УДК 621.396.662.072.078

Сайко В.Г., Сергієнко А. Ф.
Грабовецький Є О., Миронюк О.О.

ОРГАНІЗАЦІЯ СИСТЕМИ ОХОРОНИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ: ЗАХОДИ ТА ЗАСОБИ РЕАЛІЗАЦІЇ

Проведено узагальнення та аналіз заходів та засобів організації системи охорони об'єктів інформаційної діяльності. Здійснено систематизацію положень фізичного та інженерно-технічного захисту цих об'єктів і наявних інформаційних ресурсів.

Ключові слова: система охорони об'єкта, захист, інформація, доступ.

Організація охорони це складова частина загальної системи захисту конфіденційної інформації підприємства. Питання забезпечення надійної охорони території підприємства і його об'єктів нерозривно пов'язані із завданнями організації пропускного режиму на підприємстві. Головні цілі охорони підприємства наступні: запобігання спробам проникнення сторонніх осіб (зловмисників) на територію (об'єкти) підприємства; своєчасне виявлення і затримання осіб, протиправно проникних (намагалися проникнути) на територію яка охороняється; забезпечення збереження що знаходяться на території, що охороняється носіїв конфіденційної інформації та матеріальних засобів і виключення, таким чином, нанесення збитку підприємству; попередження пригод на об'єкті, що охороняється і ліквідація їх наслідків.

Для реалізації головних цілей і основних завдань охорони підприємства (його об'єктів) створюється система охорони. Система охорони підприємства - сукупність використовуваних для охорони підприємства сил і засобів, а також способів і методів охорони підприємства та його об'єктів. Вона включає особовий склад підрозділів охорони (караулів); технічні засоби охорони; місця розміщення особового складу, який виконує завдання охорони, і використовуваних технічних засобів; методи охорони об'єктів. В якості місць розміщення особового складу охорони може бути використаний один з основних елементів системи організації пропускного режиму - контрольно-пропускні пункти.

Для охорони підприємств та їх об'єктів створюються штатні підрозділи охорони, які організаційно можуть бути об'єднані в службу охорони. Служба охорони включає пости охорони, групи (підрозділу) працівників охорони (у тому числі підрозділ особистої охорони керівництва та персоналу), групу охорони і супроводу матеріальних цінностей і вантажів, «тривожну» групу (групу швидкого реагування), а також підрозділи сторожових собак (при необхідності). Але найбільш часто підрозділи охорони поряд з іншими підрозділами, вирішуючи завдання з різних напрямків захисту інформації, об'єднуються в службу безпеки підприємства.

У своїй діяльності по виконанню завдань охорони підприємства співробітники підрозділу охорони керуються посадовими обов'язками (інструкціями), які розробляються спільно зі службою безпеки підприємства, а в деяких випадках - у взаємодії з іншими зацікавленими посадовими особами, і затверджуються керівником підприємства (його заступником).

Охорона підприємства може забезпечуватися не тільки шляхом створення перерахованих підрозділів охорони, але і шляхом використання послуг приватних охоронних підприємств, що мають право відповідно до законодавства здійснювати цей вид діяльності. Порядок надання послуг такими підприємствами, права та обов'язки їх співробітників при виконанні завдань охорони об'єктів визначені Законом України «Про охоронну діяльність» (№ 4616-VI від 22 березня 2012 р.). Для організації охорони підприємства можуть бути також використані сили і засоби підрозділів Державної Служби Охорони при МВС України.

У цьому випадку застосовуються такі основні засоби охорони об'єктів підприємства: використання технічних засобів охорони (сигналізації), кінцеві пристрої яких виведені на пульти централізованого спостереження ДСО; несення чергування співробітниками ДСО

безпосередньо на об'єкті охорони. Функції, що покладаються на підрозділи ДСО, і порядок їх діяльності визначаються Положенням про Державну службу охорони при МВС України (№ 615 від 10 серпня 1993 р.).

Головна вимога, до системи охорони, - її надійність. Надійність охорони підприємства та його об'єктів досягається ефективним застосуванням сил та засобів охорони, правильною організацією і пильним несенням служби працівниками охорони (особовим складом варт) на постах охорони. Вибір конкретних сил і засобів, що застосовуються для охорони об'єкта підприємства, здійснюється на основі аналізу можливих загроз його безпеки. Важливе значення при цьому має рівень підготовки і професіоналізм співробітників охорони, безпосередньо несучих чергування. Наявність конкретних загроз і можливість їх реалізації в конкретній обстановці є найбільш важливими факторами, що впливають на прийняття керівництвом підприємства рішення про вибір сил і засобів охорони його об'єктів.

Практика показує, що найбільш часто зустрічаються наступні основні причини порушення порядку охорони об'єктів: недооцінка можливих загроз безпеки об'єкта на конкретних рубежах (територіях) охорони; неякісне (недбале) виконання обов'язків співробітниками охорони при несенні чергування; використання порушником (зловмисником) випадкової (нештатної) ситуації. Окремим випадком подібної ситуації може бути навмисне створення персоналом служби охорони умов, що сприяють таким зловмисних дій.

Створення надійної системи охорони підприємства визначається прийняттям правильного рішення на основі аналізу потенційних загроз безпеки об'єкта та реальної оцінки можливостей для створення ефективної системи охорони з урахуванням наявного вибору сил і засобів. Організація системи охорони підприємства та його об'єктів встановлюється рішенням керівника підприємства. При організації системи охорони визначають: способи охорони території підприємства і його об'єктів; кількість постів, місць несення чергування з охорони об'єктів, ділянки (зони, території) охорони; кількість і види контрольно-пропускних пунктів, порядок і особливості несення чергування на цих пунктах співробітниками охорони; порядок і особливості дій особового складу охорони у всіх випадках (у тому числі в екстрених ситуаціях); порядок і особливості застосування (використання) технічних засобів виявлення і охорони на кожній ділянці (зоні, території) охорони.

Одним з важливих завдань, що вирішуються підрозділами охорони, є супровід і охорона носіїв конфіденційної інформації, матеріальних цінностей і вантажів при їх транспортуванні та перевезення (доставки) на інші підприємства (об'єкти). У цьому випадку співробітники підрозділів охорони забезпечують захист осіб, що доставляють (перевозять) носії конфіденційної інформації, інші матеріальні цінності і вантажі в пункт призначення (на інші підприємства), і охорону перерахованого майна в порядку, визначеному спеціально розробляється на підприємстві інструкцією (положенням), або окремим розділом раніше згадуваної інструкції з організації охорони підприємства, його території і об'єктів.

Для виконання завдань перевезення (доставки) носіїв конфіденційної інформації, матеріальних цінностей та вантажів наказом керівника підприємства призначаються найбільш підготовлені співробітники підприємства, здатні в будь-яких умовах забезпечити збереження майна. Співробітники підрозділу охорони при цьому забезпечують охорону та захист від розкрадання, крадіжки чи інших навмисних дій сторонніх осіб, спрямованих на оволодіння носіями конфіденційної інформації, матеріальними цінностями і вантажами. Підготовка співробітників охорони до виконання зазначених завдань здійснюється з урахуванням вибору маршруту руху, способу доставки (автомобільним, залізничним або авіаційним транспортом) і часу прибуття в пункт призначення.

Навчання співробітників підрозділів охорони, у тому числі з метою підвищення кваліфікації, організовується за рішенням керівника підприємства в освітніх установах (на курсах, у центрах підготовки), які мають право на здійснення відповідного виду освітньої діяльності.

Фізичний захист об'єктів підприємства. Під фізичним захистом розуміється сукупність організаційних заходів, інженерно-технічних засобів і дій підрозділів охорони з метою запобігання диверсій чи розкрадань носіїв конфіденційної інформації та інших матеріальних засобів на об'єктах, що охороняються.

Створення і застосування засобів фізичного захисту для деяких категорій об'єктів є обов'язковим і регулюється законодавством. Це, в першу чергу, відноситься до об'єктів підприємств, що здійснюють діяльність з виробництва, використання, зберігання, утилізації та транспортуванні ядерних матеріалів або виробів на їх основі, а також з проектування, будівництва, експлуатації та виведення з експлуатації ядерних установок і пунктів зберігання ядерних матеріалів.

Застосування засобів фізичного захисту значно підвищує ефективність функціонування системи охорони підприємства в цілому, а, з урахуванням специфіки розташування деяких об'єктів підприємства та виконуваних ними завдань, практично гарантує досягнення головних цілей і вирішення основних завдань охорони підприємства.

При розгляді основних підходів до фізичного захисту об'єктів підприємства та принципів її організації, а також при застосуванні засобів фізичного захисту використовуються такі терміни та поняття:

- допуск - дозвіл на проведення певної роботи або на отримання певних документів і відомостей;
- доступ - прохід (проїзд) в охороняємо зони об'єкта підприємства;
- захищена зона - територія об'єкта підприємства, яка оточена фізичними бар'єрами, постійно перебувають під охороною і наглядом, і доступ до якої обмежується і контролюється;
- порушник - особа, яка вчинила або намагається вчинити несанкціоновану дію, а також особа, яка надає йому сприяння в цьому;
- несанкціонована дія - розкрадання або спроба розкрадання носіїв конфіденційної інформації та матеріальних засобів підприємства, здійснення або спроба здійснення несанкціонованого доступу, пронесення (провезення) заборонених предметів, вчинення диверсії, виведення з ладу засобів фізичного захисту;
- несанкціонований доступ - проникнення осіб, не мають права доступу, в охоронювані зони, на об'єкти, в службові приміщення підприємства;
- виявлення - встановлення факту несанкціонованого дії;
- периметр - межа зони, що охороняється, обладнана фізичними бар'єрами та контрольно-пропускними пунктами;
- підрозділ охорони - озброєний підрозділ, що виконує завдання по охороні і обороні об'єктів підприємства;
- система охоронної сигналізації - сукупність засобів виявлення, тривожної сигналізації, системи збору, відображення та обробки інформації;
- технічний засіб виявлення - пристрій, призначений для автоматичної подачі сигналу тривоги у випадку несанкціонованої дії;
- фізичний бар'єр - фізична перешкода, що ускладнює проникнення порушника в зони, що охороняються.

Завдання фізичного захисту наступні: попередження випадків несанкціонованого доступу на об'єкти підприємства; своєчасне виявлення несанкціонованих дій на території підприємства; затримка (уповільнення) проникнення порушника, створення перешкод його діям; припинення несанкціонованих дій на території підприємства; затримання осіб, причетних до підготовки або вчинення диверсії, розкраданню носіїв конфіденційної інформації або інших матеріальних цінностей підприємства.

Система фізичного захисту підприємства включає: організаційні заходи; інженерно-технічні засоби; дії підрозділів охорони.

При створенні системи фізичного захисту об'єктів підприємства необхідно: враховувати особливості підприємства, специфіку розташування його об'єктів, наявність територіально

відокремлених (віддалених) об'єктів, види робіт, що проводяться з використанням конфіденційної інформації, а також ступінь її конфіденційності; вибирати сили і засоби фізичного захисту, у тому числі структуру і склад підрозділів охорони, на основі аналізу та оцінки потенційних загроз об'єктам підприємства; обмежувати кількість співробітників підприємства, що допускаються до питань організації системи фізичного захисту, а також до використовуваних інженерно-технічних засобів; забезпечувати стійке функціонування елементів системи, підтримку в працездатному стані технічних засобів охорони.

Основу функціонування системи фізичного захисту становлять організаційні заходи. Вони включають комплекс заходів, що вживаються керівництвом підприємства для фізичного захисту його об'єктів, а також нормативно-методичні та плануючі документи, що регламентують їх здійснення.

Безпосереднє планування комплексу організаційних заходів та контроль за їх виконанням здійснює служба безпеки підприємства спільно з іншими його структурними підрозділами, що беруть участь в процесі захисту конфіденційної інформації. Діяльність цих структурних підрозділів координує заступник керівника підприємства, який відповідає за вирішення завдань по захисту конфіденційної інформації.

В цілях фізичного захисту об'єктів служба безпеки підприємства забезпечує: розробку, створення і функціонування системи фізичного захисту; проведення аналізу уразливості об'єкта для визначення внутрішніх та зовнішніх загроз і ймовірних способів їх здійснення; оцінку можливого збитку при реалізації внутрішніх і зовнішніх загроз; оцінку ефективності діючої чи проектованої системи фізичного захисту та визначення шляхів її вдосконалення; розроблення із залученням структурних підрозділів підприємства та затвердження в установленому порядку документів, що регламентують питання організації і здійснення пропускного режиму на об'єктах підприємства, охорони об'єктів підприємства; контроль за дотриманням вимог організаційно-плануючих документів з організації охорони та пропускного режиму на підприємстві.

З метою ефективного вирішення завдань фізичного захисту об'єктів використовуються інженерно-технічні засоби захисту інформації, які в свою чергу є елементом системи інженерно-технічного захисту інформації.

Система інженерно-технічного захисту інформації - сукупність органів, що вирішують завдання інженерно-технічного захисту інформації, використовуваних для цього технічних засобів та комплексу заходів, що проводяться в цілях забезпечення інформаційної безпеки підприємства.

До основних завдань інженерно-технічного захисту інформації належать: запобігання проникнення сторонніх осіб (зловмисників) до носіїв конфіденційної інформації з метою її розкрадання, знищення або зміни; захист носіїв конфіденційної інформації від знищення і нанесення іншої шкоди в результаті впливу стихійних лих та інших надзвичайних ситуацій; закриття можливих технічних каналів витоку конфіденційної інформації.

При постановці завдань інженерно-технічного захисту інформації на підприємстві визначають: перелік можливих загроз інформації, що захищається підприємства; об'єкти підприємства, що підлягають захисту; методи захисту інформації; порядок здійснення контролю ефективності вирішення завдань фізичного захисту об'єктів.

Для успішного виконання поставлених завдань в рамках системи інженерно-технічного захисту інформації реалізується комплекс відповідних організаційних і технічних заходів.

Основними принципами створення системи інженерно-технічного захисту інформації, що володіє високою ефективністю і надійністю, є:

- скритність - збереження в таємниці факту створення та особливостей побудови системи інженерно-технічного захисту інформації, а також використовуються з цією метою сил і засобів захисту інформації;

- гнучкість - можливість оперативного реагування на зміни ступеня захищеності конфіденційної інформації в залежності від вибору критеріїв, способів і методів її захисту;

- багатозональність - розміщення джерел інформації в різних зонах захисту з контрольованим рівнем безпеки, тобто поділ території підприємства на зони з різними рівнями доступу для персоналу підприємства відповідних категорій (керівництво підприємства, керівники підрозділів, окремі посадові особи і т.п.) і розміщення об'єктів в різних зонах залежно від ступеня важливості зберігається або обробляється на цих об'єктах інформації;

- багаторубіжність - створення відповідних рубежів захисту об'єктів підприємства на кордонах обраних зон захисту інформації.

Основні методи інженерно-технічного захисту інформації на підприємстві:

- створення фізичних, електронних та інших перешкод зловмисникові на шляху до носіїв конфіденційної інформації та її джерел; введення зловмисника в оману за допомогою технічних засобів шляхом підготовки та розповсюдження (нав'язування) неправдивої інформації;

- застосування різних засобів контролю несанкціонованого доступу для виявлення спроб реалізації зловмисником загроз безпеці інформації та інформування про виявлені спробах посадових осіб, що беруть участь у виробленні заходів захисту інформації на об'єктах підприємства;

- попередження посадових осіб та персоналу підприємства про виникнення надзвичайних ситуацій на об'єктах.

Інженерно-технічні засоби фізичного захисту складаються з технічних засобів і фізичних бар'єрів.

До технічних засобів фізичного захисту належать: засоби охоронної сигналізації, розміщені по периметру зон, що охороняються, будівель, споруд та інших об'єктів підприємства, а також службових приміщень в цих об'єктах; засоби контролю проходу (доступу), встановлені на контрольно-пропускних пунктах, в охоронюваних будівлях, спорудах (об'єктах) підприємства та в службових приміщеннях; засоби спостереження за периметрами охоронюваних зон, контрольно-пропускними пунктами, охоронюваними будівлями, спорудами підприємства, а також службовими приміщеннями; засоби спеціального зв'язку (в тому числі - екстренної); засоби виявлення проносу (провозу) заборонених предметів, вибухових речовин, і предметів з металу (у тому числі носіїв конфіденційної інформації); засоби систем життєзабезпечення (електроживлення, освітлення та ін.).

Переліченими засобами обладнуються периметри зон, що охороняються, будівлі, споруди та приміщення, що охороняється, а також контрольно-пропускні пункти.

У сучасних системах фізичного захисту підприємств особливе місце займають засоби охоронної сигналізації, засоби контролю доступу (проходу), засоби спостереження за охоронними об'єктами.

Засоби охоронної сигналізації призначені для своєчасного інформування відповідних посадових осіб (співробітників охорони підприємства, операторів пультів охорони в каральних приміщеннях) про порушення початкового стану або встановленого режиму роботи кінцевих пристроїв цих засобів, викликаних несанкціонованим проникненням осіб в охоронювані зони (території), а також спробами несанкціонованого відкриття охоронюваних об'єктів (службових приміщень) підприємства.

Засоби контролю доступу (проходу) осіб на територію (в службові приміщення) підприємства служать для обмеження і санкціонування пересування (переміщення) працівників підприємства, відряджених осіб і відвідувачів на території та об'єктах підприємства. Основними видами засобів контролю доступу (проходу) є загороджуючи пристрої та пристрої ідентифікації персоналу. Загороджуючи пристрої служать для створення фізичної перешкоди несанкціонованого переміщення осіб, транспортних засобів на об'єктах (в службових приміщеннях) підприємства. Приведення загороджуючих пристроїв у відкрите і закрите стан забезпечують виконавчі механізми. Існують різні типи загороджуючих пристроїв: електронні, електромеханічні, електромагнітні та ін. Пристрої

ідентифікації персоналу підприємства та інших осіб фіксують (підтверджують) наявність або відсутність у даної особи права (санкції) на переміщення через загороджуючи пристрої.

Основні принципи організації і застосування засобів контролю доступу та засобів охоронної сигналізації в чому збігаються, так як цілі використання цих засобів однакові. Разом тим, засоби охоронної сигналізації функціонують в неробочий час, коли службові приміщення (об'єкти) підприємства в установленому порядку здані під охорону караулу або оператору пульту управління охоронними засобами. Період функціонування засобів контролю доступу починається з моменту початку проходу на територію підприємства його співробітників і завершується здачею об'єктів підприємства під охорону і постановкою їх на контроль засобами охоронної сигналізації.

Засоби спостереження за охоронними об'єктами забезпечують отримання і документування відеоінформації про обстановку на об'єкті, що охороняється в цілях прийняття своєчасного рішення про застосування сил і засобів охорони для припинення (виключення) спроб несанкціонованого проникнення на об'єкт сторонніх осіб. Найбільш широке поширення в даний час отримали відео та телевізійні системи спостереження.

Системи спостереження за охоронними об'єктами призначені:

- для визначення причин спрацювання засобів охоронної сигналізації, встановленої на об'єкті; отримання оперативної інформації про проникнення на об'єкт, що охороняється сторонньої особи (зловмисника);
- контролю за діями співробітників (підрозділів) охорони і координації їх дій при виконанні завдань охорони об'єктів підприємства;
- документування інформації про події і злочини, вчинені на території об'єкту, що охороняється.

ЛІТЕРАТУРА

1. Кулицький С. П. Основи організації інформаційної діяльності у сфері управління: Навч. посіб. — К.: МАУП, 2002. — 224 с: іл. - Бібліогр.: С 209-218.
2. Богуш В.М., Юдін О.К. Інформаційна безпека держави. -К.: «МК-Прес», 2005. -432 с.
3. Браіловський М.М., Головань С.М. та інші. Технічний захист інформаціїна об’єктах інформаційної діяльності / за ред.проф. Хорошка В.О. - К.: ДУІКТ, 2007. -178 с.
4. Низенко Е.І. Забезпечення інформаційної безпеки підприємництва: Навчальний посібник/ Е.І. Низенко, В.П. Каленяк. –К.: МАУП, 2006. - 134 с.
5. Колот А.М. Мотивація, стимулювання й оцінка персоналу: Навчальний посібник. – Київ: КНЕУ, 2003. – 224 с.
6. Козаченко Г.В., Пономарьов В.П., Ляшенко О.М. Економічна безпека підприємства: сутність та механізм забезпечення: Монографія. – К.: Лібра, 2003. – 280 с.

Надійшла: 12.04.2013 р.

Рецензент: д.т.н., проф. Олійник В.Ф.