восприятия речи. Механизмы деятельности мозга / Под. ред. Н.П. Бехтеревой. — М. Наука. - 1988. – с. 504.

УДК 65.012.8, 651.928

ПОНЯТТЯ “ОХОРОНА” ТА “ЗАХИСТ” В ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ОБ’ЄКТІВ

Олексій Муратов
Інститут захисту інформації з обмеженим доступом Національної академії Служби безпеки України

Анотація: **Надаються дефініції поняттям “охорона” та “захист”, які дозволяють відмежовувати їх одне від одного під час розв’язання проблеми забезпечення безпеки інформаційних об’єктів.**
Summary: **The article deals with the definitions of the terms "guard" and "protection" which differ one another while resolving the problems of assuring the security of information objects.**
Ключові слова: **Захист, охорона, безпека інформційного об’єкта.**

І Вступ

Людина існує задовольняючи свої бажання. Процес задоволення бажань пов’язується з використанням властивостей об’єктів, що оточують людину. Якщо об’єкт є здатним задовольнити бажання людини неодноразово, то остання може прийняти рішення про збереження такого об’єкта або окремих його властивостей для використання у подальшому, тобто прийняти рішення про забезпечення безпеки об’єкта, його захист, охорону.

Незважаючи на величезний обсяг використання понять “захист” та “охорона”, сучасний тезаурус сфери інформаційної безпеці практично ототожнює всі ці поняття, дозволяє використовувати їх як синоніми.

У сфері технічного захисту інформації в стандартах України визначено термін “технічний захист інформації”; використовується, але не є визначеним термін “безпека інформації”; взагалі не використовується термін “охорона” [1]. Технічний захист інформації визначається як діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами.

Російські стандарти сфери інформаційної безпеки визначають інформаційну безпеку як захист конфіденційності, цілісності та доступності інформації [2]. Російські стандарти цієї сфери базуються на європейських і визначення, що наводяться в цих стандартах, часто є перекладом з англійської. Проте визначення терміна “інформаційна безпека” в європейських стандартах (information security: preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved [3]) основується на понятті “preservation”, яке може перекладатись як захист, як охорона, як збереження.

У чинному законодавстві України стосовно державної таємниці (секретної інформації) використовуються поняття як “охорони”, так і “захисту”. Наприклад, словосполучення “охорона державної таємниці” використовується в Законах України “Про державну таємницю”, “Про Службу безпеки України” (статті 2, 24, 25, 32), “Про контррозвідувальну діяльність” (ст. 6); “захист державної таємниці” – в Законах України “Про державну таємницю” (ст. 21), “Про розвідувальні органи України” (ст. 9); “технічний захист секретної інформації” – в Законах України “Про державну таємницю” (статті 1, 7, 8, 18, 35); “криптографічний захист секретної інформації” – в Законах України “Про державну таємницю” (статті 1, 7, 8, 18, 35); “охорона інформації, віднесеної до державної таємниці” – в Законі України “Про Національний архівний фонд та архівні установи” (ст. 16) [4 – 8].

У визначенні нормативних термінів, які містять поняття “охорона” та “захист”, останні часто сполучаються між собою. Наприклад, у ст. 1 Закону України “Про державну таємницю” термін “охорона державної таємниці” визначається як “комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв”, а норма ст. 18 того ж закону відносить технічний і криптографічний захист секретної інформації до основних організаційно-правових заходів охорони державної таємниці. Таким чином, технічний і криптографічний захист секретної інформації є складовими охорони державної таємниці.

Норми законодавчих актів, що регулюють відносини в інших сферах суспільного життя, також пов’язують між собою терміни “охорона” та “захист”. Наприклад:

охорона грунтів – система правових, організаційних, технологічних та інших заходів, спрямованих на збереження і відтворення родючості та цілісності грунтів, їх захист від деградації, ведення

сільськогосподарського виробництва з дотриманням ґрунтозахисних технологій та забезпеченням екологічної безпеки довкілля [9];

охорона державного кордону України є невід'ємною складовою загальнодержавної системи захисту державного кордону і полягає у здійсненні Державною прикордонною службою України на суші, морі, річках, озерах та інших водоймах, а також Збройними Силами України у повітряному та підводному просторі відповідно до наданих їм повноважень заходів з метою забезпечення недоторканості державного кордону України [10];

охорона культурної спадщини – система правових, організаційних, фінансових, матеріально-технічних, містобудівних, інформаційних та інших заходів з обліку (виявлення, наукове вивчення, класифікація, державна реєстрація), запобігання руйнуванню або заподіянню шкоди, забезпечення захисту, збереження, утримання, відповідного використання, консервації, реставрації, ремонту, реабілітації, пристосування та музеєфікації об'єктів культурної спадщини [11].

Характерно, що в законодавстві України в дефініціях різноманітних "захистів" поняття "охорона" майже не використовується. Разом із тим, зустрічаються нормативні терміни, при визначенні яких поняття "охорона" та "захист" використовуються одночасно. Наприклад:

благоустрій населених пунктів – комплекс робіт з інженерного захисту, розчищення, осушення та озеленення території,... що здійснюються на території населеного пункту з метою її... належного утримання та охорони, створення умов щодо захисту і відновлення сприятливого для життєдіяльності людини довкілля" [12];

внутрішній об'єктовий режим – установлений порядок перебування та пересування осіб і транспорту, а також забезпечення захисту пасажирів, членів екіпажу, повітряних суден, персоналу і об'єктів від актів незаконного втручання в межах контрольованої, стерильної зон та зон обмеженого доступу авіапідприємства (об'єкта аеропорту), що охороняються [13];

ведення лісового господарства полягає у здійсненні комплексу заходів з охорони, захисту, раціонального використання та розширеного відтворення лісів [14];

забезпечення охорони (захисту) державного кордону України [6].

II Постановка завдання

Наведені визначення чітко не відрізняють зміст понять "охорона" та "захист". Подібна тенденція спостерігається в сучасних тлумачних словниках української мови, де захист і охорона практично вважаються синонімами [15].

Таким чином, вже склалася практика традиційного використання понять "охорона" та "захист" у різних сферах діяльності щодо забезпечення безпеки, яка нині не має будь-яких суперечок чи проблем у такому використанні. Тлумаченню цих понять не приділяється будь-якої помітної уваги, хоча можна казати про те, що питання вже ставиться. Це питання виникає, по-перше, в галузях суспільної діяльності, де одночасно використовуються поняття "охорона" та "захист", наприклад, у сфері забезпечення охорони державної таємниці (охорона державної таємниці, технічний захист, криптографічний захист, контррозвідувальний захист тощо).

Питання тлумачення понять "захист" та "охорона" стосовно державної таємниці поставив Шлапаченко В. М. [16]. З метою виокремлення заходів захисту від заходів охорони він застосував критерій "ймовірність реалізації існуючої загрози і підготовка до її відвернення". Така ймовірність, на його думку, властива лише заходам охорони, а заходи захисту (на відміну від охорони) мають місце тоді, коли загрози зі стану ймовірного свого існування переходять до стану "реалізації в конкретних проявах".

Використовуючи такий підхід, можна казати про те, що захист є охороною в той час, коли немає атаки (реалізації загрози), або на етапі своєї розробки або підготовки (коли всі загрози мають ймовірний характер). У момент атаки охорона перетворюється на захист. Запропонований підхід дозволяє об'єднувати поняття "охорона" та "захист" при вирішенні загальних питань забезпечення безпеки об'єктів і передбачає об'єднання суб'єктів охорони та захисту. Однак помітна певна однобічність такого підходу, в рамках якого розглядаються лише форми або етапи функціонування захисту, а охорона перетворюється в одну з форм захисту або в охоронну функцію захисту. Під час розв'язання проблем не загального характеру, де необхідно розрізняти змістовне наповнення зазначених понять, використання такого підходу може призвести до однобічного уявлення про суть питання.

Різновидом зазначеного підходу можна вважати й такий, коли єдині засоби (сили, заходи) вважаються захисними в умовах агресивного (де здійснюється реалізація загроз) навколишнього середовища об'єкта чи охоронними в умовах відсутності агресивності з боку навколишнього середовища.

Мета статті – запропонувати дещо інший підхід, в якому й охорона й захист виявляються двома взаємопов’язаними елементами забезпечення безпеки об’єктів. Критеріями відрізнення заходів охорони від заходів захисту пропоную вважати об’єкт та мету безпосереднього впливу цих заходів. Хоча відразу слід зауважити, що як охорона, так і захист спрямовані на збереження безпеки певного об’єкта. Це можна вважати головною єдиною загальною метою впровадження охорони і захисту, яку треба відрізняти від таких, що будуть критерієм відмінності.

III Основна частина

Під безпекою певного об’єкта пропонується вважати такий стан цього об’єкта, коли йому нічого не загрожує (немає небезпеки). Будемо також вважати, що об’єкт, безпеку якого необхідно забезпечити, не створює небезпеку для інших.

Кажучи про небезпеку чи загрози будь-якому об’єкту, часто зіставляють їх з деякими властивостями цього об’єкта, небажаних змін яких бажають уникнути, тобто, зберегти ці властивості (наприклад, загроза цілісності).

Необхідність побудови системи забезпечення безпеки певного об’єкта з’являється з моменту першого виявлення деяких небажаних змін в такому об’єкті. Виявлення і вивчення причин таких небажаних змін приводить до формування переліку загроз, їх джерел, засобів та необхідних умов реалізації.

Будь-яка загроза (небезпека) завжди має свою причину та/або джерело, які часто називають дестабілізуючими факторами. Наприклад, порушенням фізичної цілісності (властивість об’єкта, що зберігається) може бути механічне пошкодження (загроза) внаслідок взаємодії об’єкта забезпечення безпеки в певних умовах з іншим об’єктом чи суб’єктом (джерело або засіб реалізації загрози). Тут засіб реалізації загрози – об’єкт, за допомогою (посередництвом) якого джерело загрози реалізує загрозу. При цьому така реалізація загрози здійснюється в певних умовах, які можуть бути сприятливими для успішної реалізації загрози (появи небажаних змін в об’єкті забезпечення безпеки), а можуть навпаки не сприяти цьому і навіть виключати її можливість (наприклад, твердість поверхні об’єкта забезпечення безпеки може бути міцніше за твердість засобу реалізації загрози). Обов’язковою умовою успішної реалізації будь-якої загрози є взаємодія з об’єктом забезпечення безпеки безпосередньо джерела загрози або опосередковано – за допомогою засобу реалізації загрози. Джерело загрози може здійснювати досягнення об’єкта забезпечення безпеки за допомогою низки декількох засобів реалізації загрози.

Таким чином, для успішної реалізації загрози необхідна наявність таких складових: джерело загрози (перше), засіб реалізації загрози (друге), їх взаємодія з об’єктом (третє) у сприятливих умовах (четверте). Виходячи з цього, для забезпечення безпеки об’єкта можна: 1) усунути (ліквідувати, нейтралізувати, локалізувати) джерело загрози; 2) позбавити джерело загрози засобів реалізації загрози; 3) виключити можливість взаємодії засобу реалізації загрози з об’єктом забезпечення безпеки або 4) створити несприятливі умови цієї взаємодії.

Необхідною умовою реалізації перших двох шляхів забезпечення безпеки об’єкта є своєчасне виявлення джерела чи засобу реалізації загрози. Для останніх двох шляхів таке виявлення може бути не обов’язковим.

Оскільки світ існує в просторово-часовому вимірі, то потрібно приділити першочергову увагу просторово-часовим характеристикам об’єктів та процесів, що розглядатимуться.

Кожне джерело загрози та засіб її реалізації (ДЗЗР) характеризуються максимальною (а іноді й мінімальною) відстанню до об’єкта забезпечення безпеки (ОЗБ), на якій стається можливим здійснення взаємодії з цим об’єктом в певних умовах – це дальність дії.

З початку взаємодії з ОЗБ в певних умовах кожному ДЗЗР необхідний деякий мінімальний час, щоб настав результат взаємодії, який можна вважати небажаним з точки зору забезпечення безпеки цього об’єкта – це час результативної атаки (час результативної реалізації загрози).

Крім того, кожне ДЗЗР може характеризуватися швидкістю переміщення в просторі, часом активності, часом життя і т. п.

Умови взаємодії ДЗЗР з ОЗБ визначаються наявністю та властивостями об’єктів навколо ДЗЗР та ОЗБ, які будь-яким чином впливають на процес такої взаємодії. Визначимо таку сукупність об’єктів як середовище взаємодії. Будемо також розрізняти: середовище ДЗЗР – об’єкти, що в певний час розташовані навколо ДЗЗР, і впливають на його характеристики (дальність дії, час реалізації загрози тощо); середовище ОЗБ – об’єкти, що в певний час розташовані навколо ОЗБ, і впливають на його характеристики з точки зору можливої взаємодії з ДЗЗР. Перетин середовища ДЗЗР та середовища ОЗБ складатиме вже зазначене середовище взаємодії.

Серед характеристик ОЗБ необхідно виокремити зону досяжності, що визначається дальністю дії ДЗЗР навколо цього ОЗБ.

Таким чином, для забезпечення безпеки об'єкта необхідно усунути із зони його досяжності всі ДЗЗР, тобто, виключити можливість взаємодії об'єкта забезпечення безпеки з об'єктами, що несуть загрози його безпеці.

Однак тут є проблема – зазначені ДЗЗР мають бути відомими та виявленими. Якщо ДЗЗР є невідомим чи невиявленим – існує небезпека. Але будь-який об'єкт виявляє себе як ДЗЗР з моменту початку реалізації загрози відносно ОЗБ. Тому, коли невідомий (чи невиявлений) ДЗЗР стане відомим (чи виявленим) внаслідок атаки ОЗБ, завдання забезпечення безпеки полягатиме в тому, щоб усунути цей ДЗЗР із зони досяжності ОЗБ за час, менший часу результативної атаки цього ДЗЗР.

Таким чином, для забезпечення безпеки об'єкта необхідно виключати можливість перебування в зоні досяжності ОЗБ всіх виявлених ДЗЗР та усувати з цієї зони всі виявлені ДЗЗР за час, менший часу результативної атаки таких ДЗЗР.

Виключення (усунення) із зони досяжності ОЗБ виявлених ДЗЗР може здійснюватись не тільки переміщенням ДЗЗР, але й переміщенням ОЗБ, а також змінами у середовищі ДЗЗР чи ОЗБ. Тобто, безпека об'єкта досягається шляхами:

1) впливом на ДЗЗР;

2) впливом на ОЗБ;

3) впливом на умови взаємодії ДЗЗР з ОЗБ:

а) впливом на середовище ДЗЗР;

б) впливом на середовище ОЗБ.

Шляхи 2,3 б називатимемо охороною, а шляхи 1 та 3, а – захистом.

Захист здійснює протидію небезпечному впливу ДЗЗР і огороджує ОЗБ від цього впливу, тобто стає шаром (бар'єром, посередником) між ОЗБ та ДЗЗР. Протидією ДЗЗР можна назвати вплив на середовище ДЗЗР, в результаті якого характеристики цього ДЗЗР погіршуються. Ступінь погіршення характеристик ДЗЗР визначає результативність, ефективність протидії.

Заходи та засоби захисту підмінюють ОЗБ у "відносинах" з ДЗЗР, безпосередньо взаємодіють з останніми. Захист засновується в першу чергу на вивченні ДЗЗР, їх ознак, умов виникнення, способів їх виявлення, ліквідації, нейтралізації, локалізації (або більш загально – протидії). ОЗБ тут займає другорядне місце (навіть може бути відсутнім).

Будь-який захист є прямим наслідком існування певного ДЗЗР (навіть уявного). Тому заходи захисту існують у безпосередньому зв'язку з ними. Впровадженню захисту передує своєчасне виявлення ДЗЗР. Захист є активним відносно останніх. При цьому окрема загроза безпеці об'єкта може створюватись декількома різними за природою джерелами і, тому, може стати причиною створення декількох видів захисту.

Таким чином, мета захисту – недопущення взаємодії ОЗБ з ДЗЗР шляхом здійснення безпосереднього впливу на ДЗЗР та їх середовище (це є об'єктами безпосереднього впливу захисту).

Основними характеристиками захисту можна вважати своєчасність та достатність (сили, міцності, часу) впливу (чи протидії) на ДЗЗР.

Інший підхід до забезпечення безпеки – охорона – на відміну від захисту забезпечує безпеку об'єктів шляхом безпосередньої взаємодії з ними. Тобто, ДЗЗР відступають на другий план і навіть взагалі можуть бути фактично відсутніми або уявними. Головний об'єкт впливу для охорони – ОЗБ та його середовище. Етимологічне походження слова "охорона" іноді пов'язується зі словами "приховування", "схоронення", "поховання", "прибирання". Тобто, охорона пов'язується з правилами розташування ОЗБ, вибором та/або створенням (природних чи штучних) сприятливих умов його існування та використання.

Як було зазначено вище необхідність побудови системи забезпечення безпеки певного об'єкта з'являється з моменту виявлення небажаних змін в такому об'єкті. Спостереження за об'єктом з метою виявлення в ньому непередбачених змін можна віднести до функцій охорони, адже захист в такому випадку ще відсутній, бо не визначено загроз – першопричини захисту. Таким чином, здійснення охорони є передумовою застосування захисту для забезпечення безпеки об'єктів. Саме під час здійснення охорони можна визначити реалізації загроз, які стають причиною створення та/або застосування захисту. Таким чином, захист виявляється наслідком, допоміжним елементом охорони. Відповідно до словника російської мови захисні дії передбачають охоронні ("защитить – охраняя, оградить от посягательств…") [17]. Охорона обумовлює наявність захисту, а іноді може його навіть не передбачати.

Охорона впливає на середовище ОЗБ, змінюючи його. Такі зміни можуть здійснюватись, виходячи з вимог-пропозицій з боку захисту щодо зручності організації можливої протидії ДЗЗР силами захисту у випадку, коли середовище ОЗБ стане середовищем взаємодії. Таким чином, захист, що є по суті породженням охорони, може здійснювати в свою чергу зворотній вплив на охорону через реалізацію охороною цих вимог-пропозицій захисту. Саме такі заходи, що за природою походження є заходами захисту,

але впроваджуються охороною ще до початку взаємодії захисту з ДЗЗР за підходом Шлапаченка В. М. називаються охороною, адже тут загрози мають ймовірний характер реалізації і здійснюється підготовка до відвернення загроз.

Дуже часто ОЗБ знаходиться поряд із іншими об’єктами або суб’єктами, для яких не може бути посередників у взаємодії з об’єктом забезпечення безпеки внаслідок необхідності їх бажаної безпосередньої взаємодії з цим об’єктом (далі – оточення). Оточення є частиною середовища ОЗБ, найбільш наближеною до нього. ОЗБ існує у нерозривній єдності зі своїм оточенням. Оточення завжди знаходиться в зоні досяжності ОЗБ. Вимоги до оточення формуються в першу чергу природою та метою існування ОЗБ, а в другу – забезпеченням відсутності в ньому ДЗЗР.

Так як захист не може бути посередником між ОЗБ і об’єктом (суб’єктом) оточення, то реалізація загрози із середовища оточення завжди є вразливою для об’єкта захисту. Своєчасне виявлення реалізації загроз стає одночасно й головним завданням й основною проблемою захисту в оточенні.

Виявляють засоби ДЗЗР за властивими їм ознаками. Для цього загрози, їх джерела та засоби їх реалізації вивчаються і формується база знань їх ознак. Наявність таких ознак у об’єктів (суб’єктів) оточення вважається неприпустимим, тому кожний об’єкт з оточення об’єкта захисту (ОЗБ) необхідно постійно контролювати на предмет наявності таких ознак. Об’єктів (суб’єктів), які скомпрометували себе наявністю таких ознак, захист повинен своєчасно “відгородити” від об’єкта захисту (ОЗБ) до моменту реалізації загрози, не завдавши шкоди іншим об’єктам (суб’єктам) оточення. Таким чином, до основних характеристик захисту можна додати ще одну – індивідуальний підхід до кожного об’єкта в оточенні.

Тут можна виокремити проблему достатності переліку ідентифікуючих ознак загроз в оточенні, які б достовірно свідчили про те, що об’єкт середовища дійсно являє собою небезпеку (джерело загроз) ще до моменту безпосередньої реалізації загрози. Недосконале розв’язання цієї проблеми дозволяє або успішно реалізовувати загрози відносно об’єкта забезпечення безпеки (занадто ускладнений або взагалі відсутній перелік ознак, коли захист не встигає встановити наявність загрози до моменту її реалізації), або “знищувати” (змінювати) оточення заходами захисту (занадто спрощений перелік ознак, коли захист розпізнає загрозу в об’єкті, який такою не є). Встановлення достатньої кількості таких ознак стосовно окремого об’єкта з оточення потребує від захисту значних витрат сил та часу. Організація одночасного постійного контролю кожного об’єкта оточення вимагатиме залучення на захист величезної кількості ресурсів.

Вказана проблема не єдина. Можна казати про такі тенденції, властиві забезпеченню безпеки об’єктів:

– обсяги ресурсів захисту власники (розпорядники) об’єктів захисту завжди прагнуть зменшити, а обсяг оточення (користувачів) – збільшити або залишити незмінним;

– загальний обсяг ознак загроз, який необхідно мати захисту для їх виявлення, має тенденцію до збільшення через збільшення загальної кількості загроз, способів їх реалізації та/або їх приховування.

Ці властивості породжують проблему достатності ресурсів щодо забезпечення захисту: потрібні ресурси мають властивість збільшуватись (через збільшення кількості оточення та загроз), в той час, коли ресурси, що виділяються мають властивість залишатись незмінними.

Ще одна проблема – захист виявляється непридатним до протидії принципово новим загрозам та/або способам їх приховування, реалізації, особливо із середовища оточення об’єкта захисту, де час реалізації загрози зменшується (проблема відставання захисту). Звичайно, ця проблема як і перша не залишається без уваги. З метою подолання зазначеного відставання захист змушений здійснювати аналітичну та/або розвідувальну роботу для прогнозування появи загроз (принципово нових або відомих, але у новій точці просторово-часового виміру) або поповнення бази знань ознак загроз. Це знаходить своє відображення, наприклад, в розвитку концепції так званих “активних систем захисту” [18].

Наявність вказаних проблем робить захист неефективним (таким, що потребує залучення величезних ресурсів) в оточенні об’єкта забезпечення безпеки.

Охорона на відміну від захисту “зосереджується”, як вже вказувалось, не стільки на загрозах та їх ознаках, скільки на характеристиках об’єктів середовища ОЗБ, на змісті їх необхідних і достатніх властивостей та порядку їх застосування відносно ОЗБ. Охорона активна скоріше до середовища ОЗБ ніж до загроз. Вона орієнтована на бажані позитивні необхідно-притаманні ознаки об’єктів цього середовища. Охорона вивчає і контролює ознаки об’єктів середовища ОЗБ та їх поведінку, але не стільки для виявлення ознак загроз з наступним вилученням об’єктів з оточення, скільки для виявлення, формування і контролю необхідних характеристик об’єктів (суб’єктів) з наступним залишенням їх в оточенні. Відсутність необхідних бажаних ознак у певного об’єкта сприймається як неприпустиме для оточення і цей об’єкт вважається зайвим (таким, що підлягає усуненню з середовища ОЗБ). Охорона під час створення середовища ОЗБ формує деяке тло, яке сприятиме виявленню та усуненню ДЗЗР із зони досяжності ОЗБ.

Такий підхід не потребує постійного залучення спеціальних ресурсів у великій кількості для організації протидії всім об'єктам з оточення; дозволяє швидко визначити ступінь придатності (корисності) окремого об'єкта оточення, виключити можливість раптової появи ДЗЗР, використовуючи само оточення.

Заходи охорони пов'язуються з правилами поводження з об'єктом охорони (чи на об'єкті охорони) і, часто, мають правову форму реалізації в суспільних відносинах у вигляді встановлення певних режимів (наприклад, охорона державної таємниці – режим секретності, внутрішньооб'єктовий режим). Ознакою будь-якого режиму (порядку), якій встановлюється з метою забезпечення охорони, є обмеження загальноприйнятих у суспільстві свобод для суб'єктів у зв'язку з провадженням ними діяльності, пов'язаної з об'єктом, безпеку якого необхідно забезпечити. Останнім часом в тезаурусі забезпечення інформаційної безпеки спостерігається використання поряд зі словом "режим" словосполучення "політика безпеки". Режим (чи охорона, чи політика безпеки) передбачає встановлення порядку (правил) формування середовища ОЗБ, поводження у середовищі ОЗБ, взаємодії оточення з ОЗБ. Формування цього порядку може вимагати спеціальних знань, властивих захисту. Однак виконання і контроль виконання такого порядку вже не потребує таких спеціальних додаткових знань. Для цього достатньо знань, притаманних суб'єктам середовища, яких вони набувають в процесі взаємодії з об'єктом охорони (щодо суб'єктів оточення) або між собою у повсякденному житті.

Що стосується заходів захисту, то правом регулюються та охороняються в основному межі, підстави та порядок застосування засобів захисту.

Застосування засобів (сил) правової охорони спрямовано на підтримання правомірної поведінки суб'єктів щодо об'єкта охорони і мають попереджувально-профілактичний характер. В той час, коли засоби захисту мають, головним чином, примусовий припиняючий характер свого застосування відносно ДЗЗР.

Слід зазначити, що сам факт наявності і дієвості засобів захисту, спроможних заподіяти шкоду ДЗЗР, має охоронне значення, бо передбачає можливу ретроспективну відповідальність суб'єкта за дії, що можуть бути розпізнані як реалізація загроз безпеці об'єкта, і схиляє суб'єкта до відмови від своїх негативних вчинків відносно об'єкта захисту.

Охорона "занадто делікатна" у поводженні з об'єктами, що реалізують загрози, тому без захисту може бути подоланою "грубою силою", в той час коли заходи захисту без врахування вимог охорони можуть бути "занадто ефективними" відносно вигаданих джерел загроз в оточенні.

Охорона формує і постійно контролює об'єкти в зоні досяжності ОЗБ на предмет необхідних позитивних ознак-властивостей та/або відповідності їх оцінок встановленим нормам. Відсутність або невідповідність нормам ознак-властивостей сприймається як небезпека (підвищення рівня ймовірності реалізації загрози). Після цього для запобігання реалізації загрози об'єкт, який скомпрометував себе, вважається ДЗЗР і взаємодія з ним починає будуватись за посередництвом захисту, який впливом на ДЗЗР та його середовище нейтралізує, локалізує або у крайньому випадку його ліквідує.

Процес компрометації об'єктів має тривалий у часі характер, на початку якого маємо "звичайний" об'єкт із середовища ОЗБ, а наприкінці – ДЗЗР. Якщо певний об'єкт починає набувати ознак ДЗЗР, але ще не набув їх у достатній кількості (а може й не набуде взагалі), до нього може бути застосовано захист, але не повною мірою. У зв'язку з цим така властивість захисту як достатність може бути доповненою адекватністю, яка відображає поступовість нарощування захистом інтенсивності протидії відповідно до поступового набуття об'єктом ознак ДЗЗР.

Заходи охорони сприяють виявленню ДЗЗР шляхом створення таких умов в середовищі ОЗБ, в якому немає умов існування ДЗЗР настільки довгого, щоб загроза реалізувалась відносно об'єкта забезпечення безпеки. При цьому один захід охорони може бути спрямованим на виявлення і попередження декількох навіть неоднотипових загроз.

Таким чином, охорона характеризується загальністю та безперервністю застосування до середовища ОЗБ.

IV Висновки

Виходячи з попередніх міркувань, можна навести визначення понять "захист" та "охорона" в рамках забезпечення безпеки деякого об'єкта:

захист об'єкта – заходи, сили та засоби, спрямовані на безпосередню протидію засобам реалізації та джерелам загроз безпеці об'єкта захисту;

охорона об'єкта – заходи, сили та засоби, спрямовані на формування та підтримання необхідних бажаних властивостей середовища об'єкта охорони та/або самого об'єкта охорони шляхом впливу на кожний елемент з цього середовища та/або на сам об'єкт охорони.

Використовуючи запропонований підхід щодо розрізнення захисту і охорони, можна проаналізувати заходи ідентифікації, автентифікації, авторизації, аудиту, які нині широко застосовуються в технічному захисті інформації, та зробити висновок, що вони мають скоріше охоронний, ніж захисний характер.

В законодавстві більшості країн колишнього СРСР (Російська Федерація, Республіка Білорусь, Республіка Казахстан, Туркменістан, Киргизька Республіка) нормативна термінологія інституту державної таємниці в питанні забезпечення безпеки спирається на захист державної таємниці. Правовий інститут державної таємниці в законодавстві України має самобутні риси і в термінологічному плані спирається не на захист, а на охорону державної таємниці. Тим самим, на мій погляд, підкреслюється головна ідея правового інституту державної таємниці в Україні – забезпечення реалізації прав окремих осіб стосовно інформаційних об'єктів, що становлять державну таємницю. Коли в законодавчій термінології акцент робиться на захист, то це, на мій погляд, свідчить перш за все про намагання законодавця ввести в правове поле виконавчий механізм протидії деяким загрозам об'єкту правової охорони і тим самим побічно підкреслити значимість цих загроз у житті суспільства або щодо його безпеки.

Запропоноване тлумачення понять "захист" і "охорона", визначення однойменних термінів в сфері забезпечення безпеки інформаційного об'єкта дозволить розрізняти їх зміст і може бути використано під час розробки науково-теоретичного підґрунтя правового регулювання в сфері забезпечення безпеки об'єктів, а також для подальшого вдосконалення тлумачення понять "охорона" та "захист" у різноманітних сферах суспільних відносин.

Література: ***1.*** *ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.* ***2.*** *ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью. – М.: Стандартинформ, 2006. – 56 с.* ***3.*** *ISO/IEC 17799:2005 Information technology – Security technologies – Code of practice for information security management. – ISO/IEC, 2005. – 115 p.* ***4.*** *Закон України "Про державну таємницю" // Відомості Верховної Ради України, 1994, № 16. – ст. 93.* ***5.*** *Закон України "Про Службу безпеки України" // Відомості Верховної Ради України, 1992, № 27. – ст. 382.* ***6.*** *Закон України "Про контррозвідувальну діяльність" // Відомості Верховної Ради України, 2003, № 12. – ст. 89.* ***7.*** *Закон України "Про розвідувальні органи України" // Відомості Верховної Ради України, 2001, № 19. – ст. 94.* ***8.*** *Закон України "Про Національний архівний фонд та архівні установи" // Відомості Верховної Ради України, 1994, № 15. – ст. 96.* ***9.*** *Закон України "Про охорону земель" // Відомості Верховної Ради України, 2003, № 39. – ст. 349.* ***10.*** *Закон України "Про державний кордон України" // Відомості Верховної Ради України, 1992, № 2. – ст. 5.* ***11.*** *Закон України "Про охорону культурної спадщини" // Відомості Верховної Ради України, 2000, № 39. – ст. 333.* ***12.*** *Закон України "Про благоустрій населених пунктів" // Відомості Верховної Ради України, 2005, № 49. – ст. 517.* ***13.*** *Правила організації охорони повітряних суден та об'єктів на авіапідприємствах цивільної авіації України. – Затверджено наказом Державної служби України з нагляду за забезпеченням безпеки авіації від 30.03.2005 № 230.* ***14.*** *Лісовий кодекс України // Відомості Верховної Ради України, 1994, № 17. – ст. 99.* ***15.*** *Тлумачний словник української мови: Понад 12500 статей (близько 40000 слів) / За ред. д-ра філологічних наук проф. В. С. Калашника. – 2-ге вид., випр. і доп. – Х.: Прапор, 2004. – 992 с.* ***16.*** *Шлапаченко В. М. Контррозвідувальна діяльність органів Служби безпеки України – основна складова системи збереження державної таємниці // Збірник наукових праць Національної академії Служби безпеки України, 2003, № 8. – С. 82-85.* ***17.*** *Ожегов С. И. Словарь русского языка. – М.: Государственное издательство иностранных и национальных словарей, 1961. – 900 с.* ***18.*** *Архипов О. Є., Бородавко І. Т., Ворожко В. П. Оцінювання ефективності системи охорони державної таємниці: Монографія. – К.: Наук.-вид. відділ Національної академії Служби безпеки України, 2007. – 63 с.*

УДК 681.5;321;322:621.391;395

ПЕРКОЛЯЦІЙНІ МОДЕЛІ ПРОТИДІЇ ФУНКЦІОНУВАННЮ НЕСАНКЦІОНОВАНОЇ НАНОСЕНСОРНОЇ МЕРЕЖІ

Ірина Кононович

Інститут комп'ютерних технологій Одеської державної академії холоду

Анотація: **Формулюється й аналізується задача організації протидії функціонуванню несанкціонованої розподіленої мережі наносенсорів із самоорганізацією. Розробляється математична модель системи протидії із залученням методів теорії перколяції. Інтерпретуються результати комп'ютерного моделювання.**

Summary: **The task of organization of counteraction to functioning of the unauthorized distributed network of nanosensors with self organization is formulated and is analyzed. The mathematical model of the system of counteraction with bringing in of methods of theory of percolation is developed. The results of computer design are interpreted.**