ТЕМА 10
РЕЖИМНИЙ ХАРАКТЕР РОБОТИ ОРГАНІЗАЦІЇ ЯК ОСНОВА КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ПЛАН

1. Розробка політики безпеки.
2. Система фізичного захисту – типові задачі та способи її реалізації. Основні характеристики системи фізичного захисту.
3. Кількісний і якісний аналіз системи фізичного захисту.
4. Інженерно-технічні засоби охорони.

1. Розробка Політики безпеки

Автоматизація процесів діяльності (бізнес-процесів) практично будь-якого сучасного підприємства сприяє росту продуктивності праці та поліпшенню управління за рахунок функціонування корпоративної інформаційної системы (КІС). З іншої сторони, одночасно з цим збільшується рівень інформаційних ризиків.

Аналіз світового та вітчизняного досвіду щодо ІБ диктує необхідність створення системи забезпечення безпеки інформації (СЗБІ) – взаємопов'язані різноманітні організаційні та технічні заходи захисту, що використовують сучасні методи прогнозування, аналізу і моделювання.

Створення повномасштабної СЗБІ вимагає значних фінансових витрат. Покрити необхідні витрати відразу, як правило, не представляється можливим. Це призводить до необхідності поетапної побудови системи (розгортання її окремих елементів з затримкою в часі). Очевидно, що для цілісного об'єднання цих елементів, що розробляються або закуповуються в різний час, необхідний єдиний архітектурний задум СЗБІ. Іншими словами, організація повинна сформувати свою Політику безпеки інформації.

Політика безпеки інформації – це сукупність нормативних документів, які встановлюють порядок забезпечення безпеки інформації на конкретному підприємстві, а також висуваючих вимоги з підтримки цього порядку. Важливо підкреслити, що документи, які розробляються при формуванні Політики безпеки, повинні мати офіційний юридичний статус (підпис першої особи).

Розробка Політики безпеки інформації є основоположним етапом при розробці та подальшому впровадженні СЗБІ. Якщо вимоги, висунуті на початку розробки не повні або помилкові, то, СЗБІ в ряді випадків не зможе повністю відповідати своєму призначенню.

Очевидно, що розробити Політику безпеки інформації, тобто побудувати повну систему правил і вимог з безпеки інформації, можливо тільки в тому випадку, якщо проаналізовані всі інформаційні ризики і визначена нормативна база, що регулює питання захисту інформації. Тому попереднім етапом для розробки Політики безпеки повинно бути Комплексне обстеження захищеності КІС організації.

Як говорилося вище, під Політикою безпеки інформації розуміється узгоджений по цілям захисту інформації пакет нормативно, організаційно-

розпорядчих та експлуатаційних документів, що регламентують всі питання організації, управління і контролю безпеки, а також експлуатації засобів захисту. Структура даного пакета документів подається у вигляді трьох ієрархічних рівнів.

Перший рівень Політики безпеки інформації містить головний документ "Концепція інформаційної безпеки", яка визначає цілі і завдання захисту інформації в КІС, корпоративні вимоги і практичні правила управління інформаційною безпекою, склад інших документів, що регламентують питання безпеки інформації. За своєю суттю це стратегія вирішення питань захисту інформації.

Даний документ є системоутворюючим, який інтегрує всі документи Політики безпеки за поставленими цілями і завданнями інформаційної безпеки.

Другий рівень, як правило, містить два документа: "Регламент забезпечення безпеки інформації" та "Профіль захисту", які є нормативними або організаційно-розпорядчими документами.

"Регламент забезпечення безпеки інформації" розробляється на підставі "Концепції безпеки інформації" і в директивної формі викладає порядок поводження із захищаємою інформацією, основні правила дій співробітників і їх відповідальність у забезпеченні безпеки інформації в будь-яких ситуаціях і на всіх стадіях життєвого циклу КІС підприємства.

"Профіль захисту" містить технічні вимоги до програмно-апаратних засобів захисту, в тому числі і вбудованим в загальносистемне програмне забезпечення на основі відповідних державних і галузевих стандартів.

Після розробки документів першого і другого рівнів проводиться наступний етап робіт – *третій рівень* – розробка виконавчої документації, що включає в себе різні посадові положення та інструкції, доцільність яких визначається за результатами першого та другого етапів. Крім того, даний рівень містить експлуатаційні документи засобів захисту інформації. Третій рівень політики безпеки спирається на експлуатаційну документацію використовуваних програмно-технічних засобів захисту, загальносистемного та прикладного програмного забезпечення, а також на стратегію і тактику захисту, що забезпечується технічними і програмними засобами СЗБІ і КІС.

2. Система фізичного захисту – типові задачі та способ її реалізації. Основні характеристики системи фізичного захисту

Система фізичного захисту (СФЗ) – сукупність людей, процедур і обладнання, які захищають майно (об'єкти) від розкрадання, диверсій та інших неправомірних дій. Кінцева мета СФЗ – запобігання успішного виконання кваліфікованим порушником відкритих або таємних зловмисних акцій.

Типові завдання СФЗ: запобігання диверсій, спрямованих на виведення з ладу обладнання; запобігання розкрадань матеріальних засобів, майна або інформації; захист співробітників об'єкта.

Основними характеристики СФЗ є:

- надійність (ешелонування, рівні захисту);
- мінімізація наслідків відмов; збалансованість.

Існує два способи організації ефективної СФЗ: стримування; виявлення, затримка і реагування.

Стримування – реалізація заходів, які сприймаються потенційним порушником як важкоподолане, страхітливе і перетворюють об'єкт в неприваблиру мету. Результат стримування – порушник припиняє напад, або взагалі його не робить.

Приклад: охорона з відповідною формою; достатнє освітлення; попереджувальні знаки; грати на вікнах; бетонний паркан, колючий дріт; наявність сигналізації та систем відеоспостереження; опечатування.

Стримування безсиле, якщо порушник вирішується на напад, незважаючи на перешкоди. Покладатися на стримування як безальтернативний захист вкрай ризиковано. До того ж якість захисту способом стримування важко виміряти і оцінити. Навіть якщо не було нападів, це не означає, що система фізичного захисту способом стримування ефективна.

Виявлення – візуальна реєстрація прихованої або відкритої акції порушника щодо проникнення в простір об'єкта. У виявленні особливо виділяються точки санкціонованого доступу, тобто виявлення при контролі входу і виходу осіб, яким не дозволено проносити матеріальні цінності та інформацію.

Показниками ефективності контролю на вході є: пропускна здатність; кількість персоналу, яка в одиницю часу має право проходу; частота помилкових проходів – частота, з якою дозволяється прохід за підробленими доку-ментами або невірно впізнаним; частота помилкових відмов - частота відмов у доступі особам, яким прохід дозволений.

Виявлення закінчується тільки за умови проведення оцінки вторгнення. Цілями оцінки є відповіді на питання Що? Хто? Де? Яка кількість?

Затримка – уповільнення просування порушника до мети. Шляхами (способами) затримки є: фізичні бар'єри, перешкоди; замки; персонал охорони (в режимі постійної готовності, або в режимі очікування).

Показник ефективності затримки – загальний час подолання кожного елемента затримки після виявлення.

Затримка до виявлення при визначенні ефективності не враховується. Це є також стримуванням. Причина полягає, в тому, що час втрачено для реакції на дії порушника.

Реагування – дія сил захисту щодо перешкод успіху порушника, перери-вання його дій. Для успішного переривання необхідна кількісна перевага охорони в очікуваній точці зупинки порушника, час на повне розгортання і точна інформація про порушника.

Завдання Виявлення та Затримки вирішуються, як правило, інженерно-технічними засобами та (або) силами охорони. В даний час ведуться відпові-дні розробки щодо створення засобів автоматичного Реагування.

3. Кількісний та якісний аналіз СФЗ

Метою аналізу є встановлення ефективності такого захисту. Кількісний аналіз СФЗ застосовується у випадках, коли втрата неприпустима навіть при

малій ймовірності нападу: АЕС, військові об’єкти, в’язниці, музеї, об’єкти енергетики, зв’язку.

Якісний аналіз СФЗ застосовується для об’єктів, що вимагають низького рівня захисту.

Аналіз виконується для: визначення стану СФЗ; підготовки до модернізації із застосуванням нових розробок; пристосування СФЗ до нових виробничих процесів, до появи нових цінних об’єктів; підвищення рівня захисту при зростанні загроз.

Нижче представлені деякі складові аналізу СФЗ на підприємствах і організаціях з внутрішньовідомчою охороною.

Шлях порушника

Шлях порушника – упорядкована послідовність дій проти об’єкта нападу, яка завершується диверсією, розкраданням або терористичним актом.

Приклади дій і шляхи порушника наведені відповідно в табл. 4 і на рис. 1.

Таблиця 4 – Приклад дій порушника

Шлях	Елемент затримки	Елемент виявлення
Подолати паркан або стіну	Матеріал паркану або міцність стіни	Датчик на паркані, шум при проломі
Пройти двері	Міцність дверей	Датчик на двері
Скопіювати файл	Час копіювання	Вхід в КІС

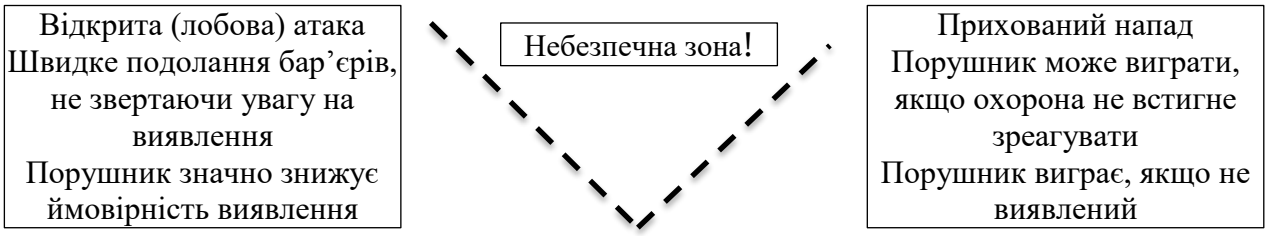

Рис. 1. Можливі шляхи порушника

Загальні обов’язки робітника охорони об’єкта з низьким рівнем захисту

Працівник охорони в будь-яких умовах повинен бути ввічливим і тактичним з громадянами, звертатися до них на “Ви”, свої вимоги і зауваження викладати в переконливій і зрозумілій формі, не допускати суперечок і дій, що ображають їх честь і гідність.

При звертанні до громадянина працівник охорони повинен назвати свою посаду і прізвище, після чого коротко повідомити причину і мету звернення. У разі звернення громадян працівник охорони, виконавши ті ж вимоги, зобов'язаний уважно вислухати і роз'яснити, куди слід звернутися для вирішення поставленого питання.

У розмові з громадянами працівники охорони зобов'язані виявляти спокій і витримку, не повинні вступати в суперечки, втрачати самовладання, відповідати грубістю на грубість і в своїх діях керуватися особистими неприязними почуттями.

Якщо порушник на зроблені йому зауваження реагує збудливо, потрібно дати йому час заспокоїтися, після чого роз'яснити неправильність його поведінки з посиланням на відповідні закони або інші правові акти. Після цього прийняти рішення про виклик начальника охорони або його помічника.

Зауваження порушникам, які мають при собі дітей, слід, по можливості, робити так, щоб діти цього не чули.

З підлітками працівник охорони повинен поводитися так само ввічливо, як і з дорослими. Зауваження дітям робляться з урахуванням їх віку та рівня розвитку.

З документами громадян при перевірці необхідно поводитися акуратно, не робити в них будь-які позначки. Якщо в документ вкладені гроші та інші цінні папери, необхідно запропонувати власнику самому взяти їх.

На місці вчинення правопорушення постової зобов'язаний:

- вжити заходів до припинення правопорушення;
- по можливості організувати затримання правопорушника;
- надати допомогу потерпілим, при необхідності викликати швидку допомогу;
- по можливості встановити свідків (очевидців);
- доповісти про те, що сталося, начальнику охорони і діяти відповідно до його вказівок.

Переслідування правопорушників ведеться тільки на території об'єкту, що охороняється.

Пропускний режим

У випадку пропускного режиму порядок забезпечується сукупністю заходів і правил, що виключають можливість безконтрольного входу-виходу осіб, в'їзду-виїзду транспортних засобів, вносу-виносу і ввезенню-вивезенню майна на об'єкти і з об'єктів, які охороняються.

Пропускний режим повинен передбачати такі основні заходи:

- встановлення та обладнання певних місць (КПП) для проходу (проїзду) на територію об'єкта;
- порядок допуску на об'єкти робочих змін, входу і виходу персоналу і відвідувачів;
- контроль за ввезенням (вивезенням), вносом (виносом) за межі охороняємого об'єкта матеріальних цінностей і т.д.;

Робочим органом по здійсненню пропускного режиму на об'єктах, що охороняються, є бюро перепусток, працівники яких входять до складу підрозділів відомчої охорони.

4. Інженерно-технічні засоби охорони

Для обладнання об'єктів охорони повинні використовуватися інженерно-технічні засоби охорони (ІТЗО), що мають державний сертифікат відповідності. Тип, кількість, місця установки і обсяг функцій, виконуваних інженерно-технічними засобами охорони, визначаються при проектуванні відповідно до технічного завдання на розробку, узгодженими та затвердженими з

компетентними органами в галузі забезпечення фізичної безпеки в установленому порядку.

Вимоги до ІТЗО об'єкта та їх елементів

Основним призначенням ІТЗО в поєднанні з організаційними заходами є своєчасне виявлення і протидія спробам вчинення актів незаконного втручання (в тому числі терористичних акцій) щодо майна, інформації, обладнання та фізичних осіб на об'єкті.

ІТЗО повинні забезпечувати: передачу сигналу тривоги на пульт чергового (начальника охорони); охорону і телеспостереження периметра і території; контрольно-пропускний режим на території об'єкта; управління доступом на об'єкт в цілому, а також в зони обмеженого доступу і окремі приміщення, ведення протоколу доступу; протипожежний контроль.

До складу ІТЗО входять: система збору, обробки і відображення інформації; технічні засоби охорони, що включають системи охоронної сигналізації (периметра, будівель і споруд), зв'язку та оповіщення, телевізійного спостереження, контролю та управління доступом, охоронного освітлення, гарантованого електропостачання.

Система збору та обробки інформації

Система збору, обробки і відображення інформації (СЗОВІ) – це сукупність пристроїв, призначених для передачі, прийому, збору, обробки, реєстрації та подання оператору інформації від засобів виявлення, а також для дистанційного керування пристроями технічних засобів охорони, контролю працездатності сповіщувачів та каналів передачі інформації. Структурно СЗОВІ повинна складатися з:

- центрального пульта управління на базі персонального комп'ютера і сертифікованих контрольних панелей, інтегрованих в єдину систему і забезпечених спеціалізованим програмним забезпеченням;
- сервера зберігання баз даних;
- апаратури локальної мережі, що розгортається на об'єктах охорони;
- станцій управління окремими системами технічних засобів охорони (ТЗО), виконаних на базі ПК або сертифікованих контрольних панелей серійного виробництва.

СЗОВІ повинна забезпечувати:

- надання за запитом уповноваженої особи інформації про стан будь-якого об'єкта та (або) технічного засобу, що входить до складу ІТЗО. Інформація надається відповідно до прав доступу користувача;
- підключення необмеженого числа користувачів, об'єктів і ТЗО в розрахунку на можливі зміни в структурі об'єкта охорони;
- відображення сигналів, які надходять на центральний пульт управління та інформації у візуальному, світловому та звуковому режимах, причому кожен сигнал повинен відображатися не менше ніж в двох режимах;
- реєстрацію сигналів та інформації, а також запитів уповноважених осіб;
- перешкоджання використанню СЗОВІ неуповноваженими особами.

Інженерні засоби охорони

До інженерних засобів охорони відносяться: огорожа периметра об'єкта охорони і внутрішніх зон обмеженого доступу; КПП з відповідним дооглядовим обладнанням; в'їзні ворота, хвіртки, шлагбауми.

Огорожа повинна виключати випадковий прохід людей (тварин), в'їзд транспорту або ускладнювати проникнення порушників на охороняєму територію, минаючи КПП. До огородження не повинні примикати будь-які прибудови, крім будівель, які є продовженням периметра. Вікна перших поверхів цих будівель, що виходять на територію без охорони, повинні бути обладнані металевими ґратами, а при необхідності й металевими сітками.

Периметри об'єкта охорони і зон обмеженого доступу, а також окремі об'єкти охорони там, де встановлений пропускний режим або планується йо-го введення, повинні бути обладнані КПП для проходу людей і проїзду транспорту (автомобільного, залізничного).

КПП повинен забезпечувати необхідну пропускну здатність проходу людей і проїзду транспорту. Територія КПП обладнується сигнальними ого-рожами, шлагбаумом і механізованими воротами.

У складі КПП рекомендується передбачити: коридор; приміщення для розміщення бюро перепусток; кімнату огляду; приміщення для співробітників охорони і розміщення технічних засобів охорони. Для виключення можливості несанкціонованого проходу на територію осіб, які не мають встановленої форми пропуску, КПП обладнуються системами контролю і управління доступом.

Для спостереження за обстановкою на території перед КПП із зовнішньої сторони периметра можливе використання вікон з однобічною видимістю, оглядових віконець дверей (воріт) і (або) систем охоронного телеспостереження.

На КПП для пропуску людей повинні бути встановлені стаціонарні металодетектори.

Електроживлення обладнання комплексної систем безпеки

Для аварійного електропостачання об'єктів охорони повинен бути передбачений аварійний дизель-генератор. Для аварійного електропостачання ТЗО можуть використовуватися джерела безперебійного електроживлення (ДБЖ). Потужність ДБЖ повинна бути достатньою для електропостачання протягом не менше 24 годин наступних систем: охоронної та пожежної сигналізації; телевізійного спостереження.

Перехід ТСО на роботу від резервного джерела електроживлення і назад повинен здійснюватися автоматично без видачі сигналів тривоги.