вчальний посібник / С.В. Албул, С.В. Андрусенко, Р.В. Мукоіда, Д.О. Ноздрін: за заг. ред. С.В. Албула. – Одеса : ОДУВС, 2016. – 270 с.

8. Подобний О.О. Кримінологічний та криміналістичний підходи щодо визначення й класифікації організованих корисливо-насильницьких злочинів / О.О. Подобний // Південноукраїнський правничий часопис. – 2010. – № 1. – С. 49-51.

9. Протидія кримінальним правопорушенням підрозділами карного розшуку МВС України: навчальний посібник / С.В. Албул, Т.С. Демедюк, О.Є. Користін, В.Ф. Паскал. – Одеса: ОДУВС, 2015. – 354 с.

10. Тищенко В.В. Корыстно-насильственные преступления: криминалистический анализ: монография / В. В. Тищенко. – Одесса: Юрид. лит, 2002. – 360 с.

11. Тищенко В.В. Механизм совершения корыстно-насильственных преступлений / О.В. Болгар, В.В. Тищенко // Актуальні проблеми діяльності ОВС по попередженню, розкриттю і розслідуванню злочинів : матеріали міжнар. наук.-практ. конф. Ч. 2. – Одеса : НДРВВ ОІВС МВС України, 2000. – 244 с.

Домніцак Р.В.,
заступник начальника -
начальник кримінальної поліції
ГУ НП у Львівській області
Надійшла до редакції: 18.03.2016

УДК 681.327.8

ОРГАНІЗАЦІЙНІ АСПЕКТИ ФУНКЦІОНУВАННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Захаров В. П.,
Зачек О. І.

У практиці боротьби зі злочинністю завжди велике значення надавалося пошуку, збору та накопиченню оперативно-пошукової та іншої криміналістичної інформації. Зокрема, значну роль в цьому відіграють підрозділи інформаційно-аналітичного забезпечення МВС. Інформація, яка збирається і обробляється цими підрозділами, є цікавою не лише поліції, але і злочинцям, які також здійснюють розвідувальні і контррозвідувальні заходи, скеровані на нейтралізацію зусиль поліції у боротьбі зі злочинністю. Сучасні інформаційні технології надають їм таку можливість, тому в останній час значно зросла кількість атак на інформаційні системи. В одних випадках злочинців цікавить інформація, яка зберігається та обробляється в таких системах. В інших випадках здійснюється намагання заблокувати функціонування інформаційних систем.

Комплексний захист інформації базується на використанні правових, фізичних, організаційних та програмно-апаратних засобів захисту інформації. Метою даної статті є аналіз організаційних аспектів захисту інформації, що забезпечують функціонування комплексних систем захисту інформації в правоохоронних органах України.

В статті розглянуті організаційні аспекти функціонування комплексних систем захисту інформації в правоохоронних органах України та даються пропозиції щодо підвищення ефективності організації захисту інформації.

***Ключові слова**: комплексний захист інформації, комплексні системи захисту інформації, організаційні аспекти захисту інформації, персонал, користувач, інформаційні технології, автоматизована система, програмне забезпечення.*

В практике борьбы с преступностью всегда большое значение предоставлялось поиску, сбору и накоплению оперативно-поисковой и другой криминалистической информации. В частности, значительную роль в этом играют подразделения информационно-аналитического обеспечения МВД. Информация, которая собирается и обрабатывается этими подразделениями, является интересной не только полиции, но и преступникам, которые также осуществляют разведывательные и контрразведывательные мероприятия, направленные на нейтрализацию усилий полиции в борьбе с преступностью. Современные информационные технологии предоставляют им такую возможность, потому в последнее время значительно выросли количество атак на информационные системы. В одних случаях преступников интересует информация, которая хранится и обрабатывается в таких системах. В иных случаях осуществляется попытка заблокировать функционирование информационных систем.

Комплексная защита информации базируется на использовании правовых, физических, организационных и программно-аппаратных средств защиты информации. Целью данной статьи является анализ организационных аспектов защиты информации, что обеспечивают функционирование комплексных систем защиты информации в правоохранительных органах Украины.

В статье рассмотрены организационные аспекты функционирования комплексних систем защиты информации в правоохранительных органах Украины и даются предложения по повышению эффективности организации защиты информации.

***Ключевые слова**: комплексная защита информации, комплексные системы защиты информации, организационные аспекты защиты информации, персонал, пользователь, информационные технологии, автоматизированная ситема, програмное обеспечение.*

In practice, the fight against crime is always a great value provides search, collection and accumulation of operational-search and other forensic information. In particular, the important role played in this unit of information and analytical support of the Ministry of Interior. Information which is collected and processed by these units, is interesting not only police, but also criminals, who also carry out intelligence and counterintelligence activities aimed at neutralizing the efforts of the police in combating crime. Modern information technologies provide them with such an opportunity, because in recent years significantly increased the number of attacks against information systems. In some cases, criminals are interested in information that is stored and processed in such systems. In other cases, an

attempt to block the functioning of information systems.

Complex protection of information is based on the use of legal, physical, organizational and software and hardware protection of information. The purpose of this article is to analyze the organizational aspects of the protection of information that ensure the functioning of complex systems of information protection in the law enforcement bodies of Ukraine.

The article deals with the organizational aspects of the functioning of complex systems of information protection in the law enforcement agencies of Ukraine and provides suggestions for improving the effectiveness of information security organization.

***Keywords**: comprehensive data protection, integrated systems of information protection, organizational aspects of information security, personnel, users, information technology, automated systems that include software.*

Постановка проблеми. У практиці боротьби зі злочинністю завжди велике значення надавалося пошуку, збору та накопиченню оперативно-пошукової та іншої криміналістичної інформації. Зокрема, значну роль в цьому відіграють підрозділи інформаційно-аналітичного забезпечення Національної поліції. Інформація, яка збирається і обробляється цими підрозділами, є цікавою не лише поліції, але і злочинцям, які також здійснюють розвідувальні і контррозвідувальні заходи, скеровані на нейтралізацію зусиль поліції у боротьбі зі злочинністю. Сучасні інформаційні технології надають їм таку можливість, тому в останній час значно зросла кількість атак на інформаційні системи. В одних випадках злочинців цікавить інформація, яка зберігається та обробляється в таких системах. В інших випадках здійснюється намагання заблокувати функціонування інформаційних систем.

Є неодноразові випадки атак кіберзлочинців на інформаційні мережі правоохоронних органів, як в дальньому зарубіжжі, так і в країнах СНД. Наприклад, в 2011 р. були зламані сайти ряду поліцейських ділянок в США, внаслідок чого в публічному доступі були розміщені повідомлення електронної пошти, паролі, номери соціального страхування, номери кредитних карток поліцейських, а також повідомлення від конфіденційних інформаторів [1]. В квітні 2012 року кіберзлочинці вивели з ладу сайт МВС Великобританії [2]. В лютому 2013 року кіберзлочинці розмістили рекламу наркотиків на сайті ГУМВС України у Львівській області [3]. Можна згадати блокування сайту МВС України в лютому 2012 р. після припинення роботи файлообмінного ресурсу EX.UA. В березні 2013 р. був зламаний сайт суда Південного Уралу в Челябінській області Росії [4].

Група хакерів КіберБеркут, яка з'явилася після розформування спецпідрозділу Беркут, атакувала сервер ЦВК під час виборів Президента України, блокувала роботу сайтів МВС та Генпрокуратури України [5].

І таких прикладів є дуже багато. Все це зайвий раз підтверджує необхідність наукових розробок в галузі комплексних систем захисту інформації в правоохоронних органах.

Стан дослідження. Проблемам створення і функціонування систем технічного захисту інформації присвячено достатньо публікацій як у відкритих, так і закритих літературних джерелах, зокрема, таких вчених: Бабичев С.Г., Бєляєв А.В., Ботюк А.О., Вертузаев М.С., Ворожко В.П., Голубєв В.О., Горбулін В.П., Гуцалюк М.В., Домарьов В.В., Захарченко В.Ю., Карпінський М.П., Лазуренко В.І., Петренко С.А., Хараберюш І.Ф., Захаров В.П. Важливість наукового здобутку та внеску у теорію і практику інформаційної безпеки згаданих вчених важко переоцінити.

Аналіз літературних джерел дає підстави стверджувати, що у процесі проектування, створення і експлуатування комплексних систем захисту інформації є певні недоліки, які знижують ефективність їх функціонування.

Мета дослідження. Комплексний захист інформації базується на використанні правових, фізичних, організаційних та програмно-апаратних засобів захисту інформації. Метою даної статті є аналіз організаційних аспектів захисту інформації, що забезпечують функціонування комплексних систем захисту інформації в правоохоронних органах України.

Виклад основних положень. Українське законодавство містить значну кількість законів та підзаконних актів, які регулюють правовідносини в галузі захисту інформації. В Україні діє близько 60 нормативних актів, які регулюють відносини в інформаційній сфері. Крім того Держкомсекретів України видало понад 15 відомчих нормативних актів, які є обов'язковими для всіх державних структур в галузі забезпечення охорони інформації з обмеженим доступом, перш за все - державної таємниці [6]. У Законі України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 року № 80/94-ВР даються визначення: "Захист інформації – це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та осіб, які користуються інформацією" та "Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації" [7]. У Законі України "Про державну таємницю" від 21.01.94 № 3856-XII дається визначення, що охорона державної таємниці – це комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв [8].

Комплексна система захисту інформації містить правовий, організаційний та технічний елементи захисту. Такі засоби повинні забезпечувати ідентифікування та аутентифікування користувачів, розподіл повноважень доступу до інформаційної системи, реєстрацію та облік спроб несанкціонованого доступу. Основною частиною системи є організаційний елемент. Він містить заходи управлінського, режимного і технологічного характеру. Заходи організаційного захисту – це 50-60 % структури комплексних систем захисту інформації [9, с. 45]. Організаційні заходи захисту інформації в інформаційних системах, як правило, спрямовані на чіткий розподіл відповідальності під час роботи персоналу з інформацією, створення декількох рубежів контролю, запобігання навмисному або випадковому знищенню та модифікуванню інформації.

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

застосування режимних заходів на об'єктах автоматизованої системи;

забезпечення фізичного захисту обладнання автоматизованої системи, носіїв інформації, інших ресурсів;

організації проведення обстеження середовищ функціонування автоматизованої системи;

порядку виконання робіт з захисту інформації, взає-

модії з цих питань з іншими суб'єктами системи технічного захисту інформації в Україні;

виконання робіт з модернізації автоматизованої системи (окремих компонентів);

регламентації доступу сторонніх користувачів до ресурсів автоматизованої системи;

регламентації доступу власних користувачів і персоналу до ресурсів автоматизованої системи;

здійснення профілактичних заходів (наприклад, попередження ненавмисних дій, що призводять до порушення політики безпеки, попередження появи вірусів та ін.);

реалізації окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до автоматизованої системи, використання мереж передачі даних загального користування, зокрема Internet, використання несертифікованого програмного забезпечення та ін.) [10].

До організаційних заходів належать:

робота з персоналом;

вимога щодо здійснення важливих робіт колективом виконавців;

вимога, щоб засоби захисту розповсюджувались на всіх користувачів, включно з керівництвом;

чітке визначення категорій доступу для користувачів;

системний періодичний контроль за якістю захисту інформації;

призначення особи, що відповідає за режим секретності;

забезпечення дотримання режиму секретності під час використання комп'ютерних систем;

створення плану відновлення системи після виходу з ладу.

Робота з персоналом – це найважливіша частина організаційного елементу систем захисту інформації. Більшість порушень режиму безпеки стається з вини працівників організацій. Деякі науковці вважають, що 75 % витоку інформації стається через персонал організацій, і лише 25 % –технічними каналами [9, с. 103].

За оцінками правоохоронців, суб'єкти комп'ютерних злочинів розподіляються наступним чином: персонал, який здійснює функції управління та обслуговування автоматизованої системи – 44,9 %; особа – користувач автоматизованої системи – 34,9 %, розробник програмних засобів, які дозволяють незаконне проникнення до автоматизованих систем – 24, 9 %; адміністратор автоматизованих систем – 18,9 %, власник таких систем – 10,8 %; розробник технічних засобів, призначених впливати на роботу комп'ютерних систем без використання програмного забезпечення – 6,8 % [11, с. 55].

Тому організація інформаційної безпеки повинна враховувати не тільки технічний і технологічний компоненти системи, але і людський фактор. Тобто, під час створення конкретної системи безпеки необхідно враховувати етичні, моральні, індивідуально-психологічні, соціально-психологічні та інші особисті характеристики персоналу, що задіяний у системі організації безпеки інформації [12, с. 260]. Зменшити загрози для безпеки інформації внаслідок незаконних дій персоналу можна шляхом підбору працівників, наявності вимог щодо захисту інформації в посадових інструкціях та завдяки постійному контролю дотримання цих вимог.

Є такі види організаційних заходів:

організація запобіжних заходів;

організація блокування (протидії) реальних загроз, що реалізуються;

організація подолання наслідків загроз, які не вдалося блокувати або запобігти їм.

Заходи протидії поділяються на активні (розвідка, дезінформація, зашумлення), пасивні (здійснення екранування приміщень та обладнання) та комплексні засоби, які поєднують вищеназвані. Подолання наслідків загроз передбачає документування методів несанкціонованих дій із доступу до інформаційної системи з метою їх дослідження; збереження слідів несанкціонованого доступу; взаємодії з правоохоронними органами з метою притягнення винних до відповідальності [12, с. 255].

Згідно з вимогами Постанови Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29 березня 2006 року № 373 захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі. План захисту інформації в системі містить:

завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;

визначення моделі загроз для інформації в системі;

основні вимоги щодо захисту інформації та правила доступу до неї в системі;

перелік документів, згідно з якими здійснюється захист інформації в системі;

перелік і строки виконання робіт службою захисту інформації [13].

План захисту інформації в автоматизованій системі розробляється на підставі проведеного аналізу технології обробки інформації, аналізу ризиків, сформульованої політики безпеки інформації. План захисту визначає і документально закріплює об'єкт захисту інформації в автоматизованій системі, основні завдання захисту, загальні правила обробки інформації в автоматизованій системі, мету побудови та функціонування комплексних систем захисту інформації, заходи із захисту інформації. План захисту має фіксувати на певний момент часу склад автоматизованої системи, перелік оброблюваних відомостей, технологію обробки інформації, склад комплексу засобів захисту інформації, склад необхідної документації [10].

Висновки. Розглянувши принципи побудови комплексних систем захисту інформації, приходимо до висновку, що організаційні заходи є важливою частиною таких систем. Також зрозуміло, що найбільші загрози інформації виникають внаслідок впливу людського фактору. Тому важливої ролі набувають питання підбору персоналу організацій, що використовують автоматизовані системи. В правоохоронних органах важливою є протидія розвідувальній діяльності з боку злочинного світу шляхом запобігання корумпуванню працівників, які мають дотичність до функціонування комплексних систем захисту інформації. Як спосіб боротьби з цим негативним явищем можна запропонувати періодичну перевірку на поліграфі осіб, відповідальних за захист інформації в правоохоронних органах, а саме персоналу, який здійснює функції управління та обслуговування автоматизованої системи, розробників програмних засобів, адміністраторів автоматизованих систем, розробників технічних засобів, призначених впливати на роботу комп'ютерних систем без використання програмного забезпечення.

Література

1. Группа хакеров Anonymous выступила против полиции // http://4b2b.biz/gruppa-xakerov-anonymous-vystupila-protiv-policii.html.

2. Яна Пашаева "Хакеры Anonymous взломали сайт полиции Британии" // Life News Online/http://lifenews.ru/news/88032.

3. "Хакеры пошутили над работниками милиции" // ИА "Пресс-центр Украина"/http://pressua.info/sobytiya/life/item/1082-hakery-poshutili-nad-rabotnikami-militsii.html.

4. Кирилл Бабушкин "Челябинская полиция ищет хакера, взломавшего сайт областного суда и разместившего в одной из новостей маску Гая Фокса"// http://www.znak.com/chel/news/2013-03-14/1003302.html.

5. Хакеры утверждают, что "положили" сайт Президента Украины. Новости@mail.ru от 29 июля 2014. [Електронний ресурс] – Режим доступу: http://news.mail.ru/inworld/ukraina/incident/19030136/?frommail=1.

6. Ворожко В.П. Деякі питання правового захисту інформації в Україні // http://www.bezpeka.com/ru/lib/spec/law/art6.html.

7. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 року № 80/94-ВР

8. Закон України "Про державну таємницю" від 21 січня 1994 року № 3855-XII // Відомості Верховної Ради України (ВВР), 1994, N 16, ст.93.

9. Гуцалюк М.В. Організація захисту інформації. Навчальний посібник. – 2-е вид., перероб. та допов. – К.: Альтерпрес, 2011. – 308 с.

10. Типове положення про службу захисту інформації в автоматизованій системі: НД ТЗІ 1.4-001-2000. – [Чинний від 2000.12.04]. – К.: ДСТСЗІ СБУ, 2000. – № 53. – (Нормативний документ системи технічного захисту інформації).

11. Кутузов В.М., Гавловський В.Д., Скалозуб Л.П., Тітуніна К.В., Шеломенцев В.П. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки: [наук.-практ. посібник] / за заг. ред. Л.П. Скалозуба, І.В. Бондаренко. – К., 2010. – 245 с.

12. Основи інформаційного права України: навч. посіб. / В.С. Цимбалюк, В.Д. Гавловський, В.М. Брижко та ін.; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. 2-е вид., перероб. та допов. – К.: Знання, 2009. – 414 с.

13. Постанова Кабінету Міністрів України від 29 березня 2006 р. N 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"// http://zakon4.rada.gov.ua/laws/show/ 373-2006-%D0%BF.

Захаров В.П.,
доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ
Зачек О.І.,
кандидат технічних наук, доцент,
доцент кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ
Надійшла до редакції: 29.03.2016

УДК 343.341:343.9.01

ПОНЯТТЯ ТА ОСОБЛИВОСТІ ОРГАНІЗОВАНОЇ ТРАНСНАЦІОНАЛЬНОЇ ЗЛОЧИННОСТІ

Плужнік О. І.

Визначено, що організована транснаціональна злочинність є одним з видів організованої злочинності, організована транснаціональна злочинність та організована злочинність співвідносяться як частка та ціле. Надано перелік чинників, якими характеризується міжнародний вимір організованої злочинної діяльності та класифікація транснаціональних злочинів.

Ключеві слова: *організована група, злочинна організація, організована злочинність, транснаціональна злочинність.*

Определено, что организованная транснациональная преступность является одним из видов организованной преступности, организованная транснациональная преступность и организованная преступность соотносятся как часть и целое. Дан перечень факторов, которыми характеризуется международное измерение организованной преступной деятельности и классификация транснациональных преступлений.

Ключевые слова: *организованная группа, преступная организация, организованная преступность, транснациональная преступность.*

It was determined that according to the new realities of political life in the country, Ukraine in recent years faced serious economic problems due to the rapid introduction of the uncontrolled market economy, which in turn led to the development of criminal groups that entering the economic, commercial, banking and other financial institutions, provided the basis for their continued existence.

Established that a fundamental change in the social and economic foundations of society, aggravation of contradictions between human needs and capabilities to meet them gradually lead to worsening crime situation, creating favorable conditions for the increase of crimes committed by organized groups, including international and transnational crimes.

Determined that organized transnational crime is a type of organized crime. Organized crime and transnational organized crime relate to the share and unit. Guestrooms thought VN Kudryavtsev, Alexander Turchinov.

Analyzed statistical indicators of characteristics of organized groups and criminal organizations for January - June 2016 in Ukraine on registered criminal offenses; on offenses relating to firearms; on the number of committed offenses against public safety; submitted to the court of criminal offenses, including those committed by the group; identified organized groups and criminal organizations ;. Of these transnational connections; the duration of action of organized groups and criminal organizations to one year; to two years; three to six years.

Available analysis of post-Soviet organized crime, analysis of international law and the fight against transnational crime

Key words: *organized group, a criminal organization, organized crime, transnational crime.*

Останнім часом, відповідно до нових реалій суспільно-політичного життя в державі, як і в більшості пострадянських країн, Україна за останні роки стикалася