Information security components: criteria analysis

Складники інформаційної безпеки: аналіз критеріїв

Taras Tkachuk

Key words:

information security, information security components, information security, information impacts, threats, information sphere.

Ключові слова:

інформаційна безпека, складники інформаційної безпеки, безпека інформації, інформаційні впливи, загрози, інформаційна сфера.

Постановка проблеми. Проблематика забезпечення інформаційної безпеки нині привертає увагу науковців та практиків у різних сферах, втім, питання визначення складників інформаційної безпеки та критеріїв, що використовуються з цією метою, досі залишається не до кінця розробленим. Не визначені складники інформаційної безпеки й на рівні законодавства. Тож актуальним є дослідження критеріїв виокремлення складників інформаційної безпеки та визначення щодо сутності останніх, що становить мету статті.

Виклад основного матеріалу. Незважаючи на те, що Конституція України з моменту свого затвердження відносить забезпечення інформаційної безпеки до найважливіших функцій держави[1], нормативне визначення інформаційної безпеки є порівняно новим. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» передбачає, що інформаційна безпека – це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації»[2]. Таке визначення, як бачимо, не дає змоги дійти чіткого висновку щодо сутності складників інформаційної безпеки, так само, як і низка опосередкованих визначень, які розглядають інформаційну безпеку у контексті більш загального поняття – національної безпеки, або ж торкаються її окремих аспектів, на кшталт інформаційної безпеки телекомунікаційних мереж[3].

На методологічному рівні предметна сфера інформаційної безпеки є єдиною, структурованою за завданнями та предметом дослідження, збалансованою за терміносистемою. Її системотвірним чинником, безумовно, виступають інформація та інформаційні процеси. Втім, із метою виокремлення складників інформаційної безпеки на доктринальному рівні використовується досить широкий спектр критеріїв, що зумовлює диференціацію підходів до розуміння системного змісту поняття «інформаційна безпека».

Якщо звернутися до зарубіжних наукових джерел, можна переконатись у тому, що найбільш популярним є погляд, за яким складниками інформаційної безпеки визнаються цілісність, доступність та конфіденційність інформації[4]. Під цілісністю інформації розуміють її властивість не бути модифікованою неавторизованим користувачем і (або) процесом, тобто, зберігатись у стані, визначеному її створювачем та законним володільцем, зокрема й достовірність інформації як її відповідність дійсності в аспекті

[1] Конституція України від 28.06.1996 р. [Електронний ресурс]. – Режим доступу : zakon5.rada.gov.ua/laws/show/254k/96-вр.

[2] Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. [Електронний ресурс]. – Режим доступу : zakon5.rada.gov.ua/laws/show/537-16.

[3] Про телекомунікації : Закон України від 18.11.2003 р. [Електронний ресурс]. – Режим доступу : zakon2.rada.gov.ua/laws/show/1280-15.

[4] Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security [Online tool]. – Available at : https://doi.org/10.6028/NIST.SP.800-12r1; National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec) [Online tool]. – Available at : www.cnss.gov/Assets/pdf/nstissi_4011.pdf; Federal Financial Institutions Examination Council (FFIEC). Information Technology Examination Handbook (IT Handbook): Information Security (2016) [Online tool]. – Available at : https://www/ffiec.gov/press/pdf/ffiec-it-handbook_information_security_booklet.pdf.

адекватності відображення. Конфіденційність означає властивість інформації бути недоступною користувачам, які не мають на це права. Ця властивість пов'язана з розмежуванням інформації за режимом доступу. Доступність інформації полягає в тому, що уповноважений користувач може використовувати її відповідно до правил, встановлених політикою безпеки, не очікуючи більше заданого проміжку часу, тобто це властивість інформації перебувати у необхідному користувачеві вигляді та місці, в той час, коли вона йому необхідна. Дійсно, належний стан вищезгаданих властивостей є важливим для забезпечення безпеки інформації. Крім того, через забезпечення безпеки інформації формується нова властивість інформації – її безпечність, котра також є важливою для інформаційної безпеки. Остання ж, окрім власне безпеки інформації, включає в себе й інші складові елементи. Так, в окремих випадках заподіяння шкоди належному стану властивостей інформації становить лише один із видів протиправних наслідків. Шкода завдається й іншим елементам інформаційної сфери, до яких, окрім інформації, належать інформаційні системи (суб'єкти й інфраструктура) та інформаційні відносини. Отже, безпека інформації має розглядатися як частина більш масштабного цілого.

Відповідно, як науковці близького зарубіжжя, так і вітчизняні дослідники приділяють значну увагу питанням інформаційно-психологічної та державно-ідеологічної складової частини інформаційної безпеки, існування яких зумовлюється поділом інформаційної сфери на інформаційно-технічну та інформаційно-психологічну[5]. На підставі критерію функціональності також пропонують визнавати складниками інформаційної безпеки її аспекти: соціальний; нормативно-правовий; економічний; фінансовий; військовий; екологічний; програмно-технічний тощо[6].

На думку Б. Кормича, інформаційна безпека має суб'єктно-об'єктний склад, тому з точки зору критерію основного об'єкта складниками інформаційної безпеки є інформаційна безпека особи, інформаційна безпека суспільства та інформаційна безпека держави. Крім того, держава, людина та суспільство одночасно виступають і як суб'єкти інформаційної безпеки, своїми діями здійснюючи захист важливої для них інформації та інформаційних процесів. Зокрема, до сфери інформаційної безпеки держави належать конкретні дії щодо забезпечення безпечних умов наявних інформаційних процесів, та забезпечення безпечного розвитку таких процесів у майбутньому, що охоплює регулювання питань захисту самої інформації, захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних умов розвитку інформаційних процесів[7].

Підкреслюючи системність інформаційної безпеки, за результатами комплексного аналізу О. Тихомиров веде мову, передусім, про «структурні складники забезпечення інформаційної безпеки» та виокремлює їх за різними критеріями, зокрема: за сферами суспільного життя (забезпечення інформаційної безпеки в економічній, політичній, воєнній, науково-технологічній, екологічній, соціальній сфері тощо); за об'єктами національної безпеки (забезпечення інформаційної безпеки особи, суспільства та держави); за сучасними аспектами розуміння інформаційної безпеки (забезпечення інформаційно-психологічної безпеки, забезпечення інформаційної безпеки у сфері прав і свобод людини та інформаційно-технічної, зокрема кібернетичної безпеки); за основними видами інформаційної діяльності (забезпечення законних можливостей створення, збирання, одержання та використання інформації, законного порядку поширення інформації, належного зберігання інформації, охорона та захист інформації, створення і розвиток інформаційних ресурсів тощо); за формами державного забезпечення інформаційної безпеки (забезпечення якісного інформування, процесів інформатизації; правова регламентація сфери інформаційних відносин; боротьба з правопорушеннями в інформаційній сфері); за напрямами пізнавального процесу в галузі забезпечення інформаційної безпеки (професійна освіта, наукові дослідження, інформаційно-просвітницька діяльність тощо); залежно від елементів змісту діяльності із забезпечення інформаційної безпеки (за об'єктами забезпечення інформаційної безпеки: розвиток і вдосконалення інформаційно-телеко-

[5] Баришполец В.А. Информационно-психологическая безопасность: основные положення / В.А. Баришполец // Информационные технологии. – 2013. – № 2. – Том 5. – С. 62; Николаев А. Государственно-идеологическая компонента информационной безопасности [Електронний ресурс]. – Режим доступу : https://cyberleninka.ru/acticle/v/gosudarstvenno-ideologicheskaya-komponenta-informatsionnoy-bezopasnosti; Гулай В.В. Загрози інформаційно-психологічній безпеці особи в реаліях інформаційно-психологічної війни як складової «гібридної війни» Російської Федерації проти України [Електронний ресурс]. – Режим доступу: www.asv.ua/content/nauka/editions/25/2016-25/233-244.pdf; Уханова Н.С. Інформаційно-психологічна безпека особистості, суспільства та держави [Електронний ресурс]. – Режим доступу : ippi.org.ua/ukhanova-ns-informatsiino-psikhologichna-bezpekaosobistosti-suspilstva-ta-derzhavi.

[6] Жатканбаева А.Е. Функциональные компоненты информационной безопасности / А.Е. Жатканбаева // Право и государство. – 2013. – № 4 (61) – С. 74.

[7] Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: [монографія] / Б.А. Кормич. – Одеса: Юридична література, 2003. – С. 28–32.

мунікаційної інфраструктури, недопущення доведення її до критичного рівня); забезпечення належного використання національних інформаційних ресурсів (захист ресурсів від несанкціонованого втручання, їх інноваційне оновлення, впровадження новітніх технологій створення, оброблення та поширення інформації, формування відкритих інформаційних ресурсів і забезпечення доступу до них громадян); захист інформації (забезпечення конфіденційності, цілісності та доступності тощо); захист свідомості суб'єктів від деструктивного інформаційного впливу (створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей); за суб'єктами забезпечення інформаційної безпеки: міжнародне забезпечення (міжнародне співробітництво в галузі забезпечення інформаційної безпеки, гарантування інформаційного суверенітету держави, сприяння задоволенню інформаційних потреб громадян за кордоном); державне забезпечення (діяльність державних організацій, спрямована на забезпечення інформаційної безпеки); недержавне забезпечення (діяльність громадських і недержавних комерційних організацій та окремих громадян, спрямована на сприяння державному забезпеченню інформаційної безпеки); за характером предмета діяльності із забезпечення інформаційної безпеки: протидія негативним інформаційним процесам і явищам; сприяння посиленню позитивних інформаційних процесів; сприяння трансформації нейтральних інформаційних процесів у позитивні; за складниками механізму протидії загрозам інформаційній безпеці: моніторинг інформаційної сфери; ранжування загроз; профілактика і попередження негативного впливу загроз; нейтралізація загроз; за характером здійснення державного впливу: безпосереднє створення необхідних умов життєдіяльності суб'єктів в інформаційній сфері; опосередкований вплив шляхом підвищення інформаційного потенціалу суб'єктів і сприяння їх самоорганізації; за засобами забезпечення інформаційної безпеки: правове забезпечення (правова регламентація відносин в інформаційній сфері; контрольно-наглядова діяльність, ліцензування, сертифікації, експертизи тощо); техніко-технологічне забезпечення; залежно від особливостей забезпечення доступу до інформації (за правовим режимом доступу до інформації; за заходами із захисту секретної інформації тощо)[8].

Звичайно, поняття «інформаційна безпека» та «забезпечення інформаційної безпеки» не є тотожними, і з точки зору функціонально-діяльнісного підходу співвідносяться як об'єкт діяльності – позитивна цінність та власне діяльність, здійснювана за допомогою певних сил і засобів. Втім, наведена вище класифікація в аспекті визначення складників забезпечення інформаційної безпеки дає змогу дійти певних висновків і щодо складників інформаційної безпеки, котрі можуть бути виокремлені за допомогою аналогічних критеріїв. Водночас, наприклад, критерій об'єкта національної безпеки дає змогу структурувати інформаційну безпеку, радше, за рівнями, ніж за складовими елементами. Поняття інформаційної безпеки тісно пов'язане з поняттям інформаційного суверенітету держави, під яким розуміють здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави. Враховуючи, що система забезпечення національної безпеки будується «від інтересів держави», більшість функцій, у тому числі у сфері забезпечення інформаційної безпеки, здійснюються саме державою, що дає змогу досягти балансу інтересів в інформаційній сфері. Щодо суспільного виміру інформаційної безпеки, то так звана «недержавна система безпеки» є не лише суб'єктом власного забезпечення, який самостійно визначає мету, принципи та методи забезпечення безпеки відповідно до законодавства України в межах загальної системи, але й становить об'єкт забезпечення інформаційної безпеки з боку держави. У свою чергу, безпека людини становить складову частину метасистеми національної безпеки, яка об'єднує безпеку особи, суспільства та держави в різних сферах, зокрема в інформаційній.

Узагальнення критеріїв сучасних аспектів розуміння інформаційної безпеки, основних видів інформаційної діяльності та змісту діяльності із забезпечення інформаційної безпеки (за класифікацією О.О. Тихомирова) дає змогу визначити, що метою забезпечення інформаційної безпеки є: попередження неправомірних дій з інформаційними ресурсами та системами, в тому числі здійснення шкідливих інформаційних впливів; захист прав та забезпечення реалізації законних інтересів суб'єктів інформаційної сфери; забезпечення належного стану ключових властивостей інформації.

Відповідно, можна припустити, що інформаційна безпека формується трьома складниками: безпека інформації, безпека «від інформації» (безпека інформаційних систем, зокрема суб'єктів інформаційної сфери та соціальних зв'язків між ними, від інформаційних впливів вербального, технічного або будь-якого іншого характеру); належний порядок реалізації прав та інтересів суб'єктів інформаційної сфери. Кожна

[8] Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: [монографія] / О.О. Тихомиров; заг. ред. Р.А. Калюжний. – Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. – С. 67–74.

з цих складових частин може проявлятися на різних рівнях залежно від: виду, приналежності, режиму доступу до інформації (для безпеки інформації); характеру, виду, способів поширення дефектної інформації, суб'єктів, якими поширюється та яким адресується дефектна інформація, характеру відповідних суспільних відносин (для безпеки від інформаційних впливів); суб'єктів інформаційної сфери з приводу реалізації ними «інформаційних» прав (для належного порядку реалізації прав та інтересів суб'єктів інформаційної сфери).

Щодо безпеки інформації варто зазначити, що йдеться про необхідність забезпечення безпеки не лише інформації з обмеженим доступом, але й іншої інформації, оскільки в умовах інформаційного суспільства надається правова охорона інформації як об'єкту цивільних прав і має бути відвернена не лише загроза несанкціонованого доступу до інформації (порушення конфіденційності), але й загроза порушення її цілісності та достовірності, а подеколи – і доступності інформації.

Не менш важливою, ніж безпека інформації, є так звана безпека «від інформації». Під нею варто розуміти безпеку інформаційних систем (в тому числі біологічних та соціальних – суб'єктів інформаційної сфери) та соціальних зв'язків між ними (зокрема й тих, що утворюються під час забезпечення інших складників національної безпеки) від інформаційних впливів, що здатні викликати знищення або пошкодження, спотворення тих чи інших об'єктів (зокрема нематеріального характеру), а також інформаційно-психологічну безпеку людини й суспільства. Забезпечення інформаційно-психологічної безпеки полягає в мінімізації негативних впливів на свідомість людини та суспільства, пов'язаних передусім із маніпулюванням свідомістю з різною метою, і поширенням суспільно небезпечної інформації, зокрема деструктивної ідеології (культу насильства та жорстокості, расизму, радикального націоналізму, порнографії тощо)[9].

Належний порядок реалізації інформаційних прав та інтересів суб'єктів інформаційної сфери як складник інформаційної безпеки безпосередньо пов'язаний із двома іншими її складниками, оскільки йдеться, по-перше, про права та інтереси суб'єктів суспільних відносин, які належать до біологічних та соціальних інформаційних систем (оскільки саме в такій якості вони виступають в інформаційній сфері), по-друге, про забезпечення взаємної нешкідливості інформаційних впливів на суб'єктів інформаційної сфери, по-третє, про права суб'єктів правовідносин як володільців інформації. Власне ж інформаційні впливи є процесами поширення інформації, зверненими до обмеженого або необмеженого кола інформаційних систем (в окремих випадках до цієї категорії можуть належати так звані «ентропійні інформаційні впливи», тобто утримання від передачі або поширення необхідної інформації).

При цьому безпека інформації становить конститутивну підоснову інформаційної безпеки, що, в свою чергу, зумовлюється конститутивним значенням інформації як елемента інформаційної сфери.

Що ж стосується кібернетичної безпеки, її виокремлення зумовлене специфікою середовища, в якому функціонують інформаційні системи, здійснюється обіг інформації, реалізації прав та законних інтересів суб'єктів інформаційної сфери тощо. Відповідно, кібернетичний аспект може бути притаманний усім складникам інформаційної безпеки, тож мова в такому разі має йти не про самостійну складову частину, а про забезпечення інформаційної безпеки у кіберпросторі (зауважимо, що в Законі України «Про основні засади забезпечення кібербезпеки України», прийнятому 5 жовтня 2017 р., кібербезпека визначена як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі)[10].

Також варто зазначити, що комплексне функціональне визначення інформаційної безпеки як постійного процесу діяльності компетентних органів, націленого на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу та сукупності умов такої діяльності, які реалізуються й здатні контролюватися тривалий час, дає змогу виділити пасивну (протидія інформаційним загрозам) та активну складову частину (створення інформаційних загроз) інформаційної безпеки.

---

[9] Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: [монографія] / О.О. Тихомиров; заг. ред. Р.А. Калюжний. – Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. – С. 70–71.

[10] Картка законопроекту «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2126%D0%B0&skl=9; Рада ухвалила закон про кібербезпеку [Електронний ресурс]. – Режим доступу : https://www.epravda.com.ua/news/2017/10/5/629817/.

Висновки. У складі визначених вище компонентів (безпеки інформації, безпеки «від інформації» та належного порядку реалізації прав та інтересів суб'єктів інформаційної сфери, щодо яких триває постійний процес протидії інформаційним загрозам та створення інформаційних загроз супротивнику) поняттям інформаційної безпеки охоплюється не лише захищеність інформаційної сфери, що є передумовою її належного функціонування, але й можливість справляння суб'єктами інформаційної сфери необхідних впливів на інші сфери життєдіяльності суспільства, взаємодії з останніми.

Нормативне закріплення системного характеру та змісту складників інформаційної безпеки сприятиме не лише більш коректному усвідомленню її сутності суб'єктами інформаційної сфери, але й забезпечить гармонійний розвиток законодавства у відповідній сфері та підвищить ефективність правового забезпечення інформаційної безпеки України. За відсутності такого концептуального визначення не може бути адекватно сформульовано визначень безпеки інформації, кібербезпеки тощо. Однак, як вже зазначалося, нині поняття інформаційної безпеки закріплено у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»[11], який фактично передбачає тимчасову стратегію, котру доцільно затверджувати та періодично оновлювати на рівні підзаконних нормативно-правових актів. Тож видається за доцільне закріпити поняття інформаційної безпеки як складника національної безпеки та системного феномена у нормах Закону України «Про основи національної безпеки України, сформулювавши його таким чином: «Інформаційна складова частина національної безпеки (інформаційна безпека) – постійний процес діяльності компетентних органів, направлений на своєчасне виявлення, попередження та протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, що реалізуються й здатні контролюватися тривалий час, за яких забезпечується формування, використання та розвиток інформаційної сфери в інтересах її суб'єктів та сталий розвиток суспільства шляхом розвитку власного інформаційного простору, зведення до мінімуму заподіяння шкоди через неповноту, невчасність і недостовірність інформації, негативні інформаційні впливи (в тому числі інформаційну експансію з боку інших держав), негативні наслідки функціонування інформаційних технологій, а також через несанкціоновані дії з інформацією».

Анотація

Статтю присвячено аналізу критеріїв виокремлення складників інформаційної безпеки та їх визначенню. Сформульовано певні рекомендації щодо внесення змін до чинного законодавства України з метою нормативного закріплення поняття «інформаційна безпека».

Summary

The article is devoted to the analysis of the criteria for identifying the components of information security and the definition of such components. Certain recommendations are formulated regarding the introduction of changes to the current legislation of Ukraine with the purpose of normative consolidation of the concept of "information security".

Використана література:

1. Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security [Online tool]. – Available at : https://doi.org/10.6028/ NIST.SP.800-12r1.
2. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec) [Online tool]. – Available at : www.cnss.gov/Assets/pdf/nstissi_4011.pdf.
3. Federal Financial Institutions Examination Council (FFIEC). Information Technology Examination Handbook (IT Handbook): Information Security (2016) [Online tool]. – Available at : https://www/ffiec.gov/press/pdf/ffiec-it-handbook_information_security_booklet.pdf.
4. Баришполец В.А. Информационно-психологическая безопасность: основные положення / В.А. Баришполец // Информационные технологии. – 2013. – № 2. – Том 5. – С. 62–104.

[11] Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. [Електронний ресурс]. – Режим доступу : zakon5.rada.gov.ua/laws/show/537-16.

5. Гулай В.В. Загрози інформаційно-психологічній безпеці особи в реаліях інформаційно-психологічної війни як складової «гібридної війни» Російської Федерації проти України [Електронний ресурс]. – Режим доступу : www.asv.ua/content/nauka/editions/25/2016-25/233-244.pdf.
6. Жатканбаева А.Е. Функциональные компоненты информационной безопасности / А.Е. Жатканбаева // Право и государство. – 2013. – № 4. – С. 74–77.
7. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: [монографія] / Б.А. Кормич. – Одеса: Юридична література, 2003. – 472 с.
8. Николаев А. Государственно-идеологическая компонента информационной безопасности [Електронний ресурс]. – Режим доступу : https://cyberleninka.ru/ acticle/v/gosudarstvenno-ideologicheskaya-komponenta-informatsionnoy-bezopasnosti.
9. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави: [монографія] / О.О. Тихомиров; заг. ред. Р. А. Калюжний. – Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. – 196 с.
10. Уханова Н.С. Інформаційно-психологічна безпека особистості, суспільства та держави [Електронний ресурс]. – Режим доступу : ippi.org.ua/ ukhanova-ns-informatsiino-psikhologichna-bezpekaosobistosti-suspilstva-ta-derzhavi.
11. Конституція України від 28.06.1996 р. [Електронний ресурс]. – Режим доступу : zakon5.rada.gov.ua/laws/show/254k/96-вр.
12. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. [Електронний ресурс]. – Режим доступу : zakon5.rada.gov.ua/laws/show/537-16.
13. Про телекомунікації : Закон України від 18.11.2003 р. [Електронний ресурс]. – Режим доступу : zakon2.rada.gov.ua/laws/show/1280-15
14. Картка законопроекту «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/ pls/zweb2/webproc4_2?pf3516=2126%D0%B0&skl=9
15. Рада ухвалила закон про кібербезпеку [Електронний ресурс]. – Режим доступу : https://www.epravda.com.ua/news/2017/10/5/629817.

Taras Tkachuk,
Candidate of Juridical Sciences, Associate Professor,
Deputy Head of Department of Organization of Restricted Information Protection,
Educational and Research Institute of Information Security,
National Academy of Security Service of Ukraine