УДК 658.012.32:004

З.П. Сташевський, Ю.І. Грицюк, *д-р техн. наук, професор*
(Львівський державний університет безпеки життєдіяльності)

АНАЛІЗ ДЖЕРЕЛ ЗАГРОЗ ІНФОРМАЦІЙНИМ СИСТЕМАМ НА ЕТАПІ ІНІЦІАЦІЇ ПРОЕКТУ

Проведено аналіз джерел загроз і вразливостей ІС структурних підрозділів Державної служби України з надзвичайних ситуацій, розглянуто та проаналізовано ряд наявних їх класифікацій. Розроблено класифікацію джерел загроз об'єктам ІБ та модель процесів реалізації атак рятувальної служби, які поділяються за видом, походженням, характером дії, джерелами і об'єктами загроз. На основі запропонованої класифікації виділено основні проблеми на етапі ініціації проекту управління ІБ структурних підрозділів ДСНС України.

Ключові слова: система захисту інформації, інформаційна система, джерела загроз, критична інформація, ініціація проекту.

Вступ. Інтенсивний розвиток і поширення інформаційних технологій (ІТ), дає змогу за допомогою спеціальних пристроїв інтегрувати, обробляти і синхронно відтворювати різноманітні типи інформації, і, як наслідок, підвищує можливість її втрати [3]. Тому надзвичайно актуальною є проблема розроблення методів і моделей управління проектами інформаційної безпеки (ІБ), що дасть змогу захистити критичну інформацію, яка зберігається та обробляється в корпоративних мережах чи передається каналами зв'язку [5]. Так звана "кібер-злочинність", завдяки використанню сучасних ІТ, стала не тільки прибутковою справою, але й достатньо безпечною для порушників роботою і з кожним днем притягує все більше і більше охочих до легкої наживи. Зрозуміло, в такій ситуації особливої уваги заслуговує превентивне створення інформаційних систем (ІС), які були б надійно захищеними від різноманітних загроз [4].

Тільки но виникла проблема захисту інформації, багато дослідників робилять спроби класифікувати джерела загроз інформаційної безпеки (ІБ) і самі загрози з метою подальшої стандартизації засобів і методів, що використовуються для їх знешкодження. У достатньо відомій монографії Л.Дж. Хофмана "Сучасні методи захисту інформації" [6] було виділено 5 груп різних загроз: розкрадання носіїв, запам'ятовування або копіювання інформації, несанкціоноване під'єднання до апаратури, несанкціонований доступ до ресурсів системи, перехоплення побічних випромінювань і наведень. Різні автори [1], в т.ч. і Л.Дж. Хофманом, пропонували різні підходи до такої класифікації. За критерії поділу загроз на класи вони використовували види небезпек, рівень зловмисного наміру, джерела прояву загроз і т.д. Проте такі підходи є неповними і не можуть повністю окреслити всю проблемну область виникнення джерел загроз ІБ, а також методи і засоби їх виявлення та знешкодження.

При проведені аналізу джерел загроз і вразливостей ІС, на етапі ініціації проекту управління ІБ структурних підрозділів Державної служби України з надзвичайних ситуацій (далі ДСНС України) було розглянуто та проаналізовано ряд відомих методів їх класифікації [2]. Спроби використання деяких з цих методів показали, що у багатьох випадках реальні джерела загроз або не належали жодній з класифікаційних ознак або, навпаки, задовольняли відразу декілька з них.

Мета роботи: провести класифікацію джерел загроз ІС структурних підрозділів ДСНС України в якнайповнішій та детальнішій їх структуризації, що дасть змогу їх ідентифікувати тільки за однією класифікаційною ознакою і виділити найнебезпечніші з них на етапі ініціації проекту управління ІБ.

Класифікація джерел загроз проводилась за допомогою програмного продукту «ГРИФ» версії 3. Тут використовуються такі терміни та визнання:

- ✓ *джерело загроз* – потенційно можлива подія, процес або явище, яке може (впливаючи на що-небудь) призвести до завдання збитку чиїмсь інтересам;

- ✓ *загроза інтересам суб'єктів інформаційних відносин* – потенційно можливі події, процеси або явища, які за допомогою впливу на інформацію, її носії та процеси обробки можуть прямо або опосередковано призвести до завдання збитку інтересам цих суб'єктів;
- ✓ *порушення безпеки* (просто порушення або атака) – реалізація загрози об’єктові ІБ;
- ✓ *атака на інформаційну систему* – дія, яка полягає в пошуку і використанні тієї або іншої вразливості ІС об’єкта ІБ;
- ✓ *вразливість інформаційної системи* – якась її невдала характеристика, яка робить можливим виникнення загрози об’єктові ІБ. Іншими словами, саме через наявність вразливостей в ІС відбуваються небажані події на об’єкт ІБ;
- ✓ таким чином, атака – це реалізація джерела загроз.

Розглянемо види джерел загроз. Параметр, який характеризує певне джерело загрози, є основоположним, якщо визначає цільову спрямованість ІС захисту інформації. Зміст значення цього параметра визначається рівнем, на якому відбувається негативна дія на інформацію. Це може бути на синтаксичний, семантичний або прагматичний рівні.

За походженням джерела загроз ІБ структурних підрозділів ДСНС України поділяють на природні (об’єктивні) та штучні (суб’єктивні). *Природні джерела загроз* переважно викликані впливами на ІС чи її елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини. *Штучні джерела загроз* викликані діяльністю людини, вони в своєю чергою поділяються на технічні та організаційні (рис. 1).

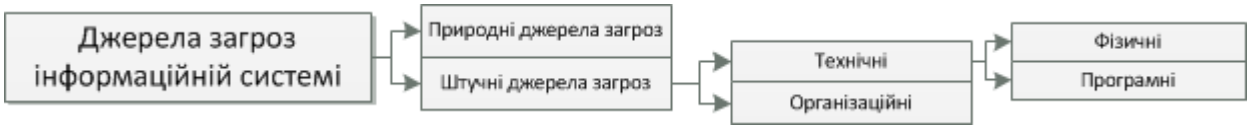

Рис. 1. *Схема поділу джерел загроз за походженням та характером дії*

Технічні джерела загроз за характером дії поділяються на фізичні та програмні (логічні). Фізичні загрози можуть виникати через дії зловмисника (людини), збіг обставин (збіг несприятливих для системи ІБ обставин, які разом утворюють умови вільного доступу до критичної інформації) і відмови обладнання та внутрішніх систем життєзабезпечення (рис. 2). Припустимо, що зловмисник має фізичний доступ до приміщення, в якому розташований інформаційний ресурс. Щоб реалізувати загрозу, тобто заподіяти шкоду, порушник може впливати безпосередньо на ресурс або на канали зв'язку (VPN-мережу, IP-телефонію, ДМЗ-зону).

Рис. 2. *Аналіз фізичних видів джерел загроз*

Згідно із статистичними даними, представленими регулярним дослідженням "CSI / FBI Computer Crime and Security Survey" [7], на даний час основною проблемою для об’єктів ІБ є програмні джерела загроз. Щорічний звіт, у складанні якого беруть участь фахівці Інституту комп'ютерної безпеки США (Computer Security Institute, CSI) і ФБР (FBI), дає змогу побудувати діаграму, на якій видно в процентному відношенні найбільш реалізовані джерела загроз об’єктам ІБ (рис. 3). Атаки, що реалізують подібні джерела загроз, в загальному вигляді мають 4 стадії (рис. 4).

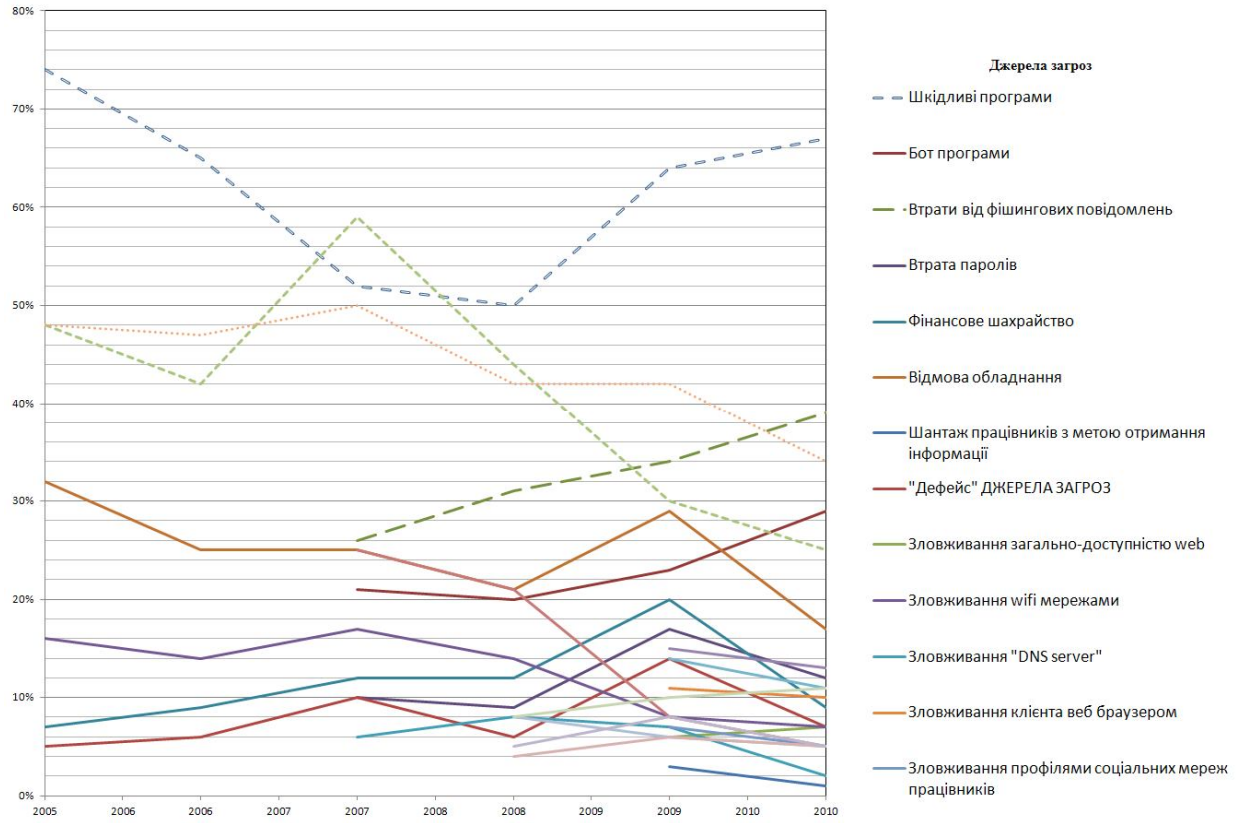

Рис. 3. *Статистичні дані реалізації джерел загроз об'єктам ІБ* [7]

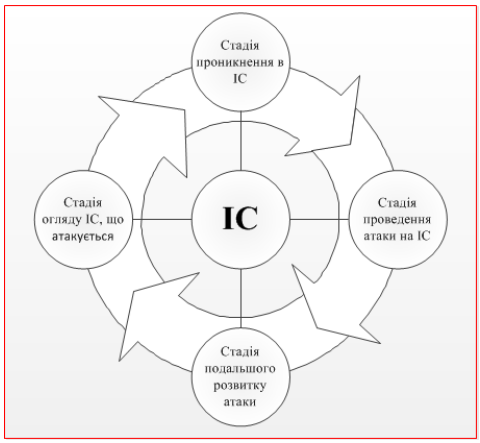

Рис. 4. *Модель процесів реалізації атак*

На стадії огляду ІС, що атакується, зловмисник намагається отримати якомога більше інформації про об'єкт атаки, на основі якої він планує подальші етапи атаки. Прикладами таких даних є: тип і версія операційної системи, встановленої на хостах ІС, список користувачів, зареєстрованих у системі, відомості про використання прикладного ПЗ та ін.

Стадія проникнення в ІС характеризується тим, що тут зловмисник отримує несанкціонований доступ до ресурсів тих хостів, на які здійснюється атака.

Стадія проведення атаки на ІС спрямована на досягнення порушником тих цілей, для яких і робилася атака. Прикладами таких дій можуть бути порушення працездатності ІС, крадіжка конфіденційної інформації, збереженої в системі, видалення або модифікація даних системи та ін. При цьому кваліфікований зловмисник тут може також здійснювати дії, які спрямовані на видалення слідів його присутності в ІС.

На *стадії подальшого розвитку атаки* зловмисник виконує дії, які потрібні йому для продовження атаки на інші об'єкти ІС.

Програмні (логічні) джерела загроз виходять від локальних чи віддалених порушників (рис. 5). При локальному доступі на програмному рівні зловмисник може реалізувати загрозу, використовуючи такі компоненти ресурсу: операційну систему, прикладне ПЗ, конфіденційні дані, а також основну критичну інформацію, яка зберігається та обробляється. Порушення фун-

кціонування системи ІБ, цілісності програмного забезпечення або конфіденційності даних може призвести до втрати критичної інформації (рис. 6). При віддаленому програмному доступі зловмисник може впливати як на ресурс, що містить критичну інформацію, так і на канали зв'язку, що пов'язують ресурси між собою (рис. 7). При цьому через ресурс порушник може впливати на такі його компоненти: операційну систему, мережеві служби і критичну інформацію, до якої може бути відкритий віддалений доступ. Через канали зв’язку зловмисник може впливати безпосередньо на мережеве устаткування або на протоколи передачі даних.

Аналіз механізмів практичних реалізацій атак у мережі Internet дає змогу сформулювати причини, згідно з якими реалізація цих загроз виявилася можливою. Вони ґрунтуються на базових принципах побудови мережної взаємодії об'єктів розподіленої обчислювальної системи.

Всі вище перераховані джерела загроз пов'язані з доступом зловмисника до конфіденційного інформаційного ресурсу; тому заходи, спрямовані на їх виявлення та ліквідацію, мають бути універсальними технічними та програмними системами захисту корпоративних мереж. На практиці, в реальній ІС захисту корпоративної мережі, ключовим моментом забезпечення ІБ є коректні дії працівника служби ІБ. Тому в даній класифікації потрібно також розглянути так звані загрози ламерів – низькокваліфікованого персоналу, тобто вплив людського фактора.

Зі статистичних даних, зібраних за результатами другого щорічного дослідження в галузі внутрішньої ІБ аналітичним центром компанії Perimetrix [8], видно, що внутрішні джерела загроз є надзвичайно небезпечними і коректні дії працівників служби ІБ відіграють не останню роль у їх реалізації (рис. 8).

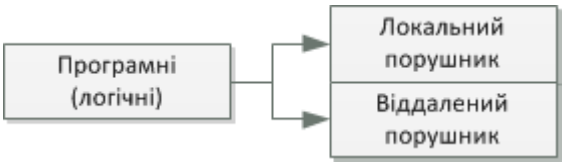

Рис. 5. *Схема поділу програмних джерел загроз за місцем розміщення порушника*

Рис. 6. *Структура локальних джерел загроз на програмному рівні*

Рис. 7. *Структура віддалених джерел загроз на програмному рівні*

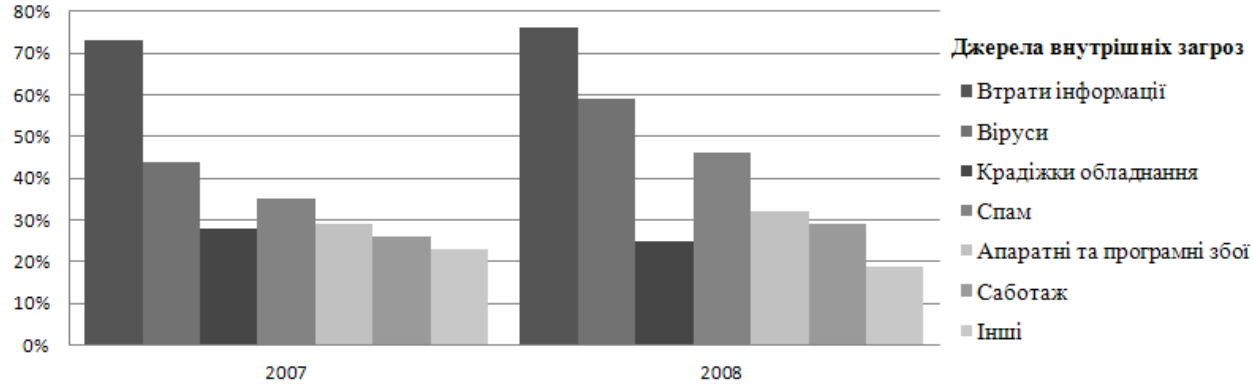

Рис. 8. *Діаграма внутрішніх джерел загроз об'єктів ІБ* [8]

Організаційні джерела загроз (внутрішні) на інформаційні ресурси, виходячи з мотивації дій, поділяються на дії, спрямовані на персонал, що призводять до несвідомої його помилки, яка корисна зловмиснику, а також усвідомлені зловмисні дії персоналу (рис. 9).

Рис. 9. *Структурна організаційних джерел загроз*

Дії зловмисника, спрямовані на персонал для отримання власної вигоди, поділяються на фізичні та психологічні, які реалізуються з метою отримання критичної інформації або порушення функціональної готовності підрозділів ДСНС до ліквідації НС. Водночас, зловмисні дії персоналу поділяються на (рис. 10):

- *випадкові (ненавмисні),* під дією яких утворюються джерела загроз, викликані помилками в проектуванні ІС та її елементів, помилками в ПЗ та в діях персоналу, що виконуються людьми випадково, через незнання, неуважність або недбалість, з цікавості, але без злого наміру і т.ін.;
- *навмисні дії персоналу*, пов'язані з корисливими, ідейними чи іншими прагненнями людей (зловмисників) заподіяти шкоду об'єкту ІБ, спрямовані на виведення ІС з ладу, проникнення в систему та несанкціонованого доступу до інформації.

Основні випадкові (ненавмисні) штучні джерела загроз ІС поділяються на:

1) ненавмисні дії персоналу, що призводять до часткової або повної відмови ІС або руйнування її апаратних, програмних і інформаційних ресурсів, а саме - ненавмисне псування устаткування, видалення, перекидання файлів з важливою інформацією або програм, в т. ч. системних, і т.ін.;

2) неправомірне від'єднання устаткування або зміна режимів роботи ключових пристроїв і програм;

3) ненавмисне псування носіїв інформації;

4) запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання або зациклення) або здійснювати необоротні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних і т.ін.);

5) нелегальне впровадження та використання ПЗ (ігрових, навчальних, технологічних та ін, які не є потрібними для виконання порушником своїх службових обов'язків) з подальшим необґрунтованим витрачанням ресурсів (завантаження процесора, захоплення оперативної пам'яті і пам'яті на зовнішніх носіях);

6) зараження комп'ютера вірусними програмами;

7) необережні дії, що призводять до розголошення конфіденційної інформації або роблять її загальнодоступною;

8) розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, перепусток і т.д.);

9) перепроектування архітектури ІС, технології обробки даних, розробки прикладних програм з можливостями, що представляють небезпеку для працездатності системи і безпеки інформації;

10) ігнорування організаційних обмежень (встановлених правил) при роботі в системі;

11) вхід в систему в обхід засобів її захисту (завантаження сторонньої операційної системи із змінних магнітних носіїв тощо);

12) некомпетентне використання, налаштування або неправомірне від'єднання засобів захисту персоналом служби ІБ;

13) пересилання даних за хибною адресою абонента (пристрою);

14) введення помилкових даних;

15) ненавмисне пошкодження каналів зв'язку.

Основні можливі навмисні негативні дії персоналу (інсайдерів), поділяються на:

1) фізичне руйнування ІС (шляхом вибуху, підпалу тощо) або виведення з ладу всіх або окремих найбільш важливих компонентів (пристроїв, носіїв важливої системної інформації, осіб із числа персоналу і т.ін.);

2) від'єднання або виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку тощо);

3) дії щодо дезорганізації функціонування ІС (зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, встановлення потужних активних радіоперешкод на частотах роботи пристроїв ІС і т.ін.);

4) впровадження агентів у штат персоналу служби ІС (у т. ч., можливо, і в адміністративну групу, яка відповідає за ІБ);

5) вербування (шляхом підкупу, шантажу і т.д.) персоналу або окремих користувачів, що мають певні повноваження;

6) застосування підслуховувальних пристроїв, дистанційна фото- та відеозйомка і т.ін.;

7) перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв та ліній зв'язку, а також наведень активних випромінювань на допоміжні технічні засоби, що безпосередньо не беруть участі у обробці інформації (телефонні лінії, безперебійна мережа живлення, опалення тощо);

8) перехоплення даних, переданих каналами зв'язку, і їх аналіз з метою з'ясування протоколів обміну, правил входження в зв'язок і авторизації користувача чи подальших спроб їхньої імітації для проникнення в ІС;

9) викрадення носіїв інформації (магнітних дисків, стрічок, чіпів, запам'ятовувальних пристроїв і цілих ЕОМ);

10) несанкціоноване копіювання носіїв інформації;

11) розкрадання виробничих відходів (роздруківок, записів, списаних носіїв інформації тощо);

12) читання залишкової інформації з оперативної пам'яті і з зовнішніх запам'ятовуючих пристроїв;

13) зчитування інформації з областей оперативної пам'яті, що використовуються операційною системою (у т. ч. підсистемою захисту) або іншими користувачами, в асинхронному режимі, використовуючи недоліки мультизадачних операційних систем і систем програмування;

14) незаконне отримання паролів та інших реквізитів розмежування доступу (агентним шляхом, використовуючи недбалість користувачів, шляхом підбору чи імітації інтерфейсу системи і т.д.), маскуванням під зареєстрованого користувача ("дефейс" атаки);

15) несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізичну адресу, адресу в системі зв'язку, апаратний блок кодування і т.ін.;

16) розкриття кодів криптозахисту інформації;

17) впровадження апаратних "спецвкладок", програмних "закладок" і "вірусів" ("троянських коней" та "жучків"), тобто таких ділянок програм, які не потрібні для здійснення заявлених функцій, але дають змогу долати систему захисту інформації, таємно і незаконно здійснювати доступ до системних ресурсів з метою реєстрації та передачі критичної інформації або дезорганізації функціонування ІС;

18) незаконне під'єднання до ліній зв'язку з метою роботи "між рядків", з використанням пауз в діях законного користувача від його імені з наступним введенням помилкових повідомлень або модифікацією переданих повідомлень;

19) незаконне під'єднання до ліній зв'язку з метою прямої підміни законного користувача шляхом його фізичного від'єднання після входу в систему і успішної аутентифікації з наступним введенням дезінформації та нав'язуванням хибних повідомлень.

З результатів другого щорічного дослідження в галузі внутрішньої ІБ аналітичним центром компанії Perimetrix [8] видно, що внутрішні джерела загроз, а саме ті, які виникають від інсайдерських протиправних дій, є надзвичайно небезпечними і мають велике значення в забезпеченні збереження критичної інформації (рис. 11).

Рис. 10. *Структура джерел загроз, які виникають від зловмисних дій працівників служб ІБ*

Найчастіше для досягнення поставленої мети зловмисник використовує не один, а деяку сукупність атак з перерахованих вище. При цьому кожна з них чи всі разом можуть загрожувати як порушенню конфіденційності інформації, так і функціональній готовності структурного підрозділу ДСНС України до виконання дій за призначенням.

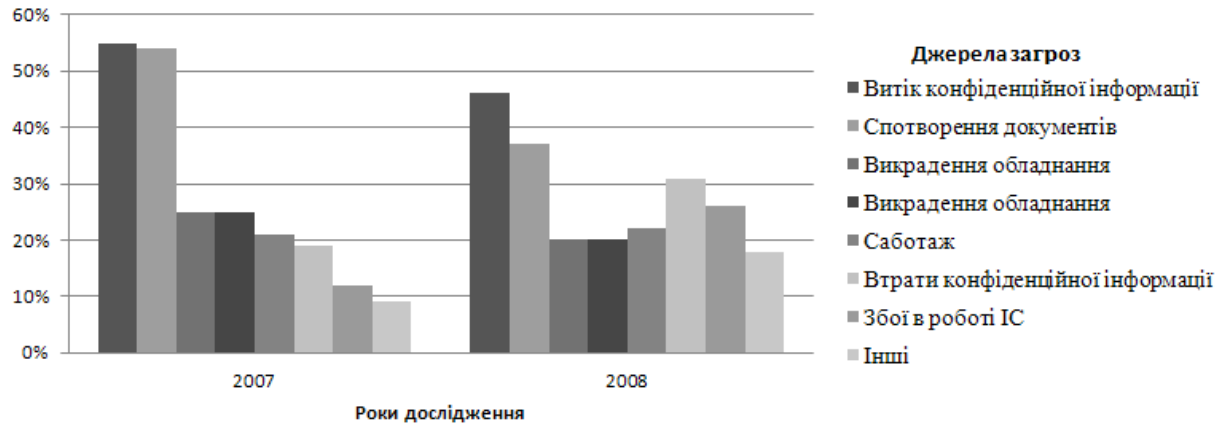

Рис. 11. *Джерела загроз, які реалізовані інсайдерами*

Таким чином, розроблену класифікацію джерел загроз об’єктам ІБ структурних підрозділів ДСНС України можна поділити за видом, походженням, характером дії, джерелами і об'єктами загроз.

На основі запропонованої класифікації, проведеної за допомогою сертифікованого програмного продукту «ГРИФ» версії 3, чітко видно, що людський фактор і рівень підготовки персоналу має ключове значення при якісній побудові і безперебійному функціонуванні системи захисту інформації Державної служби України з надзвичайних ситуацій.

Узагальнивши всі наведені вище положення, отримаємо узагальнену структуру більшості джерел загроз, що стосуються інформаційної системи ДСНС України на етапі ініціації проекту управління ІБ (рис. 12).

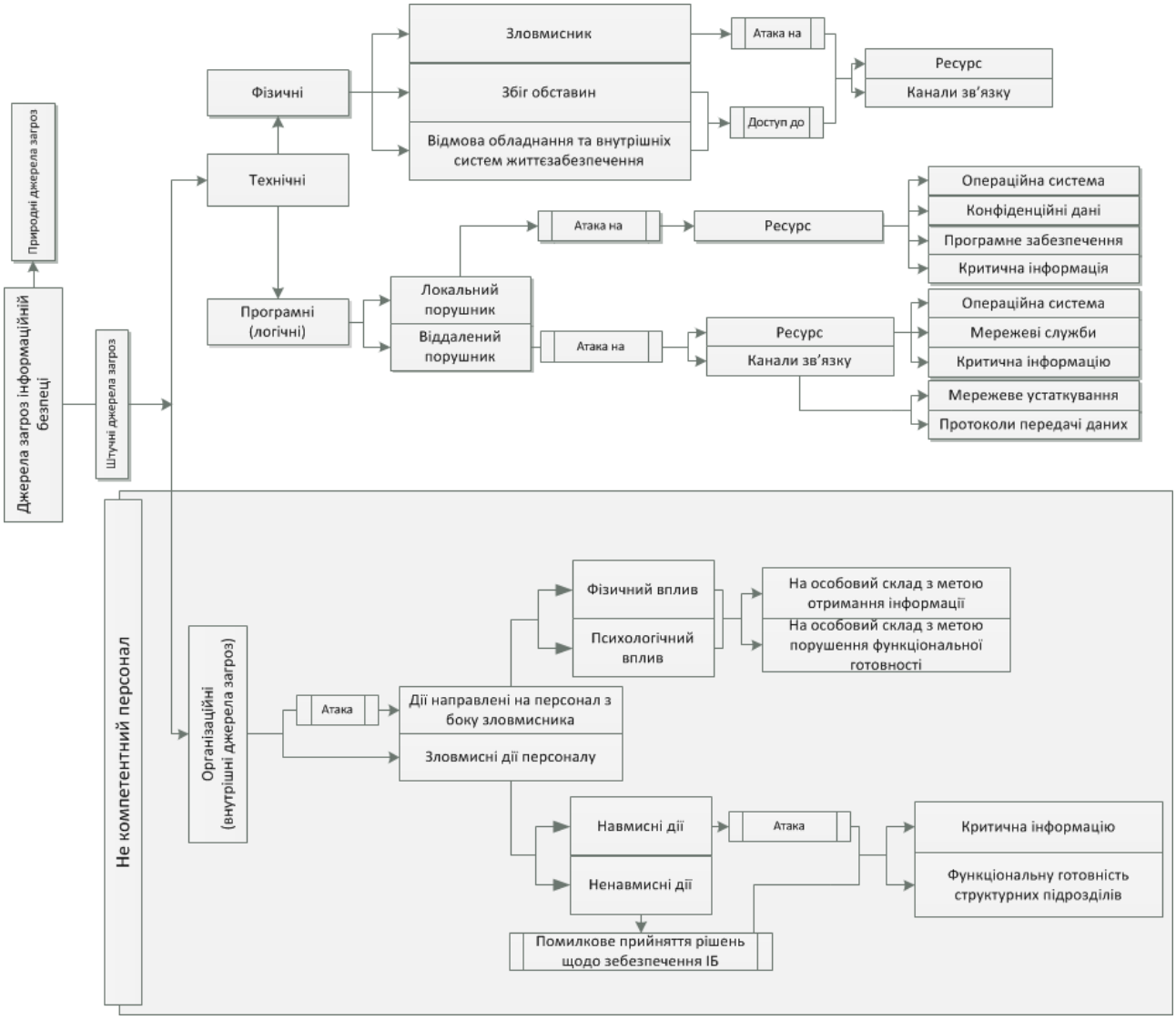

Рис. 12. *Структура імовірних джерел загроз інформаційним системам ДСНС України*

Висновок:

Проведено аналіз джерел загроз і вразливостей ІС структурних підрозділів ДСНС України, що дало змогу розробити нову класифікацію джерел загроз об’єктам ІБ та модель процесів реалізації атак. На основі запропонованої класифікації та даної моделі виділено основні проблеми на етапі ініціації проекту управління ІБ структурних підрозділів рятувальної служби.

Література:

1. **Астахов А.М.** Искусство управления информационными рисками / А.М. Астахов. – М.: ДМК-Пресс, 2010. – 312 с.

2. **Грайворонський М.В.** Безпека інформаційно-комунікаційних систем / Грайворонський М.В., Новіков О.М. – К. : Вид. група BHV, 2009. – 608 с.

3. **Грицюк Ю.І.** Проблеми захисту інформації у структурних підрозділах МНС України / Грицюк Ю.І., Рак Т.Є. // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2011. – Вип. 21.12. – С. 330-346.

4. **Мирошников Б.Н.** Борьба с киберпреступлениями – одна из составляющих информационной безопасности Российской Федерации / Б.Н. Мирошников. [Электронный ресурс]. – Доступен с http://www.crime-research.org/library/Miros1.html

5. Новиков Д.А. Модели и методы организационного управления инновационным развитием фирмы / Д. А. Новиков, А. А. Иващенко. – М. : КомКнига, 2006. – 332 с

6. Хоффман Л.Дж. Современные методы защиты информации. Пер. с англ. / Л.Дж. Хоффман – М.: Советское радио, 1980. – 264 с.

7. **CSI/FBI Computer Crime and Security Survey.** [Electronic Resource]. – Available from https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf

8. **Инсайдерские угрозы 2009.** [Электронный ресурс]. – Доступен с http://perimetrix.ru/content/view/38/149/

9. **Поспелов Д.А.** Нечеткие множества в моделях управления и искусственного интеллекта / Д.А. Поспелов. – М. : Изд-во "Наука", 1986. – 312 с.

З.П. Сташевский, Ю.И. Грыцюк

АНАЛИЗ ИСТОЧНИКОВ УГРОЗ ИНФОРМАЦИОННОЙ СИСТЕМЕ ГСЧС УКРАИНЫ НА ЭТАПЕ ИНИЦИАЦИИ ПРОЕКТА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проведен анализ источников угроз и уязвимостей ИС структурных подразделений Государственной службы Украины по чрезвычайным ситуациям, рассмотрены и проанализированы ряд существующих их классификаций. Разработана классификация источников угроз объектам ИБ и модель процессов реализации атак спасательной службы, которые делятся по виду, происхождению, характеру действия, источникам и объектам угроз. На основе предложенной классификации выделены основные проблемы на этапе инициации проекта управления ИБ структурных подразделений ГСЧС Украины.

Ключевые слова: система защиты информации, информационная система, источники угроз, критическая информация, инициация проекта.

Z.P. Stashevsky, Yu.I. Grycyuk

ANALYSIS OF THE THREAT SOURCES TO INFORMATION SYSTEMS ON PROJECT INITIATION STAGE

The analysis of the sources of threats and vulnerabilities of IS structural subdivisions of the State Service of Emergencies of Ukraine, a number of their existing classifications was reviewed and analyzed. The classification of sources of threats to objects of IS and a process realization model of Attack Rescue Service, which are divided by type, origin, nature of action, the sources and targets of threats. On the basis of the proposed classification main problems at the stage of initiation of the project management of IS structural units SSE of Ukraine were defined.

Keywords: System information security, information systems, sources of threats, critical information, initiation of the project.