державної таємниці не може не належати до політичного управління сферою забезпечення інформаційної безпеки держави, оскільки розголошення цих відомостей, згідно зі ст. 7 Закону України “Про основи національної безпеки”, вважається основною реальною та потенційною загрозою національній безпеці України, стабільності в суспільстві в інформаційній сфері [1]. Так само вона виступає елементом кримінально-правової політики держави, оскільки розголошення державної таємниці або втрата її матеріальних носіїв є суспільно небезпечним діянням та кваліфікується як злочин, на запобігання та протидію якого спрямовується цей вид державної політики. Тут має місце явище, яке в теорії систем називають перехрещенням, коли певні елементи однієї системи є одночасно підсистемою іншої системи або декількох із них.

Залежно від того, у межах якої сфери політичного управління розглядається діяльність з охорони державної таємниці, пропонуються різні підходи та шляхи вирішення цієї задачі.

Забезпечення інформаційної безпеки здійснюється передусім шляхом проведення зваженої збалансованої політики держави в інформаційній сфері, яка має три основні вектори: захист інформаційних прав і свобод людини, захист державної безпеки в інформаційній сфері та захист національного інформаційного ринку, економічних інтересів держави в інформаційній сфері, національних виробників інформаційної продукції [2, с. 119].

Специфіка кожного з цих об’єктів захисту потребує їх розмежування, оскільки це обумовлюється не лише різницею завдань, що вирішуються для забезпечення безпеки всіх перелічених об’єктів, а й різною природою норм права, якими визначаються інформаційні права і свободи людини та громадянина, а також забезпечується інформаційна безпека держави.

Якщо інформаційні права і свободи реалізуються шляхом конституційного закріплення гарантій на вільний обіг інформації та встановлення юридичної відповідальності за порушення цих прав, то інформаційна безпека держави, в рамках якої здійснюється охорона державної таємниці, забезпечується через встановлені законодавством обмеження щодо вільного обігу інформації в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання правосуддя і неупередженості правосуддя [3].

Такий підхід пояснюється тим, що охорона державної таємниці виступає лише інструментом забезпечення (засобом) іншої, більш важливої для суспільства мети – забезпечення інформаційної безпеки як важливої складової національної безпеки. Тому не дивно, що заради досягнення більш важливих для людини, суспільства та держави загальних інтересів державою обирається принцип “заподіяння меншого зла”, тобто введення певних обмежень на вільний обіг інформації та вироблення таких правил поведінки з секретною інформацією, які б унеможливили її несанкціонований виток.

Зовсім інші шляхи вирішення цієї проблеми пропонуються в межах кримінально-правової політики держави запобігання злочинності загалом та окремих її проявам зокрема. Головний напрям цієї політики – запобігання злочинності, усунення причин та умов, що її породжують і сприяють її різноманітним проявам. Тим самим створюються реальні передумови поступового ослаблення суспільної небезпечності злочинів та зменшення масштабів самої злочинності. Крім цього, одним із напрямків кримінально-правової політики держави у сфері охорони державної таємниці є видання і застосування кримінальних законів за порушення встановлених правил поведінки з такою інформацією.

Кримінально-правова політика як елемент правової держави в цілому є базою, системоутворюючим елементом цієї політики, основою для прийняття управлінських рішень у сфері охорони найважливіших для суспільства відносин, благ і цінностей [4, с. 223]. Така політика реалізується шляхом формування кримінального, кримінально-процесуального та кримінально-виконавчого законодавства, регулювання практики їх застосування, а також розробки й реалізації заходів, спрямованих на попередження злочинів, на основі кримінологічного прогнозування та планування з урахуванням соціальної та економічної ситуації, що постійно змінюється.

Останнім часом у пошуках впливу на злочинність кримінологи намагаються відійти від кримінально-каральної політики держави, де одним із дієвих засобів стримування злочинності традиційно вважається встановлення кримінальної відповідальності за протиправні діяння та притягнення винних до кримінального покарання, та переорієнтувати державу на запровадження кримінологічної політики нерепресивної протидії злочинності та її проявам. Серед основних напрямків такої політики пропонуються заохочувальні заходи [5], примирливо-компенсаційні заходи [6], компроміси [7], розвиток кримінологічного контролю [8], перешкоджання дії детермінантів злочинності [9, с. 324], залякування [10, с. 505], управління ризиками злочинності [11] та ін. Але оскільки у “періодичній таблиці” запобіжних заходів

відкриття нових елементів навряд чи можливо, усі вони хоч і пропонуються під виглядом нових “рецептів” подолання злочинності, представляють собою поєднання вже давно відомих складових, жодна з яких не має переваг над іншими.

На нашу думку, найбільш раціональним та ефективним є такий підхід до забезпечення охорони державної таємниці, який охоплює весь комплекс кримінологічних заходів щодо підвищення рівня надійності охорони державної таємниці завдяки своєчасному передбаченню, виявленню та усуненню реальних і потенційних загроз у цій сфері, а також мінімізації наслідків їх впливу.

Адекватність запобіжних заходів визначається з урахуванням конкретних загроз, тому необхідно їх дослідити та обрати ті запобіжні заходи, які унеможливають реалізацію цих загроз.

Аналіз наукових доробок з даної теми свідчить, що різні аспекти охорони державної таємниці розглядалися у працях В. Артемова, Л. Деркача, О. Довганя, С. Князева, Б. Кормича, А. Марущака, Г. Новицького, В. Пилипчука, О. Развадовського, В. Сідака, В. Шлапаченко та інших. Проте, незважаючи на значний рівень наукового осмислення цієї проблематики, питання дослідження кримінологічних загроз у сфері охорони таємної інформації залишилися за межами наукових досліджень, що й обумовлює актуальність наукової розвідки.

**Метою цієї статті** є визначення поняття та видів загроз у сфері охорони державної таємниці, їх джерел, з’ясування механізму вчинення злочинів у сфері охорони державної таємниці.

**Виклад основного матеріалу.** У діючому законодавстві поняття та види загроз у цій сфері соціальної діяльності не визначені та не закріплені, що потребує не лише розкриття змісту цього поняття, але й теоретичного обґрунтування таких загроз та встановлення їхніх джерел.

Загроза порушення конфіденційності у галузі комп’ютерної безпеки має місце тоді, коли отримано доступ до певної інформації, що зберігається у комп’ютерній системі або передається від однієї системи до іншої [12, с. 36]. Разом із тим, поняття “загроза” означає “можливість або неминучість виникнення чогось небезпечного” [13, с. 293], тобто небезпеку поки що не реалізовану. Тому поняття “загроза” припускає не лише порушення конфіденційності інформації у вигляді отримання доступу до державної таємниці сторонніх осіб, але й власне процес формування небезпеки, здатної призвести до реалізації загроз та настання несприятливих для охоронюваних об’єктів наслідків.

Окремими авторами під загрозою розуміється сукупність умов і чинників певної сфери, що створюють небезпеку життєво важливим інтересам особи, суспільства та держави [14, с. 16]. Однак, на нашу думку, таке бачення змісту поняття “загроза” є не зовсім точним, оскільки поняття “чинник” використовується для позначення різних типів детермінант: причин, умов і обставин. Причому за допомогою чинника позначається не тільки явище, процес і стан, але й умови та ситуація.

Зокрема, Б. Кевбрін зазначає, що поняттям “детермінізм фіксується існування детермінуючих чинників (єдність дії сил, взаємодій та ін.), завдяки яким забезпечується процес розвитку” [15, с. 123]. Отже, джерелами небезпеки життєво важливим інтересам суспільства виступають не чинники та умови, а причини та умови, що детермінують розвиток тих чи інших дій і подій, а в нашій ситуації – протиправних дій, внаслідок яких відбувається несанкціонований виток державної таємниці.

На думку К. Стрельнікова, загроза представляє найбільш конкретну форму прояву соціальної небезпеки, створювану цілеспрямованою діяльністю [16, с. 11].

Погоджуючись із тим, що загрозу охоронюваним інтересам становлять свідомі дії, спрямовані на завдання такої шкоди, ми вважаємо, що загрозу можуть становити також і необережні дії у формі злочинної самовпевненості (коли особа не розраховувала, що такі наслідки настануть, хоча, діючи у відповідній конкретній обстановці, могла передбачити реальний розвиток причинного зв'язку між своєю поведінкою і наслідками) та злочинної недбалості (коли особа повинна була і могла усвідомлювати можливість настання таких наслідків). Тобто таку загрозу утворюють і нецілеспрямовані дії у вигляді порушень правил поведіння з державною таємницею, які призвели до завдання шкоди охоронюваним інтересам.

Враховуючи викладене, джерела небезпеки можна поділити на *джерела реалізації загроз (реальні загрози)* у вигляді протиправних дій, спрямованих на завдання шкоди охоронюваним суспільним інтересам, та осіб, які вчинили такі дії, або від кого з високим ступенем імовірності слід їх очікувати, та *джерела формування загроз (потенційні загрози)*, до яких належать причини і умови, що сприяють формуванню намірів щодо завдання шкоди державному суверенітету, територіальній цілісності, громадській безпеці, правоохоронній діяльності із запобіганням заворушенням чи злочинності. Відповідно зміст діяльності з охорони державної таємниці полягає у попередженні або нейтралізації загроз у цій сфері шляхом впливу на їх джерела.

На нашу думку, реальну загрозу можуть нести лише певні дії (діяльність або бездіяльність), які мають прямий причинно-наслідковий зв'язок зі зміною відповідних умов і критичних параметрів, що визначають безпеку держави.

Для кожної держави існує певний набір критичних параметрів, порушення яких може призвести до втрати нею своєї самостійності і навіть припинення існування. Ці критичні параметри охоплюють сфери, пов'язані з проблемою виживання, до яких відносяться міжнародні, внутрішньодержавні політичні та соціальні відносини, економіка, наука і техніка, державна безпека та правопорядок тощо. Тому, по-перше, держава повинна зосередити свої зусилля на охороні саме тієї інформації, протиправне використання якої може завдати шкоду суспільним інтересам у цій сфері, а, по-друге, важливим критерієм наявності таких загроз має бути конкретна визначеність дій та існування реальної можливості завданням такими діями суспільно небезпечних наслідків.

Якщо ми розцінюємо певні дії як загрозу охоронюваним інтересам, ми повинні мати відповіді на питання, хто скоїв ці дії, що саме він скоїв і коли. Така визначеність щодо дій та осіб дозволяє, у свою чергу, розмежувати реальні загрози на *внутрішні та зовнішні*.

*Внутрішніми загрозами* слід вважати протиправні дії осіб, яким надано доступ до державної таємниці, які умисно використовують отриману інформацію на шкоду суспільним інтересам самостійно чи через сторонніх осіб або створили сприятливі умови для завдання такої шкоди внаслідок умисного або необережного порушення встановлених правил поведіння з державною таємницею.

*Зовнішні загрози* – це умисні дії сторонніх осіб, спрямовані на заволодіння секретною інформацією з метою її використання на шкоду охоронюваним інтересам. Такі дії полягають у добуванні, придбанні будь-яким шляхом, засобом (викрадення, підслуховування, вивідування, особисті спостереження, фотографування текстів, креслень, інших матеріальних носіїв секретної інформації) та із застосуванням спеціальних технічних засобів (оптичних приладів, електронних апаратів та ін.).

Крім з'ясування джерел реальних загроз, важливого значення набуває також встановлення джерел потенційних загроз, тобто причин та умов, які обумовлюють та

полегшують вчинення злочинів, пов’язаних із протиправним використанням державної таємниці на шкоду суспільним інтересам. Це потрібно не лише для теоретичного осмислення природи таких злочинів, але й для практичної діяльності з їх розкриття та розслідування, а також розробки механізму попередження або нейтралізації таких загроз.

Як правило, під причинністю розуміють генетичний зв’язок між окремими станами видів і форм матерії у процесах її руху й розвитку. Причина завжди має об’єктивний характер, а її сутністю є породження наслідку [17, с. 62].

Причинність є однією з форм детермінації, під якою розуміють будь-яку закономірну залежність між різними процесами і явищами [18, с. 200]. Це генетичний зв’язок між окремими станами видів і форм матерії у процесах її руху й розвитку.

У філософському розумінні причинність є всезагальною, оскільки не існує явищ, які б не мали певних причин, і водночас не існує явищ, які б не породжували тих чи інших наслідків. У нашому дослідженні виходимо з того, що зв’язок між причиною і наслідком є обов’язковим. Використання державної таємниці на шкоду суспільним інтересам у цьому комплексі виступає наслідком впливу відповідних об’єктивних та суб’єктивних причин, за яких відбувалося моральне виховання особи, формувалися її мотиваційні настанови на вчинення таких дій.

Слід погодитися з думкою тих науковців, які вважають, що з точки зору філософії не може бути чітких меж між причинами та умовами конкретного злочину. Ті самі явища в різних ситуаціях (у різних кримінальних справах) можуть виступати і в якості умови, і в якості причини [19, с. 10]. Однак при всій відносності розбіжностей між причинами та умовами можна стверджувати, що частіше за все в ролі причин фігурують обставини, за яких відбувалося моральне виховання особи, формувалися її мотиваційні настанови.

Так, відстоювання власних інтересів суб’єктами міжнародних відносин, бажання отримати важелі впливу на поведінку керівництва нашої держави у міжнародних відносинах, у т.ч. на шкоду національним інтересам, безпосередньо обумовлює потребу іноземних держав в особі їх спецслужб у здобуванні інформації щодо директив, планів, вказівок делегаціям та посадовим особам з питань зовнішньополітичної і зовнішньоекономічної діяльності України, про військове, науково-технічне та інше співробітництво України з іноземними державами, про зміст стратегічних і оперативних планів та інших документів бойового управління, про напрямки розвитку окремих видів озброєння тощо.

При цьому діяльність іноземних спецслужб щодо здобування секретної інформації, залежно від зовнішньополітичної ситуації, може лише змінювати свою інтенсивність та спрямованість. Натомість вона ніколи не припиняється та залишається постійною реальною загрозою у цій сфері, що в черговий раз знайшло своє підтвердження в оприлюднених фактах прослуховуванням американською спецслужбою лідерів європейських країн, з якими США знаходиться у військових та політичних союзах.

На даний час, коли володіння певним видом секретної інформації стає джерелом отримання прибутку, способом ведення недобросовісної конкуренції у підприємницькій та господарській діяльності, дає можливість уникнути кримінальної відповідальності (у випадку своєчасного отримання інформації про факт або методи проведення негласної слідчої (розшукової) дії або відомостей, що дають змогу ідентифікувати особу, місце або річ, щодо якої проводиться чи планується проведення негласної слідчої (розшукової) дії), цілеспрямовано намагаються отримати доступ до державної таємниці не лише представники іноземних спецслужб. До такої діяльності вдаються також

вітчизняні та іноземні промислові групи та компанії, злочинні угруповання, інші зацікавлені у такій інформації особи. Для цього вони вживають найрізноманітніші способи, включаючи підкуп, шантаж, вимагання, розбійний напад, викрадення (в т.ч. із застосуванням технічних засобів) та ін. Такий протиправний обіг секретної інформації перетворюється на злочинний бізнес. Хоча ці дії не вважаються суспільно небезпечними та кримінально каранними, загроза охоронюваним державою інтересам від цього не зменшується, адже отримана у такий спосіб інформація з великою ймовірністю буде використана на шкоду інтересам держави.

Мотивація протиправної діяльності на шкоду Україні та механізми її формування різняться, залежно від того, громадянами якої країни вони є. Якщо це представники іноземних спецслужб, то внутрішнім рушієм такої діяльності виступає, перш за все, патріотизм, який посідає важливе місце у складовій світогляді таких осіб та формується під впливом державної ідеології. Це найбільш професійно підготовлені особи, які діють із глибоким переконанням, що “служать своїй державі”. Вони не просто використовують сприятливу ситуацію для заволодіння державною таємницею, а й активно її створюють. У них цілком виразно виявляється прагнення вийти за рамки свого повсякденного існування, наповнити його “яскравими фарбами”, незвичайними подіями, ризиком, гострими переживаннями. Серед них багато тих, хто керується ігровими мотивами.

Громадяни України, які вчиняють подібні злочини, здебільшого відрізняються чітко вираженим правовим нігілізмом, антисоціальною установкою. Їх внутрішні моральні настанови формуються у мікросередовищі, де норми моралі і права систематично порушуються, злочин є наслідком звичного стилю поведінки й обумовлений стійкими антисоціальними поглядами, установками і орієнтацією суб’єкта. Часто такі дії вчиняються з корисливих мотивів під вирішальним впливом незвичних для них обставин, які виникли не з вини цієї особи, а внаслідок порушення моральних і правових норм іншими учасниками суспільних відносин. Будучи загнаними життєвими обставинами у безвихідну (на їх думку) ситуацію, такі особи знаходять вихід у подібному злочині з метою заробити певну суму грошей для розв’язання ситуативної проблеми тощо, але ця обставина не виключає їх попередньої морально-психологічної деградації.

Розглянуті вище об’єктивні та суб’єктивні причини самі по собі здатні створити лише необхідні умови для заволодіння державною таємницею та її використання на шкоду суспільним інтересам. Проте реалізація таких намірів можлива за наявності достатніх умов, якими, на нашу думку, необхідно вважати порушення встановлених правил поведінки з державною таємницею, в т.ч. невиконання суб’єктами режимно-секретної діяльності норм та вимог технічного захисту секретної інформації.

Проведеним дослідженням встановлено, що для порушників законодавства про державну таємницю характерні наступні особистісні якості: неухважність, незібраність, внутрішня недисциплінованість, неорганізованість, хибне уявлення про службові інтереси; завищена самооцінка; відсутність прогностичного мислення та невміння передбачати шкідливі наслідки своєї поведінки; надмірна довірливість. При цьому основним чинником, який сприяє формуванню у порушників звички до безвідповідального ставлення до схоронності секретної інформації, є відсутність належного контролю за забезпеченням охорони державної таємниці.

Крім цього, використання інженерних технічних засобів охорони режимних приміщень (сейфів, сховищ), автоматизованих систем виготовлення, розмноження, зберігання та передачі секретної інформації призвело до утворення техногенних загроз,

які можуть бути обумовлені відмовою або збоями в роботі технічних засобів та їх програмного забезпечення, низькою якістю (ненадійністю) технічних, програмних або програмно-технічних засобів; відсутністю або низькою ефективністю систем резервування або дублювання програмно-технічних та технічних засобів; низькою якістю (надійністю) інженерних систем (електричного живлення, охоронних систем та ін.), обслуговування з боку технічного персоналу тощо.

Лише за наявності цих важливих детермінантів (необхідних та достатніх умов) злочинні наміри на заволодіння державної таємниці та її використання на шкоду суспільним інтересам із потенційної загрози перетворюються на реальну, а така ситуація із кримінологічної точки зору є найбільш загрозливою та потребує негайного втручання суб'єктів охоронної діяльності. Наявність достатніх умов означає, що злочин безперешкодно може бути вчинений у будь-який момент. За таких умов запобігти його скоєнню можна лише шляхом негайного усунення хоча б деяких із числа достатніх умов. Однак, як зазначає В. Кудрявцев, складність полягає у тому, що достатні умови взаємозамінні [20, с. 105].

### **Висновки.**

Надійність збереження державної таємниці залежить від спроможності держави утримувати секретну інформацію у просторі, в якому вона її контролює, шляхом застосування таких запобіжних заходів, які адекватні наявним та потенційним загрозам інтересам особи, суспільства та держави, що охороняються шляхом засекречування суспільно важливої інформації.

Кримінологічний аналіз загроз у сфері охорони державної таємниці повинен представляти безперервний процес, у рамках якого необхідно ідентифікувати джерела потенційних та реальних загроз, об'єкти їх спрямування, способи та методи реалізації, оцінити ступінь вірогідності їх реалізації, можливі негативні наслідки у випадку реалізації таких загроз. При цьому вид і характер загроз та об'єктів їх спрямування має визначати основні напрямки зосередження зусиль щодо їхнього попередження, нейтралізації й усунення як на стратегічному, так і на тактичному рівні.

Чітке уявлення про джерела та носії загроз дасть можливість обрати найбільш ефективні методи охорони, побудувати організаційну структуру та визначати форми організації роботи з протидії цим загрозам, визначати суб'єктів забезпечення охорони державної таємниці та координувати їхню діяльність, а також, враховуючи принцип необхідної та розумної достатності, обрати ті засоби для вирішення поставлених завдань, які за своїми властивостями та якостями дозволять досягти максимального результату за мінімального використання ресурсів.

### **Використана література**

1. Про основи національної безпеки : Закон України // Відомості Верховної Ради України (ВВР). – 2003. – № 39. – Ст. 351.
2. Кормич Б.А. Інформаційна безпека : організаційно-правові основи : навч. посібник / Б.А. Кормич. – К. : Кондор, 2008. – 384 с.
3. Конституція України : Закон України від 28.06.96 р. № 254/96-ВР // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Ст. 141.
4. Фріс П.Л. Кримінально-правова політика Української держави : теоретичні, історичні та правові проблеми / П.Л. Фріс. – К., 2005. – 332 с.
5. Голик Ю.В. Уголовно-правовое стимулирование позитивного поведения : вопросы теории / Ю.В. Голик. – Новосибирск : Изд-во Новосибир. ун-та, 1992. – 80 с.

6. Усе А.В. Примирение вместо наказания (как течение в правоприменительной практике) // Правоведение. – 1990. – № 6. – С. 89-95.
7. Аликперов Х.Д. Компромисс в борьбе с преступностью : пособие для прокуроров / Х.Д. Аликперов, М.А. Зейналов. – М. : ИПК РК Генеральной прокуратуры РФ, 1999. – 84 с.
8. Лунеев В.В. Преступность XX века. Мировые, региональные и российские тенденции / В.В. Лунеев. – [2-е изд., перераб. и доп.]. – М. : Волтерс Клувер, 2005. – 912 с.
9. Закалюк А.П. Курс сучасної української кримінології : теорія і практика : у 3 кн. – Кн. 1 : Теоретичні засади та історія української кримінологічної науки / А.П. Закалюк. – К. : Видавничий Дім “Ін Юре”, 2007. – 424 с.
10. Современные проблемы и стратегия борьбы с преступностью ; науч. ред. В.Н. Бурлаков, Б.В. Воженкин. – С-Пб. : Издательство юридического факультета С.-Пб. Гос. ун-та, 2005. – 592 с.
11. Управління ризиками організованої злочинності в Україні / [І.М. Гріненко, А.Ю. Ковальчук, Д.М. Прокоф’єва-Янчиленко, Б.В. Сокрут]. – К. : ВАІТЕ, 2013. – 380 с.
12. Макаренко С.И. Информационная безопасность : учебное пособие для студентов вузов / С.И. Макаренко. – Ставрополь : СФ МГГУ им. М.А. Шолохова, 2009. – 372 с.
13. Великий тлумачний словник сучасної української мови ; уклад. і голов. ред. В.Т. Бусел. – К., Ірпінь : ВТФ “Перун”, 2004. – 1440 с.
14. Стахов А.И. Право безопасности как подотрасль административного права / А.И. Стахов. М., 2008. – 255 с.
15. Кевбрин Б.Ф. Развитие. Детерминизм. Закон / Б.Ф. Кебрин. – М., 1998. – 241 с.
16. Стрельников К.А. Правовые аспекты экономической безопасности современного Российского государства : автореф. дис. на соискание науч. степени канд. юрид. наук : 12.00.01. – Новгород, 2004. – 26 с. – Режим доступа : <http://law.edu.ru/book/book.asp?bookID=1369988>
17. Александров Ю.В. Кримінологія : курс лекцій / Ю.В. Александров, А.П. Гель, Г.С. Семаков – К. : МАУП, 2002. – 296 с.
18. Курс советской криминологии : Предмет. Методология. Преступность и её причины. Преступник / [Г.В. Дашков, В.Н. Кудрявцев, В.В. Панкратов и др.] ; под ред. В.Н. Кудрявцева, И.И. Карпеца, Б.В. Коробейникова. – М. : Юрид. лит., 1985. – 416 с.
19. Изучение преступности (практическое пособие по криминологии для прокурорских работников) / [М.М. Бабаїв, Л.А. Быков, В.К. Звирбуль, Э.В. Кузнецова] ; под ред. В.К. Звирбуля. – М. : Всесоюз. инст-т по изуч. причин и разработке мер предупр. преступности, 1973. – 158 с.
20. Кудрявцев В.Н. Причинность в криминологии (О структуре индивидуального преступного поведения) / В.Н. Кудрявцев. – М. : “Юридическая литература”, 1968. – 176 с.

~~~~~ \* \* \* ~~~~~