Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

О. А. Дисковський
О. О. Косиченко
Л. В. Рибальченко

ОСНОВИ ОРГАНІЗАЦІЇ ЗАХИСТУ ОБ'ЄКТІВ ТА ІНФОРМАЦІЇ ВІД ЗЛОЧИННИХ ПОСЯГАНЬ

Навчальний посібник

Дніпро
2020

УДК 351 + 004.056.5
Д 48

Рекомендовано до друку Науково-методичною радою ДДУВС
(протокол № 7 від 19 березня 2020 р.)

РЕЦЕНЗЕНТИ:

доктор економічних наук, професор **Баранник Л. Б.** – професор кафедри соціального забезпечення та податкової політики Університету митної справи та фінансів, м. Дніпро;

доктор технічних наук, професор **Зеленцов Д. Г.** – завідувач кафедри інформаційних систем ДВНЗ «Український державний хіміко-технологічний університет», м. Дніпро.

Дисковський А. О., Косиченко О. О., Рибальченко Л. В.

Д 48 Основи організації захисту об’єктів та інформації від злочинних посягань : навч. посібник для слухачів магістратури / О. А. Дисковський, О. О. Косиченко, Л. В. Рибальченко. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2020. 96 с.

ISBN 978-617-7665-94-5

Викладено основи організаційного захисту інформації, види загроз інформаційній безпеці, основні напрямки, принципи й умови захисту. Описано організаційну структуру служби безпеки, висвітлено питання забезпечення безпеки інформації під час проведення нарад, переговорів, під час роботи з персоналом. Також розглянуто питання організації охорони об’єктів і пропускного режиму.

Призначено для слухачів магістратури.

ISBN 978-617-7665-94-5

© Автори, 2020
© ДДУВС, 2020

ЗМІСТ

ВСТУП

У навчальному посібнику розглянуто ключові розділи навчального курсу «Організація захисту об'єктів та інформації від злочинних посягань», який вивчається слухачами магістратури спеціальності 262 – «Правоохоронна діяльність» (спеціалізація «Безпека підприємництва»).

Організаційний захист інформації є початком, фундаментом у загальній системі захисту конфіденційної інформації підприємства. Від повноти і якості вирішення керівництвом підприємства та посадовими особами організаційних завдань залежить ефективність функціонування системи захисту інформації загалом. Роль і місце організаційного захисту інформації в загальній системі заходів, спрямованих на захист конфіденційної інформації підприємства, визначаються важливістю прийняття керівництвом своєчасних і правильних управлінських рішень із урахуванням наявних у розпорядженні сил, засобів, методів і способів захисту інформації та на основі чинного нормативно-методичного забезпечення.

Серед основних напрямків захисту інформації поряд з організаційним виділяють правовий і інженерно-технічний захист інформації. Однак організаційний захист інформації серед цих напрямків посідає особливе місце. Організаційний захист інформації покликаний шляхом вибору конкретних дій та засобів (разом із правовими, інженерно-технічними та ін.) реалізувати на практиці спланові керівництвом підприємства заходи щодо захисту інформації. Ці заходи реалізуються залежно від конкретної обстановки на підприємстві, пов'язаної з наявністю можливих загроз, які впливають на інформацію, що захищається, і які призводять до її витоку.

1. ОСНОВНІ ПОНЯТТЯ

1.1. Мета й завдання організаційного захисту інформації, його зв'язок із правовим та технічним захистом інформації

Закордонний досвід щодо захисту інтелектуальної власності та вітчизняний досвід у захисті державних секретів показує, що ефективним може бути тільки комплексний захист, який поєднує в собі напрямки захисту, як-от: *правовий*, *організаційний, інженерно-технічний.*

Правовий напрямок передбачає формування сукупності законодавчих актів, нормативно-правових документів, положень, інструкцій, вимоги яких є обов'язковими в рамках сфери їх діяльності в системі захисту інформації.

Організаційний захист інформації – це така регламентація виробничої або службової діяльності та взаємин виконавців на нормативно-правовій основі, що несанкціонований доступ до конфіденційної інформації стає неможливим або суттєво ускладнюється за рахунок проведення організаційних заходів.

На думку фахівців, організаційні заходи мають велике значення у створенні надійного механізму захисту інформації, тому що можливості несанкціонованого використання конфіденційних відомостей значною мірою зумовлюються не технічними аспектами, а злочинними діями та недбалістю користувачів або персоналу.

Вплив цих аспектів практично неможливо виключити за допомогою технічних засобів, програмно-криптографічних методів та фізичних заходів.

До організаційних заходів можна віднести:

- заходи, які здійснюють під час проєктування, будівництва та устаткування службових і виробничих будинків і приміщень. Їх мета: виключення можливості таємного проникнення на територію й у приміщення; забезпечення зручності контролю проходу й переміщення людей, проїзду транспорту й інших засобів пересування; створення окремих виробничих зон за типом конфіденційності ро-

біт із самостійними системами доступу тощо;

- заходи, здійснювані під час підбору персоналу, включно з ознайомленням із потенційними співробітниками, навчання їх правилам роботи з конфіденційною інформацією, ознайомлення із відповідальністю за порушення правил захисту інформації та ін.;
- організація та підтримка надійного пропускного режиму й контролю відвідувачів;
- організація надійної охорони приміщень і території;
- організація зберігання й використання документів і носіїв конфіденційної інформації, включно з порядком обліку, видачі, виконання та повернення;
- організація захисту інформації: призначення відповідального за захист інформації в конкретних виробничих колективах, проведення систематичного контролю над роботою персоналу з конфіденційною інформацією, порядок обліку, зберігання та знищення документів тощо;
- організація регулярного навчання співробітників.

Інженерно-технічний напрямок містить у собі програмно-апаратні засоби захисту інформації. До апаратних засобів належать механічне, електромеханічне, електронне, оптичне, лазерне, радіотехнічне, радіолокаційне й інше обладнання, системи й спорудження, призначені для забезпечення безпеки та захисту інформації.

Ці засоби застосовують для виконання таких завдань:

- перешкоді візуальному спостереженню й дистанційному підслуховуванню;
- нейтралізації паразитних електромагнітних випромінювань і наводок (ПЕМВН);
- виявлення технічних засобів підслуховування й магнітного запису, встановлених або внесених в організацію без дозволу;
- захисту інформації, яка передається в засобах зв'язку й системах автоматизованої обробки інформації.

За призначенням апаратні засоби поділяють на засоби виявлення й засоби захисту (або істотного ослаблення) несанкціонованого доступу.

До класу захисної спецтехніки належить величезна кількість апаратів, обладнань і систем, які умовно можна розділити на

кілька груп. Наприклад, на такі:

- прилади виявлення та нейтралізації обладнань, що підслуховують і звукозаписних;
- засоби захисту абонентської телефонної мережі;
- засоби захисту від знімання інформації з приміщень;
- прилади для виявлення лазерного й відеоспостереження та інші.

Багатогранність сфери організаційного захисту інформації потребує створення спеціальної служби безпеки, що забезпечує реалізацію всіх організаційних заходів. Її штатна структура, чисельність і склад визначається реальними потребами фірми, ступенем конфіденційності її інформації й загальним станом безпеки.

Сформована сукупність правових, організаційних та інженерно-технічних заходів належить до забезпечення політики безпеки.

Політика безпеки визначає структуру системи захисту інформації у вигляді сукупності правових норм, організаційних (правових) заходів, комплексу програмно-технічних засобів і процедурних рішень, спрямованих на протидію загрозам з метою виключення або мінімізації можливих наслідків інформаційних впливів.

Можлива така ситуація, коли для зменшення ризику не існує ефективних і прийнятних за ціною заходів. У цьому разі доводиться піднімати планку прийнятного ризику й переносити центр зусиль на зменшення наслідків і розробки планів відновлення після аварій, стихійних лих та інших подій.

1.2. Види загроз інформаційній безпеці на об’єкті захисту та їх характеристика

Загроза – це потенційні або реальні можливі дії, що призводять до морального або матеріального збитку.

Загроза безпеці інформації – потенційна можливість порушення основних якісних характеристик (властивостей) інформації під час її обробки технічними засобами: конфіденційності, цілісності, доступності.

Під *загрозами конфіденційної інформації* прийнято розуміти потенційні або реально можливі дії стосовно конфіденційних інформаційних ресурсів, що призводять до неправомірного заволодіння

охоронюваними відомостями.

Такими діями є:

- ознайомлення з конфіденційною інформацією різними шляхами й способами без порушення її цілісності;
- модифікація інформації в кримінальних цілях як часткова або значна зміна складу й змісту відомостей;
- руйнування (знищення) інформації як акт вандалізму з метою прямого завдання матеріального збитку.

Протиправні дії з інформацією призводять до порушення її конфіденційності, повноти, вірогідності та доступності, що також призводить до порушення як режиму управління, так і його якості в умовах неправильної або неповної інформації. Кожна загроза спричиняє певний збиток – моральний або матеріальний, а захист і протидія загрозі покликані знизити його величину, в ідеалі – повністю, реально – значно або хоча б частково. Але й це вдається далеко не завжди.

Отже, загрози можуть бути класифіковані за такими групами:

а) за величиною завданого збитку:
- граничний, після якого фірма може стати банкрутом;
- значний, але, що не призводить до банкрутства;
- незначний, який фірма може компенсувати й ін.;

б) за ймовірністю виникнення:
- досить ймовірна загроза;
- ймовірна загроза;
- малоймовірна загроза;

в) через виникнення:
- стихійні лиха;
- навмисні дії;

г) за характером завданого збитку:
- матеріальний;
- моральний;

д) за характером впливу:
- активні;
- пасивні;

е) стосовно об'єкта:
- внутрішні;
- зовнішні.

Джерелами зовнішніх загроз є:

- несумлінні конкуренти;
- злочинні угруповання;
- окремі особи й організації адміністративно-управлінського апарату.

Джерелами внутрішніх загроз можуть бути:

- адміністрація підприємства;
- персонал;
- технічні засоби забезпечення виробничої й трудової діяльності.

Співвідношення зовнішніх і внутрішніх загроз на усередненому рівні можна охарактеризувати так:

- 82 % загроз відбуваються за прямої або опосередкованої участі власних співробітників фірми ;
- 17 % загроз відбувається ззовні – зовнішні загрози;
- 1 % загроз здійснюють випадкові особи.

1.3. Моделі порушників інформаційної безпеки на об’єкті

Кожний власник майна (суб’єкт, який у повному обсязі реалізує повноваження володіння, користування, розпорядження зазначеним майном) має завдання забезпечення його охорони від різного типу загроз, починаючи від банальної крадіжки до його повного знищення. Особливу турботу при цьому викликає проблема побудови системи охорони об’єкта (підприємства), яке має розосереджені на певній площі складські й/або виробничі приміщення з різнорідним майном, що потребує захисту. Відмітною рисою такого підприємства є протяжливий, важко контрольований периметр, що має, як правило, кілька варіантів проходу (проїзду) персоналу (службового транспорту).

У разі виникнення цієї проблеми ухвалюється рішення організувати захист майна побудовою (модернізацією наявної) системи охорони периметра (СОП) підприємства. Система охорони периметра підприємства за типом устаткування, яке використовується, та поставленим завданням належить до системи охоронної сигналізації об’єкта і її побудова повинна відповідати вимогам нормативних і керівних документів, наведених у табл. 1.1.

Таблиця 1.1

Нормативні документи з охорони периметра

Держстандарт	Назва
ДСТУ 3960-2000	Системи тривожної сигналізації. Системи охоронної і охоронно-пожежної сигналізації. Терміни та визначення
ДСТУ prEN 50136-1-1:2004	Системи тривожної сигналізації. Системи передавання тривожних сповіщень та устаткування. Частина 1-1. Загальні вимоги до систем передавання тривожних сповіщень
ДЕРЖСТАНДАРТ Р 50776–95	Системи тривожної сигналізації. Частина 1. Загальні вимоги. Розділ 4. Посібник із проєктування, монтажу та технічного обслуговування
ОСТ 25 1099–83	Засоби охоронної, пожежної й охоронно-пожежної сигналізації. Загальні вимоги й методи випробувань
РД 25.952–90	Системи автоматичні пожежогасіння, пожежної, охоронної й охоронно-пожежної сигналізації. Порядок розробки завдання на проєктування

У складі системи охорони периметра, крім технічних засобів охорони, повинні застосовуватися інженерні засоби, без яких деякі завдання охорони периметру взагалі не можуть бути реалізовані.

Під час розробки системи охорони периметра підприємства потрібно також розробити:

- модель об'єкта охорони (модель периметра);
- модель загроз (у тому числі модель порушника) і тактику охорони периметра.

Порушник – це особа, що почала спробу виконання заборонених операцій (дій) помилково, через незнання або усвідомлено зі злим умислом (з корисливих інтересів) або без (заради гри або задоволення, з метою самоствердження й т. ін.), і використовує для цього різні можливості, методи й засоби.

Зловмисник – це порушник, що навмисно йде на порушення з корисливих спонукань.

Під час розробки моделі порушника визначають:

- припущення щодо категорій осіб, до яких може належати порушник;

- припущення щодо мотивів дій порушника (переслідуваних порушником цілях);
- припущення щодо кваліфікації порушника і його технічної оснащеності (про використовувані для здійснення порушення методи і засоби);
- обмеження й припущення щодо характеру можливих дій порушників.

Порушники можуть бути *внутрішніми* (із числа персоналу) або *зовнішніми* (сторонніми особами).

Можна виділити кілька основних мотивів порушень:

- безвідповідальність;
- самоствердження;
- вандалізм;
- примус;
- помста;
- корисливий інтерес;
- ідейні міркування.

Під час порушень, викликаних безвідповідальністю, користувач виконує такі руйнівні дії, що не пов’язані зі злим наміром. Це відбувається через некомпетентність або недбалість.

Основна мета порушника полягає в потайливім подоланні зони периметра підприємства для одержання несанкціонованого доступу (НСД) до охоронюваного майна власника. Спосіб і час, витрачені ним на подолання зони периметра, прямо залежать від його поінформованості про можливості СОП підприємства, технічну й фізичну підготовленість, а також від кінцевих цілей вторгнення.

Для визначення необхідного рівня захищеності периметра (його здатності протистояти діям порушника) необхідно формування базової моделі порушника, на здатності й можливості якого повинна орієнтуватися створювана СОП.

Під моделлю порушника розуміється його описова характеристика, що відображає його можливий моральний вигляд, рівень фізичної підготовленості, знань, навченості й оснащеності, які дають можливість оцінити ступінь його здатності й зацікавленості в подоланні зони периметра підприємства, з одного боку, а з іншого – визначити припустимий рівень інженерно-технічної підготовленості рубежів охорони зони периметра.

Таблиця 1.2

Типові моделі порушника

Категорія	Тип порушника	Характеристика	Фізпідготовка	Знання про можливості ТЗО	Оснащеність	Примітка
1	Професіонал	Дуже небезпечний. Здатний добувати відомості про інженерно-технічні засоби охорони (ІТЗО), планувати і готовити вторгнення. Діє поодинці, як правило, не цікавиться матеріальними ресурсами. Побоюється розголосу	Відмінна	Високі	Спеціальний набір засобів, призначений для НСД, недоступний до вільного придбання	Тренується державою й використовується в її інтересах. Захист від проникнення порушника знаходиться під державним наглядом
2	Найманець (аматор)	Небезпечний. Здатний на нелогічні дії, має задатки плановості дій, може збирати відомості про ІТЗО. Діє як поодинці, так і групою. Його цікавить весь спектр цілей вторгнення	Достатня	Добрі	Підібраний під завдання НСД набір доступних, але вдосконалених або саморобних засобів	Його послуги коштують дорого – мета його НСД на підприємство повинна компенсувати витрати на його найм
3	Безробітний (дилетант)	Помірковано небезпечний. Вторгнення планується на дилетантському рівні за сценарієм героїв популярних фільмів. Діє, як правило, поодинці. Цікавлять або матеріальні, або інформаційні ресурси	Задовільна	Слабкі	Побутові засоби, легко доступні для придбання в магазині	Має потребу в коштах – послуги його дешеві. Може переслідувати свої цілі щодо збагачення
4	Побутовий (хуліган, наркоман, алкоголік)	Мало небезпечний. Діє імпульсивно, на підставі обривкових даних про можливу наживу. Діє як поодинці, так і групою. Цікавлять головно матеріальні (фінансові) цінності. Розраховує на силові варіанти	Погана	Відсутні	Підручні засоби (що під руку попалось)	Здійснює НСД із хуліганською метою або з метою збагачення. Послуги його дуже дешеві

5	Співробітник підприємства	Небезпечний. Здатний добувати відомості про ІТЗО, планувати і готовити НСД, зробити саботаж ТЗО. Діє потай, у робочий час як поодинці, так і групою. Цікавлять або матеріальні, або інформаційні ресурси, але малих розмірів, що дозволяє їх винести (перевезти) через КПП. Може використовувати зовнішніх пособників	Погана	Високі	Підібраний під завдання НСД набір доступних, але вдосконалених або саморобних засобів	Має велику потребу у коштах. Його послуги коштують дорого – мета його НСД на підприємство повинна відповідати витратам на його найм ання й втрату роботи. Або переслідує свої цілі щодо збагачення

У табл. 1.1 наведені типові моделі порушника для різних категорій осіб. На підставі статистики порушень режиму, установленого на підприємстві, і аналізу криміногенної обстановки навколо нього, а також оцінки можливостей кола зацікавлених у НСД до охоронюваного майна осіб (організацій), створюють модель найбільш імовірного порушника.

Таку модель наділяють максимальними для обраного типу спроможностями й можливостями по подоланню зони периметра. Створену модель порушника представляють як базову й щодо неї виконують розробку моделі загроз.

Модель загроз являє собою перелік та схему можливих дій (цілей і способів їх досягнення) порушника по подоланню зони периметра підприємства (розподіленого об’єкта охорони).

Під метою вторгнення розуміють кінцеву мету порушника, реалізовану ним після подолання зони периметра. Їхній можливий спектр досить широкий – від простої крадіжки до терористичних дій, він прямо залежить від типу охоронюваного майна.

Визначення цілей вторгнення на територію підприємства, вигляду можливого порушника й найбільш імовірних сценаріїв його дій дозволяє сформувати вимоги до інженерно-технічних засобів системи охорони периметра, під час реалізації яких можливе ефек-

тивне протистояння.

Неформальна модель порушника відображає його практичні й теоретичні можливості, апріорні знання, час і місце дії тощо. Для досягнення своїх цілей порушник повинен докласти певні зусилля, затратити певні ресурси.

Під час формування моделі загроз у розглянутому випадку необхідно враховувати тільки ті загрози охоронюваному майну підприємства, які включають несанкціоноване подолання зони його периметра порушником, що має можливості, які сформовані його базовою моделлю. Тут корисними можуть бути натурні випробування по кількісній оцінці можливостей порушника, наприклад, часу подолання зовнішнього огородження заданої конструкції або зони відчуження, обладнаної інженерними засобами затримки тощо. За таких умов, як правило, використовують принцип «гірше бути не може», тобто якщо створена СОП може протистояти (виявити) базовій моделі порушника, то вона зможе протистояти всім типам порушників з меншим рівнем підготовленості за іншим параметром.

Контрольні запитання

1. Особливості організаційного захисту інформації.
2. Організаційні заходи щодо надійного механізму захисту інформації.
3. Дії щодо загроз конфіденційної інформації.
4. Класифікація загроз конфіденційної інформації.
5. Внутрішні та зовнішні джерела загроз.
6. Моделі порушників інформаційної безпеки.
7. Мотиви внутрішніх та зовнішніх порушників інформації.

2. ОСНОВНІ НАПРЯМКИ, ПРИНЦИПИ ТА УМОВИ ОРГАНІЗАЦІЙНОГО ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Основні принципи організаційного захисту інформації

В основі діяльності щодо організації захисту інформації на підприємстві є сукупність основних принципів, що містить:

- принцип комплексного підходу – ефективне використання сил, засобів, способів і методів захисту інформації для вирішення поставлених завдань залежно від конкретної складної ситуації і наявності чинників, які послаблюють або посилюють загрозу інформації, що захищається;
- принцип оперативності прийняття управлінських рішень (суттєво впливає на ефективність функціонування й гнучкість системи захисту інформації й відображає спрямованість керівництва й персоналу підприємства на вирішення завдань захисту інформації);
- принцип персональної відповідальності – найбільш ефективний розподіл завдань щодо захисту інформації між керівництвом і персоналом підприємства й визначення відповідальності за повноту й якість їх виконання.

Серед основних умов організаційного захисту інформації можна виділити такі:

- безперервність всебічного аналізу функціонування системи захисту інформації з метою вживання своєчасних заходів щодо підвищення її ефективності;
- неухильне дотримання керівництвом і персоналом підприємства встановлених норм і правил захисту конфіденційної інформації.

У разі дотримання перелічених умов забезпечується найбільш повне і якісне вирішення завдань щодо захисту конфіденційної інформації на підприємстві.

2.2. Основні підходи та вимоги до організації системи захисту інформації

Успішне вирішення комплексу завдань щодо захисту інформації не може бути досягнуте без створення єдиної основи так званого «активного центру, ядра» підприємства, здатного концентрувати всі зусилля та ресурси, що є в наявності, для виключення витоку конфіденційної інформації й недопущення можливості завдання збитків підприємству. Таким «центром» має стати система захисту інформації на підприємстві, створювана на відповідній нормативно-методичній основі, що відображає всі напрямки й специфіку діяльності цього підприємства.

Під системою захисту інформації розуміють сукупність суб'єктів захисту інформації (структурних підрозділів або посадових осіб підприємства), засобів і методів захисту інформації, а також запланованих і проведених заходів з метою захисту.

Для вирішення організаційних завдань щодо створення й забезпечення функціонування системи захисту інформації використовують основні підходи, які створюють на підставі наявної нормативно-правової бази й з урахуванням методичних розробок з напрямків захисту конфіденційної інформації.

Один з основних підходів до створення системи захисту інформації полягає у всебічному аналізі стану захищеності інформаційних ресурсів підприємства з урахуванням спрямованості конкуруючих організацій до заволодіння конфіденційною інформацією й тим самим завданню збитків підприємству. Важливим елементом аналізу є робота з визначення переліку інформаційних ресурсів, що захищаються, з урахуванням особливостей їх розташування і доступу до них співробітників різних категорій (працівників інших підприємств).

Роботу з виконання такого аналізу безпосередньо очолює керівник підприємства і його заступники по напрямках діяльності. Вивчення захищеності інформаційних ресурсів ґрунтується на позитивному й негативному досвіді роботи підприємства, накопиченому протягом останніх декількох років, а також на ділових зв'язках і контактах підприємства з організаціями, що здійснюють аналогічні види діяльності.

Під час створення системи захисту інформації, насамперед, враховуються найбільш важливі, пріоритетні напрямки діяльності підприємства, що вимагають особливої уваги. Перевага також надається новим, перспективним напрямкам діяльності підприємства, які пов'язані з науковими дослідженнями, новітніми технологіями, інтелектуальній власності та міжнародним зв'язкам. Відповідно до названих пріоритетів формується перелік можливих загроз інформації, що підлягає захисту, і визначаються конкретні сили, засоби, способи й методи її захисту.

До організації системи захисту інформації з позиції системного підходу висувається низка вимог, що визначають її цілісність, структурність і ефективність.

Система захисту інформації повинна бути:

- централізованою – що забезпечує ефективне управління системою з боку керівника й посадових осіб, відповідальних за різні напрямки діяльності підприємства;
- плановою – що об'єднує зусилля різних посадових осіб і структурних підрозділів для виконання поставлених завдань щодо захисту інформації;
- конкретною й цілеспрямованою – розрахованою на захист абсолютно конкретних інформаційних ресурсів, що становлять інтерес для конкуруючих організацій;
- активною – що забезпечує захист інформації з достатнім ступенем наполегливості й можливістю концентрації зусиль на найбільш важливих напрямках діяльності підприємства;
- надійною й універсальною – що охоплює усю діяльність підприємства, пов'язану зі створенням та обміном інформацією.

2.3. Основні методи, сили та засоби, які використовують для організації захисту інформації

Один з найважливіших чинників, що впливає на ефективність системи захисту конфіденційної інформації – є сукупність сил і засобів підприємства, які використовуються для організації захисту інформації.

Сили та засоби різних підприємств відрізняються за структурою, характером та порядком використання. Підприємства, що

працюють із конфіденційною інформацією й вирішують завдання щодо її захисту в рамках повсякденної діяльності на постійній основі, змушені створювати самостійні структурні підрозділи й використовувати високоефективні засоби захисту інформації. Якщо підприємства тільки епізодично працюють із конфіденційною інформацією через її невеликі обсяги, то замість створення підрозділів вони можуть включати у свої штати окремі посади фахівців із захисту інформації. Ці підрозділи й посади є органами захисту інформації.

Підприємства, що працюють із невеликими обсягами конфіденційної інформації, можуть на договірній основі використовувати потенціал більших підприємств, що мають необхідну кількість кваліфікованих співробітників, високоефективні засоби захисту інформації, а також великий досвід практичної роботи в цій сфері.

Провідну роль в організації захисту інформації на підприємстві має керівник підприємства, а також його заступник, що очолює цю роботу.

Керівник підприємства є персонально відповідальним за організацію й проведення необхідних заходів, спрямованих на виключення витоку відомостей, що належать до конфіденційної інформації, і втрат носіїв інформації. Він зобов'язаний:

- знати фактичний стан справ у сфері захисту інформації, організовувати постійну роботу з виявлення й закриття можливих каналів витоку конфіденційної інформації;
- визначати обов'язки й завдання посадовим особам і структурним підрозділам підприємства в цій сфері;
- проявляти високу вимогливість до персоналу підприємства в питаннях збереження конфіденційної інформації;
- оцінювати діяльність посадових осіб і ефективність заходів щодо захисту інформації.

Заступник керівника підприємства зобов'язаний постійно вивчати всі сторони й напрямки діяльності підприємства для прийняття своєчасних заходів щодо захисту інформації; керувати роботою служби безпеки (інших структурних підрозділів, що вирішують завдання щодо захисту інформації); виконувати інші функції з організації захисту інформації в ході проведення підприємством усіх видів робіт. На підприємствах для організації робіт щодо захисту інформації можуть створюватися такі основні види струк-

турних підрозділів:

- режимно-секретні;
- підрозділ з технічного захисту інформації й протидії іноземним технічним розвідкам;
- підрозділ криптографічного захисту інформації;
- мобілізаційний;
- підрозділ охорони і пропускного режиму.

Функції, покладені на перелічені підрозділи, визначаються рішенням (наказом) керівника підприємства та відображаються у відповідних положеннях.

За рішенням керівника підприємства ці підрозділи організаційно можуть поєднуватися в службу безпеки, керівник якої в деяких випадках може бути наділений статусом заступника керівника підприємства й повноваженнями посадової особи, що здійснює керівництво роботою структурних підрозділів підприємства, діяльність яких пов'язана з використанням і захистом інформації.

Режимно-секретний підрозділ, мобілізаційний підрозділ і підрозділ з технічного захисту інформації та протидії іноземним технічним розвідкам створюються на підприємствах, які виконують роботи з використанням відомостей, що становлять державну таємницю (незалежно від наявності на підприємстві іншої інформації з обмеженим доступом).

Режимно-секретний підрозділ є основним структурним підрозділом підприємства й вирішує завдання організації, координації й контролю діяльності інших структурних підрозділів (персоналу підприємства) щодо забезпечення захисту відомостей, які становлять державну таємницю. На підприємствах, що не виконують роботи з відомостями, які становлять державну таємницю, для вирішення аналогічних завдань відповідно інших видів інформації з обмеженим доступом створюється й функціонує служба безпеки (служба захисту інформації).

Підрозділ з технічного захисту інформації й протидії іноземним технічним розвідкам вирішує завдання організації й проведення комплексу технічних заходів, спрямованих на виключення або істотне утруднення добування іноземними розвідками за допомогою технічних засобів відомостей, які належать до конфіденційної інформації.

Підрозділ криптографічного захисту інформації створюється з метою запобігання витоку конфіденційної інформації при її передачі по відкритих каналах (лініям) зв'язку за допомогою технічних засобів, а також при використанні локальних обчислювальних мереж, що мають вихід за межі території підприємства.

Підрозділ охорони і пропускного режиму створюється з метою попередження несанкціонованого (безконтрольного) перебування на території й об'єктах підприємства сторонніх осіб і транспорту, нанесення збитку підприємству шляхом крадіжок (розкрадань) з території підприємства матеріальних засобів і іншого майна. У деяких випадках для рішень завдань охорони й пропускного режиму на підприємствах можуть створюватися окремі самостійні підрозділи.

Мобілізаційний підрозділ вирішує завдання всебічної підготовки підприємства до роботи в умовах воєнного часу.

Крім перелічених підрозділів підприємства, до роботи з організації захисту інформації можуть залучатися й інші структурні підрозділи, для яких виконання заходів щодо захисту інформації не є основною функцією.

До таких підрозділів належать кадровий орган, орган юридичної служби (юрисконсульт), орган психологічної й виховної роботи, пресслужба підприємства та інші. Особливо необхідно зазначити важливість участі в організації захисту інформації виробничих так званих «тематичних» структурних підрозділів (окремих посадових осіб), які створюють продукцію й товари або надають послуги, через це взаємодіють з іншими підприємствами й органами державної влади.

Для проведення робіт з організації захисту інформації використовуються також можливості різних позаштатних підрозділів підприємства, в тому числі колегіальних органів (комісій), які створюються для вирішення специфічних завдань у цій галузі. Серед них – постійна останнім часом технічна комісія, експертна комісія, комісія з розсекречення носіїв конфіденційної інформації, комісія з надання категорій об'єктам інформатизації й ін.

Щоб досягти максимальної ефективності під час вирішення завдань захисту інформації, поряд з можливостями згаданих штатних і позаштатних підрозділів (посадових осіб) необхідно використовувати наявні на підприємстві засоби захисту інформації.

Під засобами захисту інформації розуміють технічні, криптографічні, програмні й інші засоби й системи, розроблені й призначені для захисту конфіденційної інформації, а також засоби, обладнання та системи контролю ефективності захисту інформації.

Технічні засоби захисту інформації – це обладнання (прилади), призначені для забезпечення захисту інформації.

Криптографічні засоби захисту інформації – засоби, що забезпечують захист конфіденційної інформації шляхом її криптографічного перетворення (шифрування).

Програмні засоби захисту інформації – системи захисту засобів автоматизації (комп'ютерів та їх комплексів) від зовнішнього (стороннього) впливу або вторгнення.

Ефективне вирішення завдань організації захисту інформації неможливе без застосування комплексу наявних у розпорядженні керівника підприємства відповідних сил і засобів. Визначальну роль у питаннях організації захисту інформації, застосування сил і засобів підприємства відіграють методи захисту інформації, що визначають порядок, алгоритм і особливості використання цих сил і засобів у конкретній ситуації.

Методи захисту інформації – це застосовувані з метою виключення витоку інформації універсальні й специфічні способи використання наявних сил і засобів (прийоми, заходи) з урахуванням специфіки захисту інформації.

Загальні методи захисту інформації підрозділяють на правові, організаційні, технічні та економічні.

Методи захисту інформації з погляду їх теоретичної основи та практичного використання взаємозалежні. Правові методи регламентують і всебічно нормативно регулюють діяльність щодо захисту інформації, виділяючи, насамперед, її організаційні напрямки. Тісні зв'язки організаційних і правових методів захисту інформації можна показати на прикладі вирішення завдань щодо виключення витоку конфіденційної інформації, що зокрема належить до комерційної таємниці підприємства, при його взаємодії з різними державними й територіальними інспекторськими й наглядовими органами. Ці органи, відповідно до наданих законом повноважень, здійснюють діяльність по одержанню, обробці й зберіганню інформації про підприємства й громадян (співробітників).

Передача інформації, у встановленому порядку віднесеної до комерційної таємниці або до персональних даних працівників підприємства, повинна здійснюватися на основі договору, який передбачає взаємні зобов'язання сторін щодо непоширення (нерозголошення) цієї інформації, а також необхідні заходи для її захисту.

Організаційні механізми захисту інформації визначають порядок і умови комплексного використання наявних сил і засобів, ефективність яких залежить від застосовуваних методів технічного й економічного характеру.

Технічні методи захисту інформації, які використовуються в комплексі з організаційними методами, відіграють більшу роль у забезпеченні захисту інформації під час її зберігання, накопичення й обробки з використанням засобів автоматизації. Технічні методи необхідні для ефективного застосування наявних у розпорядженні підприємства засобів захисту інформації, заснованих на сучасних інформаційних технологіях.

Серед перерахованих методів захисту інформації особливо виділяють організаційні методи, спрямовані на вирішення таких завдань:

- реалізація на підприємстві ефективного механізму керування, що забезпечує захист конфіденційної інформації й недопущення її витоку;
- здійснення принципів персональної відповідальності керівників підрозділів і персоналу підприємства за захист конфіденційної інформації;
- визначення переліків відомостей на підприємстві, що належать до різних категорій (видів) конфіденційної інформації;
- обмеження кола осіб, що мають право доступу до різних видів інформації залежно від ступеня її конфіденційності;
- підбір і вивчення осіб, призначуваних на посади, пов'язані з конфіденційною інформацією, навчання й виховання персоналу підприємства, допущеного до конфіденційної інформації;
- організація й ведення конфіденційного діловодства;
- здійснення систематичного контролю над дотриманням встановлених вимог щодо захисту інформації.

Наведений перелік організаційних методів не є вичерпним і, залежно від специфіки діяльності підприємства, ступені конфіден-

ційності інформації, обсягу робіт, що виконуються, а також досвіду роботи в галузі захисту інформації, може бути доповнений іншими методами.

Контрольні запитання

1. Основні принципи організаційного захисту інформації.
2. Основні умови організаційного захисту інформації.
3. Поняття системи захисту інформації.
4. Пріоритетні напрямки діяльності підприємства під час створення системи захисту інформації.
5. Вимоги до системи захисту інформації.
6. Методи організації захисту інформації.
7. Обов’язки керівника підприємства щодо організації заходів конфіденційності інформації.
8. Види структурних підрозділів для організації робіт щодо захисту інформації на підприємствах.
9. Організаційні механізми захисту інформації.
10. Організаційні методи захисту інформації.

3. ОРГАНІЗАЦІЯ СЛУЖБИ БЕЗПЕКИ

3.1. Функції, завдання та особливості служби безпеки об'єкта

Багатогранність сфери забезпечення безпеки й захисту інформації вимагає створення спеціальної служби, що здійснює реалізацію спеціальних захисних заходів.

Структура, чисельність і склад служби безпеки підприємства (фірми, компанії тощо) визначаються реальними потребами підприємства та ступенем конфіденційності інформації. Залежно від масштабів і потужності організації діяльність щодо забезпечення безпеки підприємства й захисту інформації може бути реалізована від абонентного обслуговування силами спеціальних центрів безпеки до повномасштабної служби безпеки компанії з розвиненою штатною чисельністю.

Основними завданнями служби безпеки підприємства є забезпечення безпеки підприємства, виробництва, продукції й захист комерційної, промислової, фінансової, ділової й іншої інформації, незалежно від її призначення й форм при різноманітті можливих каналів її витоку й різних зловмисних дій з боку конкурентів.

Основні завдання служби безпеки:

- забезпечення безпеки виробничо-торговельної діяльності й захисту інформації й відомостей, що є комерційною таємницею;
- організація роботи із правового, організаційного й інженерно-технічного (фізичного, апаратного, програмного й криптографічного) захисту комерційної таємниці;
- організація спеціального діловодства, що виключає не- санкціоноване одержання відомостей, які є комерційною таємницею;
- запобігання необґрунтованого допуску й доступу до відомостей і робіт, що становлять комерційну таємницю;
- виявлення й локалізація можливих каналів витоку конфіденційної інформації під час повсякденної виробничої діяльності в екстремальних (аварійних, пожежних і ін.) ситуаціях;
- забезпечення режиму безпеки під час виконання всіх видів

діяльності, включно з різними зустрічами, переговорами, нарадами, засіданнями, пов'язаними з діловим співробітництвом як на національному, так і на міжнародному рівнях;

- забезпечення охорони будинків, приміщень, устаткування, продукції й технічних засобів забезпечення виробничої діяльності;
- забезпечення особистої безпеки керівництва, провідних співробітників і фахівців;
- оцінки маркетингових ситуацій і неправомірних дій зловмисників і конкурентів.

Загальні функції служби безпеки:

- організовує та забезпечує пропускний і внутрішньооб'єктний режим у будівлях і приміщеннях, порядок несення служби охорони, контролює дотримання вимог режиму співробітниками, партнерами й відвідувачами;
- керує роботами із правового й організаційного регулювання відносин щодо захисту комерційної таємниці;
- бере участь у розробці основних документів з метою закріплення в них вимог забезпечення безпеки й захисту комерційної таємниці, зокрема Статуту, Колективного договору, Правил внутрішнього трудового розпорядку, Положень про підрозділи, а також трудових договорів, угод, підрядів, посадових інструкцій і обов'язків керівництва, фахівців, робітників та службовців;
- розробляє й здійснює разом з іншими підрозділами заходи щодо забезпечення роботи з документами, які містять відомості, що є комерційною таємницею, при всіх видах робіт, організовує й контролює виконання вимог Інструкції із захисту комерційної таємниці;
- вивчає всі аспекти комерційної, виробничої, фінансової й іншої діяльності для виявлення й закриття можливих каналів витоку конфіденційної інформації, веде облік і аналіз порушень режиму безпеки, накопичує й аналізує дані про зловмисні устремління конкурентів і інших організацій про діяльність підприємства і його клієнтів, партнерів;
- організовує й проводить службові розслідування по фактах розголошення відомостей, втрат документів і інших порушень безпеки підприємства;
- розробляє, веде, обновляє й поповнює «Перелік відомостей, що становлять комерційну таємницю» і інші нормативні акти, які

регламентують порядок забезпечення безпеки й захисту інформації;

- забезпечує суворе виконання вимог нормативних документів щодо захисту комерційної таємниці;
- здійснює керівництво службами й підрозділами безпеки підвідомчих підприємств, організацій, установ і інших у частині застережених у договорах умовах щодо захисту комерційної таємниці;
- організовує й регулярно проводить навчання співробітників підприємства й служби безпеки в усіх напрямках захисту комерційної таємниці, домагаючись, щоб до захисту комерційних секретів був глибоко усвідомлений підхід;
- веде облік сейфів, металевих шаф, спеціальних сховищ і інших приміщень, у яких дозволено постійне або тимчасове зберігання конфіденційних документів;
- веде облік виділених для конфіденційної роботи приміщень та технічних засобів у них, що мають потенційні канали витоку інформації;
- підтримує контакти із правоохоронними органами й службами безпеки сусідніх підприємств в інтересах вивчення криміногенної обстановки в районі (зоні).

3.2. Принципи організації служби безпеки та її типова структура

Для захисту комерційних секретів підприємства створюють власні служби безпеки, важливою передумовою створення яких є розробка їх структури, складу, положень про підрозділи й посадових інструкцій для керівного складу та співробітників.

Служба безпеки (СБ) є самостійною організаційною одиницею, що підпорядкована безпосередньо керівникові підприємства. Така структура керування системою безпеки, що має чітку вертикаль, характерна для забезпечення безпеки, де потрібна визначеність, чіткі границі, регламентація відносин на всіх рівнях – від рядового співробітника до менеджерів вищої ланки. Як показує практика, тільки на підприємствах, де проблеми безпеки перебувають під постійним контролем керівника підприємства, досягають найбільш високих результатів.

Очолює службу безпеки начальник служби на посаді заступни-

ка керівника підприємства з безпеки. До того ж керівник СБ повинен мати максимально можливе коло повноважень, що дозволяють йому впливати на інші підрозділи й різні напрямки діяльності підприємства, якщо цього вимагають інтереси безпеки.

3.3. Права, обов'язки та відповідальність співробітників служби безпеки

Співробітники підрозділів служби безпеки з метою забезпечення захисту відомостей, що становлять комерційну таємницю, мають право:

- вимагати від усіх співробітників підприємства, партнерів, клієнтів суворого й неухильного виконання вимог нормативних документів або договірних зобов'язань щодо захисту комерційної таємниці;
- вносити пропозиції з удосконалювання правових, організаційних і інженерно-технічних заходів щодо захисту комерційної таємниці.

Співробітники служби безпеки зобов'язані:

- здійснювати контроль над дотриманням Інструкції із захисту комерційної таємниці;
- доповідати керівництву про факти порушення вимог нормативних документів щодо захисту комерційної таємниці й інших дій, які можуть призвести до витоку конфіденційної інформації або втрати документів або виробів;
- не допускати неправомірного ознайомлення з документами й матеріалами із грифом «Комерційна таємниця» сторонніх осіб.

Співробітники служби безпеки відповідають за особисте порушення безпеки комерційної таємниці й за невикористання своїх прав під час виконання функціональних обов'язків щодо захисту конфіденційних відомостей співробітників підприємства.

Структура служби безпеки і її чисельність залежать від форми власності підприємства, виду його виробничої діяльності, місця підприємства на ринку товарів і послуг, кількості співробітників, наявності на підприємстві великих матеріальних цінностей, вибухо- і пожежонебезпечних речовин, інформації, що є державною таємницею, активності конкурентів і кримінальних структур.

Тому можна виділити основні структурні підрозділи, які повинні бути у складі СБ великих промислових, державних, акціонерних підприємств, у промислово-фінансових групах, холдингах тощо. Типова структура СБ наведена в табл. 3.1.

Таблиця 3.1

Типова структура служби безпеки

Підрозділ СБ	Внутрішня структура	Функції
Відділ фізичної охорони та режиму	Група охорони Група супроводу Тривожна група Група інженерно-технічного захисту Група режиму Бюро перепусток	Забезпечення фізичної безпеки людей і матеріальних цінностей Забезпечення пропускного й внутрішнього режиму
Відділ безпеки зовнішньої діяльності	Розвідувальна група Контррозвідувальна група Аналітична група	Збір і аналіз розвідувальної інформації
Відділ захисту інформації	Група технічного захисту інформації Група конфіденційного діловодства	Запобігання витоку конфіденційної інформації з охоронюваного об'єкта
Відділ психологічної безпеки		Перевірка благонадійності співробітників. Захист від «внутрішнього» порушника

Наведена структура служби безпеки не універсальна й повинна коректуватися під конкретну організацію. Склад і функції, завдання, права й обов'язки підрозділів служби безпеки визначаються відповідними положеннями й посадовими інструкціями, які регламентують загалом діяльність СБ об'єкта.

3.4. Способи та форми взаємодії служби безпеки об'єкта із правоохоронними органами

Особливу увагу в процесі повсякденної діяльності слід приділяти постійній взаємодії служби безпеки із правоохоронними органами.

Взаємодія між службою безпеки й правоохоронними органами здійснюється з метою:

- захисту від злочинних посягань на майно й інфраструктуру об'єкта засобами та методами оперативно-розшукової, кримінально-процесуальної та приватно-розшукової діяльності;
- захисту організації і його співробітників від злочинних посягань засобами й методами охоронної діяльності;
- розробки й впровадження засобів інженерно-технічного захисту організації та її інфраструктури;
- навчання й підвищення кваліфікації співробітників служб безпеки організації.

У процесі попередження й розкриття злочинів засобами й методами оперативно-розшукової, кримінально-процесуальної й приватної розшукової діяльності визначаються такі напрямки взаємодії:

1. Обмін інформацією:

- про підготовлювані й зроблені злочинні зазіхання на безпеку підприємства, про причетних до них осіб;
- про осіб – учасників організованих злочинних структур, що намагаються вступити в договірні (у тому числі трудові) відносини з підприємством;
- про факти здійснених та нерозкритих злочинів;
- про організовані злочинні структури, діяльність яких заподіяла (може спричинити) збиток безпеки підприємства;
- про осіб, оголошених у розшук через здійснення злочинів;
- про застосовувані злочинцями способи здійснення злочинів та заходи їх маскування, про інші дії, що перешкоджають здійсненню завдань судочинства;
- про ознаки й реквізити підроблених документів і грошових знаків, що використовуються для здійснення злочинів;
- про появу інших обставин, що містять можливу загрозу

безпеці організації;

- про матеріали наукових досліджень і методичних розробок;
- про пропозиції щодо підвищення ефективності інформаційного забезпечення правових, організаційних і методичних заходів боротьби зі злочинною діяльністю.

2. Спільна участь у попередженні й припиненні злочинних зазіхань, що готуються, шляхом:

- розробки й реалізації планів спільних заходів у разі загрози насильницьких злочинних зазіхань на підприємство і його персонал;
- спільної участі в плануванні й організації профілактичної роботи з боротьби зі злочинами й іншими правопорушеннями (на договірній основі);
- надання службою безпеки правоохоронним органам сприяння у виявленні й припиненні дій осіб, що скоюють злочини ненасильницького характеру;
- створення службою безпеки умов для виявлення інформації, що має доказове значення, і її фіксації в установленому законом порядку.

3. Сприяння служби безпеки правоохоронним і слідчим органам під час розслідування злочинів, що посягають на інтереси підприємства, шляхом:

- підготовки матеріалів, які слугують приводом для порушення кримінальної справи;
- участі в розслідуванні порушених кримінальних справах;
- надання правоохоронним органам інформації, яка може стосуватися розслідування по кримінальних справах;
- надання допомоги організаційного й технічного характеру під час слідчих дій на підприємстві.

4. Напрямки взаємодії в процесі захисту підприємства і його співробітників від злочинних зазіхань засобами й методами охоронної діяльності (реалізуються підрозділами позавідомчої охорони МВС на договірній основі):

- охорона майна підприємства співробітниками органів внутрішніх справ;
- сприяння підприємству в розробці заходів для забезпечення його майнової безпеки, а також особистої безпеки його працівників;
- експертна оцінки стану засобів технічного захисту, охорон-

ної, тривожної й пожежної сигналізації підприємства, розробка пропозицій з удосконалювання системи технічного захисту;

- оцінка вразливості майна підприємства від злочинних і інших протиправних зазіхань, надання службі безпеки практичної й методичної допомоги по підвищенню ефективності заходів захисту;
- здійснення технічного нагляду за виконанням проєктних і монтажних робіт з устаткування засобами охоронної сигналізації, використанням приладів і систем охорони відповідно до технічної документації, приймання їх в експлуатацію, обслуговування й ремонт;
- розробка й впровадження спеціальних засобів інженерно-технічного захисту об'єктів власності й інфраструктури підприємства;
- підготовка співробітників служби безпеки;
- навчання співробітників служби безпеки тактиці затримки правопорушників, що зазіхають на охоронюване майно, порядку реалізації пропускного режиму, правилам виробництва огляду речей, транспортних засобів, особистого огляду;
- відпрацьовування зі співробітниками служби безпеки завдань щодо захисту підприємства, організація навчальних тренувань з використання зброї.

Контрольні запитання

1. Функції служби безпеки підприємства.
2. Завдання служби безпеки підприємства.
3. Структура, чисельність служби безпеки підприємства.
4. Принципи організації служби безпеки підприємства.
5. Права та обов'язки співробітників підрозділів служби безпеки підприємства.
6. Мета та взаємодія між службою безпеки і правоохоронними органами.
7. Форми взаємодії служби безпеки підприємства із правоохоронними органами.
8. Напрямки взаємодії в процесі захисту підприємства і його співробітників від злочинних зазіхань.

4. ВІДБІР СПІВРОБІТНИКІВ І РОБОТА З КАДРАМИ

У разі приймання на роботу повинні бути перевірені ідентичність особи, заявлена кваліфікація, точність і повнота біографічних фактів, наявність рекомендацій.

Осіб, яких передбачається прийняти на роботу, пов'язану з активами або процесами, що захищаються, слід перевіряти в частині професійних навичок і оцінки професійної придатності. Рекомендується регулярно виконувати контрольні перевірки співробітників, які вже працюють, а також позапланово у разі виявлення фактів їх позаштатної поведінки або участі в інцидентах інформаційної безпеки.

Увесь персонал організації повинен давати письмове зобов'язання про дотримання конфіденційності, правил корпоративної етики, включно з вимогами стосовно недопущення конфлікту інтересів. Водночас умова про дотримання конфіденційності повинна поширюватися на всю інформацію, що захищається, довірену співробітникові або яка стала йому відомою під час виконання ним службових обов'язків.

Для зовнішніх організацій вимоги щодо ІБ регламентуються положеннями, що включаються в договори (угоди).

4.1. Основні критерії приймання на роботу, пов'язані зі збереженням таємниці

З метою захисту кадрового складу від проникнення осіб із противоправними устремліннями на стадії відбору кандидатів на роботу здійснюють заходи правового, організаційного й пошукового характеру:

а) розробку переліку вимог кваліфікаційного й іншого характеру, пропонованих при прийманні на роботу кандидатам на конкретні посади, а також внутрішнього нормативного акта, що встановлює порядок одержання й перевірки інформації, що характеризує кандидата;

б) збір і перевірку інформації, що характеризує кандидата (зокрема методами приватного розшуку та тестування із застосуванням поліграфа);

в) виявлення законодавчо встановлених обставин, які перешкоджають укладанню трудового договору:

- позбавлення права займати певні посади або займатися певною діяльністю за вироком суду;
- судимість за здійснення злочинів проти власності, господарських і посадових злочинів;
- здійснення протягом року адміністративного правопорушення у сфері торгівлі й фінансів;
- розірвання трудового договору з ініціативи адміністрації через втрату довіри;
- невідповідність дійсності поданих кандидатом анкетних даних, відомостей про колишні місця роботи, про займані посади, про освіту, про кваліфікацію;

г) виявлення ознак негативних соціальних характеристик особистості, що роблять укладання трудового договору з кандидатом небажаним (зв'язки із представниками кримінального світу; конфлікти із законом, правоохоронними органами, кредиторами; характер відносин з колишніми колегами; зловживання алкогольними напоями, вживання наркотиків, токсикоманія, захоплення азартними іграми).

Наступним етапом вибору підходящого кандидата на роботу може бути проведення анкетування й співбесіди. Кінцевим результатом цих заходів є заповнений особовий листок з обліку кадрів (анкета) і оцінний аркуш за результатами співбесіди.

Анкета може бути не тільки загальною, але й спеціально спрямованою на конкретні категорії претендентів, а також на висвітлення тих або тих відомостей їх біографії. Зазвичай вона містить питання про рівень кваліфікації, про рівень спеціальних, економічних і управлінських знань, організаційних навичок, про психологічні якості, про рівень самостійності, суспільної активності, відомості про місця роботи й причини звільнень.

Підсумковий аркуш за результатами співбесіди містить загальну оцінку кандидата, отриману в ході співбесіди на основі оцінок за такими блоками: загальноосвітній рівень, практичний досвід, індивідуальні характеристики, а також зафіксована пропозиція пре-

тендентові (можливі такі: прийняти на роботу, рекомендувати на наступну співбесіду, розглянути кандидата на іншу посаду, відмовити, зарахувати в резерв).

Важливим документом, який підписує співробітник під час приймання на роботу, є угода зі співробітником про нерозголошення конфіденційної інформації підприємства. Продовженням обов'язків співробітника щодо нерозголошення інформації є документ, що підтверджує співробітником даних зобов'язань при звільненні, а саме – заява про підтвердження зобов'язань нерозголошення конфіденційної інформації підприємства при звільненні.

Контрольні запитання

1. Перевірка особи під час прийому на роботу.
2. Критерії та особливості приймання на роботу.
3. Вимоги кваліфікаційного характеру до особи, яку приймають на роботу.
4. Анкетування і співбесіда кандидата на роботу.
5. Угода зі співробітником про нерозголошення конфіденційної інформації про підприємство.

5. ОРГАНІЗАЦІЯ РЕЖИМУ ВСЕРЕДИНІ ОБ'ЄКТА

5.1. Призначення та вимоги режиму всередині об'єкта

Основним завданням служби безпеки стосовно забезпечення режиму й охорони є організація й здійснення заходів щодо забезпечення безпеки діяльності й захисту інформації всіма можливими в конкретних умовах способами й засобами.

З метою забезпечення надійної охорони матеріальних цінностей, конфіденційних документів і інформації, що містить відомості комерційного характеру, а також своєчасного попередження несанкціонованого доступу до них, установлюється певний режим діяльності, дотримання якого обов'язкове для всіх співробітників, відвідувачів і клієнтів.

Керівники та співробітники фірми, що забезпечують режим і охорону, керуються у своїй діяльності відповідними законодавчими та нормативними документами.

Основними завданнями організації режиму охорони є:

- попередження проникнення в службові приміщення, в охоронні зони та на територію об'єкта сторонніх осіб;
- забезпечення порядку внесення (винесення), ввезення (вивезення) матеріальних цінностей і входу (виходу) співробітників і клієнтів.

Усі приміщення фірми залежно від призначення й характеру здійснюваних у них актів, дій або операцій розділяють на кілька зон доступності (безпеки), які враховують ступінь важливості різних частин об'єкта з погляду можливого збитку від кримінальних загроз. Зони безпеки розташовуються послідовно, від паркану на території об'єкта до сховища цінностей і інформації, створюючи ланцюг перешкод, які доведеться долати зловмиснику.

Внутрішньооб'єктний режим – це встановлений на фірмі порядок виконання правил внутрішнього трудового розпорядку, спрямованих на забезпечення загальної та економічної безпеки, збереження матеріальних ресурсів і захисту конфіденційної інфор-

мації.

Внутрішньооб'єктний режим передбачає такі основні вимоги:

- установлення чіткого розпорядку робочого часу;
- суворе дотримання співробітниками правил економічної й інформаційної безпеки, правил протипожежної й протиаварійної безпеки та техніки безпеки;
- установлення порядку приймання й роботи з відвідувачами сторонніх організацій;
- забезпечення фірми технічними засобами забезпечення виробничої діяльності (зв'язок, автоматизація, охоронна й пожежна сигналізація, замки, огородження та ін.);
- порядок здачі й приймання приміщень під охорону;
- порядок ведення телефонних, факсових і телекомунікаційних обмінів інформацією з дотриманням режиму конфіденційності й економії.

Робота із представниками сторонніх організацій здійснюється в такому порядку:

- фахівець, що приймає «гостей», напередодні робить заявку на наступний день із вказівкою ПІБ тих, хто прибувають, їх місце роботи й час прибуття;
- у день прибуття запрошених канцелярія (або інший підрозділ) фіксує їх прибуття в журналі обліку відвідувачів і запрошує фахівця фірми;
- фахівець зустрічає прибулих, одержує в канцелярії ключі від кімнати переговорів і супроводжує відвідувачів. Забороняється приймання представників сторонніх організацій в інших приміщеннях офісу без спеціального на те дозволу директора або його заступника;
- у ході роботи необхідно щільно зачиняти вікна і закривати штори;
- по закінченню роботи з відвідувачами, спеціаліст що їх супроводжує, проводжає гостей до виходу з офісу й робить у журналі обліку відвідувачів відповідні замітки про час їх виходу. Під час прибування відвідувачів фахівець, що їх супроводжує, повинен контролювати їхнє перебування та дії. Після завершення зустрічі фахівець фірми закриває кімнату переговорів і здає ключі від неї у відповідне місце.

Перелік предметів, заборонених до принесення/привезення на

територію організації, наявний у посадовій інструкції начальника зміни (начальника варти) сектору охорони. Цей документ розробляють співробітники служби безпеки організації за підписом начальника служби безпеки організації. Після того документ підписують співробітники юридичного відділу організації.

5.2. Визначення межі контрольованої зони

Контрольована зона (КЗ) – це територія об'єкта, на якій виключено неконтрольоване перебування осіб, що не мають постійного або разового доступу.

Контрольована зона може обмежуватися периметром охоронюваної території частково, охоронюваною територією, що охоплює будівлі і споруди, у яких проводяться закриті заходи, частини будівель, кімнат, кабінетів, у яких проводяться закриті заходи.

Контрольована зона може встановлюватися на більшій частині охоронюваної території та забезпечує постійний контроль за територією, яка не підлягає охороні. У контрольованій зоні за допомогою проведення технічних і режимних заходів повинні бути створені умови, які запобігають можливості витоку з неї конфіденційної інформації.

Постійна контрольована зона – це зона, межі якої установлюють на тривалий строк.

Тимчасова контрольована зона – це зона, установлювана для проведення закритих заходів разового характеру.

5.3. Вимоги розмірів контрольованої зони захисту перехоплення побічних електромагнітних випромінювань

Згідно з вимогами нормативних документів технічного захисту інформації (НДТЗІ) повинна забезпечуватися контрольована зона таких розмірів:

- першої категорії універсального об'єкта потрібно 50 м контрольованої зони;
- другої категорії об'єкта потрібно 30 м;
- третьої категорії об'єктів потрібно 15 м контрольованої

зони.

- Також потрібен певний розмір контрольованої зони для різних типів спеціалізованих об'єктів (СО), табл. 5.1.

Таблиця 5.1

Розмір контрольованої зони різних типів спеціалізованих об'єктів

Тип спеціалізованих об'єктів (СО)	Контрольована зона (КЗ), м
1	250
2	100
3	50
4	45
5	40
6	35
7	30
8	20
9	15

5.4. Вимоги до приміщень, у яких знаходиться інформація обмеженого доступу

Приміщення, у якому знаходиться інформація, що захищається, повинне бути в контрольованій зоні, обладнане надійними автоматичними замками, засобами сигналізації та контролю доступу, а також постійно бути під охороною або наглядом, що виключає можливість безконтрольного проникнення в приміщення сторонніх осіб.

Прибирання приміщень із установленими в них комп'ютерами повинно виконуватися тільки з дозволу відповідального, за яким закріплені ці технічні засоби, або з дозволу чергового по підрозділу з дотриманням заходів, що виключають доступ сторонніх осіб до ресурсів, які захищаються.

У приміщеннях під час обробки на комп'ютерах інформації обмеженого доступу повинен бути присутнім тільки персонал, допущений до роботи з цією інформацією. Забороняється приймання відвідувачів у приміщеннях, коли здійснюється обробка інформації, що захищається.

По закінченню робочого дня приміщення із установленими захищеними комп'ютерами, серверами, мережевим і комутаційним устаткуванням повинні здаватися під охорону на підставі спеціально розробленої інструкції, затвердженої керівництвом служби безпеки організації.

Для зберігання службових документів і машинних носіїв з інформацією, що захищається, приміщення забезпечуються сейфами й металевими шафами.

Приміщення повинні бути забезпечені засобами знищення документів.

5.5. Атестація об'єктів інформатизації

Під атестацією об'єктів інформатизації розуміють комплекс організаційно-технічних заходів, у результаті яких за допомогою спеціального документа – «Атестата відповідності» підтверджується, що об'єкт відповідає вимогам стандартів або інших нормативно-технічних документів з безпеки інформації, затверджених ДСТК (Держтехкомісія) України.

Наявність на об'єкті інформатизації чинного «Атестата відповідності» надає право обробки інформації з рівнем таємності (конфіденційності) і на той період часу, який установлений в «Атестаті відповідності».

Під час атестації об'єкта інформатизації підтверджується його відповідність вимогам щодо захисту інформації від несанкціонованого доступу, у тому числі від комп'ютерних вірусів, від витоку за рахунок побічних електромагнітних випромінювань і застосувань при спеціальних впливах на об'єкт (високочастотне нав'язування і опромінення, електромагнітні і радіаційні спеціальні обладнання, вбудовані в об'єкти інформатизації.

Атестація передбачає комплексну перевірку (атестаційні випробування) об'єкта інформатизації, що захищається, в реальних умовах експлуатації з метою оцінки відповідності застосовуваного комплексу заходів і засобів захисту необхідному рівню безпеки інформації.

Атестацію здійснює орган з атестації у встановленому порядку відповідно до схеми, обраної цим органом під час підготовки до

атестації з основного переліку робіт:

- аналіз вихідних даних щодо об'єкту інформатизації, що атестується;
- попереднє ознайомлення з об'єктом інформатизації, що атестується;
- експертне обстеження об'єкта інформатизації й аналіз розробленої документації щодо захисту інформації на цьому об'єкті з погляду її відповідності вимогам нормативної й методичної документації;
- проведення випробувань окремих засобів і систем захисту інформації на об'єкті інформатизації, що атестується, за допомогою спеціальної контрольної апаратури й тестових засобів;
- проведення випробувань окремих засобів і систем захисту інформації у випробувальних центрах (лабораторіях) по сертифікації засобів захисту інформації з вимог безпеки інформації;
- проведення комплексних атестаційних випробувань об'єкта інформатизації в реальних умовах експлуатації;
- аналіз результатів експертного обстеження й комплексних атестаційних випробувань об'єкта інформатизації й затвердження висновку за результатами атестації.

5.6. Визначення категорій приміщень

Усі приміщення фірми залежно від призначення й характеру актів, що у них відбуваються, дій або операцій розділяють на кілька зон доступності (класів безпеки), які враховують ступінь важливості різних частин об'єкта з погляду можливого збитку від кримінальних загроз. Зони безпеки розташовують послідовно, від паркану на території об'єкта до сховища цінностей і інформації, створюючи ланцюг перешкод, що доведеться долати зловмисникові.

Для визначення категорії приміщення створюється комісія, що складається з голови й не менше ніж трьох членів. У результаті дії комісії створюється Акт визначення категорії приміщення. Повторні визначення категорії приміщення проводять щорічно.

Таблиця 5.2

Класифікація категорій приміщень

Клас категорії приміщень	Найменування категорії	Функціональне призначення	Умови доступу співробітників	Умови доступу відвідувачів	Наявність охорони	Наявність технічних засобів охорони
0	Вільна	Зона вільного відвідування	Вільний	Вільний	Немає	Немає
1	Спостережена	Зона приймання відвідувачів	Вільний	Вільний	Обмежена	Засоби спостереження й запису
2	Реєстраційна	Зона службових приміщень і кабінетів співробітників	Обмежений службовою потребою	Реєструється за разовою перепусткою	В окремих зонах	Засоби охорони й контролю
3	Режимна	Зона керуючого складу спеціальних підрозділів, фінансових служб	Суворо обмежений	Реєструється за разовими перепустками із супроводженням	Посилена багатозональна	Засоби охорони, контролю й спостереження

Акт визначення категорій приміщення містить такі пункти:

- вищий гриф таємності інформації, яка знаходиться в приміщенні, що захищається;
- обсяг інформації з вищим грифом секретності, що знахо-

диться в приміщенні;

- підстава для визначення категорії приміщення;
- раніше встановлена категорія;
- встановлена категорія.

На підставі вищевказаних класів визначають категорії приміщень в умовах конкретної організації.

5.7. Забезпечення режиму в приміщеннях, що захищаються

Забезпечення режиму в приміщенні, що захищається, зводиться в основному до регламентації доступу й використання технічних засобів забезпечення виробничої й трудової діяльності й обробки конфіденційної інформації в традиційних або автоматизованих режимах. Забезпечення режиму, здійснюють силами служби безпеки шляхом використання найпростіших організаційних заходів і доступних для цього технічних засобів.

Забезпечення режиму передбачає:

- визначення категорій приміщень;
- визначення границь контрольованої зони;
- визначення технічних засобів, використовуваних для обробки конфіденційної інформації в межах контрольованої зони;
- визначення небезпечних з погляду можливості створення каналів витоку інформації або способів *несанкціонованого доступу* (НСД) до неї через технічні засоби;
- реалізацію заходів локалізації або заборони можливих каналів витоку конфіденційної інформації або способів НСД до неї;
- організацію контролю (пошуку й виявлення) можливого неконтрольованого випромінювання небезпечних сигналів за рахунок *побічних електромагнітних випромінювань і наведень* (ПЕМВН) або спеціально використовуваних для цього сигналів;
- організацію системи допуску персоналу в контрольовану зону;
- організацію суворого контролю проходу й пронесення будь-яких предметів, обладнань, засобів, механізмів у контрольовану зону, що можуть бути технічними засобами одержання й передачі конфіденційної інформації.

У межах системи допуску персоналу в контрольовану зону

встановлюють таке:

- право входу в контрольовану зону;
- час входу в контрольовану зону;
- предмети, обладнання, засоби, механізми, які дозволено пронести в контрольовану зону;
- час перебування в контрольованій зоні;
- предмети, обладнання, засоби, механізми, які дозволено винести з контрольованої зони.

У межах системи допуску до інформації встановлюють: хто, кому, яку інформацію й для якого типу доступу може надати й за яких умов; система розмежування доступу, яка припускає визначення для всіх користувачів автоматизованої інформаційної системи інформаційних і програмних ресурсів, доступних їм для конкретних операцій (читання, запис, модифікація, видалення, виконання) за допомогою заданих програмно-технічних засобів доступу.

Допуск співробітників організації до роботи з автоматизованою системою й доступ до її ресурсів повинен бути суворо регламентований. Будь-які зміни складу й повноважень користувачів підсистем повинні здійснюватись встановленим порядком згідно з Інструкцією із внесення змін у списки користувачів і наділенню їх повноваженнями доступу до ресурсів системи, зумовленою політикою безпеки організації. Основними користувачами є співробітники організації.

Рівень повноважень кожного користувача визначається індивідуально шляхом дотримання таких вимог:

- відкриту та конфіденційну інформацію розміщають на різних серверах (це спрощує забезпечення захисту);
- кожний співробітник користується тільки запропонованими йому правами стосовно інформації, з якою він працює відповідно до посадових обов'язків;
- начальник має право на перегляд інформації своїх підлеглих тільки у встановлених межах згідно з посадовими обов'язками;
- найбільш відповідальні технологічні операції повинні виконувати за правилом «у дві руки» – правильність уведеної інформації підтверджується іншою посадовою особою, що не має права введення інформації.

Усі співробітники, допущені до роботи (користувачі), та обслуговуючий персонал повинні нести персональну відповідальність

за порушення встановленого порядку автоматизованої обробки інформації, правил зберігання, використання й передачі ресурсів системи, що перебувають у їхньому розпорядженні та захищаються. Обробка інформації, що захищається в підсистемах, повинна здійснюватися відповідно до затверджених технологічних інструкцій для цих підсистем.

Для користувачів захищених комп'ютерів (на яких обробляють інформацію, що захищається, або які розташовують у захищених підсистемах, на яких установлені відповідні засоби захисту) повинні бути розроблені необхідні технологічні інструкції, що містять вимоги щодо забезпечення безпеки інформації.

Контрольні запитання

1. Завдання служби безпеки щодо забезпечення режиму й охорони на підприємстві.
2. Своєчасне попередження несанкціонованого доступу до конфіденційних документів та інформації.
3. Особливості внутрішньооб'єктного режиму.
4. Порядок здійснення роботи із представниками сторонніх організацій.
5. Перелік предметів, заборонених до пронесення/провезення на територію організації.
6. Визначення поняття контрольована зона.
7. Постійна та тимчасова контрольована зона.
8. Вимоги розмірів контрольованої зони захисту перехоплення побічних електромагнітних випромінювань.
9. Обладнання приміщень, в яких зберігається конфіденційна інформація.
10. Комплекс організаційно-технічних заходів щодо атестації об'єктів інформатизації.
11. Класифікація категорій приміщень щодо розділу на зони безпеки.
12. Регламент доступу щодо забезпечення режиму в приміщенні, що захищається.

6. РОБОТА З ВІДВІДУВАЧАМИ

Відсутність порядку в роботі з відвідувачами часто стає причиною витоку комерційної таємниці. Серед першочергових заходів – облік відвідувачів, порядок відвідування ними виробничих приміщень, порядок ведення переговорів.

Мета встановленого порядку ведення переговорів з відвідувачами: по-перше, не допустити витоку комерційної таємниці, а по-друге, одержати найбільш повну інформацію про наміри відвідувачів.

Якщо на підприємстві встановлений і діє пропускний режим, то облік відвідувачів входить у функції бюро перепусток і не становить особливих труднощів. У разі відсутності бюро перепусток обов'язки щодо обліку відвідувачів покладають на працівників кадрових підрозділів або чергового по кімнаті приймання відвідувачів, які ведуть спеціальний журнал обліку відвідувачів. Записи в журналі повинні робитися особисто фахівцем, відповідальним за приймання відвідувачів, тому що допуск до ведення журналу сторонніх загрожує витоку важливої інформації про зв'язки підприємства.

Обов'язковим моментом у роботі з відвідувачами є наявність супровідників, які залишаються поруч з ними ввесь період знаходження на підприємстві. Важливим елементом підтримки встановленого режиму є інструктаж персоналу з вимогою не видавати жодної інформації відвідувачу без супроводу.

Мінімальний обсяг правил роботи з відвідувачами, до яких можна віднести:

- усі відвідувачі знаходяться в суворо визначених кімнатах;
- у разі потреби відвідування основних робочих приміщень відвідувачів не залишають одних;
- на час знаходження в приміщенні відвідувача повинна бути припинена робота з документами, що не стосуються цієї бесіди (документи заздалегідь прибирають зі столу в сейф), з базами даних комп'ютерів, відкладені переговори зі співробітниками та телефонні розмови стосовно службових питань.

6.1. Порядок ведення переговорів

Після підписання договору про співробітництво під час ділових переговорів може виникати потреба передачі партнерові інформації, що містить комерційну таємницю. Це повинно бути оформ-

лено юридично. Винятки, що допускаються в такій ситуації, одночасно ґрунтуються на:

- взаємному обміні такою інформацією;
- довгочасних довірчих відносинах між фірмами й можливості контролювати дотримання партнером правил конфіденційності;
- наявності спільного інтересу в збереженні виробничих секретів і ймовірності серйозних матеріальних втрат для кожної зі сторін, що беруть участь, у разі втрати комерційної інформації.

Окремої уваги потребують засідання, де серед учасників конференцій, семінарів представники фірми виступають із повідомленнями. Найбільшу небезпеку має час «питань до доповідача». Необхідно також звертати увагу на ведення переговорів по телефону, тому що, крім підслуховування, існує елементарне вивідування, а приятеля або родича не потрібно обтяжувати зайвою для нього інформацією.

Телефонні розмови повинні бути короткі. Краще призначати для переговорів особисту зустріч і скоротити інформацію про зміст роботи фірми, яка не входить у рекламний проспект.

Схоронність комерційної таємниці більшою мірою залежить від секретаря, осіб, відповідальних за зв'язок із громадськістю й пресою, а також за контакти із клієнтами. Цих осіб потрібно проінструктувати про правила спілкування по телефону, а саме:

- виключення повідомлення відомостей про точне місце знаходження керівника фірми, планах його пересування;
- виключення пояснень, що підтверджують, заперечують або уточнюють нібито зроблені заяви в пресі, на зустрічі тощо;
- відмова в інформації про склад учасників переговорів, про замовлення, угоди й інше тільки на підставі того, що хтось дзвонить по телефону та представляється їх учасником;
- необхідно ввести правило, щоб секретар під час відсутності директора повідомляв про готовність передати йому тільки сутність прохання й координати особи, яка звертається.

Контрольні запитання

1. Чи може бути відсутність порядку в роботі з відвідувачами причиною витоку комерційної таємниці?
2. До функцій якого підрозділу входить облік відвідувачів?
3. Хто повинен робити записи в журналі відвідувачів?
4. Що є обов'язковим моментом у роботі з відвідувачами?
5. Яких правил повинен дотримуватись секретар керівника для зберігання комерційної таємниці?

7. ОРГАНІЗАЦІЯ ОХОРОНИ ОБ'ЄКТІВ

Під охороною об'єкта розуміють комплекс оперативно-режимних, організаційно-управлінських та інженерно-технічних дій, проведених з метою забезпечення схоронності матеріально-технічних і фінансових коштів власника. Охороні підлягають усі матеріальні цінності незалежно від їх місця розташування (усередині або за межами об'єкта).

Охорона об'єкта протистоїть свідомим діям порушників. Метою охорони є забезпечення надійного захисту будинків, приміщень, устаткування, валютних і матеріальних цінностей, а також особистої охорони керівного складу у звичайних і екстремальних умовах.

До завдань охорони належать:

1. Попередження несанкціонованих дій (профілактика) усіма можливими способами.
2. Своєчасне виявлення несанкціонованих дій. Це може бути не тільки проникнення через периметр об'єкта, але й будь-які інші несанкціоновані дії, які може мати на меті правопорушник.
3. Затримка проникнення порушника. Уповільнення виконання ним будь-якої поставленої мети. Цей час необхідний охороні на відповідну реакцію.
4. Припинення несанкціонованих дій – це головне завдання охорони, тобто силової збройної відповідної дії.
5. Затримка осіб, причетних до підготовки (здійснення) диверсії або розкрадання матеріальних цінностей з об'єкта.

Зона об'єкта, яка знаходиться під охороною – ділянка території об'єкта під охороною, обладнана фізичними бар'єрами, що перебуває під охороною та наглядом, доступ до якого обмежується та контролюється.

Реалізацію життєво важливих інтересів будь-якого підприємства (об'єкта) забезпечують його корпоративні ресурси. Ці ресурси повинні бути надійно захищені від прогнозованих загроз безпеки.

Для промислового підприємства такими важливими для життєдіяльності ресурсами, а отже, предметами захисту й охорони є:

1. Люди (персонал підприємства).
2. Важливе або дефіцитне технологічне устаткування.
3. Секретна та конфіденційна документація.

4. Матеріальні та фінансові цінності.
5. Готова продукція.
6. Інтелектуальна власність (ноу-хау).
7. Засоби обчислювальної техніки (ЗОТ).
8. Контрольно-вимірювальні прилади (КВП) і ін.
9. Конфіденційна інформація на матеріальних носіях, а також інформація, яка циркулює у внутрішніх комунікаційних каналах зв'язку, у кабінетах керівництва підприємства, на нарадах і засіданнях.
10. Фінансово-економічні ресурси, що забезпечують ефективний та сталий розвиток підприємства (капітал, комерційні перспективи, бізнес-плани, договірні документи і зобов'язання тощо).

Втрата перерахованих ресурсів може призвести до:

1) великого матеріального збитку;
2) створення загроз для життя та здоров'я людей;
3) розголошення конфіденційної інформації або відомостей, що мають державну таємницю;
4) банкрутства підприємства.

7.1. Склад системи охорони

Люди і засоби інженерного захисту та технічної охорони об'єктів утворюють систему охорони.

Підсистема інженерного захисту призначена для механічного запобігання проникненню зловмисника до об'єктів захисту. Вона має інженерні конструкції, що створюють механічні перешкоди на шляху зловмисника, і комплекси керування доступом людей і автотранспорту на територію, що охороняється.

Підсистема виявлення повинна сповіщати співробітників служби безпеки, насамперед, охоронців, органів позавідомчої охорони, поліцію, пожежну охорону про проникнення зловмисників на охоронювану територію, про пожежу або інші стихійні лиха, захист від яких передбачено завданнями системи. Основу цієї підсистеми становлять технічні засоби охорони.

Усе ширше застосовуються відеозасоби спостереження, які складають основу підсистеми спостереження. До неї належать також засоби чергового освітлення, що забезпечують необхідний рівень освітленості охоронюваної території в нічний час. Підсистема

спостереження забезпечує можливість візуального дистанційного контролю над охоронюваною територією та діями зловмисників.

Підсистема нейтралізації загроз має у своєму складі людей і засоби для фізичного та психологічного впливу на зловмисників, які проникають на охоронювану територію, а також засоби гасіння пожеж.

7.2. Об'єкти охорони

Найбільш велику групу охоронюваних об'єктів становлять стаціонарні та рухливі (але стаціонарно встановлені) об'єкти, які є орендовані або перебувають у власності акціонерних підприємств чи приватних фірм.

Усі об'єкти можна розділити на дві великі групи:

1. *Особливо важливі об'єкти* – підприємства, через які проходять матеріальні цінності (МЦ) стратегічного значення (ядерні та збройові матеріали; токсичні, наркотичні та отруйні речовини; енергоносії; зброя та боєприпаси тощо) особливо високої грошової (грошові знаки, дорогоцінні метали і т. ін.), інформаційної, культурно-історичної або духовно-моральної цінності, коли можливий збиток максимальний, а за значенням і масштабом порушення режиму руху МЦ може мати катастрофічні наслідки транскордонного, національного або регіонального рівнів.

2. *Промислово-комерційні об'єкти* – підприємства, компанії, банки, корпорації тощо, у яких можливий збиток від порушення руху МЦ має майновий, переважно комерційний характер, що призводить до фінансово-економічних втрат і до зниження ефективності життєдіяльності суб'єктів господарювання (власників) підприємства.

Також охоронювані стаціонарні об'єкти можна класифікувати в такий спосіб:

1. За розміром об'єкта, площі його території:

а) малі об'єкти (до 100 м^2) – квартири, малі офіси, об'єкти, що знаходяться окремо: торговельні намети та ларьки, розташовані в прибудовах будинків (наприклад, в одній із прохідних арок адміністративного або житлового будинку), у колишніх службових приміщеннях тощо;

б) *середні об'єкти (від 100 до 500 м^2)* – великогабаритні квартири в будинках поліпшеного планування, частини будинку з на-

двірними будівлями та присадибною ділянкою, що окремо розміщено або прилягають до інших будинків, офіси разом зі складами та виробничими приміщеннями, великі пункти обміну валюти, невеликі комерційні банки, автостоянки місткістю до 50…60 автомашин тощо;

в) *великі стаціонарні об'єкти (500…4000 м^2)* – середні підприємства із чисельністю до 300…400 осіб, бази зберігання продукції, великі автомобільні стоянки, склади тощо;

г) *дуже великі стаціонарні об'єкти (площею більше ніж 4000 м^2)* – великі промислові (акціонерні) підприємства, фермерські господарства, великі бази.

2. *За режимом роботи персоналу об'єкта*:

а) об'єкти, персонал яких працює в одну зміну;

б) об'єкти, що працюють у дві зміни;

в) об'єкти, що працюють цілодобово.

3. За районом розташування об'єкта, який охороняється:

а) об'єкти, розташовані поза основною промисловою, виробничою або охоронюваною зоною, наприклад, склад підприємства на залізничній станції, склад сировини (наприклад, будматеріали) на під'їзних шляхах підприємства;

б) об'єкти в окремих будинках або тих, що займають частину іншого приміщення чи території (наприклад, кілька кімнат або квартир у будинку, поверх або крило будинку):

- у виробничій зоні;
- на охоронюваній або поблизу від охоронюваної території;
- поряд із криміногенними об'єктами (ринки, ресторани, вокзали).

4. *За технічним зміцненням об'єкта*:

а) дуже добре зміцнені об'єкти, що практично не мають уразливих місць;

б) добре зміцнені об'єкти, що мають невелику кількість вразливих місць, які відомі охороні та контролюються її працівниками;

в) слабко зміцнені об'єкти, що мають велику кількість вразливих місць, багато з яких охорона не контролює.

5. *За типом охорони*:

а) об'єкти із простим типом охорони (шляхом періодичного обходу охоронюваної території без використання вогнепальної зброї та спеціальних засобів);

б) об’єкти з ускладненим типом охорони (співробітники використовують спеціальні засоби та службових собак, частина приміщень на охоронюваному об’єкті виведена на пульт централізованого спостереження);

в) об’єкти з комбінованим типом охорони (для патрулювання об’єкта використовують автотранспорт, охоронці екіпіровані вогнепальною зброєю та спеціальними засобами, використовують собак, найбільш значущі приміщення обладнані засобами відеоконтролю території об’єкта).

Ця класифікація може бути використана для визначення вартості послуг приватної охорони, для прогнозування кримінальних ситуацій на об’єкті. Для вирішення цих та інших питань також варто враховувати вид товарно-матеріальних цінностей, що перебувають на об’єкті, придатність об’єкта для роботи охорони.

7.3. Пости охорони та забезпечення зв’язку

У практиці охорони використовують два види постів: стаціонарний і обхідний. На ділянках з великою довжиною охорона використовує вело-, мото- або автопатрулі.

Стаціонарним вважається такий пост, на якому здійснюють охорону одного відособленого об’єкта або декількох об’єктів на відкритому майданчику або обгородженій території, якщо загальна протяжність обходу їх постовим не перевищує 150 м.

У практиці охорони слід використовувати як відкриті, так і закриті стаціонарні пости, тобто такі, на яких охоронця не видно з боку території, що суміжна або прилягає до охоронюваного об’єкта.

Обхідним постом уважається пост, на якому охорона одного або декількох об’єктів здійснюється шляхом їхнього обходу, коли довжина маршруту становить понад 150 м, але не більше ніж 1500 м.

Під час виставляння постів треба забезпечити:

а) максимально повний контроль над охоронюваним будинком, приміщенням або територією (ділянкою місцевості);

б) можливість візуального контролю охоронцем одного поста хоча б частини території сусіднього поста;

в) можливість взаємодопомоги сусідніх постів;

г) зв'язок охоронців один з одним і зі старшим зміни.

У практиці охорони застосовують такі прийоми контролю та огляду охоронюваного об'єкта:

– Фронтальний огляд об'єкта, за яким частина охоронців рухається в одному напрямку до межі охоронюваного об'єкта, а потім – у зворотний бік.

– Огляд об'єкта назустріч один одному, за яким охоронці рухаються від межі об'єкта до центру (точка зустрічі), після чого знову розходяться в напрямку периметра охоронюваного об'єкта.

– Концентричний і ексцентричний спосіб контролю та огляду об'єкта, за яким один або два охоронці рухаються по спіралі від центру охоронюваної території на периферію, і навпаки.

– Послідовний огляд окремих ділянок охоронюваного об'єкта по складній траєкторії залежно від планування та конструкції об'єкта.

– Вибірковий огляд ділянок об'єкта залежно від значущості збережених товарно-матеріальних цінностей, наявності на об'єкті вразливих місць.

– Рух по об'єкту з постійно змінним маршрутом застосовують у складних ситуаціях для запобігання нападу на охоронця.

– Рух по об'єкту з тимчасовими зупинками та оглядом уразливих місць і інших ділянок із закритого поста (із засідки).

Практично всі служби безпеки та охорони у своїй діяльності використовують радіозв'язок для організації взаємодії та управління співробітниками.

Під час охорони об'єктів повинно бути забезпечення зв'язку як усередині охоронюваного об'єкта, так і за його межами. Щоб уникнути небажаних контактів охоронців із кримінальними елементами, пости на об'єкті повинні бути обладнані тільки внутрішнім зв'язком зі старшим зміни (або з начальником варти). Якщо ж на охоронюваному об'єкті тільки один пост, то його слід обладнати як внутрішнім зв'язком з ділянками або відділами підприємства (організації), так і зовнішнім зв'язком. Значною мірою негативних контактів охоронців під час телефонних розмов можна уникнути за рахунок використання на об'єкті засобів радіозв'язку, по каналах якого легше контролювати переговори.

У цей час для зв'язку найчастіше використовують транкінгові системи. Обсяг і якість послуг на основі цих систем відповідає ви-

могам служб безпеки та оренда ресурсів цих систем є єдиним рішенням, особливо де щільність абонентів досить висока, а радіочастотний ресурс практично відсутній.

7.4. Технічні засоби охорони та відеоспостереження об’єкта

Для збільшення ефективності охорони на об’єкті можуть використовуватися такі види технічних засобів:

- засоби затримки;
- засоби охоронної сигналізації;
- засоби контролю доступу;
- обладнання тривожної сигналізації;
- прилади, що реєструють винесення заборонених матеріалів і виробів;
- засоби спостереження за приміщеннями та територією;
- обладнання, що контролюють правильність виконання посадовими особами обов’язків;
- прилади-пастки;
- засоби обліку та нагромадження даних з питань безпеки.

Усі перелічені обладнання можуть працювати незалежно та самостійно, але можуть і поєднуватися в так звані інтегровані системи безпеки, а також можуть бути складовою частиною комплексних систем управління будинками та приміщеннями.

Система сертифікації технічних засобів захисту та охорони об’єктів відіграє велику роль щодо підвищення рівня безпеки життя та діяльності підприємств. Наявність сертифіката якості на виробі захисної техніки серйозно підвищує його авторитет і конкурентоспроможність.

Розвиток міжнародної інтеграції та кооперації привів до створення міжнаціональних стандартів. Зокрема, останнім часом розробляється та впроваджується в межах Європейського комітету зі стандартизації ціла серія стандартів на такі вироби, як сейфи, замки підвищеної надійності та таємності, системи контролю доступу, системи охоронної сигналізації тощо.

Подібно тому, як функції, покладені на фізичну охорону, визначають вид і кількість постів охорони, так і функції, покладені на технічні засоби, визначать склад цих засобів і вимоги, які будуть закладені в основу проєктування технічної системи захисту. Розг-

лянемо функції, які можуть бути покладені на сучасні системи технічного захисту:

- блокування приміщень, які повинні контролюватися із центрального поста охорони;
- забезпечення затримки осіб, що не мають права безперешкодного проходу в охоронювані приміщення;
- ідентифікація особистості співробітників і відвідувачів, яким надано право проходу в охоронювані приміщення;
- реєстрація спроб пронесення на територію об'єкта заборонених речовин і предметів (радіоактивні ізотопи, зброя, вибухові речовини та ін.);
- контроль цілісності комунікацій і працездатності апаратури системи технічного захисту;
- збір, обробка та відображення в наочній формі інформації, що надходить із охоронюваної території на центральний пункт охорони;
- реєстрація спроб позаштатного обігу з технічними засобами охорони персоналу об'єкта і відвідувачів;
- виявлення каналів витоку інформації з об'єкта із використанням технічних засобів;
- контроль правильності несення служби персоналом охорони й реєстрація фактів відхилення від запропонованого порядку поведінки під час охорони;
- нагромадження оперативної інформації із усіх подій, пов'язаних із забезпеченням безпеки з ієрархією доступу та накопиченням відомостей.

Необхідність виконання перерахованих вище функцій визначає перелік вимог до технічних засобів охорони та контролю.

Контрольні запитання

1. Перелічіть основні завдання охорони об'єкта.
2. З чого складається система захисту об'єкта?
3. Призначення системи інженерного захисту.
4. Призначення підсистеми виявлення.
5. Призначення підсистеми нейтралізації загроз.
6. На яки дві групи можна розділити усі об'єкти?
7. У який спосіб можна класифікувати охоронювані стаціонарні об'єкти?
8. Які пости використовують в практиці охорони об'єктів?
9. Які прийоми контролю та огляду охоронюваного об'єкта застосовують в практиці охорони?

8. ОРГАНІЗАЦІЯ ПРОПУСКНОГО РЕЖИМУ

8.1. Поняття пропускного режиму

Побудова надійної системи безпеки підприємства – складний і багатогранний процес. Одним з важливих чинників забезпечення надійного захисту об'єкта є організація та підтримка певного контрольно-пропускного режиму.

Контрольно-пропускний режим – це комплекс організаційно-правових обмежень і правил, що встановлює порядок пропуску через контрольно-пропускні пункти в окремі будівлі (приміщення) співробітників об'єкта, відвідувачів, транспорту та матеріальних засобів.

Контрольно-пропускний режим є одним із головних моментів в організації системи безпеки на підприємстві. Зважаючи на це, контрольно-пропускний режим являє собою комплекс організаційних заходів (адміністративно-обмежувальних), інженерно-технічних рішень і дій служби безпеки.

Організація контрольно-пропускного режиму відрізняється своєю складністю. Справа в тому, що механізм здійснення контрольно-пропускного режиму ґрунтується на застосуванні «заборон» і «обмежень» щодо суб'єктів, які перетинають межі охоронюваних об'єктів, для забезпечення інтересів підприємства. Такий механізм має бути бездоганним з погляду узгодженості з вимогами чинного законодавства.

8.2. Цілі та завдання пропускного режиму

Контрольно-пропускний режим (як частина системи безпеки) повинен відповідати чинному законодавству, статуту підприємства, а також іншим нормативно-правовим актам, що регулюють діяльність підприємства.

Основними цілями створення контрольно-пропускного режи-

му є:

- захист законних інтересів підприємства, підтримка порядку внутрішнього керування;
- захист власності підприємства, її раціональне і ефективне використання;
- зростання прибутків підприємства;
- внутрішня і зовнішня стабільність підприємства;
- захист комерційних секретів і прав на інтелектуальну власність.

Контрольно-пропускний режим як частина системи безпеки дозволяє вирішувати такі завдання:

- забезпечення санкціонованого проходу співробітників і відвідувачів, ввозу (вивозу) продукції та матеріальних цінностей, ритмічної роботи підприємства;
- запобігання безконтрольного проникнення сторонніх осіб і транспортних засобів на охоронювані території і в окремі будинки (приміщення);
- своєчасне виявлення загроз інтересам підприємства, а також потенційно небезпечних умов, що сприяють нанесенню підприємству матеріального і морального збитку;
- створення надійних гарантій підтримки організаційної стабільності зовнішніх і внутрішніх зв'язків підприємства, відпрацьовування механізму оперативного реагування на загрози і негативні тенденції;
- припинення зазіхань на законні інтереси підприємства, використання юридичних, економічних, організаційних, соціально-психологічних, технічних і інших засобів для виявлення та послаблення джерел загроз безпеці підприємства.

Контрольно-пропускний режим можна визначити як систему забезпечення нормативних, організаційних і матеріальних гарантій виявлення, попередження і припинення зазіхань на законні права підприємства, його майно, інтелектуальну власність, виробничу дисципліну, технологічне лідерство, наукові досягнення та охоронювану інформацію і як сукупність організаційно-правових обмежень і правил, що встановлюють порядок пропуску через контрольно-пропускні пункти співробітників об'єкта, відвідувачів, транспорту й матеріальних цінностей.

Нормативні гарантії полягають у тлумаченні і реалізації норм

права, з'ясуванні меж їх дії, у формуванні необхідних правовідносин, визначенні і забезпеченні правомірної діяльності підрозділів і працівників фірми для її безпеки, використання обмежувальних заходів, застосування санкцій до фізичних і юридичних осіб, що зазіхають на законні інтереси фірми.

Організаційні гарантії формують шляхом розробки, побудови і підтримки високої працездатності загальної організаційної структури керування процесом виявлення і зменшення загроз діяльності фірми, використання ефективного механізму стимулювання її підготовки, за що відповідають надійні кадри.

Матеріальні гарантії формуються за рахунок виділення та використання фінансових, технічних, кадрових, інтелектуальних, інформаційних і інших ресурсів фірми, що забезпечують своєчасне виявлення, ослаблення і придушення джерел загрози, запобігання і локалізацію можливого збитку, створення сприятливих умов для діяльності фірми. Ці гарантії нормативні і організаційні заходи безпеки практичним змістом, створюють реальну основу розвитку культури безпеки фірми.

На кожному підприємстві повинна бути Інструкція про контрольно-пропускний режим, що визначає:

- порядок пропуску співробітників підприємства, відряджених осіб, відвідувачів, клієнтів;
- порядок допуску на територію об'єкта транспортних засобів, вивозу (ввозу) продукції, документів і матеріальних цінностей;
- види і групи перепусток, порядок їх оформлення та видачі;
- обов'язки посадових осіб щодо підтримки контрольно-пропускного режиму;
- систему обліку і звітності, порядок зберігання перепусток, печаток і шифрів тощо.

8.3. Розробка Інструкції про пропускний режим

Практичне вирішення питань, пов'язаних з організацією пропускного режиму, оформляють у вигляді Інструкції про пропускний режим. Зазначена інструкція повинна визначати систему організаційно-правових охоронних заходів, що встановлюють дозвільний порядок (режим) проходу (проїзду) на об'єкт (з об'єкта), і може мі-

стити:

1. Загальні положення. У цьому розділі вказують:

- нормативні документи, на підставі яких створювалася інструкція;
- визначення контрольно-пропускного режиму і мета його введення;
- посадові особи, на яких покладається організація і практичне керівництво контрольно-пропускною системою;
- санкції щодо порушників контрольно-пропускного режиму;
- вимоги щодо устаткування різних приміщень.

2. Порядок пропуску співробітників підприємства, відряджених осіб і відвідувачів через контрольно-пропускні пункти. У цьому розділі рекомендується:

- перелічити всі КПП і їх призначення, опис, розташування і встановити їх єдину нумерацію;
- викласти вимоги до встаткування КПП;
- установити порядок проходу співробітників і відвідувачів на територію об'єкта та у категорійні приміщення;
- визначити права і основні обов'язки контролерів КПП;
- установити приміщення, де забороняється бути відвідувачам та представникам сторонніх організацій.

3. Порядок допуску на об'єкт транспортних засобів, вивозу продукції, документів і матеріальних цінностей. У цьому розділі вказують:

- порядок допуску на територію об'єкта (з об'єкта) автотранспорту, що належить об'єкту;
- порядок в'їзду і стоянки на території об'єкта транспорту, що належить співробітникам на правах особистої власності;
- порядок пропуску автомашин сторонніх організацій, які прибули з вантажем на адресу об'єкта в робочий і неробочий час;
- порядок вивозу (ввозу) товарно-матеріальних цінностей;
- правила оформлення документів на вивіз (винос) матеріальних цінностей з території об'єкта.

4. Види перепусток, порядок їх оформлення. У цьому розділі визначають:

- види перепусток, їх кількість і статус;
- опис перепусток;

- порядок оформлення і видачі перепусток;
- порядок заміни й перереєстрації перепусток;
- заходи, якщо загублено перепустку співробітником.

5. Обов'язки посадових осіб щодо підтримки контрольно-пропускного режиму.

6. Облік і звітність, порядок зберігання перепусток, печаток.

Така інструкція залежно від структури підприємства і характеру його діяльності може містити й інші розділи.

Під час розробки Інструкції про контрольно-пропускний режим визначають види і групи перепусток, які будуть діяти на підприємстві.

На великих підприємствах, як правило, встановлюють кілька видів перепусток. Це можуть бути постійні, тимчасові, разові і матеріальні перепустки.

8.4. Оформлення перепусток

На великих підприємствах, як правило, встановлюють такі види пропускних документів, що дають право проходу співробітників і відвідувачів на територію фірми, внесення (винесення), ввозу (вивозу) матеріальних цінностей:

- посвідчення;
- постійні, тимчасові, разові, матеріальні перепустки.

На посвідченнях і перепустках проставляються печатки, передбачені правилами режиму, і цифрові знаки, що визначають зону доступу, період їх дії, право пронесення портфелів (кейсів, папок і ін.). Період перебування співробітників на території фірми в робочий і неробочий час визначається керівництвом із проставлянням цифрового знака на посвідченні або перепустці. Зразки посвідчень і перепусток розробляються службою безпеки і затверджуються керівництвом фірми.

Затверджені зразки посвідчень особи, перепусток, відбитків цифрових знаків, печаток (штампів), що проставляються на посвідченнях і перепустках, списки зі зразками підписів керівників або уповноважених осіб, що мають право підписувати посвідчення і перепустку, передаються начальникові відділу режиму і охорони під підпис.

Повну заміну посвідчень і постійних перепусток здійснюють, як правило, через 3 – 5 років. Щороку проводиться перереєстрація із проставлянням відповідної оцінки.

Для перереєстрації, заміни або зміни пропускних документів щорічно за станом на 1 січня в службу безпеки направляються відділом кадрів списки співробітників із вказівкою посади, прізвища, імені, по батькові й найменування документа з відповідними позначками (цілодобово, робочий час з __ по __, з портфелем, у яку зону тощо).

Посвідчення і постійні перепустки можуть видаватися особам, що не працюють на цій фірмі, відповідно до окремого затвердженого керівництвом списку із вказівкою установи, посади, прізвища, імені, по-батькові та супровідних позначок. Ці документи повинні постійно зберігатися в бюро перепусток (або в уповноваженої особи) і видаватися відвідувачеві в момент його прибуття. Після завершення роботи ці особи здають документи в бюро перепусток.

Зразки бланків перепусток розробляються адміністрацією об'єкта (службою безпеки). За зовнішнім виглядом і змістом перепустки повинні відрізнятися одна від одної та мати деякі ступені захисту. Усі види перепусток, за винятком матеріальних, оформляються і видаються бюро перепусток (або іншим підрозділом) за письмовими заявками. Види перепусток визначаються залежно від специфіки підприємства.

Постійні перепустки видаються співробітникам об'єкта, прийнятим на постійну роботу, а також працівникам інших організацій, що постійно обслуговують об'єкт. Постійні перепустки можуть ділитися на групи, їх кількість і призначення визначаються Інструкцією про контрольно-пропускний режим. Постійні перепустки можуть зберігатися як на руках у співробітників об'єкта, так і в кабінах на КПП. Постійні перепустки осіб, що вибувають із об'єкта на тривалий час (відпустка, хвороба, відрядження і т. ін.), здаються на зберігання в бюро перепусток (відділ кадрів), а у разі зберігання таких перепусток у кабіні КПП (де зберігається перепустка) робиться відповідна відмітка. Перепустки звільнених з роботи знищуються у встановленому порядку.

Тимчасові перепустки видаються особам, що працюють за контрактом, перебувають на тимчасовій роботі, прикомандированим до підприємства, і зберігаються, як правило, на КПП. Термін дії і

порядок оформлення тимчасових перепусток визначається Інструкцією про контрольно-пропускний режим. Тимчасові перепустки можуть бути з фотокарткою і без фотокартки. Тимчасові перепустки без фотокартки дійсні тільки у разі пред'явлення документа, що засвідчує особистість.

Разові перепустки. Ця перепустка надає право пройти в супроводі співробітника організації в службові приміщення організації. Супровід зобов'язаний організувати начальник відділу (підрозділу), до якого прибув відвідувач. Співробітник, призначений для супроводу, прибуває в бюро перепусток і одержує перепустку для супроводу. Після завершення роботи відвідувач супроводжується співробітником на вихід.

Разові перепустки видаються на одну особу і тільки для разового відвідування підприємства і його підрозділів. Перепустка оформляється і дійсна у разі наявності документа, що засвідчує особистість. Разові перепустки повинні періодично мінятися за кольором бланків і іншими ознаками.

Разова перепустка, видана водієві транспортного засобу, може слугувати одночасно і разовою перепусткою для транспорту.

Разова перепустка дійсна для входу на територію об'єкта або його підрозділу протягом певного часу.

Контроль відвідувачів підприємства за разовою перепусткою здійснюється за допомогою позначки на зворотному боці перепустки, де вказується час відвідування, завірений підписом особи, що приймає відвідувача.

Разова перепустка вилучається на КПП контролером під час виходу відвідувача з об'єкта і здається в бюро перепусток. Про осіб, які не вийшли з об'єкта після закінчення терміну дії перепустки, контролер доповідає начальникові (черговому по КПП) для вживання заходів щодо з'ясування причин затримки. Прізвища осіб, що відвідали об'єкт за разовою перепусткою, можуть записуватися в спеціальну книгу обліку.

Матеріальні перепустки для вивозу (виносу) товарно-матеріальних цінностей видаються адміністрацією підприємства. Термін дії перепустки визначається Інструкцією про контрольно-пропускний режим. Матеріальні перепустки повинні вилучатися на КПП і здаватися в бюро перепусток.

8.5. Організація проходу співробітників, відвідувачів, представників контрольних і правоохоронних органів на об'єкт, який охороняється

Прохід співробітників і відвідувачів на територію об'єкта в категоріальні підрозділи і назад здійснюється за встановленими на об'єкті перепустками через контрольно-пропускні пункти. Перепустка повинна бути основним документом, що дає право на прохід.

Допуск відряджених (відвідувачів) здійснюється за тимчасовими, разовими перепустками у встановлений і визначений в перепустці час, у виняткових випадках – за затвердженими начальником служби безпеки списками.

Представники засобів масової інформації допускаються на об'єкт на загальних підставах у супроводі представників адміністрації.

У неробочий час, вихідні і святкові дні допуск співробітників на об'єкт повинен бути обмежений і здійснюватися за попередніми заявками (списками) керівників підрозділів, завізованими начальником служби безпеки із пред'явленням постійної перепустки. На підприємствах зі змінним режимом роботи до перепустки можуть видаватися спеціальні змінні вкладиші.

Чергові спеціальних служб об'єкта (електрики, сантехніки, робітники зв'язку тощо), що працюють позмінно, допускаються на територію об'єкта в неробочий час, у вихідні і святкові дні за списками, підписаними начальниками відповідних служб і затвердженими начальником служби безпеки.

На підставі чинного законодавства і рішення адміністрації окремі категорії осіб користуються правом проходу на об'єкт без перепустки при пред'явленні службового посвідчення. До них належать:

- працівники прокуратури і інших правоохоронних служб;
- працівники поліції;
- інспектори праці, котлонагляду, енергонагляду по територіальності;
- посадові особи і окремі категорії працівників санітарно-епідеміологічної служби органів охорони здоров'я, що здійснюють санітарний нагляд.

Категорії осіб, що мають право проходу на об’єкт без перепустки (за службовими посвідченнями), повинні бути чітко відображені в Інструкції про контрольно-пропускний режим.

З метою здійснення пропускного режиму на території об’єкта та у його структурних підрозділах наказом керівника підприємства затверджується перелік категорійних підрозділів (приміщень), сховищ. У цих приміщеннях установлюються спеціальний режим і підвищена відповідальність за його дотримання працівниками цих підрозділів.

Допуск у ці приміщення здійснюється суворо за списком, погодженим зі службою безпеки. Приймання відвідувачів сторонніх організацій і підприємств, як правило, максимально обмежується.

У всіх приміщеннях категорійних підрозділів повинні бути вивішені в засклених рамках списки працівників, що мають допуск у ці приміщення. Усі приміщення по закінченню робіт оглядають чергові по підрозділах і особи, відповідальні за протипожежний стан. Електроосвітлювальну і електронагрівальну апаратуру знеструмлюють, вікна і кватирки зачиняють, двері зачиняють на замок і опечатують. По закінченню робочого дня обладнані охоронною сигналізацією категорійні приміщення, спецсховища, склади та інші об’єкти закривають і опечатують відповідальні особи цих підрозділів. Приміщення здають під охорону. Представник охорони перевіряє сигналізацію в присутності робітників, що здають приміщення. Ключі від цих приміщень в опечатуваних пакетах здають під підпис в спеціальному журналі.

Отримують ключі, відкривають приміщення, обладнані охоронною сигналізацією, особи, що мають допуск на право відкриття цих приміщень із пред’явленням постійної перепустки. Списки осіб, що мають право відкривати (закривати) зазначені приміщення, з контролем номерів особистих печаток, якими опечатуються приміщення, і номерів службових телефонів підписує начальник підрозділу і затверджує начальник служби безпеки.

Усіх осіб, що намагаються пройти через КПП без пред’явлення перепустки або за чужою, неправильно оформленою перепусткою, намагаються пронести на об’єкт (з об’єкта) заборонені предмети, затримують і на об’єкт не допускають.

8.6. Допуск на територію підприємства транспортних засобів, вивіз матеріальних цінностей

Допуск на територію (з території) підприємства транспортних засобів, що належать підприємству, здійснюють у разі пред'явлення водієм особистої перепустки зі спеціальним шифром або транспортної перепустки і подорожнього листа. Вантажників і супровідників, які їдуть із транспортом, пропускають через КПП на загальних підставах.

В'їзд і стоянка транспорту на території підприємства належить співробітникам на правах особистої власності, дозволяється за спеціальними списками.

Автомашини сторонніх організацій, що прибули з вантажем на адресу підприємства в робочий час, допускаються на територію за службовими записками. В'їзд машин на територію підприємства здійснює штатний водій у супроводі представника адміністрації.

Залізничний транспорт і бригади, що його обслуговують, пропускають на підприємство за перепустками установленого зразка, за списками або іншим порядком, установленим Інструкцією про пропускний режим. Для пропуску залізничного транспорту від підрозділу охорони виділяють спеціальну групу.

Опломбовані вагони і контейнери пропускають через КПП після їх зовнішнього огляду, якщо відбитки пломб відповідають відбиткам у супровідних документах або накладних. У разі невідповідності відбитків, виявлення проламів вагона (контейнера) або обриву пломби вагон (контейнер) підлягає відкриттю й огляду в присутності представників адміністрації залізниці.

Вивіз і винос готової продукції та інших матеріальних цінностей з території об'єкта здійснюють за матеріальними перепустками встановленого зразка.

Переконавшись у правильності оформлення документів і їх повній відповідності із цінностями, що вивозяться, охоронець залишає на КПП перепустку, ставить на ній дату і час вивозу вантажу, підписує й дає дозвіл на вивіз матеріальних цінностей.

Усі документи, матеріальні цінності, що вивозяться (виносяться) з підприємства, реєструються в бюро перепусток у книзі обліку і протягом наступного дня передаються в бухгалтерію. Документи

на вивіз (винос) матеріальних цінностей повинні бути виписані тільки на ту кількість вантажу (місць, ваги й т. ін.), яку може бути вивезено (винесено) одночасно, і дійсні тільки на дату, зазначену в документі дозволу.

Будівельні і дерев'яні відходи, макулатуру, металобрухт, металеву стружку рекомендується вивозити з території підприємства як матеріальні цінності. Вивіз із території об'єкта різного сміття, землі і снігу може проводитися без оформлення документів, але з обов'язковою реєстрацією на автотранспортному КПП.

8.7. Устаткування пропускних пунктів

Для організації пропускного режиму на підприємстві обладнують контрольно-пропускні пункти. Устаткування КПП повинне забезпечувати необхідну пропускну здатність і можливість ретельної перевірки перепусток і документів осіб, огляду всіх видів транспорту, вантажів, які провозяться, і відповідати таким вимогам:

- виключати можливість несанкціонованого проникнення через КПП на об'єкт (з об'єкта) людей і транспортних засобів;
- сприяти скороченню часу на перевірку документів, огляд транспорту і матеріальних цінностей;
- сприяти недопущенню (відомості до мінімуму) помилок охоронця під час пропуску людей і транспорту;
- забезпечувати заходи безпеки охоронця під час огляду транспортних засобів.

Усі види КПП повинні бути обладнані необхідними видами зв'язку і тривожної сигналізації для виклику резерву охорони. На КПП рекомендується розташовувати внутрішній телефон і список телефонів адміністрації підприємства.

КПП для проходу людей. Для контролю проходу людей на об'єкт і в окремі будинки (приміщення) будують КПП. Кожне КПП рекомендується обладнати кімнатою для охорони, кімнатою для огляду громадян, камерою схову, гардеробом, турнікетом з фіксувальними засувами.

Розміщення приміщень визначається проєктами й залежить від засобів механізації, автоматизації КПП і особливостей підприємства.

У контрольно-пропускному залі влаштовують проходи, які

обладнані технічними засобами охорони і фізичними бар'єрами. У комплект устаткування, як правило, входять:

- засоби механізації, автоматизації системи контролю доступу;
- фізичні бар'єри (огородження, турнікети, хвіртки);
- основне й резервне освітлення;
- засоби зв'язку і тривожної сигналізації;
- системи відеоконтролю.

Для контролю доступу можуть використовуватися різні турнікети. Турнікети призначені для керування потоками людей і регулювання входу (виходу). Останнім часом найчастіше застосовують електромеханічні турнікети.

Електромеханічні турнікети, на відміну від громіздких і незручних у керуванні механічних, легко управляються з пульта охоронника і можуть працювати в складі автоматизованої системи контролю доступу.

Під час вибору турнікета потрібно мати на увазі, що вони бувають «нормально відкриті» і «нормально закриті». Для здійснення надійного контролю частіше використовують «нормально закриті» турнікети: роторні турнікети-вертушки, турнікети-триподи і хвіртки.

Хвіртки застосовують для керування потоками людей, організації вільного проходу в одну сторону (на вхід або вихід) і заборони проходу в іншу. Хвіртки широко використовують в магазинах, аеропортах, на вокзалах. Застосування хвірток для контролю доступу неефективно, бо хвіртки не розділяють потік людей по одному, тому що після відчинення хвіртки через неї можуть пройти кілька людей. Хвіртки можуть встановлювати для організації вільного виходу. Контроль входу довіряють триподам або вертушкам.

Турнікети-триподи із трьома планками, що перепиняють прохід, є одним з найбільш оптимальних засобів для здійснення контролю санкціонованого проходу. Триподи мають сучасний елегантний вигляд і легко монтуються. Триподи дозволяють здійснювати ефективний контроль доступу, тому що розділяють потік людей по одному, забезпечуючи при цьому високу пропускну здатність. Триподи можуть застосовуватися в системах електронних прохідних, у тому числі в умовах великого потоку людей. Для запобігання можливості підлізти під планки турнікета або перестрибнути через них на турнікеті рекомендується встановлювати спеціальні датчики, які спрацьовують у разі спроби несанкціонованого проходу.

Роторні турнікети-вертушки застосовують тоді, коли необхідне повне перекриття зони проходу. Вони можуть бути різними по висоті – від поясних до турнікетів у повний зріст, конструкція яких подібна до обертових дверей.

Транспортні КПП. До складу транспортного КПП входить оглядовий майданчик і службове приміщення. Оглядовий майданчик призначений для розміщення автомобілів під час огляду. Ці майданчики можуть розташовуватися як на території підприємства, так і за її межами, на території, безпосередньо пов'язаною з основними воротьми КПП. Оглядовий майданчик повинен відповідати таким вимогам:

- мати достатню площу для розміщення транспорту, що оглядають, технічні засоби для забезпечення нормальних умов роботи охоронця;
- виключати можливість несанкціонованого проникнення на об'єкт (з об'єкта) людей і транспортних засобів;
- забезпечувати при встановленій інтенсивності руху в будь-який час доби і року огляд автомобільного транспорту та перевезених вантажів;
- бути ізольованим від інших споруджень, що не стосуються охорони об'єкта і устаткування КПП;
- забезпечувати заходи безпеки охоронця під час виконання обов'язків.

Розміри оглядового майданчика встановлюють залежно від габаритів транспорту й перевезених вантажів і можуть бути: 10 – 12 м завдовжки й 5–6 м завширшки.

На території, відведеній для будівництва оглядового майданчика, здійснюють планування місцевості з таким розрахунком, щоб на ній не затримувалися дощові й поталі води. Поперечний ухил оглядового майданчика має бути не менше ніж 2 % від місця виставляння охоронця в напрямку його бічних сторін (перпендикулярно проїзній частині). Поверхню оглядового майданчика покривають бетоном або асфальтом.

На проїзній частині майданчика виділяється місце зупинки транспорту для огляду, обмежене двома лініями з написом «СТОП», нанесеними білою фарбою.

Перед в'їздом на оглядовий майданчик із зовнішнього боку основних і допоміжних воріт (шлагбаума), не ближче ніж 3 м від них, також наносять поперечну лінію з написом «СТОП». З метою забез-

печення безпеки руху транспорту не менше ніж 100 м від воріт із правого боку або над дорогою встановлюють вказівний знак «Рух в один ряд», а 50 м від воріт – знак обмеження швидкості до 5 км/год.

Транспортні КПП можуть бути обладнані світлофорами, вагами для зважування автомобілів, оглядовою ямою або естакадою для огляду вантажів, механізованими обладнанням для автоматичного відкриття і закриття воріт з фіксаторами.

Оглядові майданчики по периметру обладнують фізичними бар'єрами і сигналізацією. Майданчик, як правило, обладнують парканом з металевої сітки, який проглядається, або з декоративних ґрат висотою до 2,5 м. На майданчику обладнують основні і допоміжні механізовані ворота. Основні ворота встановлюють на лінії основного огородження об'єкта, а допоміжні – з протилежного боку оглядового майданчика. Замість воріт можуть застосовуватися механізовані шлагбауми. На автомобільних КПП використовують ворота з обмеженням і без обмеження габаритів по висоті.

Для регулювання руху транспорту, що проходить через проїзди оглядових майданчиків КПП, можуть застосовуватися двосекційні світлофори з лінзами червоного і зеленого кольору.

До складу електромеханічного устаткування КПП для автомобільного транспорту звичайно належать:

- електродвигуни, привід воріт;
- кінцеві вимикачі автоматичного відключення електродвигунів при повністю закритих і відкритих стулках воріт;
- магнітні пускачі електродвигунів;
- електроустаткування світлофорів;
- кабельні, силові лінії.

Груповий розподільний щит (щит керування) може встановлюватися в приміщенні КПП, а у разі відсутності будинку КПП – у спеціальній металевій шафі безпосередньо на оглядовому майданчику.

Контрольні запитання

1. Що встановлює контрольно-пропускний режим?
2. Що входить до складу транспортного КПП організації?
3. За яких умов необхідні роторні турнікети-вертушки?
4. Що частіше використовують для здійснення надійного контролю проходу?
5. Які завдання дозволяє вирішувати контрольно-пропускний режим?
6. Види перепусток.
7. Які види пропускних документів дають право проходу співробітників і відвідувачів на територію фірми, внесення (винесення), ввозу (вивозу) матеріальних цінностей?
8. Що визначає Інструкція про контрольно-пропускний режим?

9. ПЛАНУВАННЯ ЗАХОДІВ ЩОДО ОРГАНІЗАЦІЙНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

9.1. Основні цілі планування

Одним з найбільш важливих напрямків діяльності підприємства, що здійснює роботу з відомостями конфіденційного характеру, є планування заходів щодо захисту конфіденційної інформації. Планування зазначених заходів посідає особливе місце в системі керування діяльністю як підприємства загалом, так і його структурних підрозділів (окремих посадових осіб) зокрема. Важко також переоцінити значення цього напрямку в загальній системі організаційних заходів забезпечення інформаційної безпеки підприємства.

Основними цілями планування заходів щодо захисту інформації є:

- організація проведення комплексу заходів щодо захисту конфіденційної інформації, спрямованої на виключення можливих каналів витоку цієї інформації;
- установлення персональної відповідальності всіх посадових осіб підприємства за рішення питань захисту інформації в ході виробничої та іншої діяльності підприємства;
- визначення строків (часу, періоду) проведення конкретних заходів щодо захисту інформації;
- систематизація (об’єднання) усіх проведених на плановій основі заходів щодо різних напрямків захисту конфіденційної інформації;
- установлення системи контролю над забезпеченням захисту інформації на підприємстві, а також системи звітності про виконання конкретних заходів;
- уточнення (конкретизація) функцій і завдань, які вирішують структурні підрозділи підприємства й окремі посадові особи.

Основою для планування заходів щодо захисту інформації на підприємстві слугують:

- вимоги законодавчих і інших нормативних правових актів щодо захисту конфіденційної інформації, що відповідають нормативно-методичним документам виконавчої влади (за наявності відомчої приналежності), вищої організації, а під час планування заходів щодо захисту інформації філією або представництвом підприємства – вказівки головного підприємства;
- вимоги замовників виконаних підприємством у межах відповідних договорів (контрактів) спільних і інших робіт;
- положення міжнародних договорів (угод) і інших документів, що визначають участь підприємства в тих або тих формах міжнародного співробітництва;
- положення внутрішніх організаційно-розпорядчих документів підприємства (наказів, директив, положень, інструкцій), які визначають порядок ведення виробничої та іншої діяльності, захисту, що також конкретизують питання конфіденційної інформації на підприємстві;
- результати комплексного аналізу стану справ у сфері захисту інформації, виконаного службою безпеки (режимно-секретним підрозділом) на підставі матеріалів перевірок структурних підрозділів (філій, представництв) підприємства;
- результати перевірок стану захисту інформації, проведених вищими організаціями, національними органами виконавчої влади (за наявності відомчої приналежності) і замовниками робіт (у межах виконуваних договорів або контрактів), вироблені на підставі цих результатів пропозиції та рекомендації;
- результати контролю над станом захисту інформації, який проводиться органами безпеки й іншими контролюючими органами (у частині, їх дотичної);
- особливості повсякденної діяльності підприємства і специфіка виконання на підприємстві робіт з використанням різних видів конфіденційної інформації.

Планування заходів щодо захисту конфіденційної інформації проводиться одночасно із плануванням основної виробничої та іншої діяльності підприємства. Планування може виконуватися на календарний рік, календарний місяць, тиждень, а також на інший певний строк, зумовлений проведенням важливих заходів (робіт) за видами діяльності підприємства, якщо вони пов'язані з питаннями конфіденційного характеру. Плани заходів, розроблювані на строк

більше ніж календарний рік, належать, як правило, до стратегічного планування, інші плани вирішують тактичні завдання.

З метою ефективного рішення завдань щодо захисту конфіденційної інформації в межах найбільш важливих і масштабних робіт, а також у ході реалізації на підприємстві цільових, державних, відомчих і інших програм можуть розроблятися окремі плани, що мають характер програмно-цільового планування. Такими програмами можуть бути реконструкція підприємства, впровадження нових технологій, у тому числі інформаційних тощо.

Плани заходів щодо захисту інформації належать до документів з обмеженим доступом, обліковуються і зберігаються в службі безпеки (режимно-секретному підрозділі) підприємства в порядку, встановленому для документів відповідного ступеня конфіденційності (таємності).

Розробка документів щодо захисту інформації на підприємстві, що плануються, здійснюється службою безпеки (режимно-секретним підрозділом) у тісній взаємодії з підрозділами (окремими посадовими особами), у веденні яких є завдання, що безпосередньо стосуються питань захисту інформації (підрозділ протидії іноземним технічним розвідкам, служба охорони, кадровий орган і ін.). Крім того, під час підготовки планів ураховуються пропозиції структурних підрозділів підприємства, що займаються виробничою (фінансово-господарською) діяльністю або її забезпеченням.

Від повноти і якості розробки організаційно-планових документів повною мірою залежить ефективність проведення заходів, спрямованих на виключення витоку конфіденційної інформації, втрат її носіїв, а також виникнення передумов подібних подій.

9.2. Структура та основний зміст плану заходів щодо захисту конфіденційної інформації

Основним організаційно-плановим документом підприємства є план заходів щодо захисту конфіденційної інформації на календарний рік. Цей план найбільш повно і всебічно визначає заходи щодо захисту інформації, передбачувані до проведення в ході по-

всякденної діяльності підприємства протягом календарного року. Під час підготовки плану враховують знову прийняті (підписані, затверджені) нормативні правові акти і методичні документи щодо захисту конфіденційної інформації, поточні вказівки, що діють, накази і вищих органів державної влади та організацій (при наявності відомчої приналежності або іншого підпорядкування).

План заходів щодо захисту конфіденційної інформації на підприємстві на календарний рік затверджується керівником підприємства до початку календарного року, на який він розроблений. У разі потреби план узгоджується з відповідним органом безпеки. Затверджений план під підпис доводиться до відома заступників керівника підприємства, керівників структурних підрозділів і окремих посадових осіб, відповідальних за проведення зазначених у плані заходів.

Типовий план заходів щодо захисту конфіденційної інформації на календарний рік містить такі основні розділи:

1. Організаторська робота керівництва підприємства – розробка організаційно-планових документів у ході повсякденної діяльності підприємства і під час виконання підприємством усіх видів робіт; доповіді і повідомлення про стан захисту інформації, що подаються до органів і організацій, вищих за підпорядкуванням; підготовка і видання наказів керівника підприємства по різних питаннях у сфері захисту конфіденційної інформації; переробка і уточнення посадових обов'язків співробітників і ін.

2. Підготовка персоналу з питань захисту інформації – організація і проведення занять із усіма категоріями співробітників підприємства з урахуванням специфіки виконуваної ними роботи; вивчення положень нормативно-методичних документів у сфері захисту інформації і в разі потреби доведення їх вимог до відома співробітників під підпис; прийняття заліків і проведення занять із новоприбулими або призначеними на посаду співробітниками; заходи щодо навчання співробітників підприємства в освітніх установах вищої, середньої й додаткової професійної освіти.

3. Контроль захисту інформації і наявності носіїв конфіденційної інформації – організація і проведення всіх видів перевірок стану захисту інформації та наявності носіїв конфіденційної інформації. Особлива увага приділяється плануванню проведених по за-

кінченню календарного року заходів щодо перевірки наявності носія інформації комісією підприємства. Для підприємств, які працюють із відомостями, що становлять державну таємницю, проведення перевірок наявності носіїв цих відомостей планується відповідно до строків, встановлених у нормативних правових актах щодо забезпечення режиму таємності. У разі наявності в підприємства підлеглих організацій, філій і представництв плануються перевірки стану захисту інформації в цих організаціях комісіями головного підприємства.

4. Допуск і доступ персоналу до конфіденційної інформації і її носіям – заходи, що стосуються розробки, переробки та погодження номенклатури посад працівників підприємства, які підлягають оформленню на допуск до відомостей, що становлять державну таємницю; питання оформлення і переоформлення матеріалів на допуск до державної таємниці співробітників підприємства, зокрема контрактів, трудових договорів і карток про допуск; розробка і переробка списків осіб, що допускаються до конфіденційної інформації, а також осіб, що допускаються до конкретних матеріалів; заходи, спрямовані на розмежування доступу до носіїв конфіденційної інформації залежно від ступеня їх таємності або конфіденційності, а також залежно від тематики проведених підприємством робіт. За необхідністю окремим пунктом визначаються питання організації обліку поінформованості осіб у відомостях особливої важливості і зовсім секретних відомостях, підготовки відповідних положень.

5. Організація і ведення конфіденційного діловодства – заходи служби, що безпосередньо стосуються діяльності, безпеки або режимно-секретного підрозділу підприємства, а також спеціально створюваних на підприємстві комісій з відбору конфіденційних документів і матеріалів для знищення, перегляду стану таємності або конфіденційності матеріалів, інструктажу осіб, що вибувають із носіями конфіденційної інформації за межі підприємства; питання обліку, зберігання, розмноження і знищення носіїв конфіденційної інформації, порядок роботи з ними персоналу підприємства.

6. Захист інформації під час здійснення рекламної і публічної діяльності – заходи, пов’язані з роботою експертної комісії із прийняття рішень про можливість публікації наукових матеріалів, ін-

формації про діяльність підприємства, використання цих матеріалів під час проведення рекламних акцій; заходів, направлених під час підготовки матеріалів до відкритого опублікування.

7. Захист інформації під час використання технічних засобів – організаційні заходи щодо підготовки і введення в експлуатацію об'єктів інформатизації, що обробляють інформацію з обмеженим доступом, щодо технічного захисту інформації, захисту інформації від несанкціонованого доступу і від витоку по технічних каналах; робота посадових осіб щодо протидії іноземним технічним розвідкам, запобіганню витоку інформації під час використання засобів відкритого зв'язку, наприклад факсимільного, телеграфного, голосового, телефонного.

8. Захист інформації в ході здійснення міжнародного співробітництва – заходи щодо захисту інформації під час підготовки і реалізації міжнародних договорів і інших документів, під час прийому іноземних делегацій на підприємстві. Заходи передбачаються з урахуванням розподілу функцій щодо захисту інформації між структурними підрозділами підприємства (відділами, службами) і посадовими особами.

9. Виїзд за кордон співробітників, допущених до конфіденційної інформації. Для підприємств, що працюють із відомостями, що є державною таємницею, планування заходу в цьому розділі здійснюється у суворій узгодженості з державним законом. Плановані заходи не повинні бути спрямовані на обмеження права співробітників підприємства, допущених до конфіденційної інформації (за винятком відомостей особливої важливості і зовсім секретних відомостей), на виїзд із держави.

10. Захист інформації під час виконання спільних і інших робіт – заходи, спрямовані на виключення витоку конфіденційної інформації при участі підприємства у виконанні спільних та інших робіт, передбачених статутом підприємства; порядок і умови питань захисту інформації, встановлені в договорах із замовниками або виконавцями робіт, зміст відповідних пунктів зазначених договорів; заходи щодо захисту державної таємниці в ході діяльності конкурсних комісій з вибору виконаних робіт; під час участі підприємства у виконанні робіт у межах державного оборонного замовлення – особливості виконання цих робіт.

11. Для спільних робіт, в яких підприємство є замовником або

головним виконавцем, передбачаються заходи щодо контролю ефективності захисту виконавцями цих робіт конфіденційної інформації, переданої їм підприємством як результативні дані. Під час виконання підприємством робіт з використанням відомостей, що містять державну таємницю, передбачаються заходи щодо відповідальності замовників, головних виконавців і виконавців робіт за недотримання встановлених вимог тощо.

12. Захист інформації в надзвичайних ситуаціях – порядок формування, завдання і основні напрямки діяльності позаштатного підрозділу підприємства – спеціальної комісії, створюваної наказом керівника підприємства з метою вироблення заходів щодо запобігання надзвичайних ситуацій на підприємстві, а також заходів щодо захисту інформації у разі виникнення надзвичайних ситуацій; практичні заходи, спрямовані на недопущення завдання збитків інформаційній безпеці підприємства внаслідок виникнення надзвичайної ситуацій, зокрема на запобігання витоку захищеної інформації, втрати, розкрадання або знищення носіїв конфіденційної інформації; аналіз можливих загроз і різних чинників, що призводять до виникнення на підприємстві надзвичайних ситуацій. Особлива увага приділяється питанням координації дій усіх структурних підрозділів, що беруть участь у вирішенні завдань захисту інформації.

Під час планування заходів щодо захисту інформації враховують всі можливі види і способи прояву надзвичайних ситуацій. Заходи щодо захисту інформації у разі виникнення надзвичайних ситуацій відображають у відповідних планах роботи підприємства (його структурних підрозділів) на календарний місяць. У цьому розділі плану (або в окремому додатку до плану) вказують також:

- прізвище, ім’я, по батькові, домашня адреса і контактні телефони (у тому числі мобільного зв’язку) кожного співробітника, що бере участь у ліквідації наслідків надзвичайної ситуації на об’єктах підприємства;
- черговість і порядок виклику (оповіщення) усіх співробітників, що беруть участь у виконанні робіт з ліквідації наслідків надзвичайної ситуації, залежно від її виду, строків прибуття цих працівників на об’єкти підприємства;
- обов’язки кожного співробітника підприємства і послідов-

ність виконання ним заходів (робіт) відповідно до конкретного плану дій;

- перелік сил і засобів (у тому числі транспортних засобів і засобів зв'язку), залучених до вирішення завдань ліквідації наслідків надзвичайних ситуацій;
- місця стоянки і маршрути руху транспортних засобів, прилади, що евакуюють носії конфіденційної інформації (у тому числі великогабаритні);
- маршрути евакуації носіїв конфіденційної інформації, місця їх зосередження, способи і порядок охорони евакуйованих носіїв (великогабаритних виробів), залучені для охорони сили й засобу (у тому числі штатних підрозділів охорони).

13. Пропускний режим і охорона об'єктів підприємства – організаційні заходи щодо створення та удосконалювання системи пропускного режиму і охорони, такі як підготовка наказів про запровадження в дію або про висновок з дії всіх видів перепусток, про призначення відповідальних посадових осіб, розробка й переробка інструкцій і положень, заходи щодо матеріально-технічного забезпечення, встановлення та експлуатації технічних засобів охорони й ін.

14. Аналітична робота на підприємстві – усі види оглядів і звітів про стан справ у сфері захисту інформації на підприємстві, оформлюваних для керівництва підприємства, а також для керівників вищих органів державної влади або вищих організацій; заходи щодо формування матеріалів, що містять підсумки роботи підприємства і його структурних підрозділів щодо захисту інформації, для ознайомлення всіма співробітниками підприємства. Особливе місце в розділі посідають аналітичні звіти за підсумками календарного місяця і календарного року, які готовить служба безпеки (режимно-секретний підрозділ) підприємства.

Особлива увага під час розробки і реалізації плану заходів приділяється ролі керівників структурних підрозділів підприємства як посадових осіб, відповідальних за забезпечення захисту інформації в безпосередньо підлеглих їм підрозділах.

Контроль над виконанням конкретних заходів згідно з цим планом здійснює керівник підприємства і його заступник, до обов'язків якого належать питання захисту конфіденційності інформації. Служба безпеки (режимно-секретний підрозділ) підприємс-

тва здійснює поточний контроль за практичною реалізацією включених у план заходів і інформує про їх виконання зазначених посадових осіб.

Контрольні запитання

1. Назвіть основні цілі планування заходів щодо захисту інформації.
2. Хто контролює виконання конкретних заходів щодо захисту конфіденційності інформації на підприємстві?
3. Які основні розділи входять до типового плану заходів щодо захисту конфіденційної інформації на календарний рік?
4. Чи необхідні заходи, спрямовані на виключення витоку конфіденційної інформації за участі підприємства у виконанні спільних та інших робіт, передбачених статутом підприємства?
5. Чи є необхідним захист інформації під час здійснення рекламної діяльності?
6. Чи потрібно визначати окремим пунктом питання організації обліку поінформованості осіб у відомостях особливої важливості і зовсім секретних відомостях?
7. Чи необхідна підготовка персоналу з питань захисту інформації?
8. Чи належать плани заходів щодо захисту інформації до документів з обмеженим доступом?

10. ОРГАНІЗАЦІЯ АНАЛІТИЧНОЇ РОБОТИ В НАПРЯМКУ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

10.1. Основні напрямки аналітичної роботи. Функції аналітичного підрозділу

Аналіз стану захисту інформації – це комплексне вивчення фактів, подій, процесів, явищ, пов'язаних із проблемами захисту інформації, у тому числі даних про стан роботи з виявлення можливих каналів витоку інформації, про причини і обставини, які сприяють витоку та порушенню режиму таємності (конфіденційності) у ході повсякденної діяльності підприємства.

Основне призначення аналітичної роботи – вироблення ефективних заходів, пропозицій і рекомендацій керівництву підприємства, спрямованих на недопущення витоку конфіденційної інформації про діяльність підприємства та роботи, які воно виконує. Аналітична робота повинна включати елементи прогнозування можливих дій супротивника щодо одержання важливої інформації, що захищається.

Основні напрямки аналітичної роботи на підприємстві такі:

- аналіз об'єкта захисту;
- аналіз внутрішніх і зовнішніх загроз інформаційній безпеці підприємства;
- аналіз можливих каналів несанкціонованого доступу до інформації;
- аналіз системи комплексної безпеки об'єктів;
- аналіз наявних порушень режиму конфіденційності інформації;
- аналіз передумов до розголошення інформації, а також втрати носіїв конфіденційної інформації.

Функції аналізу на підприємстві покладають на спеціально створений в його структурі аналітичний підрозділ, який комплектується кваліфікованими фахівцями в галузі захисту інформації. Водночас ці фахівці повинні повною мірою володіти інформацією із

усіх напрямків діяльності підприємства: знати види, характер і послідовність виконання робіт, організації, які взаємодіють, специфіку діяльності структурних підрозділів підприємства тощо. Як правило, аналітичний підрозділ належить до складу служби безпеки підприємства.

Аналітичний підрозділ повинний забезпечувати керівництво підприємства достовірною та аналітично обробленою інформацією, необхідною для прийняття ефективних управлінських рішень в усіх напрямках захисту інформації.

Основними функціями аналітичного підрозділу є:

- забезпечення своєчасного отримання достовірних і всебічних відомостей із проблем захисту інформації;
- облік, узагальнення й постійний аналіз матеріалів про стан справ у системі захисту інформації підприємства (його філій і представництв);
- аналіз можливих загроз захисту інформації, моделювання реального сценарію можливих дій конкурентів (зловмисників), що зачіпають інтереси підприємства;
- забезпечення ефективності роботи з аналізу наявної інформації, виключення дублювання під час її збору, обробки і поширенні;
- моніторинг ситуації на ринку продукції, товарів і послуг, а також у зовнішньому середовищі з метою виявлення подій і фактів, які можуть мати значення для діяльності підприємства;
- забезпечення безпеки власних інформаційних ресурсів, обмеження доступу співробітників підприємства до аналітичної інформації;
- підготовка висновків і пропозицій, спрямованих на підвищення ефективності планованих і прийнятих заходів щодо захисту інформації, а також уточнення (коректування) організаційно-планових документів підприємства і його структурних підрозділів;
- вироблення рекомендацій стосовно внесення змін і доповнень у методичні документи, що регламентують алгоритм дій працівників підприємства щодо захисту інформації (стандарти підприємства).

Наявність постійної аналітичної роботи, її характер і результати визначають необхідність створення системи, основи її організації, структуру і зміст системи комплексного захисту інформації,

вимог до її ефективності і напрямку її розвитку та досконалості. Аналіз стану системи захисту інформації суттєво впливає на кількість, склад і структуру підрозділів підприємства, що безпосередньо вирішують завдання забезпечення ІБ (служба безпеки підприємства, служба охорони, режимно-секретний підрозділ і ін.).

Від ефективності і якості ведення на підприємстві аналітичної роботи повною мірою залежить стан захищеності інформаційних ресурсів підприємства, віднесених до категорії охоронюваних, а також своєчасність і обґрунтованість вживання заходів щодо виключення витоку конфіденційної інформації та втрат носіїв інформації. Ефективність аналітичної роботи і її результати є основою для прийняття керівництвом підприємства управлінських рішень із питань організації захисту інформації. З урахуванням результатів аналітичної роботи можуть створюватися такі основні заходи:

- уточнення планів роботи підприємства щодо захисту інформації, включення в них додаткових заходів;
- уточнення розподілу завдань і функцій між структурними підрозділами підприємства;
- переробка (уточнення) посадових (функціональних) обов'язків співробітників підприємства, у тому числі керівної ланки, удосконалювання систем пропускного і внутрішньооб'єктного режимів;
- обмеження кола осіб, що допускаються до конфіденційної інформації по різних напрямках діяльності підприємства;
- перегляд ступеня конфіденційності відомостей і їх носіїв;
- посилення системи охорони підприємства і його об'єктів, застосування особливих заходів захисту інформації на окремих об'єктах (у службових приміщеннях);
- прийняття рішень про обмеження публікацій у відкритому друку, використання в рекламній і видавничій діяльності окремих матеріалів (матеріалів за окремими темами), доступі відряджених осіб, про виключення розгляду цих матеріалів на конференціях, семінарах, зустрічах тощо.

Ведення ефективної аналітичної роботи можливе тільки, якщо є необхідна інформація. Для її одержання потрібна чітко сформована мета, що визначає конкретні джерела інформації. Аналітична робота на підприємстві повинна вестися послідовно і безупинно, являти собою повною мірою цілісне дослідження.

10.2. Основні етапи аналітичної роботи

В аналітичній роботі можна виділити такі основні етапи:

- формулювання цілей аналітичної роботи, розробка програми досліджень, формулювання попередніх гіпотез (результатів аналітичної роботи);
- відбір і аналіз джерел інформації, збір і узагальнення інформації;
- повноцінний аналіз наявної інформації й підготовка висновків.

Основна форма ведення аналітичної роботи – аналітичні дослідження.

Аналітичні дослідження вимагають чіткої організації процесу, оцінки наявних ресурсів для досягнення необхідного результату. Підсумком дослідження повинні бути висновки, пропозиції і рекомендації щодо удосконалювання системи захисту інформації.

На першому етапі аналітичного дослідження формулюють цілі і завдання дослідження, розробляють програму дослідження, яка становить наукову основу збору, узагальнення, обробки і аналізу всієї отриманої інформації. Типова програма досліджень містить такі основні розділи:

- цілі і завдання аналітичного дослідження;
- предмети і об’єкти дослідження;
- строки (період) проведення аналітичного дослідження;
- методики проведення дослідження;
- очікувані результати і передбачувані висновки.

Під час формулювання цілей і завдань дослідження потрібно враховувати, хто є його організатором і безпосереднім виконавцем, які сили і засоби можуть бути задіяні для його проведення, які будуть використовуватися джерела інформації, способи і методи її збору, обробки і аналізу, які існують можливості для реалізації пропозицій і рекомендацій, що будуть вироблені в ході досліджень.

Залежно від поставлених цілей і завдань визначають конкретні методи, технології дослідження, а також процедури збору й обробки інформації.

Найбільш типові завдання аналітичного дослідження:

- одержання даних про стан системи захисту інформації на

підприємстві (його конкретних об'єктах, у філіях, представництвах);

- виявлення можливих каналів витоку інформації, що підлягає захисту;
- визначення обставин, причин і чинників, що сприяють виникненню каналів витоку і створенню передумов для витоку інформації;
- підготовка для керівництва підприємства (філії, представництв) і його структурних підрозділів конкретних рекомендацій щодо закриття виявлених каналів витоку.

Під об'єктом дослідження розуміють все те, що вивчається і аналізується в ході дослідження. Предмет дослідження – та сторона об'єкта, яка безпосередньо підлягає вивченню в ході аналітичного дослідження.

Особливе значення на першому етапі аналітичної роботи має формулювання попередніх гіпотез (версій). Попередні гіпотези повинні пояснити роль і місце висновків аналітичних досліджень у логічній послідовності подій, що відбуваються, у сфері захисту охоронюваної інформації.

Побудова попередніх гіпотез проводиться в такому порядку. Спочатку формується повний список відомостей, які пропонується досліджувати (проаналізувати). Відомості, що ввійшли в список, систематизуються і розташовуються за ступенем важливості.

Далі із усього обсягу інформації виділяється група найбільш значущих відомостей, роль яких особливо очевидна в ситуації, що аналізується і оцінюється. Обрані відомості класифікуються за актуальністю, способом одержання і ступенем вірогідності джерела. Найбільш актуальні відомості аналізуються передусім.

Потім проводиться вибір попередніх гіпотез, що пояснюють прояв тих або тих подій (появу тих або тих відомостей). Причому стосовно однієї події здійснюється перевірка неякісних гіпотез (версій). Під час послідовної перевірки гіпотез особлива увага приділяється найбільш реальним. Ці гіпотези фіксуються. Найменш реальні гіпотези відхиляються.

Отже, послідовно вибираються і формуються найбільш імовірні припущення, що пояснюють появу тих або тих конкретних подій (виникнення відомостей). Можливі протиріччя в отриманих висновках щодо передбачуваних версій подій, що відбуваються, усу-

ваються шляхом всебічної послідовної перевірки реальності гіпотез.

Результатом роботи з формулювання попередніх гіпотез є вибір версії, яка найбільш точно порівняно з іншими версіями пояснює причину виникнення конкретної ситуації, пов'язаної з появою можливого каналу витоку конфіденційної інформації, і характеризує стан системи захисту інформації, у тому числі дії відповідних посадових осіб, якість виконання заходів тощо.

На другому етапі проводиться відбір і аналіз джерел інформації, збір і узагальнення даних з метою виявлення каналу несанкціонованого доступу до відомостей конфіденційного характеру, виключення можливості виникнення такого каналу.

Для цього здійснюється постійний контроль об'єктів захисту (інформаційних ресурсів), а також ступені захищеності у них інформації, проводиться аналіз даних, одержуваних з різних джерел.

Для вирішення конкретного завдання аналітичного дослідження в межах другого етапу із усіх наявних у розпорядженні аналітичного підрозділу джерел інформації відбираються ті, з яких надходить інформація, найбільш близька до досліджуваних проблем, й одночасно досить достовірна.

Аналітичне дослідження джерел інформації передбачає проведення таких основних заходів:

- формування вичерпного переліку джерел конфіденційної інформації на підприємстві;
- формування і своєчасне уточнення переліку та складу конфіденційної інформації, що реально циркулює (оброблюється) на об'єктах підприємства, із вказівкою конкретних носіїв, на яких вона зберігається;
- організація і ведення обліку поінформованості співробітників підприємства в конфіденційній інформації, накопичення даних про їх ознайомлення з конкретними відомостями конфіденційного характеру із вказівкою носіїв цих відомостей;
- вивчення і оцінка відповідності ступеня конфіденційності, якому привласнена інформація, реальній цінності цієї інформації;
- вивчення внутрішніх і зовнішніх загроз кожному наявному на підприємстві джерелу конфіденційної інформації;
- виявлення підприємств, зацікавлених в одержанні конфіденційної інформації (фірм-конкурентів), а також окремих осіб злов-

мисників і їх систематизація (класифікація);

- аналіз повноти і якості заходів щодо захисту конфіденційної інформації, прийнятих у конкретних ситуаціях. Облік і аналіз спроб представників фірм-конкурентів, а також інших зловмисників одержати конфіденційну інформацію;
- облік і аналіз контактів співробітників підприємства із представниками фірм-конкурентів незалежно від того, чи стосувалися вони питань конфіденційного характеру або ні.

У ході вивчення і дослідження джерел інформації виконується їх оцінка з критеріїв надійності та вірогідності одержуваної з них інформації. Оцінка джерел інформації здійснюється методом ранжирування (класифікації) самих джерел, з яких надходить інформація, і способів її одержання. Може використовуватися система експертної оцінки (безпосередньо аналітиком) надійності і вірогідності отриманих даних. Рівень підготовки і практичні навички дозволяють співробітникові аналітичного підрозділу найбільш точно оцінити інформацію, її джерело й спосіб її одержання.

Під час виконання оцінки зазначених елементів, як правило, використовують такі критерії:

1. Оцінка джерела:
   - надійне джерело;
   - звичайно надійне джерело;
   - досить надійне джерело;
   - не завжди надійне джерело;
   - ненадійне джерело;
   - джерело невстановленої надійності.
2. Оцінка отриманої інформації:
   - інформація, підтверджена іншими фактами;
   - інформація, підтверджена іншими джерелами;
   - інформація, яка з високим ступенем імовірності відповідає дійсності;
   - інформація, яка можливо відповідає дійсності;
   - сумнівна інформація;
   - неправдоподібна інформація;
   - інформація, установити (підтвердити) вірогідність якої неможливо.
3. Оцінка способу одержання інформації джерелом:
   - інформація, отримана джерелом самостійно;

- інформація, отримана джерелом з іншого постійного джерела інформації (наприклад, відкритого джерела);
- інформація, отримана джерелом з іншого «разового» джерела (наприклад, у ході переговорів, неформального спілкування).

У ході оцінки вірогідності інформації і її джерела необхідно враховувати можливість навмисної дезінформації, а також отримання ненавмисно перекрученої інформації. В обох випадках необхідне проведення додаткової перевірки і більш докладного всебічного аналізу отриманої інформації для ухвалення рішення про її використання в ході аналітичних досліджень.

З урахуванням результатів оцінки отриманої інформації, а також джерел і способів її одержання здійснюються збір і узагальнення (систематизація) необхідних для проведення повноцінного аналізу відомостей.

У ході третього етапу аналітичної роботи здійснюють повноцінний аналіз отриманої інформації і за його результатами – всебічний аналіз стану системи захисту інформації, готують ефективні заходи щодо її вдосконалювання. На цьому етапі оформляють результати аналітичних досліджень, готують висновки, рекомендації і пропозиції у сфері захисту охоронюваної інформації. Аналіз стану системи захисту інформації включає вивчення можливих каналів витоку інформації, оцінку ефективності заходів для їхнього перекриття, оцінки дій персоналу підприємства за вирішенням завдань у сфері захисту інформації, визначення основних напрямків діяльності щодо захисту інформації.

10.3. Основні види та зміст аналітичних звітів

Основною формою результатів аналітичних досліджень є аналітичний звіт. Звіти можуть оформлятися в письмовій формі, також вони можуть бути подані в усній формі, супроводжуватися графіками, діаграмами, малюнками, таблицями, які пояснюють або відображають результати виконаної роботи.

Основні розділи аналітичного звіту можуть бути такі:

- зміст аналітичного дослідження (цілі і завдання аналітичного дослідження, шляхи вирішення поставлених завдань, питан-

ня, що підлягають аналізу та оцінці; передбачувані результати дослідження);

- джерела інформації, ступінь вірогідності отриманої інформації (оцінки отриманої інформації, джерел і способів її одержання, результати аналізу ступеня вірогідності отриманої з використанням цих джерел аналітичної інформації);
- узагальнення отриманої інформації (алгоритм збору і узагальнення необхідної для виконання повноцінного аналізу інформації – із усього обсягу отриманої і обробленої інформації виділяють найбільш значущі факти);
- основні і альтернативні версії або гіпотези (мотивований розподіл версій на основні і додаткові або альтернативні, що пояснюють або характеризують досліджувані події і факти);
- відсутня інформація (додаткова інформація, необхідна для підтвердження основної версії, її джерела і способи одержання);
- висновки (результати аналізу і оцінки поставлених питань, висновки щодо ступеня важливості отриманої і обробленої інформації, значення цієї інформації для прийняття конкретних рішень у сфері захисту конфіденційної інформації, взаємозв'язок результатів цього аналітичного дослідження з іншими напрямками аналітичної роботи в сфері захисту інформації, можливі загрози захисту інформації, а також можливі наслідки впливу негативних чинників);
- пропозиції й рекомендації щодо удосконалювання роботи у сфері захисту інформації (конкретні пропозиції і рекомендації керівництву підприємства та керівникам структурних підрозділів щодо вдосконалювання роботи у сфері захисту конфіденційної інформації; вироблені на основі виконаного аналізу отриманої інформації, а також на основі різних подій і фактів конкретні заходи, прийняття яких необхідно для закриття можливих каналів витоку інформації і запобігання потенційних загроз інформації, що захищається).

В окремих випадках за результатами більш глибокого аналізу стану системи захисту інформації створюється алгоритм і способи дій персоналу підприємства в конкретних ситуаціях.

Залежно від призначення використовують такі основні види аналітичних звітів:

- оперативний (тактичний) звіт;
- перспективний (стратегічний) звіт;

- періодичний звіт.

Оперативні (тактичні) звіти містять результати аналітичних досліджень, виконаних для підготовки і прийняття якого-небудь оперативного (екстреного) рішення щодо питання короткочасного (термінового) характеру. Під час таких досліджень аналізу і оцінки зазнає інформація, як правило, невеликого обсягу.

Перспективні (стратегічні) звіти містять інформацію, найбільш повну за змістом. Аналіз цієї інформації не обмежений за терміном (часом) його проведення. У такі звіти, як правило, включається інформація, що містить більш повний аналіз передумов конкретних ситуацій, фактів, подій. У звітах викладаються прогнози і перспективи розвитку цих ситуацій. Звіти цього виду відповідають постійним напрямкам аналітичних досліджень.

Періодичні звіти призначені для аналізу стану системи захисту інформації (окремих напрямків захисту інформації) відповідно до розробленого і затвердженого керівництвом підприємства графіком. Ці звіти не залежать від подій, що відбуваються (виникнення різних ситуацій), пов'язаних із захистом інформації. Такі звіти готуються відповідно до проблем, що є об'єктами постійної уваги з боку служби безпеки підприємства (його аналітичного підрозділу).

До створення звітів, незалежно від форми, є загальні вимоги, а саме: наявність глибокого аналізу подій (фактів, отриманої інформації), простота, чіткість і грамотність викладу матеріалу, логічність міркувань і висновків, відповідність звітів установленій формі.

Одна з найбільш важливих вимог, пропонованих до звітів, полягає в тому, що їх зміст і рівень підготовки аналітичного матеріалу повинні відповідати запитам конкретних споживачів аналітичної інформації – керівників структурних підрозділів або окремих співробітників підприємства.

10.4. Класифікація методів аналізу інформації

Повнота і якість виконання аналітичних досліджень, достовірність отриманих результатів і ефективність вироблених пропозицій і рекомендацій повною мірою залежать від тих методів аналізу інформації, які були обрані і використовувалися співробітниками аналітичного підрозділу безпосередньо під час досліджень.

Застосовувані в ході аналітичних досліджень методи аналізу інформації ділять на три групи:

- загальнонаукові (якісні);
- кількісні;
- приватно-наукові.

Основні методи аналізу, що належать до першої групи, включають метод висування гіпотез, метод інтуїції, метод спостереження, метод порівняння, метод експерименту.

З кількісних методів найпоширеніший метод статистичних досліджень.

До третьої групи належать методи письмового та усного опитування, метод індивідуальної бесіди і метод експертної оцінки.

Метод висування гіпотез полягає в процедурі відділення відомого від невідомого і вичленовування в невідомому окремих, найбільш важливих елементів і фактів (подій).

Метод інтуїції полягає у використанні аналітиком своєї здатності до безпосереднього збагнення істини (досягненню необхідного результату) без попереднього логічного міркування. Багато в чому цей метод ґрунтується на особистому досвіді аналітика.

Метод спостереження полягає в безпосередньому дослідженні (обстеженні) конкретного об'єкта (джерела інформації, події, дії, факту), у самостійному описі аналітиком яких-небудь фактів (подій, процесів), а також їх логічних зв'язків протягом визначеного часу.

Мета методу порівняння полягає в більш глибокому вивченні процесів (подій), що відбуваються на підприємстві й стосуються питань захисту охоронюваної інформації. Порівнюються різні чинники, що зумовлюють причини і обставини, які призводять до витоку конфіденційної інформації або до виникнення наслідків до її витоку. Під час використання методу порівняння обов'язково дотримуються таких основних умов: об'єкти (дії, явища, події) повинні бути порівняні за своїми якісними особливостями; порівняння повинне визначити не тільки елементи подібності, але й елементи відмінності між досліджуваними об'єктами.

Метод експерименту використовується для перевірки результатів діяльності за конкретним напрямком захисту інформації або для пошуку нових рішень, удосконалювання системи її захисту.

Роль кількісних методів аналізу полягає в інформаційному, статистичному забезпеченні якісних методів. Найбільш характер-

ний метод статистичних досліджень, який полягає у виконанні кількісного аналізу окремих сторін досліджуваного явища (факту, події). У ході цього аналізу накопичуються цифрові дані про стан і динаміку порушень режиму конфіденційності (таємності) у процесі виконаних робіт, про ефективність рішення службою безпеки (режимно-секретним підрозділом) завдань щодо їх недопущення, про тенденції розвитку ситуації у сфері інформаційної безпеки тощо.

Методи письмового та усного опитування полягають в одержанні шляхом анкетування (або іншим способом) необхідної інформації від співробітників підприємства, керівників підрозділів, а також осіб, що допускають порушення встановленого режиму таємності (конфіденційності інформації). Водночас в анкеті вказують кілька можливих варіантів відповідей на кожне поставлене питання.

Метод індивідуальної бесіди відрізняється від методу письмового та усного опитування необхідністю особистого спілкування зі співробітником підприємства. Використання цього методу дозволяє в бесіді, що динамічно розвивається, одержати конкретну інформацію залежно від цілей аналітичного дослідження.

Метод експертної оцінки включає облік і аналіз різних думок щодо певного кола питань, які висловлюють фахівці сфери діяльності підприємства, пов’язаної з конфіденційною інформацією.

Вибір конкретних методів аналізу під час аналітичних досліджень у сфері захисту конфіденційної інформації залежить від цілей і завдань досліджень, а також від специфіки діяльності підприємства, складу і структури служби безпеки та її аналітичного підрозділу.

Контрольні запитання

1. На які групи поділяють методи аналізу інформації щодо безпеки підприємства?
2. Який з кількісних методів аналізу інформації є найпоширенішим?
3. У чому полягає метод висування гіпотез?
4. У чому полягає метод інтуїції?
5. У чому полягає метод спостереження?
6. У чому полягає метод порівняння?
7. У чому полягає метод експерименту?
8. У чому полягає метод письмового та усного опитування?
9. У чому полягає метод індивідуальної бесіди?
10. У чому полягає метод експертної оцінки?
11. Перелічіть основні види аналітичних звітів.
12. Перелічіть основні найбільш типові завдання аналітичного дослідження.

ВИСНОВКИ

Захист інформації в наш час є одним з головних напрямків забезпечення безпеки держави, суспільства та окремої особистості. Проблеми різних аспектів безпеки стають усе більш актуальними з подальшим розвитком інформаційно-комунікаційних технологій. Наслідком від порушень інформаційної безпеки може бути колосальна сума в грошовому вираженні. Саме це визначає особливу увагу до питань вивчення методів організації захисту інформації, першочергової складової у тріаді комплексного забезпечення інформаційної безпеки, поряд із правовими та інженерно-технічними методами.

Зміст пропонованого навчального посібника відображає основні напрямки діяльності щодо організації захисту інформації на підприємствах, організаціях і установах. Організаційне забезпечення інформаційної безпеки містить у собі роботу із забезпечення вивіреної кадрової політики, розподілу відповідальності за призначені ділянки робіт, регламентацію всіх напрямків захисту інформації, ліцензування і сертифікацію у сфері інформаційних технологій, забезпечення режиму таємності у діловодстві і діяльності підприємства, організацію внутрішньооб'єктного режиму і охорону об'єктів підприємства.

Динаміка розвитку законодавства в галузі інформаційної безпеки потребує постійної зміни методів і форм забезпечення інформаційної безпеки. Зокрема, безупинно розвиваються методи організації захисту інформації відповідно до знову прийнятих законів України, указів Президента, постановами уряду тощо.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Основні нормативні акти

1. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
2. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.
3. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650–651.
4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286 (із змінами 2005 р.).
5. Про затвердження Концепції технічного захисту інформації в Україні : Постанова Кабінету Міністрів України від 08.10.1997 р. № 1126-97-п. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF
6. Про затвердження Положення про технічний захист інформації в Україні : Постанова Кабінету Міністрів України від 09.09.1994 р. № 632-94-п. URL: https://zakon.rada.gov.ua/laws/show/632-94-%D0%BF
7. Про затвердження Концепції технічного захисту інформації в Україні : Постанова Кабінету Міністрів України № 1126 від 08.11.1997 р. № 1126-97-п. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF
8. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.
9. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.
10. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

2. Нормативні документи в галузі технічного захисту інформації та державні стандарти України (ДСТУ)

1. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835
2. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96. URL:

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836
3. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=102122&showHidden=0
4. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf
5. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407
6. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-008-2002.pdf
7. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/2.5-010-03.pdf
8. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. URL: https://tzi.com.ua/downloads/3.7-001-99.pdf
9. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/3.6-001-2000.pdf
10. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.ua/assets/files/%D0%9D%D0%94%20%D0%A2%D0%97%D0%98%201.1-002-99.pdf
11. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=68935
12. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911

3. Навчальні посібники, інші дидактичні та методичні матеріали

1. Зубок М. І. Інформаційна безпека в підприємницькій діяльності : підручник. Київ : ГНОЗІС, 2015. 216 с.
2. Толюпа С. В., Оксіюк О. Г., Бурячок В. Л., Вялкова В. І. Захист об'єктів інформаційної діяльності : навч. посіб. Київ : ККБ та ЗІ ФІТ КНУ імені Тараса Шевченка. 2018. 322 с.
3. Андрушків Б. М., Малюта Л. Я. Економічна та майнова безпека бізнесу : навч. посіб. Тернопіль : ФОП Паляниця В. А. 2016. 180 с.
4. Аверченков В. И., Рытов М. Ю. Организационная защита информации : учеб. пособ. для вузов. Москва : Изд-во «ФЛИНТА», 2017. 184 с.
5. Гришина Н. В. Комплексная система защиты информации на предприятии : учеб. пособ. Москва : Форум, 2015. 240 с.
6. Вдовенко Л. А. Информационная система предприятия : учеб. пособие. Москва : ИНФРА-М, 2016. 237 с.
7. Дворский М. Н., Палатченко С. Н. Техническая безопасность объектов предпринимательства : в 2 т. Киев : А-ДЕПТ, 2013. I т. 304 с.
8. Дворский М.Н., Палатченко С.Н. Техническая безопасность объектов предпринимательства : в 2 т. Киев : А-ДЕПТ, 2013. II т. 255 с.
9. Косиченко О. О. Правові інформаційні ресурси Інтернет : довідник. Дніпро : Дніпропетр. державний ун-т внутрішніх справ, 2017. 65 с.
10. Косиченко О. О., Махницький О. В. Інформаційне забезпечення юридичної діяльності : посібник. Дніпро : Дніпропетр. державний ун-т внутрішніх справ, 2018. 205 с.
11. Косиченко О. О., Махницький О. В. Захист службової інформації під час використання електронної пошти на основі асиметричного шифрування з відкритим ключем : метод. вказівки. Дніпро : Дніпропетр. державний ун-т внутрішніх справ, 2018. 35 с.
12. Вишня В. Б., Косиченко О. О. Інформаційно-бібліографічний пошук у мережі Internet : навч. посіб. Дніпропетровськ : Дніпропетр. державний ун-т внутрішніх справ, 2013. 60 с.
13. Вишня В. Б., Косиченко О. О., Трусов В. О. Інформаційне забезпечення юридичної діяльності : навч. посіб. для студентів : у 2 ч. Дніпропетровськ : Дніпропетр. державний ун-т внутрішніх справ, 2006. Ч. 1. 164 с.
14. Бурячок В. Л., Толубко В. О., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник; за заг. ред. д-ра техн. наук, проф. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.
15. Рибальський О. В., Смаглюк В. М., Хахановський В. Г. Основи інформаційної безпеки : підруч. для курсантів ВНЗ МВС України. Київ : НАВС, 2016. 255 с.
16. Лужецький В. А., Кожухівський А. Д., Войтович О. П. Основи інформаційної безпеки : навч. посіб. Вінниця : ВНТУ, 2016. 268 с.

17. Камский В. А. Защита личной информации в Интернете, смартфоне и компьютере. Санкт-Петербург : Наука и Техника, 2017. 272 с.
18. Гришина Н. В. Информационная безопасность предприятия : учеб. пособ. Москва : Форум, 2015. 240 с.
19. Мельничук Т. В. Кримінологічна безпека економічної діяльності : навч.-метод. посіб.; рец.: Стрельцов Є. Л., Аркуша Л. І. Одеса : Гельветика, 2018. 96 с.

4. Інтернет-ресурси

1. Журнал «Бизнес и безопасность», м. Київ (www.bsm.com.ua)
2. Журнал «Сучасна спеціальна техніка», м. Київ
3. https://infocity.kiev.ua – Центр комп'ютерної безпеки, м. Київ
4. http://www.naiau.kiev.ua – сайт Національної академії внутрішніх справ
5. http://ci.uz.gov.ua/common/acts.html
6. http://info.resourcecorp.net
7. http://www.legal.com.ua
8. http://www.liga.kiev.ua
9. http://www.mdoffice.com.ua

Навчальне видання

Дисковський Олександр Андрійович
Косиченко Олександр Олександрович
Рибальченко Людмила Володимирівна

ОСНОВИ ОРГАНІЗАЦІЇ ЗАХИСТУ ОБ'ЄКТІВ ТА ІНФОРМАЦІЇ ВІД ЗЛОЧИННИХ ПОСЯГАНЬ

Навчальний посібник

Редактор, оригінал-макет, дизайн – *А. В. Самотуга*
Редактор О. М. Врублевська

Підп. до друку 20.08.2020. Формат 60x84/16. Друк – RISO.
Гарнітура – Times. Ум.-друк. арк. 5,75. Обл.-вид. арк. 6,00. Тираж – 50 прим.
Зам. № 01/20-нп

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Гагаріна, 26, т. (056) 756-46-41
Свідоцтво про внесення до державного реєстру ДК № 6054 від 28.02.2018