4) *Использование мультимедийных файлов.*

Для того, чтобы хранит файлы мультимедии, таких как изображения и загружаемые документы, в Системе доступно центрально хранилище для быстрого и удобного поиска. Модуль управления мультимедией позволяет пользователям расширить восприятие информации с использованием изображений, аудио, видео и т.д.

5) *Кеширование.*

Система позволяет сохранять уже ранее отображенную информацию и хранить для будущего вывода без обращений к серверу. Текущий модуль позволяет значительно снизить нагрузку на сервер и повысить производительность. Также повышается количество пользователей которые могут одновременно работать с системой.

6) *Удобство интерфейса.*

Интерфейс системы должен представлять собой подобия операционных системы с поддержкой оконного интерфейса. Данная идея позволяет пользователям ранее не работавшим с системой быстро привыкнуть к ней и начать работу.

7) *Поисковая оптимизация.*

Расширенный поиск может быть добавлен для отображения на страницу. Мощный "двигатель" внутреннего поиска позволяет поисковым системам обнаруживать и направлять пользователей на желаемое содержание в пределах системы.

**Выводы.** Разработка такого ядра программного обеспечения позволит интегрировать в одну систему несколько с разными функциональными назначениями. То есть, если раньше было создано несколько отдельных проектов (дистанционное обучение, документооборот и т.д.), то сейчас система позволит сделать взаимодействие между ними как на уровне программного кода, так и на уровне отображения конечной системы пользователю. У каждой системы может оставаться своя уникальная информация, но также доступ из определенного проекта можно расширить на использование и в других системах. Рабочий процесс управления позволяет пользователям легко проектировать и автоматизировать процессы, что позволяет вести создание и утверждение содержания документов между географически удаленными участниками, в рамках защищенного интерфейса браузера.

1. Пфаффенбергер Б., Шафер С., Уайт Ч., Кароу Б. HTML, XHTML и CSS. Библия пользователя, 3-е издание.: Пер. С англ. – М.: ООО "И.Д.Вильямс", 2007. – 752. 2. Хольцшлаг М. 250 секретов HTML и Web-дизайна. Пер с англ. Д.Ремизова. – М.: НТ Пресс, 2006. – 496 с. 3. Соколов С. HTML и CSS в примерах типовых решениях и задачах. Профессиональная работа: – М.: Издательский дом "Вильямс", 2007. – 416 с.

Надійшла до редколегії 17.03.2010р.

**УДК 004.056.53(045)**

**І.М. Сащук, канд.техн.наук, с.н.с.**
**С.І. Болобан, канд.техн.наук**
**Р.М. Жовноватюк, канд.техн.наук**

# ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

***У статті визначено основні властивості інформації та автоматизованої системи відносно впливу на які рекомендується розглядати загрози безпеки інформації; проаналізовано вплив потенційних навмисних і випадкових загроз безпеки інформації, що викликані діяльністю людини на визначені властивості інформації та автоматизованої системи (АС); сформовано загальний орієнтовний перелік потенційних навмисних і випадкових загроз безпеки інформації в АС з визначенням їх спрямованості щодо порушення розглянутих властивостей інформації та АС .***

***Ключові слова: автоматизовані системи, загрози безпеки інформації, технічний захист інформації.***

***In article the basic properties of the information and the automated system concerning what are defined it is recommended to consider threats of safety of the information; influence of potential deliberate and casual threats of safety of the information which are caused by activity of the person on the specified properties of the information and the automated system (AS) is analysed; the general rough list of potential deliberate and casual threats of safety of the information in the AS with definition of their orientation under the relation of the considered properties of the information and the AS is generated.***

***Keywords: automated systems, threats of safety of information, technical protection of information.***

**Постановка проблеми.** Важливою проблемою національної безпеки держави є забезпечення технічного захисту інформаційних ресурсів. Відомо [1 – 8], що для того, щоб якісно вирішувати питання захисту інформаційних ресурсів в автоматизованій системі (АС), необхідно застосовувати комплексну систему захисту інформації (КСЗІ). Визначено [9], що КСЗІ – це сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС. Один із важливих організаційних заходів КСЗІ це план захисту інформації в АС, що є сукупністю документів, згідно з якими здійснюється організація захисту інформації на всіх етапах життєвого циклу АС [10].

План захисту має декілька розділів, одним з яких є складання переліку загроз інформації в АС. Він є результатом комплексного обстеження АС. При цьому робота зі складання переліку загроз значно ускладнюється з причини відсутності загального (орієнтовного) переліку потенційних загроз безпеці інформації (ЗБІ). Який має бути максимально повним. Також для кожної із загроз необхідно визначити, на порушення яких властивостей інформації або АС вона спрямована.

**Аналіз останніх досліджень і публікацій.** Останнім часом питанню складання переліку потенційних загроз з визначенням їх спрямованості приділяється значна увага.

Так, у [8] пропонується складати перелік загроз відносно їх впливу на конфіденційність, доступність та цілісність інформації. Цей підхід не враховує вплив ЗБІ на властивості АС.

У [7] розроблено перелік ЗБІ щодо порушення конфіденційності, цілісності, доступності інформації та спостережності АС. Не вказано дію ЗБІ на цілісність та керованість АС.

**Виклад основного матеріалу.**У цей же час нормативними документами системи технічного захисту інформації [1, 3, 5, 6, 10] рекомендовано розглядати вплив ЗБІ на такі властивості інформації та АС [9]:

конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути

отримана неавторизованим користувачем і/або процесом;

цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом;

доступність інформації – властивість ресурсу системи (послуги, об'єкта, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний;

цілісність АС – властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки;

спостережність АС – властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії;

керованість АС – властивість системи, що дозволяє належним чином реагувати на команди керування і/або переходити з одного стану в інший без порушення політики безпеки.

Таким чином, для якісного складання переліку ЗБІ конкретної АС необхідно мати повний перелік потенційних ЗБІ з визначенням їх спрямованості щодо порушення рекомендованих до розгляду властивостей інформації та АС. Тому **мета статті**, що полягає в створенні загального переліку потенційних ЗБІ та визначенні характеру їх впливу на властивості інформації та АС (рис. 1), є актуальною.

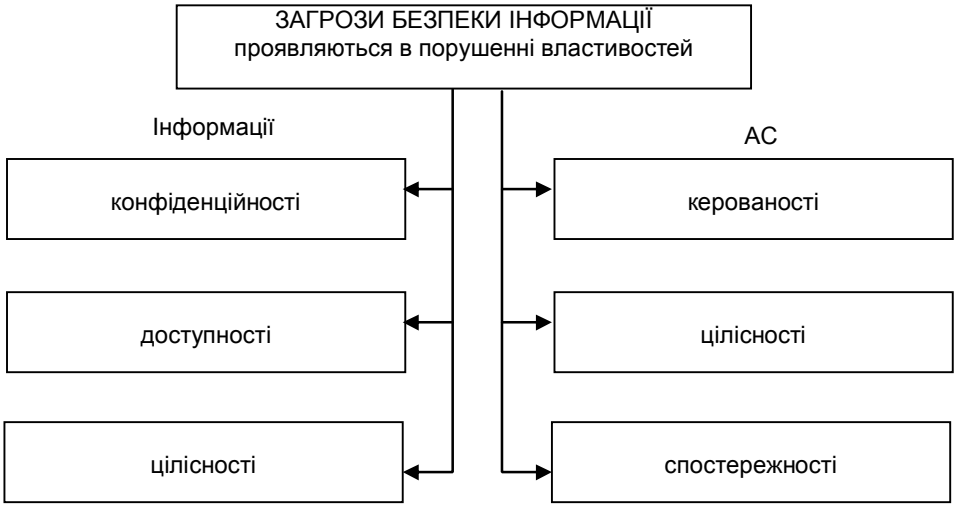


**Рис. 1. Щодо дій ЗБІ на властивості інформації та АС**

У таблиці 1 наведено перелік потенційних ненавмисних (випадкових) та навмисних (невипадкових) ЗБІ, що викликані діяльністю людини.

***Таблиця 1***

**Потенційні ЗБІ, що викликані діяльністю людини**

| № з/п | ЗБІ | Порушується | | | | | |
|---|---|---|---|---|---|---|---|
| | | конфіденційність інформації | доступність інформації | цілісність інформації | цілісність АС | спостережність АС | керованість АС |
| Ненавмисні загрози | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | Дія потужного магнітного поля на магнітні носії інформації або обладнання, що призводить до руйнування інформації | - | + | + | - | - | + |
| 2 | Неохайне зберігання та облік носіїв інформації | + | + | + | - | - | - |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 3 | Нечітка ідентифікація носіїв інформації | + | + | - | - | - | - |
| 4 | Програми користувачів, що працюють в мультипрограмному режимі і мають невиявлені помилки, які несуть загрозу для правильно функціонуючих програм | + | + | + | - | + | + |
| 5 | Помилки в програмах обробки, що можуть призвести до втрати або пошкодження інформації | - | + | + | - | - | - |
| 6 | Помилки при введенні даних | - | - | + | - | + | + |
| 7 | Помилки та збої в роботі апаратури, що викликані перепадами напруги живлення, несправністю енергопостачання, тимчасовими або постійними помилками в схемах живлення | - | + | + | + | + | + |
| 8 | Ненавмисні дії, що призводять до часткової або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів АС | - | + | + | + | + | + |
| 9 | Неправомірне вмикання (вимикання) обладнання або зміна режимів роботи пристроїв і програм (ненавмисне створення файлів, програм у тому числі системних і т. ін.) | - | + | + | - | + | + |
| 10 | Ненавмисне пошкодження носіїв інформації | - | + | + | + | + | + |
| 11 | Запуск технологічних програм, здатних при некоректному використанні призвести до втрати працездатності АС (зависання або зациклювання) або таких, що виконують незворотні зміни в АС | - | + | + | + | + | + |
| 12 | Нелегальне впровадження і використання необліковання програм, що не є необхідними для виконання службових обов'язків | + | + | + | + | + | + |
| 13 | Розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, перепусток тощо) | + | - | + | - | - | - |
| 14 | Проектування архітектури системи, технології обробки даних, розробка прикладних програм з можливостями, що становлять небезпеку для працездатності АС і безпеки інформації | + | + | + | + | + | + |
| 15 | Вхід в АС в обхід засобів захисту (завантаження сторонньої операційної системи із змінних носіїв інформації тощо) | + | - | + | - | + | + |
| 16 | Некоректне використання, настроювання або неправомірне вимикання засобів захисту персоналом служби безпеки | + | - | - | + | + | - |
| 17 | Необережні дії, що призводять до розголошення конфіденційної інформації | + | - | - | - | - | - |
| 18 | Пересилання даних за помилковою адресою абонента (пристрою) | + | - | - | - | - | - |
| 19 | Ненавмисне пошкодження каналів зв'язку | - | + | - | + | - | + |
| 20 | Зараження АС вірусами | + | + | + | + | + | + |
| 21 | Ігнорування організаційних обмежень (встановлених правил) в АС | + | + | + | + | + | + |
| | Навмисні загрози | | | | | | |
| 22 | Використання відомих способів доступу до АС з метою нав'язування заборонених дій, звернень до файлів, що мають цікаву порушникові інформацію | + | - | + | - | - | - |
| 23 | Маскування під справжнього користувача шляхом нав'язування характеристик авторизації такого користувача | + | - | + | - | - | - |
| 24 | Маскування під справжнього користувача після отримання характеристик доступу (авторизації) | + | - | + | - | - | - |
| 25 | Використання службового положення для незапланованої ревізії (перегляду) інформації | + | - | + | - | - | - |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 26 | Фізичне руйнування АС або виведення з ладу важливих її елементів | - | + | + | + | - | + |
| 27 | Відключення або виведення з ладу підсистем забезпечення безпеки інформаційної АС | + | + | + | + | + | - |
| 28 | Зміна режимів роботи пристроїв або програм АС | + | + | + | + | + | + |
| 29 | Підкуп або шантаж персоналу чи окремих користувачів, що мають певні повноваження | + | + | + | + | + | + |
| 30 | Викрадення носіїв інформації | + | + | - | + | - | - |
| 31 | Несанкціоноване копіювання інформації | + | - | - | - | - | - |
| 32 | Читання залишкової інформації із оперативної пам'яті із зовнішніх запам'ятовуючих пристроїв | + | - | - | - | - | - |
| 33 | Незаконне отримання паролів та інших реквізитів розмежування доступу з подальшим маскуванням під законного користувача | + | + | + | + | + | - |
| 34 | Злам шифрів криптографічного захисту інформації | + | - | + | - | - | - |
| 35 | Впровадження апаратних і програмних закладок і вірусів, що дозволяють подолати систему захисту, скрито і незаконно здійснити доступ до інформаційних ресурсів АС | + | + | + | - | - | - |
| 36 | Незаконне підключення до ліній зв'язку з метою використання пауз у діях законного користувача та введення від його імені хибних повідомлень або модифікації інформації | - | - | + | + | - | - |
| 37 | Незаконне підключення до ліній зв'язку з метою безпосередньої заміни законного користувача шляхом його фізичного відключення після входу до системи й успішної аутентифікації з подальшим введенням дезінформації і нав'язуванням хибних повідомлень | + | + | + | + | - | - |
| 38 | Перехоплення даних, що передаються по лініям зв'язку та їх аналіз з метою визначення протоколів обміну, правил входження в зв'язок і авторизації користувача з подальшими спробами їх імітування для проникнення в АС | + | - | + | - | - | - |
| 39 | Відключення або виведення з ладу підсистем забезпечення функціонування АС (електроживлення, охолодження, лінії зв'язку і т. ін.) | - | + | + | + | - | + |
| 40 | Дезорганізація функціонування АС (страйки, саботаж персоналу) | - | + | - | - | - | + |
| 41 | Постановка потужних активних перешкод | - | + | + | - | - | - |
| 42 | Впровадження агентів до числа персоналу системи (навіть в адміністративну групу, що відповідає за безпеку системи) | + | + | + | + | + | + |
| 43 | Використання "підслуховуючих" пристроїв, дистанційного фото- та відео- знімання і т. ін. | + | - | - | - | - | - |
| 44 | Перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв і ліній зв'язку, а також наведень активних випромінювань на допоміжні технічні засоби, які безпосередньо не беруть участь в обробці інформації (мережі живлення, мережі опалення тощо) | + | - | - | - | - | - |
| 45 | Викрадання виробничого сміття (роздрукованих матеріалів, записів, списаних або пошкоджених носіїв інформації) | + | - | - | - | - | - |
| 47 | Незаконне використання терміналів користувачів, що мають такі унікальні фізичні характеристики, як номер робочої станції в мережі, фізична адреса, адреса в системі зв'язку, апаратний блок кодування і т. ін. | + | + | + | - | - | - |

Загальний перелік потенційних ЗБІ сформовано шляхом аналізу результатів наукових досліджень у сфері інформаційної безпеки [2, 7, 8, 11] та з використанням ЗБІ, що вказані в нормативних документах системи технічного захисту інформації [1, 3, 10].

З аналізу даних таблиці 1 видно, що із загальної кількості потенційних ЗБІ спрямовано на порушення

конфіденційності інформації 70%, доступності інформації 60%, цілісності інформації Продовження таблиці – 72% , цілісності АС – 43%, спостережності АС – 38%, керованості АС – 43% ЗБІ. При цьому тільки на властивості інформації впливає приблизно 47% загроз, решта 53% здійснюють комплексний вплив як на властивості інформації, так і на властивості АС. З тих ЗБІ, що порушують тільки властивості інформації, біля 86% – впливають на конфіденційність, 27% – на доступність і 55% – на цілісність інформації (рис. 2).

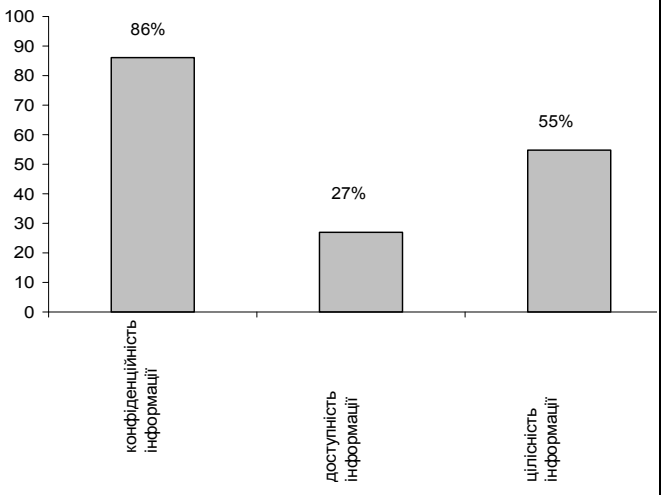


Рис. 2. Вплив ЗБІ на властивості інформації

Необхідно зазначити, що 78% модальних і 57% дуальних ЗБІ спрямовано на порушення конфіденційності інформації.

**Висновок.** Отже, більшість потенційних ЗБІ носить комплексний характер, що підтверджує необхідність створення саме КСЗІ. Значну увагу при побудові КСЗІ слід приділити захисту конфіденційності інформації. Запропонований перелік потенційних ЗБІ та проведений аналіз може бути використано як апріорна інформація при побудові КСЗІ конкретних АС.

1. Концепція технічного захисту інформації в Україні. Постанова Кабінету Міністрів України № 1126 від 8 жовтня 1997 р. 2. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін – К.: "МК-Прес", 2005. – 432 с., іл. 3. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. 4. Положення про технічний захист інформації в Україні. Указ Президента України № 1229 від 27 вересня 1999 р. 5. НД ТЗІ 3.6-001-200. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. 6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. 7. Методы и средства защиты информации. В 2-х томах / Ленков С. В., Перегудов Д. А., Хорошко В. А., Под ред. В. А. Хорошко. – К.: Арин, 2008. – 464 с. 8. Бабак В. П. Теоретичні основи захисту інформації: Підруч. / В. П. Бабак – К. : Книжкове вид-во НАУ, 2008. – 752 с. 9. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. 10. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

**Надійшла до редколегії 21.01.2010р.**