УДК 004.056.55:004.312.2

Г.С. Грибенюк, А.В. Тарасенко

Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля Національного університету цивільного захисту ДСНС України, Черкаси

ТИПОЛОГІЯ ЗАГРОЗ ТА ПОРУШНИКІВ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ДСНС УКРАЇНИ

У статті аналізуються особливості організації функціонування інформаційних систем аварійно-рятувальної служби цивільного захисту. Розкрито основні категорії порушників безпеки і можливі загрози, сформульовано умови зниження ризиків несанкціонованих дій у розподілених обчислювальних мережах ДСНС України, на основі аналізу діяльності користувачів і класифікації мережевого трафіку.

Ключові слова: *автоматизована система управління ДСНС України, розподілені обчислювальні мережі, порушник безпеки, загрози, ризик, безпека.*

Вступ

Постановка проблеми. В умовах відмобілізування інформаційне забезпечення аварійно-рятувальної служби цивільного захисту та її систем управління має надзвичайно важливе значення і заслуговує на те, щоб бути предметом спеціального дослідження. Оскільки, інформаційне забезпечення визначає готовність не лише формувань ДСНС України до відмобілізування, а й загалом, готовність сфери захисту національної безпеки. Розробка моделей та методів оцінювання уразливості інформаційних систем підтримки стану мобілізаційної готовності формувань ДСНС України, дозволить на основі використання засобів подання ієрархічної побудови параметрів інформаційних систем підтримки та визначення змісту необхідної інформації, розрахувати ступінь реальної готовності формувань центрального підпорядкування, територіальних підсистем, зведених загонів ДСНС України відповідно до визначеного керівними документами рівня. Це дасть змогу мінімізувати та унеможливити суб'єктивне викривлення чи недбалість кількісно-якісної оцінки окремих показників готовності формувань ДСНС України.

Для досягнення поставленої мети необхідно провести аналіз шляхів, способів протидії порушенням безпеки, розкрити поняттєві засоби оцінювання ризиків і небезпек в розподілених обчислювальних мережах(РОМ).

Аналіз останніх досліджень і публікацій. Наявність повної та достовірної інформації у змісті інформаційних потоків розподіленої обчислювальної мережі є важливою умовою забезпечення безпеки.

Теоретичні аспекти проблеми складників безпеки інформаційних потоків розкрито О.Г. Додоновим, В.Г. Кравченко, Т. Писаренко, С.В. Запечников [3, 4]. В роботах Ю.В. Синещук [5] проведено аналіз методичних питань безпеки розподілених мереж, їх значення в управлінні безпекою інформаційних систем.

Тому **метою статті** була визначена необхідність з'ясувати особливості організації функціонування інформаційних систем та розкрити типологічні особливості порушників безпеки і можливі загрози. Що дасть можливість знизити ризики несанкціонованих дій в розподілених обчислювальних мережах.

Основний матеріал

Інформаційне забезпечення відомостями про готовність до відмобілізування формувань ДСНС України здійснюється з використанням автоматизованих інформаційно-управлінських системи (АІУС) і передбачає наявність технічних систем із засобами зв'язку, оповіщення та автоматизації, а також інформаційних ресурсів, які забезпечують обмін даними, підготовку, збір, зберігання, обробку, аналіз і передачу інформації. АІУС виконують функції інформатизації та автоматизації в діяльності органів управління ДСНС України, зокрема, в умовах попередження та ліквідації НС, під час виконання заходів цивільного захисту в масштабі регіонального, місцевого та об'єктового рівнів [1]. З огляду на специфіку повноважень ДСНС України, – скоординувати взаємодію органів державного управління у розв'язанні завдань мінімізації наслідків надзвичайних ситуацій та мобілізації передбаченого людино-технічного потенціалу, – АІУС покликана займати центральне місце, поєднуючи інформаційні ресурси інших відомств, їх автоматизованих систем, які здійснюють збір інформації на території України.

В умовах множинності джерел і користувачів інформації, РОМ з необхідністю стають матеріально-технічною основою реалізації АІУС, зокрема, і в ДСНС України. Оскільки вони є розгалуженими складними системами, призначеними для обробки, зберігання і передачі інформації, то необхідною є значна увага для того, щоб забезпечити безпеку обчислювальних мереж [2]. Перевага обробки інформації в РОМ не викликає сумніву, проте, обертається значними труднощами в організації їх захисту.

Підкреслимо проблемні питання, зокрема, такі:

– розширення зони контролю;

– комбінування програмно-апаратних засобів;

– невідомі межі периметру;

– наявність значної кількості точок атаки;

– складність управління і контролю за доступом з боку суб'єктів інформування (СІ).

Заходи забезпечення безпеки у розподілених обчислювальних мережах значною мірою залежать від прогнозної моделі загроз, і тому є необхідність опрацювати належні заходи та попередньо провести оцінювання і класифікацію інформаційних загроз [3, 4]. Така класифікація розкриває реальні загрози, які існують для конкретних РОМ (табл. 1).

Таблиця 1

Класифікація інформаційних загроз

	Характер загрози	Вид впливу загрози	Спрямування загрози	Джерело загрози
Загрози інформаційної безпеки	Технологічні загрози	Фізичний	зовнішня	Людина
			внутрішня	
			зовнішня	Форс-мажор
			внутрішня	
			зовнішня	Відмова обладнання і внутрішніх систем
			внутрішня	
		Програмні (логічні)	внутрішня	Локальний порушник
			зовнішня	Віддалений порушник
			внутрішня	
	Організаційні загрози	Впливи на СІ	внутрішня	Фізичний вплив на СІ
			внутрішня	Психологічний вплив на СІ
		Дії СІ	внутрішня	Умисні порушення
			внутрішня	Випадкові порушення

Аналіз планувальних документів відмобілізування, проведений, з огляду на типологічні характеристики загроз, дає можливість стверджувати, що кількість внутрішніх загроз має значну питому вагу і може перевищувати кількість зовнішніх. Про випадки використання впливу на відповідальних осіб, СІ з метою перетворити їх у джерело загрози свідчить практика ведення бойових дій у «гібридних» війнах. Тому необхідно передбачати можливість попередження зовнішніх впливів за допомогою внутрішніх засобів. У широкому контексті внутрішні загрози складають генеральну сукупність практично повністю пов'язану з користувачами обчислювальних мереж, СІ. Узагальнений склад найбільш небезпечних внутрішніх загроз порушення безпеки інформації подано у табл. 2.

Таблиця 2

Внутрішні загрози порушення безпеки інформації

Загрози	%
Втрата інформації	7
Крадіжки обладнання	6
Збої в роботі ІС	15
Спотворення інформації	62
Порушення конфіденційності інформації	98
Інші	28

Разом з тим, аналіз існуючих засобів і методів захисту інформації свідчить про те, що у переважній більшості рішень, які забезпечують інформаційну безпеку, пропонується захист даних виключно від загроз зовнішніх. На протилежний полюс континуума безпеки, де зосереджено заходи протидії внутрішнім загрозам, не звертають уваги. Ґрунтом такої позиції відповідальних за планування осіб є припущення про сумління та професійну компетентність користувачів, СІ. Проте, це не так. Є необхідність розробляти заходи безпеки, зважуючи, на можливі типи порушників, яких ми класифікували таким чином (табл. 3).

Таблиця 3

Класифікація порушників інформаційної безпеки

Зовнішні порушники	Внутрішні порушники
Представники ймовірного супротивника	Посадові, відповідальні особи, начальники служб, СІ
Представники задіяних у відмобілізуванні організацій, громадяни	Співробітники відділів розробки і супроводу ПЗ (прикладні та системні програмісти)
Випадкові відвідувачі	Користувачі (оператори) системи
Хакери	Керівники різних рівнів посадової ієрархії
Злочинні організації	Технічний персонал

На підтвердження власних висновків наведемо результати іншого дослідження. Відповідно до результатів вивчення Агентства CNews Analytics (CNA) найбільш серйозними загрозами інформаційної безпеки є планомірний витік інформації (70%) і недбалість персоналу, який допустив витік даних (70%). Обмеженість сучасних систем безпеки пов'язують з тим, що внутрішні проблеми значно важче виявляються та діагностуються, ніж зовнішні. Дії власних працівників можуть бути непередбачуваними та посиленими можливостями несанкціонованого доступу або крадіжки даних. Міра нанесеної шкоди може бути значно більшою, ніж від дії зовнішніх зловмисників.

Щодо заходів попередження, то вважається, що жорстке обмеження доступу працівників не дієве і може призвести до зупинки роботи. Внутрішня безпека – це завжди компроміс між організаційними і технічними методами, прагненням до захищеності і потребами СІ. Водночас, це безперервний процес, який передбачає не лише впровадження та налаштування програмних рішень, а також роботу і навчання працівників. Повністю захиститися від внутрішніх

загроз можливо, проте, необхідно намагатися мінімізувати ризики їх реалізації. Внутрішній порушник є легітимним СІ, який має право на доступ до інформаційних ресурсів. Його навмисні або помилкові дій можуть призвести до шкоди, значно більшої, ніж від зовнішнього зловмисника.

Нами було використано підхід до визначення внутрішніх порушників залежно від міри умислу та неправомірної активності в діях СІ по відношенню до чинних норм середовища СІ та змісту мобілізаційних документів. На нашу думку, підставами визначення порушника є ознаки умислу чотирьох рівнів:

– СІ, працівники, які випадково, вкрай рідко, порушують чинні організаційні норми і, переважно, не створюють загроз змісту мобілізаційних документів;

– порушники, до складу яких віднесено частину СІ, працівників, які дозволяють собі незначні похибки в документах та організаційні недбалості, зокрема, «фамільярності» з персональної веб-поштою, комп'ютерні ігри тощо;

– порушники дисципліни (або «відступники» від чинних норм) – СІ, працівники, які витрачають час на те, що не повинні робити: виявляють недбалість під час розробки мобілізаційних документів, зловживають наданими можливостями доступу до інтернету, самовільно встановлюють і використовують FTP-сервери. Такі СІ, працівники можуть відсилати конфіденційну інформацію зовнішнім адресатам, зацікавленим в ній. Отже, порушники дисципліни становлять серйозну загрозу безпеці інформації;

– зловмисники («зрадники»), – СІ, працівники, які, навмисно і регулярно спотворюють, викривлюють службову, конфіденційну інформацію у мобілізаційних документах, створюють умови, для того, щоб вона попала в умови небезпеки. Такі СІ, працівники створюють найбільшу загрозу, їх складніше знешкодити.

Захист від внутрішніх загроз з кожним роком стає все більшою проблемою. Вимоги та рекомендації щодо покрашення захисту інформації стосуються впровадження комплексного підходу та посилення контрою, зокрема, передбачають наступне:

– комплексне застосування заходів і засобів захисту інформації від несанкціонованого доступу (НСД);

– постійний контроль (суцільний, вибірковий, за критичними точками) за експлуатацією засобів обчислювальної техніки.

Такі вимоги не голослівні, а вироблені практикою. Подібні формулювання містяться і в британському стандарті BS 7799 «Практичні правила управління безпекою інформації», у німецькому стандарті BSI і в стандартах інших країн.

Розподіленої обчислювальної мережі призначені для підготовки, обробки, зберігання, документування та доставки електронних документів та інформаційних масивів між об'єктами ДСНС України, а також для обміну інформацією в електронному вигляді з іншими відомствами.

До складу автоматизованої системи (АС), зокрема, ДСНС України, в межах одного домену входять: організації (клієнти) та сервера. ЇЇ технічною основою є комплекси засобів телекомунікації, що розвертаються на об'єктах і з'єднуються між собою закритими каналами зв'язку. Документальний обмін інформацією різних рівнів конфіденційності може здійснюватися між автоматизованими робочими місцями підрозділів органів управління і окремих посадових осіб органів управління. Інформаційний обмін може здійснюватися між будь-якими засобами обчислювальної техніки зі складу автоматизованої системи або підключених до локальних мереж об’єктів. Базовим принципом побудови автоматизованої системи є об'єднання незалежних мереж (підмереж), яке з точки зору користувача функціонує як одна мережа.

За взаємною локалізації об'єкта загрози та порушника ми вирізняємо порушників зовнішніх і локальних. Зовнішні порушники – це СІ та обслуговуючий персонал зовнішніх локальних обчислювальних мереж, а також СІ та обслуговуючий персонал взаємодіючих об'єктів. Локальні порушники – це користувачі (оператори) даного об'єкта.

За ступенем обмежень у використанні технічних і програмних засобів доступу виділяються наступні групи порушників:

– порушники замкненого функціонального середовища (ЗФС) – посадові особи, допущені до засобів доступу в АС, проте, обмежені у власних можливостях, що визначається характером отриманих завдань. Дії таких порушників ЗФС регулює правило: «що не дозволено, то заборонено». Під засобами доступу в АС розуміються обчислювальні засоби і програмне забезпечення зовнішніх локальних обчислювальних мереж (ЛОМ), з яких надається доступ до АС ДСНС України;

– порушники відкритого функціонального середовища (ВФС) – посадові особи, які допущені до засобів доступу в АС та мають можливість запускати довільні програми та використовувати довільні протоколи. Дії порушників ВФС регулює правило – «що не заборонено, те дозволено»;

– порушники, яким не довірено доступ до функціонального середовища, (НФС) і використання яких не передбачено і не припустимо в системі засобів захисту інформації та організаційних заходах забезпечення безпеки інформації (ЗБІ), які необхідні для обробки конфіденційної інформації.

Для реалізації НСД порушниками ЗФС можуть бути використані такі можливості:

– фізичний вплив на засоби доступу до АС і носіїв інформації (стаціонарним і знімним) в процесі роботи;

– використання на засобах доступу до АС програм обробки інформації з обмеженого переліку, встановленого для ЗБІ;

– взаємодія в АС з використанням заданих прикладних протоколів і форматів повідомлень у мережі.

Модель порушників ЗФС припустима щодо зовнішніх і локальних порушників без обмеження на гриф таємності інформації та режим використання АС. Для реалізації НЕСД, порушники ВФС, в доповнення до можливостей порушників ЗФС, можуть використовувати:

– засоби розробки і налагодження програм в засобах доступу в АС, а також можливість самостійно встановлювати і використовувати програмне забезпечення;

– взаємодію з використанням довільних прикладних протоколів і форматів даних (документів).

Модель порушника ВФС припустима для обслуговуючого персоналу та окремих пунктів АС зовнішніх ЛОМ за умови використання лише в інформаційному обміні без допуску до інформації, що обробляється. Порушники НФС в доповнення до можливостей порушників ВФС можуть використовувати засоби доступу до АС, зокрема, й програмне забезпечення яке їм не довіряли. Використання моделі порушника НФС може бути лише для обробки відкритої інформації.

Висновок

Таким чином, в АІУС ДСНС України зазнавати інформаційних атак можуть: глобальна мережа інформаційного обміну, локальні мережі органів управління та окремі комп'ютери. У зв'язку з цим для захисту інформаційних ресурсів формувань ДСНС України необхідний комплексний підхід до забезпечення інформаційної безпеки. Для успішного вирішення цього завдання необхідно розвиток в АІУС підсистеми забезпечення безпеки інформації та розробка продуманої довгострокової політики інформаційної безпеки, що забезпечує захист інформації відповідно до вимог українського законодавства. На підсистему забезпечення безпеки інформації покладаються завдання щодо організації захисту і запобігання шкоди, якої може бути завдано державі за рахунок розкрадання, розголошення, витоку, втрати, спотворення і знищення інформації, порушення роботи технічних засобів загального і прикладного програмного забезпечення інформаційних систем АІУС ДСНС України. Згідно з українським законодавством автоматизовані системи, які обробляють інформацію обмеженого доступу, повинні виконуватися в захищеному вигляді і забезпечувати рівень захисту інформації, відповідно до ступеня її конфіденційності [5]. Також потребує захисту і відкрита документована інформація, яка знаходиться у віданні ДСНС України, та є державним інформаційним ресурсом. Тому захист конфіденційності, цілісності і доступності інформаційних, обчислювальних і комунікаційних ресурсів АІУС ДСНС України є обов'язковим і життєво необхідним державним завданням. Важливою складовою частиною цього завдання є зниження ризиків, пов'язаних з несанкціонованою діяльністю у розподілених обчислювальних мережах ДСНС України на основі аналізу видів діяльності та класифікації мережевого трафіку.

Список літератури

1. Птіцина Л.А. Основні підходи до управління інформаційними потоками [Текст] / Л.А. Птіцина // Вісник економічної науки України. – 2010. – № 2. – С. 121-124.

2. Литвак Б.Г. Разработка управленческого решения: учебн. / Б.Г. Литвак. – М.: Дело, 2001. – 392 с.

3. Додонов О.Г. Інформаційні потоки в глобальних комп'ютерних мережах. [Текст] / О.Г. Додонов, Д.В. Ланде, В.Г. Путятин. – К.: Наукова думка, 2009. – 295 с.

4. Малигін В.Р. Методи забезпечення безпеки розподілених інформаційних систем, заснованих на аналізі трафіку і контроль мережевої діяльності користувачів / В.Р. Малигін, Д.В. Козьмовский // Проблеми упр. ризиками в техносфери. – 2013. – № 2 (26). – С. 78-82.

5. Основні загрози і напрямки забезпечення безпеки інформаційного простору / Ю.В. Синещук [та ін] // Вестн. С.-Пб. ун-ту МВС Росії. – 2013. – № 2. – С. 150-154.

Надійшла до редколегії 4.11.2014

Рецензент: д-р техн. наук, проф. В.М. Рудницький, Черкаський державний технологічний університет, Черкаси.

ТИПОЛОГИЯ УГРОЗ И НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ГСЧС УКРАИНЫ

Г.С. Грибенюк, А.В. Тарасенко

В статье анализируются особенности организации функционирования информационных систем аварийно-спасательной службы гражданской защиты. Раскрыты основные категории нарушителей безопасности и возможны угрозы, сформулированы условия снижения рисков несанкционированных действий в распределенных вычислительных сетях ГСЧС Украины, на основе анализа деятельности пользователей и классификации сетевого траффика.

Ключевые слова: *автоматизированная система управления ГСЧС Украины, распределенные вычислительные сети, нарушитель безопасности, угрозы, риск, безопасность.*

TYPOLOGY OF THREATS AND INTRUDERS SECURITY INFORMATION SYSTEMS OF THE STATE EMERGENCY SERVICE OF UKRAINE

H.S. Grybeniuk, A.V. Tarasenko

The article analyses the peculiarities of the organization of functioning of information systems. Discuss the main categories of offenders security and possible threats, the task is formulated to reduce the risks of unauthorized activities in distributed computing networks of State Emergency Service of Ukraine, based on the analysis of users activities and classification of network traffic.

Keywords: *Control system of of State Emergency Service of Ukraine, distributed computing network, intruder security, threats, risk, safety*