УДК 681.3.004

ДЕЯКІ ПИТАННЯ УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ СЛУЖБИ БЕЗПЕКИ (РЕЖИМНО-СЕКРЕТНОГО ОРГАНУ) УСТАНОВИ ТА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ЇЇ СПЕЦІАЛІСТІВ

Анатолій Грива
Військовий інститут Національного технічного університету України "КПІ"

Анотація: **В цій статті подані основні концептуальні положення комплексної системи безпеки організації (банку, підприємства), особливу увагу приділено вирішальній ролі людського фактору в системі збереження державної та комерційної таємниці. Запропоновано варіант штатної структури служби безпеки підприємства, подані пропозиції по підготовці спеціалістів для цих підрозділів.**
***Summary*: In this article the basics conceptual positions of an overall system of safety of organization (bank, enterprise) are conveyed, the especial attention is given main roles of the human factor in a system of conservation state and trade secret. The version of nominal frame of security of organization is offered, the proposals on preparation of the experts for these subdividings are conveyed.**
Ключові слова: **Комплексна система безпеки, служба безпеки, підготовка спеціалістів.**

I Вступ

Значення інформації на сучасному етапі розвитку людства безумовно важливе. Інформація сьогодні уже розглядається не тільки, як спосіб одержання різних відомостей, але й як продукт продажу. Тому проблема її збереження постала дуже гостро. А особливо це стосується інформації з обмеженим доступом, яка може бути віднесена до комерційної та державної таємниці.

Проблема захисту інформації та несанкціонованого доступу до неї прийняла антагоністичний характер в постановці, відомій із теорії гри. Стосовно проблеми захисту інформації це означає, що для її рішення необхідна не просто розробка окремих механізмів захисту, а організація цілого комплексу заходів по захисту в широкому розумінні цього питання, т.т. використання спеціальних засобів, механізмів і заходів з метою попередження втрати інформації.

Аналіз стану справ в області захисту інформації показує, що у розвинутих країнах склалася достатньо сформована концепція та інфраструктура захисту, основу якої складають:

- дуже розвинутий арсенал технічних засобів захисту, які створюються на промисловій основі;
- значна кількість фірм, які спеціалізуються на вирішенні питань захисту інформації;
- досить чітка система концептуальних поглядів на цю проблему;
- наявність значного практичного досвіду.

Але безумовно, як засвідчує зарубіжна преса, загрози для інформації не тільки не зменшуються, але й мають досить стійку тенденцію до зростання.

II Основні концептуальні положення комплексної системи безпеки інформації організації (банку, підприємства та інших установ)

Досвід показує, що для боротьби з цією тенденцією необхідна чітка та цілеспрямована організація процесу захисту. Для цього необхідно активно залучати професійних спеціалістів, керівництво організаціями, співробітників і користувачів. Ці факти визначають підвищену значимість організаційної суті питання.

Забезпечення безпеки інформації не може бути одноразовим актом. Це безперервний процес, який зводиться до обгрунтування та реалізації найбільш раціональних методів, способів і шляхів удосконалення та розвитку системи захисту, безперевному контролі, виявленні її слабких місць та можливих каналів витоку інформації.

Безпека інформації може бути забезпечена тільки при комплексному використанні усього арсеналу засобів захисту у всіх структурних елементах виробничої системи і на усіх етапах обробки інформації. Найбільший ефект досягається тоді, коли усі засоби, методи та заходи об"єднуються в єдиний комлекс - комплексну систему безпеки інформації організації (КСБІ). При цьому функціонування системи захисту повинно контролюватись, поновлюватись та доповнюватись в залежності від зміни зовнішніх і внутрішніх умов.

Ніяка КСБІ не може забезпечити необхідного рівня безпеки інформації без належної підготовки користувачів і виконання ними усіх встановлених правил, направлених на захист інформації.

КСБІ можна визначити як організовану сукупність спеціальних органів, засобів, методів і заходів, які забезпечують захист інформації на підприємстві.

З позиції системного підходу до захисту інформації установлюються такі вимоги: захист інформації повинен

- непреривним,
- плановим,
- централізованим,
- цілеспрямованим,
- конкретним,
- активним,
- надійним,
- універсальним,
- комплексним.

Основні вимоги до КСБІ:

- чіткість визначених повноважень і прав користувачів до доступу на певні види інформації;
- надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;
- зведення до мінімуму кількості загальних для декількох користувачів засобів захисту;
- облік випадків і спроб несанкціонованого доступу до конфіденційної інформації ;
- забезпечення оцінки ступеня конфіденціальності інформації;
- забезпечення контролю цілосності засобів захисту.

Надійність функціонування КСБІ також не можлива без постійного контролю за роботою її складових елементів.

Контроль КСБІ має за мету:

- своєчасно виявити та закрити потенційні канали витоку інформаці.;
- встановити відповідність змісту запланованих і проведених заходів по забезпеченню безпеки інформації (ЗБІ) системи вимогам розроблених інструкцій, пам"яток і інших документів;
- визначити правильність організації робіт по ЗБІ і ступінь їх виконання;
- визначити ступінь підготовки органів безпеки до виконання поставлених перед ними завдань, персоналу підприємства - з питань розробки, зберігання, обліку та роботи з документами, які вміщують конфіденційну інформацію і офісним обладнанням;
- узагальнити досвід організації та проведення заходів з питань ЗБІ для використання його в процесі удосконалення системи безпеки;
- перевірити організацію і результати роботи по удосконаленню системи санкціонованого доступу на підприємство, організацію допуска персоналу до конфіденційної інформації;
- перевірити участь керівників структурних підрозділів підприємства в організації та забезпеченні виконання заходів по ЗБІ.

КСБІ як і будь-яка інша система, повинна мати певні види забезпечення, спираючись на які вона буде спроможна виконати свою цільову функцію.

З врахуванням цього КСБІ повинна мати:

- правове забезпечення (нормативні документи);
- організаційне забезпечення (наявність спеціальних служб: захисту документів; служби режиму, допуску та охорони; служби захисту інформації з допомогою технічних засобів та ін.);
- апаратне забезпечення (технічні засоби захисту інформації);
- інформаційне забезпечення (інформація для забезпечення роботи служби безпеки);
- програмне забезпечення (програми захисту та оцінки наявності каналів витоку інформації);
- математичне забезпечення (математичні заходи розрахунку загроз від технічних засобів розвідки, зон та норм необхідного захисту);
- лінгвістичне забезпечення (спеціальні мовні засоби спілкування спеціалістів та користувачів в сфері захисту інформації);
- нормативно-методичне забезпечення (методики, які забезпечують діяльність користувачів в умовах жорстких вимог захисту інформації).

КСБІ може бути охарактеризована рядом показників, які визначають її організаційну і функціональну структуру. До таких характеристик можна віднести спрямованість захисту, спосіб попередження несанкціонованого доступу до інформації, масштабність системи, часові характеристики впливу по ступеню активності..

Найбільш важливою характеристикою КСБІ являється направленість захисту. Розглядаються також такі напрямки захисту як правовий, організаційний і інженерно-технічний захист. Останній реалізується фізичними, апаратними та програмними засобами та математичними методами захисту.

III Вирішальна роль людського фактору в системі збереження державної та комерційної таємниці

Незалежно від того, на скільки добре розроблена та впроваджена КСБІ, вона в решті-решт грунтується на людській діяльності, в якій можливі помилки або свідомі дії, направлені на знищення інформації, або передачу її зацікавленим організаціям.

Неможна, також, не відзначити, що сьогодні, як і завжди між державами світу йде постійна боротьба за сфери своїх інтересів. І метиди цієї боротьби різноманітні, починаючи від дипломатичної діяльності і закінчуючи збройними конфліктами.

Велику актуальність сьогодні мають методи "Психологічної війни".

Відомо що завданнями психологічної війни є вплив на особу, як носія інформації та як основну ланку в системах управління різноманітного призначення.

Таким чином, особа сьогодні може розглядатися як основний об"єкт атаки нетрадиційними методами ведення війни. Тому на сучасному етапі розвитку методів і засобів захисту інформації, одним із головних напрямків необхідно виділити процес виявлення і оперативної ліквідації загроз для інформації, які можуть виникати в процесі діяльності персоналу установ і організацій.

Ніяка технічна система безпеки не забезпечить надійний захист інформації, якщо хтось із персоналу установи буде свідомо здійснювати її несанкціоноване копіювання, або навмисне пошкодження.

Відомо багато методів впливу на особу з метою одержання від неї потрібної інформації, які завжди активно використовуються зацікавленими особами.

Методи впливу:

- підкуп;
- шантаж;
- погрози;
- одержання потрібної інформації при веденні звичайної розмови;
- обмін інформацією;
- переконання;
- використання психологічних методів;
- впровадження співробітником організації "своєї людини".

Усі ці факти свідчать, що для створення та надійного функціонування усіх елементів КСБІ, забезпечення кадрової безпеки організації (банку, підприємства) повинен бути створений спеціальний структурний підрозділ - **служба безпеки.**

IV Варіант організації штатної структури служби безпеки організації (банку, підприємства та інших установ)

Для організацій України, що проводять роботу з інформацією, яка становить державну таємницю, статус служб безпеки (режимно-секретних органів), їх підпорядкованість, основні обов"язки та права співробітників визначені Постановою КМУ № 609 від 4 серпня 1995 року.

Враховуючи досвід діючих служб безпеки (РСО) в установах України, а також зарубіжний і вітчизняний досвід по створенню і організації діяльності служб безпеки для недержавних установ, пропонується приблизний варіант її організаційно-штатної структури.

Служба безпеки організації повинна підпорядковуватись безпосередньо керівнику установи, а керівник служби повинет бути заступником керівника організації.

До складу служби безпеки можуть входити структурні підрозділи по збору інформації та контролю за її використанням, підрозділи технічного захисту інформації та підрозділи охорони.

Склад підрозділів служби безпеки:

1. Департамент інформації та планування:

1.1. Відділ планування та контролю:

Склад:

1.1.1. Група скритого спостереження;

1.1.2. Група проведення розслідувань;

1.1.3. Група по роботі з інформаторами;

1.1.4. Група по технічному забезпеченню проведення операцій.

Основні завдання департаменту інформації та планування:

- планування роботи по забезбеченню безпеки інформації на підприємстві;
- ведення скритого спостереження за організаціями та особами;
- проведення розслідувань фактів витоку інформації, або втрат документів;
- проведення навчання персоналу організації з питань безпеки інформації;
- проведення роботи з персоналом інших організацій-конкурентів з метою їх вербування, або переходу на роботу до своєї організації;
- проводить заходи по забезпеченню безпеки інформації при використанні персональних комп"ютерів, а також при їх роботі в мережі;
- технічне забезпечення проведення різних заходів безпеки.

1.2. Інформаційний центр:

Склад:

1.2.1. Група стратегічного планування;
1.2.2. Аналітична група;
1.2.3. Група по виявленню і збору відкритих і закритих публікацій (ведення діловодства);
1.2.4. Група експертів і консультантів.

Основні завдання інформаційного центру:

- проводить оцінку зовнішніх загроз для організації та розробляє комплекс заходів по їх попередженню;
- проводить збір та аналізує інформацію в середині організації;
- проводить збір літератури та нормативних документів;
- ведення діловодства;
- проводить оцінку матеріалів.

2. Департамент технічного захисту інформації:

Склад:

2.1. Група об"єктового захисту;
2.2. Група комп"ютерної безпеки;
2.3. Група безпеки зв"язку.

Основні завдання департаменту технічного захисту інформації:

- проводить встановлення та забезпечує функціонування технічних засобів охорони будівель та приміщень організації;
- проводить заходи по забезпеченню безпеки інформації при використанні персональних комп"ютерів, а також при їх роботі в мережі;
- проводить заходи по забезпеченню безпеки інформації при використанні засобів зв"язку (телефон, факс та ін.).

3. Департамент охорони:

Склад:

3.1. Група охорони об"єктів;
3.2. Група особистої охорони;
3.3. Група забезпечення безпеки масових заходів;
3.4. Група охорони перевезень.

Основні завдання департаменту охорони:

- проводить заходи по фізичній охороні та обороні будівлі та приміщень організації;
- забезпечує особисту охорону керівництво та персоналу організації;
- забезпечує охорону персоналу та майна організації при проведенні виставок, презентацій та інших масових заходів;
- забезпечує охорону перевезень майна та інших цінностей організації.

Із спеціальних питань РСО також необхідно підпорядкувати відділ кадрів установи по підбору та розстановці працівників.

Структура, чисельність і склад служби безпеки організації визначається реальними фінансовими можливостями, масштабами діяльності, ступенем конфіденційності інформації. В залежності від таких факторів склад служби безпеки може бути від двох - трьох чоловік, які працюють за сувмісництвом, до повномасштабної служби з розвинутою структурою.

В умовах, коли основним об"єктом злочинних дій став капітал банків і комерційних підприємств, на перший план в діяльності їх особистих служб безпеки виходить інформаційно-аналітичне забезпечення, економічна розвідка та контррозвідка, а також організація оперативних заходів.

V Сучасні вимоги до підготовки спеціалістів служби безпеки

Враховуючи сучасні вимоги до роботи співробітників служб безпеки (РСО) система підготовки, перепідготовки та підвищення їх кваліфікації повинна передбачати оволодіння знаннями додатково в областях:

1. Інформаційно - аналітичної роботи.
2. Методів розвідки та контррозвідки.
3. Оперативної роботи.
4. Соціальної психології та психології особистості.
5. Основ банківської справи та бугалтерського обліку.
6. Основ менеджмента та маркетинга.
7. Цивільного та кримінального права.

Спеціаліст служби безпеки організації сьогодні повинен вміти:

1. Розробляти комплексні заходи по забезпеченню безпеки державної та комерційної таємниці організації та особистої безпеки її керівництва.
2. Здійснювати захист інформації, в тому числі і тієї, що зберігається в комп"ютерній пам"яті.
3. Використовувати технічні засоби скритого спостереження та прослуховування.
4. Протидіяти проведенню аналогічних заходів організаціями-конкурентами.
5. Розбиратися у фінансовій звітності.
6. Проводити профілактику правопорушень в організації.
7. Проводити внутрішнє розслідування випадків викрадення матеріальних цінностей, саботажу та фінансових злочинів.
8. Організовувати перевірки (в тому числі таємно) благонадійності співробітників організації.
9. Виявляти (попереджувати) випадки співробітництва працівників організації з конкурентами або кримінальними структурами.
10. Взаємодіяти із слідчими органами та міліцією при розслідуванні злочинів і інших подій.
11. Готувати документи з аналізом фінансово-економічного положення партнерів, оцінювати конкурентів і потенційних клієнтів.
12. Вирішувати конфлікти між співробітниками організації.
13. Коротко та точно висловлювати свох думки.

Наведені вище вимоги потрібно враховувати при організації підготовки, перепідготовки та підвищення кваліфікації спеціалістів системи захисту інформації.

Література: 1. Положення про технічний захист інформації в Україні, затверджено Указом Президента України від 27 вересня 1999 року № 1229/99. 2. Положення про режимно-секретні органи на підприємствах, в установах і організаціях, затверджено постановою Кабінету Міністрів України від 4 серпня 1995 року № 609. 3. Э.Соловьев Коммерческая тайна и ее защита. 1996 г. 4. Ронин Р. Своя разведка: Способы вербовки агентуры, методы проникновения в психику, форсированное воздействие на личность, технические средства скрытого наблюдения и съема информации: Практическое пособие. OCR Палек, 1998 г.