Фтоян А.М.
студент,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВ

Інформаційна безпека кожного підприємства цілком індивідуальна. Її повнота та дієвість залежать від існуючої в державі законодавчої бази, від обсягу матеріально-технічних та фінансових ресурсів, виділених керівниками підприємств, від розуміння кожним з працівників важливості забезпечення інформаційної безпеки, а також від досвіду роботи керівників служб безпеки підприємств.

Надійний захист інформації на об'єктах інформаційної діяльності підприємств можливий лише при комплексному та системному підході. Тому організація технічного захисту інформації на об'єктах інформаційної діяльності підприємств передбачає такі етапи:

- 1 етап – визначення й аналіз загроз;
- 2 етап – розроблення системи захисту інформації;
- 3 етап – реалізація плану захисту інформації;
- 4 етап – контроль функціонування та керування системою захисту інформації [1].

На першому етапі здійснюється аналіз об'єктів ТЗІ, ситуаційного плану, умов функціонування Підприємства, також необхідно оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати дані для побудови окремої моделі загроз.

Джерелами загроз може бути діяльність конкурентних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб.

Опис загроз і схематичне подання шляхів їх здійснення складають окрему модель загроз.

На другому етапі розробляється план ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту інформації з обмеженим доступом (ІзОД), визначаються зони безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу об'єктів інформаційної діяльності.

Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів ТЗІ.

На третьому етапі слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

Технічний захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації (далі – засоби ТЗІ) та

контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів системи УкрСЕПРО або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем (далі – засоби забезпечення ТЗІ).

Засоби ТЗІ можуть функціонувати автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів.

Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, що володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами системи ТЗІ [2].

Надання послуг з ТЗІ, атестацію та сервісне обслуговування засобів забезпечення ТЗІ можуть здійснювати юридичні і фізичні особи, що мають ліцензію на право проведення цих робіт, видану уповноваженим Кабінетом Міністрів України органом.

Контроль за функціонуванням системи ТЗІ на об’єктах інформаційної діяльності Підприємства здійснюється з метою визначення й удосконалення стану ТЗІ в підрозділах Підприємства, щодо яких здійснюється ТЗІ, виявлення та запобігання порушенням з ТЗІ в інформаційних системах та об’єктах.

Контроль стану ТЗІ в підрозділах Підприємства організується відповідно до планів, затверджених керівниками зазначених органів, шляхом проведення перевірок.

Перевірки стану ТЗІ здійснюються безпосередньо комісіями, на які покладається забезпечення ТЗІ.

Організація проведення перевірок стану ТЗІ, заходи з ТЗІ, які підлягають контролю, висновки та рекомендації визначаються цим Положенням та іншими нормативно-правовими актами з питань ТЗІ.

Контрольно-інспекційна робота з питань ТЗІ включає планування та проведення перевірок стану ТЗІ в підрозділах Підприємства, щодо яких здійснюється ТЗІ, проведення аналізу та надання рекомендацій щодо вдосконалення заходів з ТЗІ.

Перевірки поділяються на комплексні, цільові (тематичні) та контрольні.

При комплексній перевірці вивчається та оцінюється стан ТЗІ в підрозділах Підприємства, щодо яких здійснюється ТЗІ.

При цільовій (тематичній) перевірці вивчаються окремі напрямки ТЗІ, перевіряється виконання рішень (розпоряджень, наказів, вказівок) органів державної влади з питань ТЗІ в підрозділах, щодо яких здійснюється ТЗІ, виконання завдань або провадження діяльності в галузі ТЗІ за відповідними дозволами та ліцензіями суб’єктами системи ТЗІ.

При контрольній перевірці перевіряється усунення недоліків, які були виявлені під час проведення попередньої комплексної або цільової перевірки.

Зазначені перевірки можуть бути планові та позапланові, з попередженням та раптові [3].

Позапланова перевірка здійснюється за вказівкою керівництва Підприємства в разі виникнення потреби визначення повноти та достатності

заходів з ТЗІ за наявності відомостей щодо порушень виконання вимог нормативно-правових актів з питань ТЗІ.

Перевірки здійснюються комісіями Підприємства на які покладено виконання завдань щодо здійснення контролю за функціонуванням системи ТЗІ.

При проведенні перевірки стану ТЗІ контролю підлягають організаційні, організаційно-технічні, технічні заходи з ТЗІ в виділених приміщеннях, інформаційних системах і об'єктах, повнота та достатність робіт з атестації виділених приміщень.

Необхідно провести аналіз функціонування системи захисту інформації, перевірку виконання заходів ТЗІ, контроль ефективності захисту, підготувати та видати дані для керування системою захисту інформації. Керування системою захисту інформації полягає у адаптації заходів ТЗІ до поточного завдання захисту інформації. За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший строк.

Список використаних джерел:

1. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення системи захисту інформації в автоматизованій системі, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.

2. Михайлюк В.А. Безпека інформаційної сфери – основа стійкого розвитку соціуму // Безпека життєдіяльності. – 2007. – № 6. – С. 15-16.

3. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальні кіберцивілізації) // Підприємництво, господарство і право. – 2004. – № 3. – С. 88-91.

Харицька О.М.

студент,

Навчально-науковий інститут інформаційної безпеки

Національної академії Служби безпеки України

ФЕЙКОВА ІНФОРМАЦІЯ ЯК ІНСТРУМЕНТ ДЕСТАБІЛІЗАЦІЇ СУСПІЛЬСТВА

Сучасний світ сильно ускладнюється завдяки технологізації та інформатизації практично всіх сфер життя суспільства. Не має сумніву, що названі процеси можуть як полегшувати працю та життєдіяльність людей, так і обтяжувати, оскільки збільшується інформаційне й технологічне (техногенне) навантаження на людину, особливо в технополісах і великих промислових регіонах, відволікаючи її від соціального та природного середовища, в якому вона живе й працює. Під впливом інформатизації змінюється спосіб і характер життя, обмежуються «живі» міжособистісні комунікації, натомість формується штучно створений віртуальний світ, який набуває здебільшого надуманих, нерідко мімікрійних (маскувальних, імітаційних) форм, за якими приховується, а подекуди й пригнічується «жива» та динамічна людська природа [3].