*Д.В. Дячков,*
*к.е.н., доцент,*
*Полтавська державна аграрна академія, м. Полтава*

# КОМПЛЕКСНА СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасні підприємства встановлюють більш високі вимоги до засобів забезпечення безпеки, що передбачає створення і підтримку функціонування єдиної системи контролю та забезпечення всіх видів безпеки підприємства. При цьому комплексна система безпеки повинна охоплювати всі можливі види методичного, технічного та організаційного забезпечення заходів щодо протидії загрозам порушення функціонування підприємства та витоку інформації.

Комплексне управління безпекою підприємства включає в себе організацію заходів, спрямованих не тільки на охорону інформації, а й на захист всіх бізнес-процесів підприємства. Тому, суть автоматизації комплексного управління безпекою повинна полягати в централізації, тобто створенні єдиної системи підтримки прийняття рішень.

Для цього потрібно вирішити два завдання:

по-перше, необхідно забезпечити централізоване накопичення та постійне оновлення актуальних знань про всі бізнес-процеси підприємства;

по-друге, потрібно організувати обробку цієї інформації в автоматичному або автоматизованому режимі і генерування можливих керуючих впливів [2].

Для вирішення першого завдання пропонується використовувати єдиний інформаційний простір підприємства. Організація єдиного інформаційного простору відповідно до сучасних тенденцій розвитку інформаційних технологій полягає в інтеграції всіх інформаційних ресурсів підприємства. При цьому відбувається впровадження автоматизованих систем з різною функціональністю, розробка нового програмного забезпечення і активне використання сучасних інформаційних технологій на підприємстві.

Другий,більш функціонально навантажений аспект сучасної автоматизації управління безпекою – це використання єдиного інформаційного простору в якості джерела актуальної інформації для системи підтримки прийняття рішень.

Знання про безпеку підприємства є невід'ємною частиною єдиного інформаційного простору. У зв'язку з цим, нові технології зберігання даних та їх аналітичної обробки затребувані і в підрозділах сучасних підприємств, що здійснюють управління безпекою. Однак, з урахуванням характеру інформації і пов'язаних з її обробкою процесів, частини єдиного інформаційного простору вимагають нового програмного забезпечення, яке має задовольняти особливі вимогами надійності зберігання та захисту інформації.

Автоматизація цього процесу полягає у веденні бази даних заходів і накопиченні статистики їх використання. ця база даних по суті є основним інструментом фахівця з безпеки, який використовується для обліку виконуваних робіт.

Організаційно необхідно забезпечити роботу служби безпеки з цією системою таким чином, щоб інформація про всі заходи і виставляються перешкодах зберігалася в базі даних.

Зробити це можна в такий спосіб: автоматизувати формування звітності за результатами роботи і забезпечити регулярний характер перевірки створюваної звітності. Непрямим перевагою в цьому випадку буде забезпечення більш жорсткого контролю діяльності служби безпеки з боку керівництва підприємства та інших контролюючих органів [3].

Враховуючи вищезазначене доцільно запропонувати компоненти моделі комплексної інформаційної безпеки (рис. 1).

Таким чином, надійний захист інформації забезпечується поєднанням організаційних заходів із застосуванням програмних, криптографічних і апаратних засобів захисту. Суттєвою є обставина, що жоден із названих засобів захисту окремо не є надійним і достатнім для забезпечення необхідного рівня інформаційної безпеки. На підставі вітчизняного та зарубіжного досвіду можна стверджувати, що тільки комплексне використання усіх зазначених засобів забезпечить надійний захист [1].

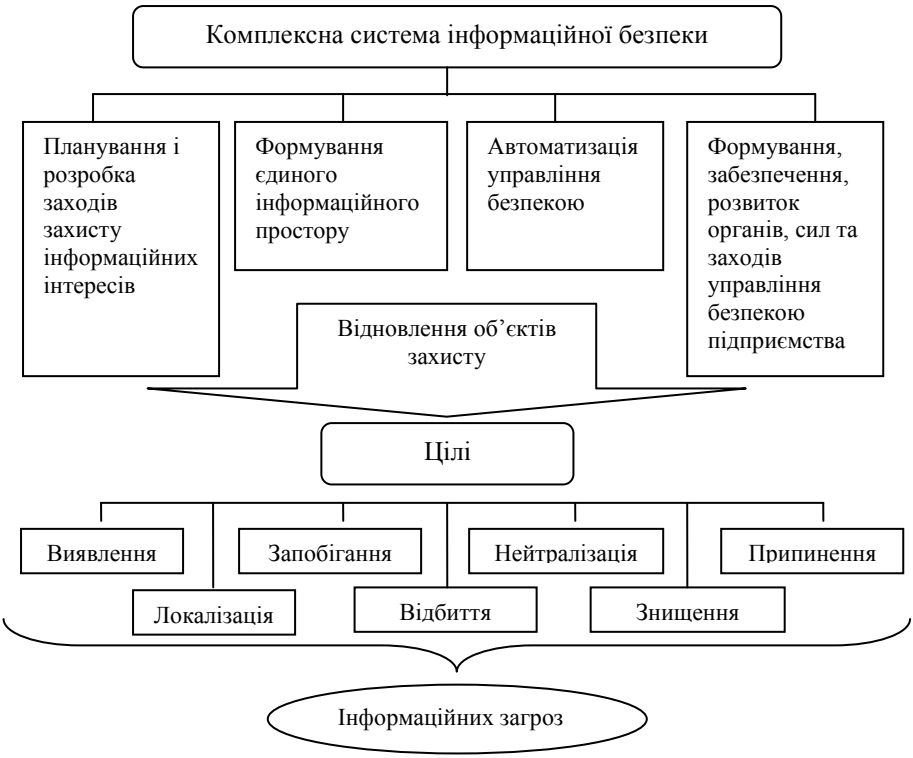


Рис. 1. Комплексна система інформаційної безпеки [розроблено на основі 2,3]

При цьому організаційні заходи виконують одночасно дві функції в системі захисту: є самостійним інструментом захисту, а також об'єднують всі засоби і методи в цілісний механізм захисту інформації.

**Список використаних джерел:**

1. Комплексные системы информационной безопасности. – [Електронный ресурс]. – Режим доступу : http://www.inform sviaz.co.ua/inform_tech/complexsecurity.html

2. Прохоров С. А. Автоматизация комплексного управления безопасностью предприятия / Прохоров С. А., Федосеев А. А., Иващенко А. В. – Самара: СНЦ РАН, 2008. – 55 с.

3. Ярочкин В. И. Информационная безопасность: [учеб. для студентов вузов] / В. И. Ярочкин. – М.: Академический Проект; Гаудеамус, 2-е изд. – 2004. – 544 с.