

2004- 384с. **11.** Питання концепції реформування інформаційного законодавства України / Р. Калюжний, В. Гавловський, В. Цимбалюк, М. Гуцалюк // Збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні”. К.: НТУУ „КПІ”, Міністерство освіти і науки України, СБУ. – К. – 2000. – С. 17-21. **12.** Бачило И. Л. Информационное право: основы практической информатики. – М., 2001. – С. 253. **13.** Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. // Российская газета. – 2000. – 28 сентября. **14.** Актуальні проблеми інформаційної безпеки України (аналітична доповідь УЦЕПД) // Національна безпека і оборона. – 2001. – № 1. – С. 2–50. **15.** Скакун О. Ф. Теорія держави і права: Підручник / Пер. з рос. – Х.: Консул, 2001. – 352 с. **16.** Безпека авіації/Бабак В. П., Марченко В. П., Максимов В. О. та ін. – К.: Техніка, 2004. – 584 с. **17.** Державна програма авіаційної безпеки цивільної авіації затверджена Законом України від 20 лютого 2003 року №545 –IV // Відомості Верховної Ради України. – 2003. - N 17. - ст.140. **18.** Толковый словарь живого великорусского языка В. Даля [Электронный ресурс]. – Режим доступа до документа : <http://slovardalja.net/word.php?wordid>. **19.** Толковый словарь Ожегова [Электронный ресурс]. – Режим доступа до документа : <http://www.ozhegov.ru/slovo>. **20.** Конституція України 28 червня 1996 року//Відомості Верховної Ради (ВВР).- 1996.- N 30. - ст. 141.

УДК 681.3.06

## СУЩНОСТЬ И МЕТОДЫ КОМПЬЮТЕРНОЙ РАЗВЕДКИ

Сергей Емельянов

Одесская национальная юридическая академия

**Аннотация:** Рассматриваются возможные подходы к определению сущности и методов компьютерной разведки и ее места в общей системе добывания информации о разведываемом объекте информатизации.

**Summary:** The possible manners of essence definition and computer methods intelligence and its place in the general system acquire information about searching object of informatization are looking through.

**Ключевые слова:** Компьютерная разведка, техническая разведка, технические каналы утечки информации, несанкционированный доступ, объект информатизации, компьютерная информация.

### I Введение

Возрастающее по экспоненциальному закону общее количество информации [1], ужесточение требований по ее хранению, поиску и обработке, увеличение трафика и скорости передачи информации предопределили появление информационных систем (ИС) различных поколений и назначения. Сегодня термин ИС охватывает автоматизированные системы, компьютерные сети или системы связи [2], информационно-телекоммуникационные системы [3] и т.д. В ИС концентрируется и циркулирует большой объем как открытой, так и информации с ограниченным доступом (ИсОД).

В связи с этим приобрела широкий размах и деятельность по гласному и негласному добыванию информации из открытых и закрытых ИС, баз и банков данных, контролю за сообщениями, передаваемыми в вычислительных сетях, получению персональных данных пользователей ИС и другой ценной компьютерной информации. Для характеристики подобной деятельности стали широко использоваться термины: «компьютерный шпионаж», «компьютерная разведка», «информационно-аналитическая работа в Интернет», «аналитическая разведка», «компьютерный анализ и разведка» и др.

Однако в нормативно-методических документах и многочисленных публикациях по данной тематике до сих пор отсутствует единое терминологическое толкование сущности, задач и методов компьютерной разведки (КР), что и обуславливает актуальность рассматриваемой проблемы.

Ряд авторов, специализирующихся на теории и практике экономической разведки (называемой также конкурентной, деловой, коммерческой, competitive intelligence, business intelligence и др.), определяют КР как аналитическую обработку огромного числа данных из разнообразных открытых источников информации, прежде всего из Интернет. Сущность КР они видят в поиске и передаче информации из открытых компьютерных систем и сетей “всемирной паутины” с последующей верификацией и аналитической обработкой [4 – 5].

Термин «аналитическая разведка» впервые появился в нормативных документах МВД России в 1992 году для обозначения особой формы деятельности оперативно-поисковых подразделений [6 – 7]. Аналитическая разведка была определена как разведывательный поиск, техническая разведка, комплексное изучение материалов скрытого наблюдения и оперативной установки, а также анализ сообщений, публикаций и выступлений в средствах массовой информации, статистических данных, сведений автоматизированных банков данных. КР рассматривалась при этом как один из видов аналитической разведки, целенаправленно используемой для мониторинга компьютерных систем.

Однако большинство авторов [8 – 9], опираясь на определение технической разведки как способа добывания информации с помощью технических средств, небезосновательно относят КР к одному из

видов технической разведки. В нормативном документе РФ [10] КР также рассматривается как один из методов доступа к защищаемой информации с применением технических средств разведки (ТСР).

В работе [11] автор трактует КР как метод добывания информации путем перехвата и анализа побочных электромагнитных излучений и наводок (ПЭМИН) средств ЭВТ, т. е. рассматривает ее как разновидность радиоэлектронной разведки, которая, в свою очередь, является одним из видов технической разведки.

Таким образом, ранее нерешенной частью проблемы является вопрос: что же такое компьютерная разведка, какие каналы утечки информации она может использовать и какими методами проводится?

Цель статьи – определение сущности компьютерной разведки, ее места в общей системе добывания информации из типовой ИС и систематизация возможных методов ее ведения.

## II Основная часть

На наш взгляд, **сущность** КР заключается в добывании:

- компьютерной информации, обрабатываемой, хранимой и передаваемой в ИС;
- данных и сведений о характеристиках (параметрах) программных, аппаратных и программно-аппаратных комплексов, применяемых в ИС;
- данных и сведений о применяемых в ИС методах, способах и механизмах защиты информации;
- персональной информации о пользователях ИС.

Известно [7 – 8], что одним из основных (базовых) классифицирующих признаков ТСР является физический принцип построения их аппаратуры (Рис. 1), который перекрывает все существующие и потенциально-возможные технические каналы утечки информации (ТКУИ) с разведываемого объекта. Основные ТКУИ также классифицируют по физическим полям, посредством которых может распространяться защищаемая информация: радиоканалы, акустические, электрические, оптические и материально-вещественные каналы, которые достаточно хорошо известны, систематизированы и изучены [12 – 13]. Сложнее обстоит дело с техническим каналом утечки компьютерной информации (ТКУКИ).

Во-первых, сам термин «компьютерная информация» до сих пор не имеет однозначного законодательно закрепленного определения. Так, например, в специальном Разделе XVI КК Украины в диспозициях статей 361 – 363 [14] речь идет об информации, которая сохраняется, обрабатывается или распространяется с помощью автоматизированных систем, компьютерных сетей или сетей связи. В ст. 2 Закона Украины [3] отмечается, что *“объектами защиты являются информация, которая обрабатывается ... и программное обеспечение, которое предназначено для обработки этой информации”*. В ст. 1 Закона Украины [15] указывается, что *“информация - сведения, представленные в виде сигналов, знаков, звуков, движущихся или неподвижных изображений или другим способом”*. В ряде международных нормативно-правовых документов [16] чаще используется термин «компьютерные данные» для обозначения информации в форме, пригодной для обработки в компьютерной системе, вместе с соответствующим программным обеспечением и т. д.

Во-вторых, имеются определенные расхождения и противоречия в трактовке физической природы ТКУКИ. Если, например, исходить из классического определения канала утечки как канала передачи информации в виде: **источник**→**физическая среда**→**получатель** [8 – 9, 12 – 13], то ТКУКИ формально может рассматриваться как самостоятельный канал утечки, поскольку он имеет все указанные элементы. Источник информации здесь ИС, среда (тракт) распространения – телекоммуникационные линии связи (нижние физический и канальный уровни модели открытых систем OSI), получатель информации – другие государства, отдельные юридические или физические лица, добывающие ИсОД с объекта информатизации путем бесконтактного проникновения в ИС.

Однако, существует и другое мнение [13, с. 227] о нецелесообразности выделения явлений, приводящих к утечке информации из компьютерных систем и сетей, в отдельную группу, образующую самостоятельный технический канал утечки информации, поскольку многие из них при более детальном рассмотрении могут быть приведены к одному из описанных ТКУИ, например, электромагнитному или материально-вещественному.

Исходя из сущности КР, следует, что она не привязывается к физическим полям и сигналам (не является видовой или сигнальной) в отличие от других способов ведения технической разведки.

**Предметом** исследования КР являются не побочные (нежелательные) эффекты, неизбежно сопровождающие функционирование технических средств ИС и лежащие в основе образования непреднамеренных ТКУИ, а различные виды компьютерной информации, являющиеся результатом как раз штатного функционирования ИС и реализации ее основного предназначения – сбора, анализа, обработки, хранения, передачи информации и др.

Основным **методом** ведения КР является несанкционированный доступ (НСД) к компьютерной информации, циркулирующей в ИС. Однако в терминах компьютерной безопасности [17] речь идет не о технической (компьютерной) разведке и о каналах утечки информации, а, соответственно, об угрозах конфиденциальности компьютерной информации и о скрытых (тайных) каналах проникновения в компьютерные системы и сети (КСС), которые могут проявляться как на физическом уровне

(физический доступ к элементам ИС, хищение носителей информации и т. д.), так и на логическом уровне (отключение или обход системы защиты, захват привилегий, ложная маршрутизация потоков данных, сбор “мусора” и др.).

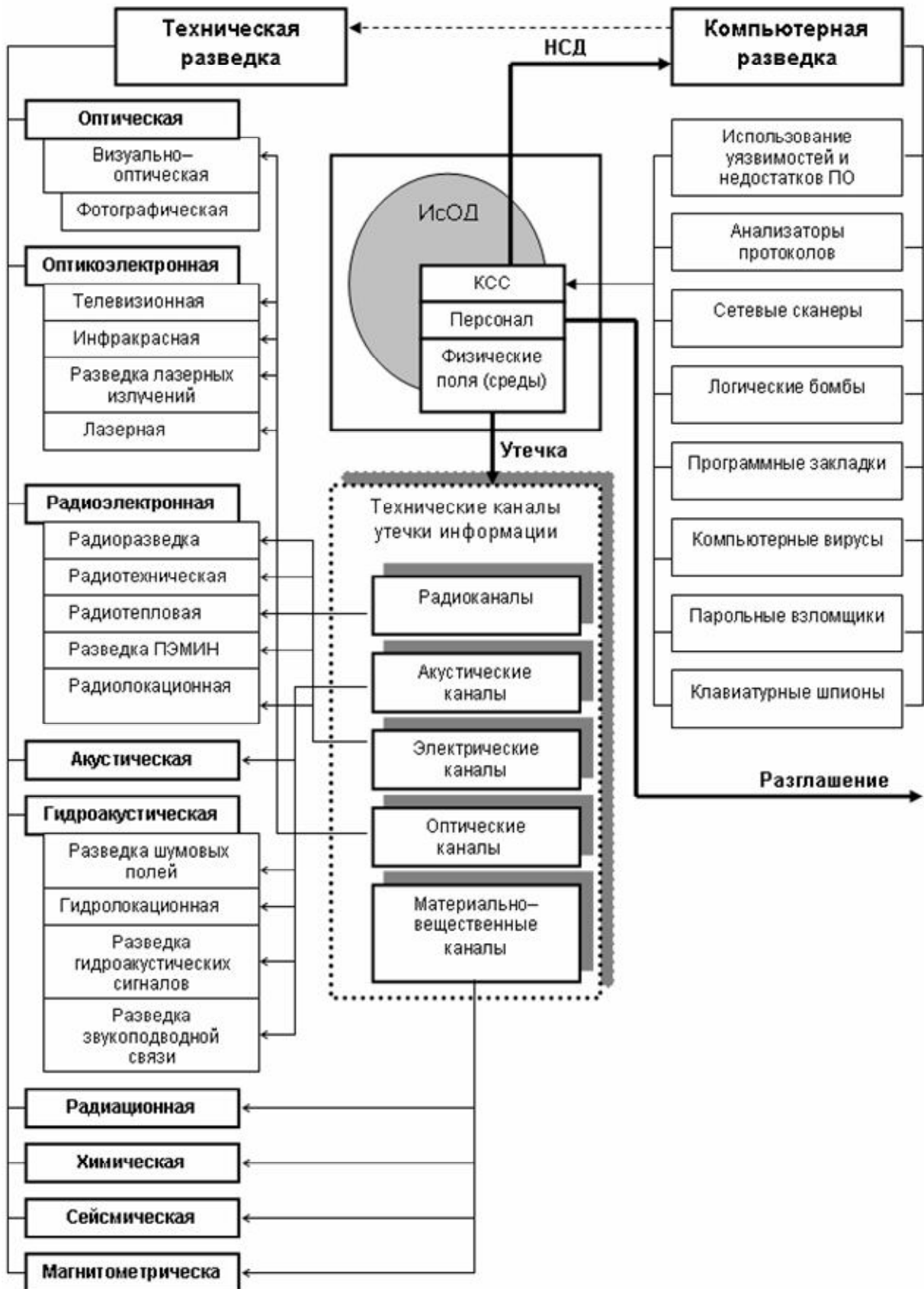


Рисунок 1 – Роль и место КР в добывании информации с типового объекта информатизации

Способы бесконтактного НСД в компьютерные системы и сети основаны (Рис. 1) на использовании недостатков языков программирования, наличии уязвимостей (брешей, “люков”, “дыр” и т. д.) в штатном программном обеспечении (ПО) ИС и применении специального ПО, называемого атакующим [18].

Его применение, как правило, предполагает работу на более высоких уровнях упомянутой модели OSI (транспортном и сетевом, сеансовом и представительском, прикладном). В отмеченной работе [8, с. 31] указано, что “...к компьютерной разведке нельзя относить средства активного воздействия на информационные системы противника: почтовые и логические бомбы, электронные черви, SYN-наводнения, атаки типа “Салями”, большинство вирусов”.

Однако, в КР, как и в технической разведке, могут применяться пассивные и активные методы добывания информации. Например, радиолокационная или лазерная виды технической разведки основаны на активной локации разведываемых объектов или их элементов с помощью излучения специальных зондирующих сигналов и приема отраженных откликов. Другие виды ТСР используют собственное излучение разведываемых объектов или их элементов в различных частотных диапазонах.

Аналогично, при добывании информации через ТКUI могут применяться как активные (ВЧ-навязывание, облучение лазерным лучом поверхности стекол, использование аппаратных закладок, радиомикрофонов и др.), так и пассивные методы перехвата информационных сигналов (ПЭМИН, акустики помещений и др.). Поэтому и в КР возможен как пассивный перехват информации (прием и анализ сетевого трафика, сканирование жесткого диска и др.), так и активные методы добывания компьютерной информации, с помощью, например, внедрения в КСС вирусов, троянцев, или логических бомб, срабатывающих при наступлении определенных условий или инициируемых сигналами извне.

На наш взгляд, не относятся к КР:

- выведывание сведений через персонал ИС, поскольку это самостоятельный канал утечки информации через субъекты-носители информации (разглашение);
- анализ и обработка, в том числе с использованием компьютерных систем, открытых текстов СМИ, Интернет;
- применение аппаратных закладок в средствах ЭВТ;
- передача разведанных с помощью КСС;
- физическое проникновение к элементам ИС, наблюдение за их работой, копирование информации или хищение ее носителей, поскольку это другие методы НСД;
- перехват и анализ ПЭМИН средств ЭВТ.

### III Выводы

1. Компьютерная разведка является относительно новым и самостоятельным видом технической разведки.

2. С формальной точки зрения могут рассматриваться каналы утечки компьютерной информации как самостоятельные каналы распространения ИсОД с объекта информатизации, однако они нуждаются в дальнейшем исследовании.

3. Сущность компьютерной разведки заключается в добывании:

- компьютерной информации, обрабатываемой, хранимой и передаваемой в ИС;
- данных и сведений о характеристиках (параметрах) программных, аппаратных и программно-аппаратных комплексов, применяемых в ИС;
- данных и сведений о применяемых в ИС методах, способах и механизмах защиты информации;
- персональной информации о пользователях ИС.

4. Основным методом ведения компьютерной разведки является несанкционированный бесконтактный доступ к компьютерной информации, циркулирующей в ИС.

5. Компьютерная разведка может вестись с помощью как активных, так и пассивных методов.

6. Изложенный подход к определению сущности и методов компьютерной разведки не противоречит существующим нормативно-методическим документам по защите информации, а лишь дополняет их, сохраняя базовый подход к возможным путям (каналам) утечки информации с объекта информатизации за счет [19]:

- разглашения информации персоналом;
- применения технических средств разведки (по техническим каналам утечки информации);
- НСД к компьютерной информации.

7. Целесообразно законодательно определить термин «компьютерная информация».

*Литература:* 1. Гаврилов О. А Курс правовой информатики: Учебник для вузов. – М.: Издательство НОРМА (Изд. группа НОРМА-ИНФРА-М), 2002. – 432с. 2. Положение о технической защите информации на Украине: Утв. Указом Президента Украины от 27.09.1999 г. №1229. 3. Закон Украины “О защите информации в информационно-телекоммуникационных системах” от 05 июля 1994 г. // Ведомости Верховной Рады. – 1994, № 31. – Ст. 286. 4. Доронин А. И. Бизнес-разведка. – 2-ое изд.,

перераб. и доп. – М.: Изд-во «Ось-89», 2003. – 384с. 5. Мисюк С. Компьютерная разведка: взгляд на сайт компании из недр Интернета [Электронный ресурс *cdaily.sec.ru*]. – Доступ к ресурсу: <http://www.daily.sec.ru/dailyprblshow.cfm?rid=17&pid=8872>. 6. Скрыль С. В., Киселев В. В. Аналитическая разведка в оценке угроз информационной безопасности // Системы безопасности, 2003. – № 6(48). – С. 96-97. 7. Киселев В. В., Золотарева Е. А. Признаки распознавания вредоносных программ в компьютерных сетях [Электронный ресурс]. – Доступ к ресурсу: <http://agps-2006.narod.ru/konf/2003/sb-2003/sec-1/20.pdf>. 8. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки. М.: Российск. гос. гуманит. ун-т, 2002. – 399 с. 9. Халяпин Д. Б. Защита информации. Вас подслушивают? Защищайтесь! - М.: НОУ ШО “Баярд”, 2004. – 432 с. 10. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. 11. Ржавский В. К. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учебное пособие. – Волгоград: Изд-во ВолГУ, 2002. – 122с. (Серия «Информационная безопасность»). 12. Хорев А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: Учебное пособие. – М.: Гостехкомиссия России, 1998. – 320 с. 13. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. – Юниор. – 2003. – 504 с. 14. Криминальный кодекс Украины от 5 апреля 2001 г. // Официальный вестник Украины. – 2001. – №21. – ст.920. 15. Закон Украины “О телекоммуникациях” от 18 ноября 2003 г. // Ведомости Верховной Рады. – 2004. – № 12. – Ст. 155. 16. Конвенция о киберпреступности (официальный перевод) // Официальный вестник Украины. – 2007. – № 65. – С. 107. – Ст. 2535. 17. НД ТЗИ 1.1-003-99. Терминология в сфере защиты информации в компьютерных системах от несанкционированного доступа. Утв. приказом ДСТСЗИ от 28 апреля 1999 г. – [Электронный ресурс Государственной службы специальной связи и защиты информации Украины]. – Доступ к ресурсу: <http://www.dstszi.gov.ua/dstszi/control/uk/publish>. 18. Анин Б. Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с. 19. Ярочкин. В. И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект, Гаудеамус, 2-е изд., 2004. – 544 с. (Gaudeamus).

УДК 354:007

## ОХОРОНЮВАНА ІНФОРМАЦІЯ В КРИМІНАЛЬНОМУ ПРОЦЕСІ

Євген Скулиш, Дарія Прокоф'єва

Головне управління по боротьбі з корупцією та організованою злочинністю СБ України

**Анотація:** Досліджуються проблеми правового захисту інформації в кримінальному процесі.

**Summary:** The article represents the research of problems the defense of the information in the criminal process.

**Ключові слова:** Інформація, таємниця, Кримінально-процесуальний кодекс.

### І Вступ

На виконання Указу Президента України від 20 січня 2006 року № 39 [1] Національною комісією зі зміцнення демократії та утвердження верховенства права за участю Міністерства Юстиції розроблено проект Кримінального процесуального кодексу України (надалі – КПК) [2].

На думку авторів проекту, новий КПК спрямований на формування кримінального процесу, який дозволить досягти, насамперед, двох цілей:

- високої ефективності роботи органів забезпечення правопорядку із захисту осіб та суспільства від злочинності;

- забезпечення захисту прав людини і основоположних свобод відповідно до вимог міжнародних стандартів.

Як одне з основних завдань нового Кодексу позиціонується запровадження позбавленої обвинувального ухилу процедури досудового слідства, що додатково гарантуватиме дотримання прав і свобод людини. Зокрема, одним з принципів кримінального процесу проголошується повага до приватного життя особи.

Так, відповідно до ст. 14 проекту, під час кримінального провадження ніхто не може збирати, зберігати, використовувати та поширювати конфіденційну інформацію про особу без її згоди, крім випадків та в порядку, передбаченому Кодексом. При цьому ч. 3 зазначеної статті визначає, що кожен, кому наданий доступ до конфіденційної інформації, зобов'язаний запобігати розголошенню такої інформації.

В цьому контексті привертають увагу також ст. 147 – 148 проекту, які визначають обмеження доступу до окремих категорій матеріальних носіїв інформації.

Зокрема, ст. 147 визначає, що заборонений доступ до листування або інших форм обміну інформацією між захисником та його клієнтом або будь-якою особою, яка представляє його клієнта в