**Тема:** Комплексна система безпеки об'єкта, поняття, класифікація, вимоги

Створенню служби безпеки підприємства зазвичай передують дві події: або це гостре бажання керівників підприємства відреагувати на раптово виниклі реальні загрози майну, фізичної розправи з персоналом і т.д., або це заснований на результатах дослідження висновок про незадовільний стан безпеки підприємства. У першому випадку створена поспішно служба безпеки здатна в деякій мірі відобразити загрози і надалі реагувати на їх появу за принципом «загроза – відображення». Справа змінюється істотно при реалізації другого варіанту. Після детального вивчення стану безпеки підприємства (із залученням фахівців, якщо їх немає на підприємстві) у його керівників з’явиться реальне уявлення про систему безпеки підприємства.

Таке системне уявлення (зафіксоване в письмовій формі) дозволяє усвідомлено і цілеспрямовано проводити роботу щодо забезпечення безпеки підприємницької діяльності і самого підприємства усіма його підрозділами і співробітниками. При цьому провідна роль служби безпеки не зникає, навпаки, розуміння своєї ролі і місця в системі безпеки підприємства призведе тільки до позитивних результатів.

Слід однак підкреслити, що до теперішнього часу немає єдиного підходу до визначення поняття «система безпеки підприємства». Щоб дати таке визначення, необхідно попередньо виявити елементи цієї системи. Вивчення спеціалізованої літератури і практики дозволили автору прийти до висновку, що структурними елементами системи безпеки підприємства є наукова теорія його безпеки, політика і стратегія безпеки, засоби та методи забезпечення безпеки і, нарешті, концепція безпеки підприємства.

Сукупність перерахованих вище елементів становить систему безпеки підприємства.

Наукова теорія безпеки підприємства строго кажучи, така теорія знаходиться в стадії формування. Стосується це, перш за все, до понятійного апарату. Розберемо деякі з цих понять.

У російському законодавстві (українське в цьому плані, на жаль, значно відстає) поняття безпеки приведено в ст. 1 Закону РФ від 5 березня 1992 року «Про безпеку»: «стан захищеності життєво важливих інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз». Розкриття цього поняття терміном «захищеність» значно звужує її зміст, підкреслює пасивність при реагуванні на загрози. Сутність безпеки, як видається, пов’язана з поняттями «розвиток» і «стійкість». У зв’язку з цим під безпекою слід розуміти стан об’єкта (в нашому випадку – підприємства) у системі його зв’язків з точки зору здатності до стійкості (самовиживання) і розвитку в умовах внутрішніх і зовнішніх загроз, дій непередбачуваних і важко прогнозованих факторів. Відштовхуючись від цього поняття, визначимо такі функції безпеки: виявлення, попередження, зниження, ослаблення, нейтралізація, припинення, локалізація, відображення і усунення загроз.

Під загрозою безпеки підприємства слід розуміти потенційно або реально можлива подія, дія, процес або явище, яке здатне порушити його стійкість і розвиток або привести до зупинки його діяльності. Загрозу можна класифікувати за різними підставами і виміряти їх в кількісних параметрах. Наприклад, можливий збиток оцінюється числом загиблих людей, які втратили (ухудшивших) здоров’я, грошовій сумі економічних втрат і т.д. За ступенем ймовірності загроза оцінюється як неймовірна, малоймовірна, ймовірна, вельми вірогідна і цілком ймовірна. За ступенем розвитку загроза проходить чотири етапи: виникнення (зародження), експансія, стабілізація і ліквідація. Віддаленість загрози в часі визначається як безпосередня, близька (до 1 року) і далека (понад 1 року), а віддаленість в просторі – територія підприємства, прилегла до підприємства територія, територія регіону, територія країни, зарубіжна територія. Темпи наростання загрози вимірюються по місяцях, кварталах, роках. Напруженість загрози відбивається в двох вимірах:

а) нормальна, підвищена, близька до межі (поріг), надлишкова;

б) зростання, стабільність або зниження.

Крім цього, загрози поділяються за своєю природою їх виникнення на два класи:

1) природні (об’єктивні), тобто викликані стихійними природними явищами, що не залежать від людини (повені, землетруси, урагани і т.п.);

2) штучні (суб’єктивні), тобто викликані діяльністю людини, ненавмисні (ненавмисні) і навмисні (навмисні) загрози.

Розрізняють також економічні, соціальні, правові, органи заційного, інформаційні, екологічні, технічні та кримінальні загрози.

Під об’єктом безпеки підприємства слід розуміти ступінь стійкості і розвитку підприємства, його здатність протистояти загрозам. В об’єкти безпеки підприємства можна виділити:

– різні структурні підрозділи або групи співробітників, або власники акцій підприємства;

– ресурси підприємства (інформаційні, кадрові, матеріально-технічні, інформаційні, інтелектуальні і фінансові);

– різні види діяльності (управлінська, виробнича, постачальна і т.д.).

Метою забезпечення безпеки підприємства є комплексний вплив на потенційні і реальні загрози, що дозволяє йому успішно функціонувати в нестабільних умовах зовнішнього і внутрішнього середовища.

Досягнення цієї мети вимагає реалізації наступних завдань:

– виявлення загроз для стабільності і розвитку підприємства і вироблення заходів по їх протидії;

– забезпечення захисту технологічних процесів;

– реалізація заходів протидії всіх видів шпигунства (промислового, науково-технічного, економічного і т.д.);

– своєчасне інформування керівництва підприємства про факти порушення законодавства з боку державних і муніципальних органів, комерційних і некомерційних організацій, які зачіпають інтереси підприємства;

– попередження переманювання співробітників підприємства, що володіють конфіденційною інформацією;

– всебічне вивчення ділових партнерів;

– своєчасне виявлення і адекватне реагування на дезинформаційні заходи;

– розробка і вдосконалення локальних правових актів, спрямованих на забезпечення безпеки підприємства;

– реалізація заходів щодо захисту комерційної та іншої інформації;

– організація заходів з протидії недобросовісної конкуренції;

– забезпечення захисту всіх видів ресурсів підприємства;

– реалізація заходів щодо захисту інтелектуальної власності;

– організація і проведення заходів щодо запобігання надзвичайним ситуаціям;

– виявлення негативних тенденцій серед персоналу підприємства, інформування про них керівництва підприємства і розробка відповідних рекомендацій;

– організація взаємодії з правоохоронними та контролюючими органами з метою попередження і припинення правопорушень, спрямованих проти інтересів підприємства;

– розробка і реалізація заходів щодо попередження загроз фізичній безпеці майну підприємства і його персоналу;

– відшкодування матеріальної та моральної шкоди, завданої підприємству в результаті неправомірних дій організацій і окремих фізичних осіб.

Система безпеки підприємства може бути побудована на основі наступних принципів:

1) Пріоритет заходів попередження. Зміст цього принципу передбачає своєчасне виявлення тенденцій і передумов, що сприяють розвитку загроз, на основі аналізу яких виробляються відповідні профілактичні заходи щодо недопущення виникнення реальних загроз.

2) Законність. Заходи безпеки підприємства розробляються на основі і в рамках чинних правових актів. Локальні правові акти підприємства не повинні суперечити законам і підзаконним актам.

3) Комплексне використання сил і засобів. Для забезпечення безпеки використовуються всі наявні в розпорядженні підприємства сили та засоби. Кожен співробітник повинен в рамках своєї компетенції брати участь у забезпеченні безпеки підприємства. Організаційною формою комплексного використання сил і засобів є програма забезпечення безпеки підприємства.

4) Координація та взаємодія всередині і поза підприємством. Заходи протидії загрозам здійснюються на основі взаємодії та скоординованості зусиль всіх підрозділів, служб підприємства, а також встановлення необхідних контактів із зовнішніми організаціями, здатними надати необхідне сприяння в забезпеченні безпеки підприємства.

5) Поєднання гласності з конспірацією. Доведення до відома персоналу підприємства та громадськості в допустимих межах заходів безпеки виконує найважливішу роль – запобігання потенційних і реальних загроз. Така гласність, однак, повинна неодмінно доповнюватися в виправданих випадках заходами конспіративного характеру.

6) Компетентність. Співробітники та групи співробітників повинні вирішувати питання забезпечення безпеки на професійному рівні, а в необхідних випадках спеціалізуватися по основним його напрямам.

7) Економічна доцільність. Вартість фінансових витрат на забезпечення безпеки не повинна перевищувати той оптимальний рівень, при якому втрачається економічний сенс їх застосування.

8) Планова основа діяльності. Діяльність із забезпечення безпеки повинна будуватися на основі комплексної програми забезпечення безпеки підприємства, підпрограм забезпечення безпеки по основним його видам (економічна, науково-технічна, екологічна, технологи чна і т.д.) і розробляються для їх виконання планів роботи підрозділів підприємства та окремих співробітників .

9) Системність. Цей принцип передбачає врахування всіх факторів, що впливають на безпеку підприємства, включення в діяльність щодо його забезпечення всіх співробітників підрозділів, використання в цій діяльності всіх сил і засобів.

Система безпеки підприємства включає в себе ряд наступних підсистем.

Економічна безпека – стан найбільш ефективного використання всіх видів ресурсів з метою запобігання (нейтралізації, ліквідації) загроз і забезпечення стабільного функціонування підприємства в умовах ринкової економіки.

Техногенна безпека – сукупність дій по забезпеченню проектування, будівництва і експлуатації складних технічних пристроїв з дотриманням необхідних вимог безаварійної їх роботи.

Екологічна безпека – стан захищеності життєво важливих інтересів персоналу підприємства і його майна від потенційних або реальних загроз, що створюються наслідками антропогенного впливу на навколишнє середовище, а також від стихійних лих і катастроф.

Інформаційна безпека – це здатність персоналу підприємства забезпечити захист інформаційних ресурсів і потоків від загроз несанкціонованого доступу до них.

Психологічна безпека – стан захищеності від негативних психологічних впливів персоналу підприємства та інших осіб, залучених до її діяльність.

Фізична безпека – стан захищеності життя і здоров’я окремих осіб (груп, всіх осіб) підприємства від насильницьких злочинів.

Науково-технічна безпека – здатність персоналу підприємства забезпечити захист власної цінної науково-технічної продукції від недобросовісних конкурентів.

Пожежна безпека – стан об’єктів підприємства, при якому заходи попередження пожеж та протипожежного захисту відповідають нормативним вимогам.

Слід зазначити, що вищевказані підсистеми другого рівня можуть включати в себе підсистеми третього рівня. Наприклад, підсистемами економічної безпеки можуть бути – фінансова, комерційна, майнова, а також інші підсистеми безпеки.

Крім цього, самі підсистеми не розділені між собою непрохідною кордоном, оскільки вони настільки взаємопов’язані один з одним, що в органічній єдності утворюють єдину систему безпеки підприємства. Поділ же єдиної системи безпеки підприємства на підсистеми другого і третього рівня проводиться з методичних міркувань, оскільки це дозволяє більш детально вивчити всі його елементи.

Надійність і ефективність системи безпеки підприємства оцінюється на основі одного критерію – ступеня відсутності або наявності завданої йому матеріальної та моральної шкоди. Зміст цього критерію розкривається через ряд показників:

1) недопущення фактів витоку конфіденційних відомостей;

2) попередження або припинення протиправних дій з боку персоналу підприємства, його відвідувачів, клієнтів;

3) збереження майна та інтелектуальної власності підприємства;

4) попередження надзвичайних ситуацій;

5) припинення насильницьких злочинів щодо окремих (спеціально виділених) співробітників і груп працівників підприємства;

6) своєчасне виявлення і припинення спроб несанкціонованого проникнення на охоронювані об’єкти підприємства.

Політика і стратегія безпеки

Політика безпеки підприємства – це загальні орієнтири для дій і прийняття рішень, які полегшують досягнення цілей. Таким чином, для встановлення цих загальних орієнтирів необхідно спочатку сформулювати цілі забезпечення безпеки підприємства (загальна мета нами вже визначена раніше). Такими цілями можуть бути:

– зміцнення дисципліни праці і підвищення його продуктивності;

– захист законних прав та інтересів підприємства;

– зміцнення інтелектуального потенціалу підприємства;

– збереження і примноження власності;

– підвищення конкурентоспроможності продукції, що виробляється;

– максимально повне інформаційне забезпечення діяльності підприємства та підвищення його ефективності;

– орієнтація на світові стандарти і лідерство в розробці та освоєнні нової технології і продукції, що випускається;

– виконання виробничих програм;

– надання сприяння управлінським структурам в досягненні цілей підприємства;

– недопущення залежності від випадкових і несумлінних ділових партнерів.

З урахуванням вищевикладеного можна визначити наступні загальні орієнтири для дій і прийняття рішень, які полегшують досягнення цих цілей:

– збереження і нарощування ре ресурсного потенціалу;

– проведення комплексу превентивних заходів щодо підвищення рівня захищеності власності та персоналу підприємства;

– включення в діяльність по забезпеченню безпеки підприємства всіх його співробітників;

– професіоналізм і спеціалізація персоналу підприємства;

– пріоритетність несилових методів запобігання і нейтралізації загроз.

Для успішного виконання цієї політики необхідно реалізувати стратегію безпеки підприємства, під якою розуміється сукупність найбільш значущих рішень, спрямованих на забезпечення прийнятного рівня безпеки функціонування підприємства.

Виділяються такі типи стратегій безпеки:

1) орієнтовані на усунення існуючих або запобігання виникненню можливих загроз;

2) націлені на запобігання впливу існуючих або можливих загроз на предмет безпеки;

3) спрямовані на відновлення (компенсацію) завдається шкоди.

Перші два типи стратегій передбачають таку діяльність із забезпечення безпеки, в результаті якої не відбувається загрози або створюється заслін її впливу. У третьому випадку збиток допускається (виникає), проте він компенсується діями, які передбачає відповідна стратегія. Цілком очевидно, що стратегії третього типу можуть розроблятися і реалізовуватися стосовно ситуацій, де збитки надолужуваних, або тоді, коли немає можливості здійснити будь-яку програму реалізації стратегій першого або другого типу.

Суб’єкти безпеки підприємства

Забезпеченням безпеки підприємства займаються дві групи суб’єктів. Перша група займається цією діяльністю безпосередньо на підприємстві і підпорядкована його керівництву. Серед цієї групи можна виділити спеціалізовані суб’єкти (рада або комітет безпеки підприємства, служба безпеки, пожежна частина, рятувальна служба і т.д.), основним призначенням яких є постійна професійна діяльність із забезпечення безпеки підприємства (в рамках своєї компетенції). Іншу частину суб’єктів цієї групи умовно можна назвати полуспеціалізірованной, тому що частина функцій цих суб’єктів призначена для забезпечення безпеки підприємства (медична частина, юридичний відділ і т.д.). Нарешті, до третьої частини цієї групи суб’єктів належить увесь інший персонал і підрозділи підприємства, які в рамках своїх посадових інструкцій і положень про підрозділи зобов’язані вживати заходів до забезпечення безпеки. Слід мати на увазі, що ефективно забезпечувати безпеку підприємства ці суб’єкти можуть тільки в тому випадку, якщо цілі, завдання, функції, права та обов’язки будуть розподілені між ними таким чином, щоб вони не перетиналися один з одним.

До другої групи суб’єктів відносяться зовнішні органи і організації, які функціонують самостійно і не підкоряються Керівництву підприємства, але при цьому їх діяльність має суттєвий (позитивне чи негативне) вплив на безпеку підприємства. Суб’єктами цієї групи є:

1) Законодавчі органи.

2) Органи виконавчої влади.

3) Суди.

4) Правоохоронні органи.

5) Науково-освітні установи.

Останні (особливо недержавні установи з підготовки приватних охоронців) покликані забезпечити науково-методичну опрацювання проблем безпеки підприємства та підготовку відповідних фахівців у сфері безпеки підприємств.

Очевидно, що суб’єкти другої групи за своєю ініціативою підключаються епізодично (або ніколи) до діяльності підприємства щодо забезпечення своєї безпеки. Організаційною формою такого підключення може стати комплексна програма безпеки підприємства, в якій необхідно передбачити форми і методи цієї роботи. Крім того, можна рекомендувати розробку планів структурних підрозділів і всього підприємства в цілому по організації взаємодії з вищевказаними органами та організаціями.

Засоби і методи забезпечення безпеки

Серед існуючих засобів забезпечення безпеки можна виділити наступні:

1) Технічні засоби. До них відносяться охоронно-пожежні системи, відео-радіоапаратура, засоби виявлення вибухових пристроїв, бронежилети, загородження і т.д.

2) Організаційні засоби. Створення спеціалізованих орг-структурних формувань, що забезпечують безпеку підприємства.

3) Інформаційні засоби. Перш за все, це друкована і відеопродукція з питань збереження конфіденційної інформації. Крім цього, найважливіша інформація для прийняття рішень з питань безпеки зберігається в комп’ютерах.

4) Фінансові кошти. Цілком очевидно, що без достатніх фінансових коштів неможливе функціонування системи безпеки, питання лише в тому, щоб використовувати їх цілеспрямовано і з високою віддачею.

5) Правові засоби. Тут мається на увазі використання не тільки виданих вищими органами влади законів та підзаконних актів, але також розробка власних, так званих локальних правових актів з питань забезпечення безпеки.

6) Кадрові кошти. Мається на увазі перш за все достатність кадрів, що займаються питаннями забезпечення безпеки. Одночасно з цим вирішують завдання підвищення їх професійної майстерності в цій сфері діяльності.

7) Інтелектуальні засоби. Залучення до роботи висококласних фахівців, науковців (іноді доцільно залучати їх зі сторони) дозволяє впроваджувати нові системи безпеки.

Слід зауважити, що застосування кожного з вищевказаних коштів окремо не дає необхідного ефекту, він можливий тільки на комплексній основі. У той же час необхідно відзначити, що одночасне використання всіх вищевказаних коштів в принципі неможливо. Воно проходить зазвичай ряд етапів.

I етап. Виділення фінансових коштів.

II етап. Формування кадрових і організаційних засобів.

III етап. Розробка системи правових засобів.

IV етап. Залучення технічних, інформаційних і інтелектуальних засобів.

Переведені з статичного в динамічний стан вищевказані кошти стають методами, тобто прийомами, способами дії. Відповідно, можна говорити про технічні, організаційних, інформаційних, фінансових, правових, кадрових та інтелектуальних методах. Наведемо короткий конкретний перелік цих методів:

– технічні – спостереження, контроль, ідентифікація і т.д .;

– організаційні – створення зон безпеки, режим, розслідування, пости, патрулі і т.д .;

– інформаційні – складання характеристик на співробітників, аналітичні матеріали конфіденційного характеру і т.д .;

– фінансові – матеріальне стимулювання співробітників, що мають досягнення в забезпеченні безпеки, грошове заохочення інформаторів і т.д .;

– правові – судовий захист законних прав та інтересів, сприяння правоохоронним органам і т.д .;

– кадрові – підбір, розстановка і навчання кадрів, що забезпечують безпеку підприємства, їх виховання і т.д .;

– інтелектуальні – патентування, ноу-хау і т.д.

Концепція безпеки підприємства

Після вивчення всіх вищеописаних елементів системи безпеки підприємства необхідно перейти до написання її концепції. Концепція визначається як система поглядів, ідей, цільових установок, пронизаних єдиним, визначальним задумом, провідною думкою, що містить постановку і шляхи вирішення виявлених проблем. До будь-якої концепції існують такі вимоги:

1) Конструктивність. Така вимога буде визнано реалізованим, якщо в концепції буде враховано:

а) початковий стан об’єкта, на перетворення якого спрямована концепція;

б) стан об’єкта, досягнуте в результаті реалізації концепції;

в) заходи, необхідні для досягнення сформульованих в концепції цілей;

г) кошти, необхідні і достатні для досягнення поставлених цілей;

д) джерела ресурсного забезпечення, що використовуються в ході реалізації концепції;

е) механізм реалізації концепції, тобто способи (методи) використання виділених коштів і ресурсів.

2) Вписуваність. Мається на увазі те, що концепція перетворення будь-якого об’єкта повинна гармонійно вписуватися в систему перетворень взаємопов’язаних в єдину систему об’єктів, одним з компонентів якої він є.

3) Відкритість. Розроблена концепція повинна давати можливість в її рамках реагувати на зміну умов реалізації концепції і вносити корективи в реалізацію в разі їх необхідності.

Вищевказані вимоги диктують як обов’язкову умову включення в логічну структуру концепції наступних позицій:

1) Виявлення об’єкта і предмета, визначення їх сутності, місця серед безлічі інших.

2) Чітке формулювання ролі реалізації концепції і завдань, що стоять при її реалізації.

3) Виділення умов, необхідних і достатніх для реалізації концепції, і зіставлення їх з реально існуючими.

4) Визначення кола заходів, що забезпечують перетворення об’єкта реалізації концепції, а також шляхів її реалізації.

5) Формулювання критеріїв успішності заходів щодо розробки концепції, а також за оцінкою результатів її реалізації.

Концепція безпеки підприємства являє собою офіційно затверджений документ, в якому відображена система поглядів, вимог і умов організації заходів безпеки персоналу і власності підприємства. Орієнтовна структура концепції може виглядати наступним чином:

І. Опис проблемної ситуації в сфері безпеки підприємства:

– перелік потенційних і реальних загроз безпеки, їх класифікація та ранжування;

– причини і фактори зародження загроз;

– негативні наслідки загроз для підприємства.

ІІ. Механізм забезпечення безпеки:

– визначення об’єкта і предмета безпеки підприємства;

– формулювання політики і стратегії безпеки;

– принципи забезпечення безпеки;

– цілі забезпечення безпеки;

– завдання забезпечення безпеки;

– критерії та показники безпеки підприємства;

– створення орг-структури з управління системою безпеки підприємства.

III. Заходи по реалізації заходів безпеки:

– формування підсистем загальної системи безпеки підприємства;

– визначення суб’єктів безпеки підприємства та їх ролі;

– розрахунок коштів та визначення методів забезпечення безпеки;

– контроль і оцінка процесу реалізації концепції.

Необхідно мати на увазі, що найбільш повне уявлення про систему безпеки підприємства можна отримати після вивчення офіційних документах по концепції безпеки підприємства, комплексної програми забезпечення безпеки підприємства та планів підрозділів підприємства по реалізації цієї програми. Сформована на науковій основі система безпеки підприємства є організаційною основою створення її структурного підрозділу – служби безпеки.