ЕМЕЦ К.Н., КРИВОДЕРЕВ В.В., ЖЕРНОКЛЬОВ К.В. РЕАЛИЗАЦИЯ КОМПЛЕКСНОГО ПОДХОДА К ОБУЧЕНИЮ СТРЕЛЬБЕ В СОВРЕМЕННЫХ ТРЕНАЖЕРНЫХ СИСТЕМАХ
Предлагается комплексный подход к формированию навыков стрельбы с помощью технических средств - проанализированы характеристики существующих тренажерных систем обучения стрельбе из пистолета; указано на принципиальные положительные отличия предложенного устройства от существующих тренажеров.

***

EMETS K.N., KRIVODEREV V.V., ZHERNOKLEV K.V. IMPLEMENTATION OF A COMPREHENSIVE APPROACH TO TRAINING TO FIRE IN MODERN TRAINING SYSTEMS
The comprehensive approach to formation of skills of fire with the help of means - is offered the characteristics of present training systems of training to fire from a pistol are parsed; is indicated on principled positive differences of the offered device from present simulators.

УДК 621.396:004.056

П.І. ОРЛОВ, *канд. юрид. наук, проф.,*
М.Ф. ЛОГВИНЕНКО, *канд. техн. наук,* ***С.Ф. ШИБАЛКІН, В.П. КОВАЛЬ***

Національний університет внутрішніх справ

ФОРМУВАННЯ КВАЛІФІКАЦІЙНИХ ВИМОГ ДО ФАХІВЦІВ З ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ ОБМЕЖЕНОГО ДОСТУПУ

Використовуючи сучасну нормативну базу з технічного захисту інформації, надано системний аналіз службових обов'язків організатора робіт із захисту інформації обмеженого доступу на підприємствах і установах різних форм власності; визначені основні кваліфікаційні вимоги до відповідних фахівців захисту інформації.

Вступ.

Згідно статті 6 Закону України "Про інформацію" [1], одним з основних напрямків державної інформаційної політики є створення загальної системи захисту інформації, тобто, даним законом визначена необхідність організації державної системи інформаційної безпеки (ІБ) за допомогою комплексної державної системи захисту інформації (СЗІ).

В умовах інформаційного суспільства та конкуренції проблема інформаційної безпеки як всієї держави, так і окремих відомств, корпорацій, фірм, інших юридичних і фізичних осіб з часом стає все актуальнішою.

Виходячи з того, що в більшості випадків вибір форм і методів захисту інформації (ЗІ) є наукомістким процесом, всі складові частини державної СЗІ також повинні базуватися на їх сучасний науково-технічний супровід. До таких складових слід віднести:

- вивчення і видачу експертних оцінок каналів витоку інформації;
- розробку законів та інших нормативно-правових документів з ІБ;
- підготовку і перепідготовку фахівців в області ІБ;
- створення спецзасобів і спеціалізованої контрольно-вимірювальної апаратури;
- розробку захищеної техніки загального і спеціального застосування;
- розробку та впровадження захищених телекомунікаційних систем;
- атестацію та сертифікацію систем та засобів в галузі технічного захисту інформації (ТЗІ).

Слід наголосити на тому, що проблема захисту інформації є перш за все комплексною, яка не вирішується одним чи декількома методами та засобами.

Є сенс звернути увагу на підготовку фахівців в області ІБ, а, особливо, на розробку таких загальнодержавних та відомчих кваліфікаційних стандартів їх підготовки та перепідготовки, які будуть гарантувати мінімально необхідну службову відповідність молодого фахівця без потреби у його подальшій адаптації на майбутньому місці роботи.

Це особливо важливо саме на даному етапі, коли існує дефіцит повноцінних фахівців в галузі ІБ, пов'язаний з тим, що реальний досвід їх підготовки в Україні є лише на протязі близько 40 років у Військовому інституті "КПІ" (колишньому Київському військовому інститут управління та зв'язку), Національному авіаційному університеті (більш ніж 7 років), Національному університеті внутрішніх справ (4 роки), та тільки в 2000 р. відбувся перший випуск інженерів з ІБ у Харківському національному університеті радіоелектроніки.

В більшості інших вищих навчальних закладів, в яких можлива підготовка фахівців з ІБ, а саме: Вінницькому державному технічному університеті; Національному гірничому університеті України (м. Дніпропетровськ); Запорізькому національному технічному університеті; Національному технічному університеті України "Київський політехнічний інститут"; Київському інституті зв'язку Одеської національної академії зв'язку ім. О.С. Попова; Національному університеті "Львівська політехніка"; Українському державному морському технічному університеті ім. адмірала Макарова (м. Миколаїв); Національному університеті внутрішніх справ (м. Харків, в т.ч. для Кримського факультету у м. Сімферополі); Чернівецькому національному університеті ім. Юрія Федьковича; Товаристві з обмеженою відповідальністю "Науково-технічний центр нових технологій "Дельта" (м. Київ); Асоціації "Київський Банківський союз"; Товаристві з обмеженою відповідальністю фірма "Успіх" (м. Київ); Товаристві з обмеженою відповідальністю "Бартек XXI" (м. Київ) [2], роботи або ще не розпочиналися, або не закінчені. Пов'язано це, в першу чергу, з необхідністю великих фінансових витрат для організації повноцінного навчального процесу.

Постановка задачі.

Слід наголосити, що автори в даній роботі не структурують проблеми захисту інформації в телекомунікаційних та комп'ютерних мережах, що вже зроблено сьогодні в багатьох вітчизняних і закордонних монографіях. Однак означений комплекс проблем ще не закінчився розробкою надійного державного переліку всіх спеціальностей та спеціалізацій з ІБ, який би був апробований практикою.

Метою даної статті є системний аналіз обов'язків організатора захисту інформації та визначення на його основі основних кваліфікаційних вимог до фахівців-організаторів робіт із захисту ІзОД (державна та комерційна таємниця, конфіденційна інформація) на підприємствах та установах різних форм власності (далі - підприємство), які проходять підготовку в НУВС за спеціальністю "Захист інформації з обмеженим доступом та автоматизація її обробки".

Системний аналіз обов'язків фахівця.

Більш чи менш реальні кваліфікаційні вимоги будь-якого фахівця з ІБ можуть бути визначені тільки з вивчення його службових обов'язків в конкретних умовах, для чого проаналізуємо, опираючись на сучасну нормативну базу, коло задач і обов'язків відповідального за організацію ЗІ на підприємстві.

Мета ЗІ може бути досягнута побудовою комплексної СЗІ, що є організованою сукупністю методів і засобів забезпечення ЗІ. Означені роботи повинні виконуватися силами підприємства під керівництвом організатора робіт з ЗІ при участі інших технічних спеціалістів з ІБ.

ЗІ здійснюється поетапно в наступній послідовності (див. рис.).

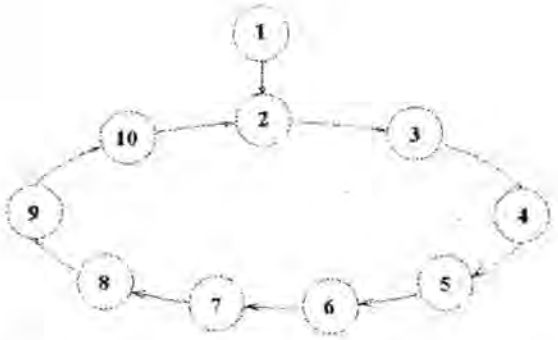

Рисунок - Етапи побудови системи захисту інформації підприємства

Перелічимо умови проведення, повний обсяг робіт і кінцеві результати по кожному з 10 етапів, використовуючи відповідні нормативні документи.

1. Одержання дозволу на проведення робіт із ЗІ для власних потреб (згідно [3]).

Для одержання дозволу на проведення робіт із ЗІ для власних потреб підприємство повинно мати:

1.1. Призначених наказом керівника підприємства спеціалістів для проведення обраних видів робіт, які мають вищу освіту відповідного професійного спрямування або пройшли перепідготовку та підвищення кваліфікації у галузі інформаційної безпеки чи мають стаж роботи відповідного професійного спрямування не менше 3 років, а також мають оформлені у встановленому порядку допуски до державної таємниці.

1.2. Нормативно-правові акти та нормативні документи з технічного захисту інформації, що необхідні для проведення обраного виду роботи.

1.3. Власні або орендовані, повірені в установленому порядку засоби вимірювань і контролю та (або) засоби електронно-обчислювальної техніки в обсязі, що забезпечує проведення обраного виду роботи.

1.4. Приміщення та (або) об'єкти електронно-обчислювальної техніки, атестовані на відповідність вимогам нормативних документів з питань технічного захисту інформації (за потреби).

1.5. Спеціальний дозвіл на провадження діяльності, пов'язаної з державною таємницею.

2. Категоріювання виділених приміщень на підприємстві (згідно [4]).

Етап починається створенням за наказом керівника підприємства комісії по категоріюванню приміщень, яка визначає:

2.1. Підставу для категоріювання приміщень (первинне, планове, у зв'язку зі змінами), в яких циркулює інформація з обмеженим доступом.

2.2. Вищий гриф таємності інформації, що циркулює в цих приміщеннях.

2.3. Обсяг інформації, що циркулює в цих приміщеннях з вищим грифом таємності (звичайний, значний).

2.4. Можливість застосування стаціонарних засобів розвідки поблизу об'єктів.

Комісія готує до наказу категорії виділених приміщень згідно з затвердженими комісією Актами категоріювання.

3. Визначення межі контрольованої території (згідно [5]-[6]).

Визначається відповідальною з ІБ особою згідно з планом-схемою розташування підприємства і затверджується наказом керівника підприємства.

4. Проведення обстеження виділених приміщень (згідно [5]-[14] та ін.).

Обстеження повинно бути проведено комісією, склад якої визначається відповідальною за ТЗІ особою і затверджується наказом керівника підприємства. У ході обстеження необхідно:

4.1. Провести аналіз умов функціонування підприємства, його розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз.

4.2. Дослідити засоби забезпечення інформаційної діяльності (ІД), які мають вихід за межі контрольованої території.

4.3. Вивчити схеми засобів і систем життєзабезпечення підприємства (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізації), а також інженерних комунікацій та металоконструкцій.

4.4. Дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання (далі - оброблення) інформації і провести необхідні вимірювання (спеціальні дослідження [7]-[14]).

4.5. Визначити наявність та технічний стан засобів забезпечення ТЗІ.

4.6. Перевірити наявність на підприємстві нормативних документів, які забезпечують функціонування системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує ІД.

4.7. Виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, контурів і проводів.

4.8. Визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю, і які підлягають демонтуванню.

4.9. Визначити технічні засоби, що потребують переобладнання (перемонтування) та встановлення засобів ТЗІ.

За результатами обстеження складається акт, який повинен бути затверджений керівником підприємства.

5. Розробка окремої моделі загроз (згідно [5]-[6]).

Матеріали обстеження виділених приміщень (див. п.3) використовуються під час розроблення окремої моделі загроз, яка повинна включати:

5.1. Генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території.

5.2. Схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до ІзОД.

5.3. Оцінку шкоди, яка передбачається від реалізації загроз.

6. Організація розроблення системи захисту інформації (згідно [5]-[14]).

На підставі матеріалів обстеження та окремої моделі загроз необхідно визначити головні задачі захисту інформації і скласти технічне завдання (ТЗ) на розроблення системи захисту інформації.

ТЗ повинно включати основні розділи:

6.1. Вимоги до системи захисту інформації.

6.2. Вимоги до складу проектної та експлуатаційної документації.

6.3. Етапи виконання робіт.

6.4. Порядок внесення змін і доповнень до розділів ТЗ.

6.5. Вимоги до порядку проведення випробування системи захисту.

Основою функціонування СЗІ є план ТЗІ, що повинен містити такі документи:

6.6. Перелік розпорядчих, організаційно-методичних, нормативних документів з ТЗІ, а також вказівки щодо їхнього застосування.

6.7. Інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту.

6.8. Інструкції, що встановлюють обов'язки, права та відповідальність персоналу.

6.9. Календарний план ТЗІ.

ТЗ і план ТЗІ розробляють спеціалісти з ТЗІ та узгоджують із зацікавленими підрозділами. Затверджує їх керівник підприємства.

7. Розроблення і реалізації заходів ТЗІ (згідно [5]-[14]).

7.1. Реалізація організаційних заходів захисту.

У процесі розроблення і реалізації організаційних заходів потрібно:

7.1.1. Визначити окремі задачі захисту ІзОД.

7.1.2. Обґрунтувати структуру і технологію функціонування системи захисту інформації.

7.1.3. Розробити і впровадити правила реалізації заходів ТЗІ.

7.1.4. Визначити і встановити права та обов'язки підрозділів та осіб, що беруть участь в обробленні ІзОД.

7.1.5. Придбати засоби забезпечення ТЗІ та нормативні документи і забезпечити ними підприємство.

7.1.6. Установити порядок упровадження захищених засобів обробки інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ.

7.1.7. Установити порядок контролю функціонування системи захисту інформації та її якісних характеристик.

7.1.8. Визначити зони безпеки інформації.

7.1.9. Установити порядок проведення атестації системи захисту інформації, її елементів і розробити програми атестаційного випробування.

7.1.10. Забезпечити керування системою захисту інформації.

7.2. Реалізація первинних технічних заходів захисту.

У процесі реалізації первинних технічних заходів потрібно забезпечити:

7.2.1. Блокування каналів витоку інформації.

7.2.2. Блокування несанкціонованого доступу до інформації чи її носіїв.

7.2.3. Перевірку справності та працездатності технічних засобів забезпечення ІД.

7.3. Реалізація основних технічних заходів захисту.

У процесі реалізації основних технічних заходів захисту потрібно:

7.3.1. Установити засоби виявлення та індикації загроз і перевірити їхню працездатність.

7.3.2. Установити захищені засоби оброблення інформації, засоби ТЗІ та перевірити їхню працездатність.

7.3.3. Застосувати програмні засоби захисту в засобах обчислювальної техніки, автоматизованих системах, здійснити їхнє функціональне тестування і тестування на відповідність вимогам захищеності.

7.3.4. Застосувати спеціальні інженерно-технічні споруди, засоби (системи).

8. Приймання робіт з ТЗІ (згідно [5]-[6]).

За результатами виконання рекомендацій акта обстеження та реалізації заходів захисту ІзОД слід скласти у довільній формі акт приймання робіт з ТЗІ, який повинен підписати виконавець робіт і особа, відповідальна за ТЗІ, та затвердити керівник підприємства.

9. Атестація засобів (систем) забезпечення ІД на відповідність вимогам нормативних документів з ТЗІ (згідно [5]-[14]).

Для визначення повноти та якості робіт з ТЗІ слід провести атестацію яка виконується організаціями, що мають ліцензії на право діяльності в галузі ТЗІ. У ході атестації потрібно:

9.1. Установити відповідність об'єкта, що атестується, вимогам ТЗІ.

9.2. Оцінити якість та надійність заходів захисту інформації.

9.3. Оцінити повноту та достатність технічної документації для об'єкта атестації.

9.4. Визначити необхідність внесення змін і доповнень до організаційно-розпорядчих документів тощо.

10. Контроль функціонування та керування системою захисту інформації (згідно [5]-[6]).

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. У разі потреби підвищення рівня захисту інформації необхідно виконати роботи, передбачені п.2-п.10 побудови системи захисту інформації.

Порядок проведення перевірок і контролю ефективності захисту інформації відповідальною за ТЗІ особою встановлюється нормативними документами.

Таким чином, з даної схеми робіт можна сформулювати наступні вимоги до фахівця організатора робіт з ЗІ. Незалежно від типу ІзОД організатор робіт з ЗІ повинен:

І. Знати:

1. Правові засади захисту інформації, структуру і основні положення інформаційного права України.
2. Порядок використання, обробки, передачі та збереження інформації обмеженого доступу відповідно чинних нормативно-правових норм в державі.
3. Основи психології.
4. Структуру нормативної бази з ІБ та основні її положення.
5. Основи системного аналізу складних систем.
6. Основи теорії захисту інформації.
7. Структуру сертифікації спеціальних інформаційних систем та окремих зразків спецтехніки.
8. Основи інформатики.
9. Основні поняття побудови комплексної СЗІ.
10. Основні методи та засоби фіксації порушень режиму доступу до ІзОД.
11. Фізичні принципи функціонування засобів зняття та захисту інформації.
12. Фізичні основи та принципи роботи сучасних контрольно-вимірювальних засобів.
13. Принципи побудови та функціонування телекомунікаційних систем та засобів обчислювальної техніки.
14. Принципи функціонування засобів оргтехніки.
15. Принципи побудови та роботи розподілених захищених інформаційних систем.
16. Порядок документообігу при використанні інформації обмеженого доступу.

ІІ. Вміти:

1. Використовувати нормативно-правові документи при виконанні своїх прямих обов'язків.
2. Проектувати та впроваджувати комплексні СЗІ.
3. Користуватись окремими зразками спецтехніки ТЗІ і проводити спеціальні дослідження.
4. Проводити вимірювання нормативних показників з ТЗІ.
5. Розробляти окремі моделі загроз інформації обмеженого доступу.
6. Проводити комплексне дослідження об'єктів захисту інформації.
7. Проводити структурний аналіз інформаційних потоків за їхньою цінністю, важливістю та ступенями вразливості.
8. Оцінювати шкоду від можливих втрат та спо-

творень інформації.

9. Оцінювати якість та ефективність різноманітних засобів захисту.

10. Організовувати контроль та управління СЗІ.

ІІІ. Бути ознайомленим з:

1. Вітчизняним та зарубіжним ринком засобів ЗІ.

2. Світовими тенденціями розвитку засобів та методів розвитку СЗІ.

3. Фундаментальними та прикладними дослідженнями, що існують в країні та світі в даній предметній області.

4. Переліком теоретично можливих каналів витоку інформації.

Висновки

Відповідно з означеними вище вимогами фахівець за спеціальністю "Захист інформації з обмеженим доступом та автоматизація її обробки" – це психологічно витриманий системний аналітик, якому притаманні: висока ерудиція з гуманітарних та фізико-технічних дисциплін, серйозна юридична підготовка, практичні навички роботи із спецтехнікою. Робота такого фахівця знаходиться на межі таких областей як: право, управління, інформатика та техніка.

Автори вважають, що важливими задачами розвитку освіти за напрямком "1601. Інформаційна безпека" є формування повного переліку всіх спеціальностей та розробка відповідних стандартів освіти, яка повинна починатись з системного аналізу обов'язків фахівця в конкретних умовах і визначення кваліфікаційних вимог до фахівця.

ЛІТЕРАТУРА

1. Закон України "Про інформацію" від 02.10.1992 р., № 2657-XII. –URL: www.rada.kiev.ua.

2. Перелік навчальних закладів, ліцензованих із захисту інформації (Інформація надана Управлінням ліцензування та акредитації Міністерства освіти і науки України) // Бизнес и безопасность. –2002. -№ 3. -С.3.

3. Наказ ДСТЗІ СБ України "Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб" від 23.02.2002, № 9.

4. Наказ ДСТСЗІ СБ України "Тимчасове положення по категоріюванню об'єктів (ТПКО-95)" від 10.07.1995 № 35.

5. ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення". –Введ. з. 1996 р.

6. ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робот". – Введ. з 1997 р.

7. НД ТЗІ 4.7-001-2001 "Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань".

8. НД ТЗІ 2.3-002-2001 "Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань".

9. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

10. ПЕМВН-95 9.06.95. "Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок" № 25 .

11. ТР-2015-2001 р. "Моделі технічних розвідок (ТР-215)".

12. № 86-2 12.06.90 ГТК СССР «Нормативно-методические документы по противодействию средствам фотографической и оптикоэлектронной разведок».

13. АЗП-81 «Руководящий материал. Акустическая защищенность помещений, выделенных для проведения секретных совещаний и переговоров. Нормы эффективности. Методики контроля. АЗП-81».

14. РД.107.46.-640.023-89 «Методика измерения эффективности экранирования сооружений, обеспечивающих защиту вычислительных центров и АСУ от ИТР в диапазоне частот 150 кГц-1000 МГц. Общие требования».

Надійшла до редколегії 03.12.2002

ОРЛОВ П.И., ЛОГВИНЕНКО Н.Ф., ШИБАЛКИН С.Ф., КОВАЛЬ В.П. ФОРМИРОВАНИЕ КВАЛИФИКАЦИОННЫХ ТРЕБОВАНИЙ К СПЕЦИАЛИСТАМ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Используя современную нормативную базу по технической защите информации, представлен системный анализ служебных обязанностей организатора работ по защите информации ограниченного доступа на предприятиях и учреждениях разных форм собственности; определены основные квалификационные требования к соответствующим специалистам защиты информации.

***

ORLOV P.I., LOGVINENKO N.F., SHIBALKIN S.F., KOVAL' V.P. FORMATION OF THE QUALIFYING REQUIREMENTS TO THE SPECIALISTS OF A SOFTWARE OF ORGANIZATION OF PROTECTION OF THE INFORMATION OF RESTRICTED ACCESS

Using modern normative base on engineering of protection of the information, the systems analysis of the official duties of the organizer of activities on protection of the information of restricted access on firms and entities of miscellaneous patterns of ownership is submitted; the main qualifying requirements to the applicable specialists of protection of the information are determined.