Лише зацікавленість власників в забезпечені безпеки свого підприємства є основною запорукою зменшення ризиків на підприємствах.

Правильність дій персоналу при пожежі може мінімізувати завданий збиток, необхідно забезпечувати приміщення засобами первинного пожежогасіння.

Будь-яку небезпечну ситуацію легше попередити ніж усувати її наслідки. Наука і техніка кожного року удосконалюється і щороку розробляються нові системи протипожежного захисту, негорючі матеріали, засоби пожежогасіння. Тому лише дотримання правил пожежної безпеки здатне забезпечити безпеку даних підприємств та забезпечити зменшення кількості небезпечних ситуацій.

УДК 614.8

Здобувач З.П. Сташевський; професор Ю.І. Грицюк, доктор технічних наук
Львівський державний університет безпеки життєдіяльності

РОЗРОБКА СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ І МЕРЕЖ У СТРУКТУРНИХ ПІДРОЗДІЛАХ ДСНС УКРАЇНИ

Відомо, що стрімке збільшення кількості комп'ютерної техніки у структурних підрозділах ДСНС України, вільний доступ до мережі Інтернет і швидкий розвиток ринку нових комунікаційних пристроїв змінили і способи проведення спілкування, і методи виконання роботи. Змінюються способи скоєння інформаційних і комп'ютерних злочинів [3]. Розвиток глобальних інформаційних технологій відкриває нові можливості для діяльності зловмисників. За останні роки багато державних служб позбавилися конфіденційної, а часто і таємної інформації за допомогою інформаційних зловмисників, що володіють комп'ютерними знаннями [2]. Комп'ютери та глобальні інформаційні мережі часто використовуються для того, щоб викликати тривогу та посіяти паніку серед населення, очікування насильницьких нападів різних маніяків – і навіть для координації та здійснення терористичних дій.

Найбільш ефективне вирішення питань інформаційної безпеки у структурних підрозділах ДСНС України зводиться до постійної та систематичної роботи компетентних фахівців у кожному з підрозділів залежно від масштабів вирішуваних завдань. Хоча проблема підготовки фахівців з захисту інформації донедавна була актуальною для спеціальних служб силових відомств [1], проте на сьогодні, в силу специфіки виконуваних робіт і вирішуваних завдань, вона стосується і навчальних закладів ДСНС України, одним із яких є Львівський ДУ БЖД. Запроваджені тут методики навчання поряд із традиційними методами і засобами захисту інформації пропонують курсантам і студентам вивчати сучасні технології забезпечення безпеки інформаційних

ресурсів і комунікаційних систем. Насамперед це пов'язано зі збереженням і передачею оперативної інформації, яка стосується стану функціонування потенційно-небезпечних об'єктів чи складів з небезпечними речовинами чи радіоактивними матеріалами. Складність і різноманіття цих методів і засобів оброблення інформації, а також розширення можливостей каналів її передачі, відображення та збереження висувають ряд принципово нових вимог до фахівців з інформаційної безпеки.

Ще донедавна поняття "інформаційна злочинність" у правових актах офіційно не вказується. Разом з тим, саме це поняття закріпилося в лексиконі правоохоронних органів багатьох держав і має на увазі злочинність у сфері комп'ютерної інформації та телекомунікацій, незаконний обіг радіоелектронних і спеціальних технічних засобів, поширення неліцензійного програмного забезпечення для комп'ютерного обладнання, а також деякі інші види злочинності. Донедавна багато техніків-професіоналів не розуміли феномена інформаційної злочинності й не виявляли інтересу до нього. Ще й до сьогодні у багатьох випадках працівники структурних підрозділах ДСНС України відчувають відсутність інструментарію, необхідного для того, щоб зайнятися цією проблемою.

З огляду на інформаційну безпеку України, то тут спостерігається небезпечна тенденція, пов'язана зі збільшенням технічної та технологічної їх залежності від транскордонних проявів інформаційних терористів, яка зумовлена такими чинниками:

- бурхливим розвитком глобальної системи інформаційної телекомунікації, на зразок мережі Інтернет; приєднанням до процесу формування так званої глобальної інформаційної цивілізації нових країн через спеціальні національні програми, розвитку інформаційних технологій, суспільства, держави та подібних до них за змістом;
- зростанням у структурі національних економік і міжнародній економіці сектору торгівлі та надання послуг через електронні (комп'ютерні) засоби телекомунікації (зокрема, Інтернет-торгівля).

Що стосується структурних підрозділах ДСНС України, то варто відзначити такі негативні чинники, що стримують активну боротьбу з інформаційними злочинами і не дають змоги нашим працівникам на рівноправній основі включитися у світове інформаційне співтовариство:

- відсутність достатньої державної фінансової підтримки фундаментальних і прикладних вітчизняних досліджень у сфері попередження та боротьби з інформаційною злочинність; практично відсутній розвиток вітчизняного виробництва конкурентоспроможних систем захисту;
- інформатизація державних і комерційних структур здійснюється переважно на базі закордонної технології та комп'ютерної техніки (стратегічна технічна і технологічна залежність від інших держав);
- недостатні професійні знання працівників структурних підрозділах ДСНС України у сфері боротьби з інформаційними злочинами.

Перш за все, керівникам головних управлінь ДСНС України слід звернути особливу увагу на діяльність працівників відповідних структурних підрозділах, тому що тільки в їх обов'язки входить боротьба з інформаційною злочинність. Лише від якісної їхньої боротьби з інформаційною злочинність залежить, чи зможемо ми говорити про існування інформаційної безпеки особи, суспільства та держави загалом.

Проведені нами дослідження діяльності працівників структурних підрозділах ДСНС України щодо боротьби з інформаційною злочинність виявило ряд обставин, що не сприяють активізації та координації їх діяльності:

- низький рівень їх технічного та технологічного оснащення; прояви нездорової конкуренції між спецпідрозділами різних відомств: нерідко працівники СБУ передають до спецпідрозділів МВС та ДСНС оперативні матеріали про факти тільки тих інформаційних зловмисників, які вважаються безнадійними для розкриття;
- спецпідрозділи СБУ (де сконцентровано найкращий потенціал фахівців і які оснащені за останнім словом техніки) не вважають за доцільне ділитися досвідом зі спецпідрозділами інших відомств щодо методів і способів виявлення, документування та розкриття інформаційних зловмисників, мотивуючи тим, що це є засобами подвійного використання технологій (хоча нерідко зазначені технології описані у відкритих публікаціях);
- низький рівень інформаційно-правової культури в більшості суддівського корпусу, особливо на районному рівні.

Сучасні темпи розвитку інформаційних технологій вимагають від працівників структурних підрозділів ДСНС України високого рівня захисту конфіденційної інформації. Колективне використання інформаційних ресурсів потребує відповідного захисту дисків і каталогів, окремих папок і файлів, а також усіх локальних і глобальних мереж від несанкціонованого втручання інформаційних зловмисників, вірусів і небезпечних програм. Найважливішим завданням на цьому рівні є фізичний захист самого інформаційного ресурсу. Якщо ж на такому ресурсі зберігаються конфіденційні дані, то він має бути надійно захищеним за допомогою вбудованих засобів операційних систем, апаратного та програмного забезпечення. Немаловажне значення при цьому має забезпечення належного функціонування системи захисту інформації шляхом регулярного аналізу приміщень структурних підрозділів ДСНС України, у яких розташовуються інформаційні ресурси колективного користування.

Основне завдання систем інформаційної безпеки – забезпечити безперебійну роботу структурних підрозділів ДСНС України, тобто звести до мінімуму нанесені збитки від потенційних джерел загроз як конфіденційній інформації, так і іншим інформаційним ресурсам шляхом їхнього передбачення, випередження чи запобігання. Управління інформаційною безпекою дає змогу колективно використовувати будь-яку конфіденційну інформацію та