ISSN 1995-6134

УДК 343.1:65.012.8+004
О.В. МАНЖАЙ, канд. юрид. наук, Харківський національний університет внутрішніх справ
А.В. ВІНАКОВ, Прокуратура Харківської області

ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПРОВАДЖЕННЯ ОКРЕМИХ СЛІДЧИХ ДІЙ ТА ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ

Ключові слова: *програмне забезпечення, оперативно-розшукова діяльність, досудове розслідування, докази, боротьба зі злочинністю*

Останнім часом науковці і практики все більше уваги приділяють питанням, пов'язаним з ефективним використанням комп'ютерних технологій у боротьбі зі злочинністю. Особливо часто такі технології, а відтак і відповідне програмне забезпечення, доводиться застосовувати проти такого негативного явища, як кіберзлочинність.

У Посланні Президента України до Верховної Ради України 2011 року було наголошено, що вияви кіберзлочинності у вигляді хакерських атак на комп'ютерні системи банківських та інших фінансових установ, крадіжок електронних коштів, широкого використання мережі Інтернет для наркоторгівлі, торгівлі людьми, інших протиправних дій стають реальною загрозою національній безпеці. Кібернетичний простір дедалі більше стає полем протистояння між окремими державами, джерелом небезпек для національної інфраструктури з боку військових і розвідувальних структур, організованих злочинних угруповань, що прагнуть використовувати Інтернет і новітні інформаційно-комп'ютерні технології для досягнення своїх підривних або кримінальних цілей [1]. Отже, проблема ефективного використання програмних продуктів правоохоронними органами у боротьбі зі злочинністю стає все більш актуальною.

Питанням боротьби з кіберзлочинністю присвячені праці таких вітчизняних вчених, як О.М. Бандурка, Л.В. Борисова, Н.Л. Волкова, І.О. Воронов, В.О. Голубєв, М.В. Гуцалюк, О.Ф. Долженков, В.Ю. Журавльов, В.П. Захаров, М.Ю. Літвінов, Ю.Ю. Орлов, Е.В. Рижков, М.М. Перепелиця, С.М. Рогозін, Л.П. Скалозуб, Ю.В. Степанов, В.П. Шеломенцев та ін. Різні аспекти застосування інформаційних технологій в оперативно-розшуковій діяльності розглядали російські дослідники С.С. Овчинський, В.С. Овчинський, А.С. Овчинський, А.Л. Осипенко, В.І. Попов, А.В. Борбат, В.В. Зорін, А.В. Макієнко, дослідники зі США С. Хейман, Д. Грін, В. Вайтлідж, білоруський дослідник В.Є. Козлов та ін.

Однак, питання практичного застосування програмного забезпечення під час здійснення оперативно-розшукової та слідчої діяльності залишаються недостатньо вивченими.

Враховуючи положення нового Кримінального процесуального кодексу України, вважаємо, що допустимість використання програмного забезпечення для створення доказової бази у кримінальному провадженні забезпечується:

– нормами ст.ст.69, 71, 104, 237, 266, 359 Кримінального процесуального кодексу [2];

– належним чином оформленими матеріалами кримінального провадження;

– кваліфікацією працівників ОВС, спеціалістів, експертів та інших осіб, які беруть участь у використанні програмного забезпечення для вирішення завдань кримінального провадження;

– можливістю залучення експерта або спеціаліста до аналізу носіїв інформації та технічних засобів (див., наприклад, ч.3 ст.266 Кримінального процесуального кодексу України);

– сертифікацією програмного забезпечення:

– як інформаційної системи, спираючись на законодавство України у сфері сертифікації;

– як захищеної від несанкціонованого доступу системи, що пройшла державну експертизу у сфері технічного захисту інформації.

Проведення робіт з розроблення програмного забезпечення (ПЗ) та оцінки його якості

ISSN 1995-6134

ґрунтується на ряді нормативно-правових документів, основними серед яких є державні стандарти України та міжнародні стандарти імплементовані Україною.

Вирішення питання щодо придатності ПЗ до слідчої чи оперативної діяльності органів внутрішніх справ, на нашу думку, має вирішуватися спеціально уповноваженим органом МВС України. На підставі цього рішення МВС України ініціюватиме проведення державної експертизи щодо відповідності ПЗ вимогам захисту інформації.

До ПЗ, призначеного для слідчих та оперативних потреб, висувається ряд додаткових вимог, зокрема щодо його відповідності певному профілю захищеності (див., наприклад, ч.3 ст.232 Кримінального процесуального кодексу України [2]).

Розроблення відповідної системи захисту ПЗ (комплексна система захисту інформації) та вимоги до неї регламентовано нормативно-правовими документами у сфері технічного захисту інформації.

Після завершення створення комплексної системи захисту інформації, проводиться відповідна державна експертиза [3]. Види державної експертизи і порядок її організації та проведення проілюстровані на рис.1, 2.

Рисунок 1 – Види та зміст експертиз

Рисунок 2 – Порядок проведення експертизи

ISSN 1995-6134

У результаті проведення державної експертизи системи захисту інформації необхідно мати:

– виконання робіт відповідно до окремої методики експертизи комплексної системи (засобу) технічного захисту інформації;

– експертний висновок, зареєстрований і затверджений експертною радою Держспецзв'язку;

– атестат відповідності, зареєстрований і виданий у Держспецзв'язку [4, с.156–157].

Належним чином сертифіковане програмне забезпечення може використовуватися у боротьбі зі злочинністю з метою:

– перехоплення вмісту повідомлень або службової інформації цільового об'єкту;

– дослідження даних, у тому числі виявлення закодованих стеганографічних повідомлень, порівняння ідентифікованих та ідентифікуючих об'єктів, зокрема зображень з метою виявлення в Інтернеті дитячої порнографії;

– фіксації інтелектуальних слідів вчинення злочину, у тому числі документування сесій чатів та інших подібних сервісів;

– відстеження серверу, з якого було відправлено те або інше електронне повідомлення або розміщено WEB-сторінку;

– спілкування;

– автоматизації процесів накопичення та аналізу інформації;

– активної дії на цільовий об'єкт.

Використання програмного забезпечення у боротьбі зі злочинністю в цілому узгоджується із нині діючим законодавством України. Наведемо декілька прикладів.

Працівники ОВС мають право отримувати інформацію з сайтів та он-лайн ресурсів, які не містять обмежень доступу, за допомогою відповідного програмного забезпечення так само, як інформацію з загальнодоступних джерел, які можна одержати за допомогою відповідних усних чи письмових запитів (див., наприклад, п.17 ст.11 Закону України «Про міліцію» від 20.12.1990 р. [5]).

При спілкуванні в мережі користувачі часто використовують глобальні системи, за допомогою яких можуть дискутувати один з одним в реальному часі шляхом обміну письмовими повідомленнями. Такі дискусії мають публічний або приватний характер. При цьому оперативні та слідчі працівники ОВС мають право в пасивному режимі оглядати та документувати електронні повідомлення, зроблені в режимі реального часу, в порядку п.9 ст.8 Закону України «Про оперативно-розшукову діяльність» [6] та ст.264 Кримінального процесуального кодексу України. При цьому здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту може відбуватися без отримання спеціального дозволу.

Використання програмного забезпечення для відвідування електронних ресурсів обмеженого доступу можуть здійснювати лише спеціально уповноважені суб'єкти у порядку ст.264 Кримінального процесуального кодексу України за наявності дозволу слідчого судді.

Слідчі та оперативні працівники мають право використовувати для зв'язку електронні сервіси та спеціальне програмне забезпечення. Важливі для кримінального провадження повідомлення мають бути зафіксованими в установленому законом порядку (див., наприклад, ст.232 Кримінального процесуального кодексу України, яка встановлює порядок проведення допиту, впізнання у режимі відеоконференції під час досудового розслідування).

У загальному випадку працівник ОВС під час он-лайн спілкування повинен представлятися своїми справжніми даними. Це випливає з вимог ч.2 ст.5 Закону України «Про міліцію» від 20.12.1990 р.: при звертанні до громадянина працівник міліції зобов'язаний назвати своє прізвище, звання та пред'явити на його вимогу службове посвідчення. Вказані обмеження можуть не поширюватися на спеціально уповноважених суб'єктів під час проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій (п.17 ст.8 Закону України «Про оперативно-розшукову діяльність» [6] та ст.273 Кримінального про-

ISSN 1995-6134

цесуального кодексу України [2]), які мають право на зашифроване спілкування в установленому законом порядку.

Під час здійснення оперативно-розшукових заходів або слідчих дій з використанням інформаційно-телекомунікаційних систем у мережі Інтернет, оперативні працівники або слідчі повинні докласти достатніх зусиль для з'ясування питання щодо розташування комп'ютерної системи, даних, очевидців (свідків) чи суб'єктів, які мають відношення до злочину, в межах іноземної юрисдикції. Якщо виявиться, що один з вищеназваних об'єктів знаходиться за межами України, то в загальному випадку оперативні працівники або слідчі повинні діяти за Інструкцією «Про порядок організації співробітництва органів внутрішніх справ України з правоохоронними органами іноземних держав з питань попередження, розкриття та розслідування злочинів», тобто через інститут співробітництва і лише через структурні підрозділи центрального апарату МВС України за напрямами службової діяльності, Управління міжнародних зв'язків та робочий апарат Національного центрального бюро Інтерполу в Україні (п.3.2 [7]). Ігнорування цієї вимоги може призвести до настання небажаних міжнародних наслідків, оскільки мова йде про порушення суверенітету іншої держави. Така ж процедура застосовується для отримання електронних доказів, які зберігаються в інших державах [8, с.218].

Підсумовуюче вищевикладене, слід зазначити, що сьогодні в Україні назріла потреба у розробці та впровадженні у практичну діяльність Інструкції МВС України «Про мережну активність оперативних працівників органів внутрішніх справ України», у якій пропонуємо передбачити такі розділи:

– основні поняття;

– порядок отримання інформації із загальнодоступних мережних ресурсів та ресурсів обмеженого доступу;

– порядок отримання ідентифікаційної інформації про користувачів, інформаційні, телекомунікаційні системи та мережі;

– порядок здійснення мережних комунікацій оперативних працівників між собою та іншими особами;

– створення та використання несправжніх (імітаційних) засобів;

– набуття та використання мережних ідентифікаційних даних іншої особи (за згодою особи та без її згоди);

– міжнародна діяльність.

Очевидно, що вказану інструкцію необхідно розробляти з урахуванням вимог нового Кримінального процесуального кодексу України, який незабаром вступить у дію.

ЛІТЕРАТУРА

1. Послання Президента України до Верховної Ради України 2011 рік «Модернізація України – наш стратегічний вибір» : від 07.04.2011 р.

2. Кримінальний процесуальний кодекс України : від 13.04.2012 р. // Голос України. – 19.05.2012. – № 90-91.

3. Положення про державну експертизу в сфері технічного захисту інформації / затв. наказом Адміністрації державної служби спеціального зв'язку та захисту інформації України : від 16.05.2007 р., № 93 // Офіційний вісник України. – 2007. – № 52. – Ст. 2153.

4. Носов В. В. Організація та забезпечення інформаційної безпеки : навч. посіб. / В. В. Носов, О. В. Манжай. – Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2007. – 216 с.

5. Закон України «Про міліцію» : від 20.12.1990 р. // ВВР УРСР. – 1991. – № 4. – Ст. 20.

6. Закон України «Про оперативно-розшукову діяльність» : від 18.02.1992 р. // ВВР України. – 1992. – № 22. – Ст. 303.

7. Інструкція про порядок організації співробітництва органів внутрішніх справ України з правоохоронними органами іноземних держав з питань попередження, розкриття та розслідування злочинів / затв. наказом МВС України «Про організацію міжнародної діяльності органів внутрішніх справ України» : від 15.05.2007 р., № 158.

ISSN 1995-6134

8. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності / О. В. Манжай // Право і безпека. – 2009. – № 4 (31). – С. 215–219.

Манжай О. В. Використання програмного забезпечення для провадження окремих слідчих дій та оперативно-розшукових заходів / О. В. Манжай, А. В. Вінаков // Форум права. – 2012. – № 2. – С. 437–441 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2012-2/12movorz.pdf

Проаналізовано механізм застосування програмного забезпечення під час здійснення оперативно-розшукової діяльності та кримінального провадження. Враховано вимоги нового Кримінального процесуального кодексу. Наведено приклади. Запропоновано розробити спеціальну інструкцію щодо мережної активності для правоохоронних органів.

***

Манжай А.В., Винаков А.В. Использование программного обеспечения для проведения отдельных следственных действий и оперативно-розыскной деятельности

Проанализирован механизм применения программного обеспечения во время осуществления оперативно-розыскной деятельности и уголовного производства. Учтены требования нового Уголовного процессуального кодекса. Приведены примеры. Предложено разработать специальную инструкцию о сетевой активности для правоохранительных органов.

***

Manzhai O.V., Vinakov A.V. Use of Software for Some Investigative and Special Investigative Actions

The mechanism of application of software is analyzed during realization of special investigative activity and criminal investigation. The requirements of the new Criminal Procedure Code are taken into account. Examples are demonstrated. It is suggested to develop the special instruction about online activity for law enforcement authorities.