Комплексні системи захисту інформації (КСЗІ) - це сукупність організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу.

Організаційні заходи є обов'язковою складовою побудови КСЗІ.

Інженерно-технічні заходи здійснюються в міру необхідності.

1.1 Означення, позначення та скорочення

Технічний захист інформації (ТЗІ) – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Система ТЗІ – сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та їхня матеріально-технічна база.

Контрольована зона – територія, на якій унеможливлюється несанкціоноване перебування сторонніх осіб.

Модель загроз – формалізований опис методів та засобів здійснення загроз для інформації.

Інформаційна система – автоматизована система, комп'ютерна мережа або система зв'язку.

Виділені приміщення – приміщення, в яких циркулює інформація з обмеженим доступом.

Контрольно-інспекційна робота з питань ТЗІ – діяльність, спрямована на визначення та вдосконалення стану ТЗІ органів, щодо яких здійснюється ТЗІ, та на проведення контролю за виконанням суб'єктами системи ТЗІ завдань або проведенням діяльності в галузі ТЗІ за відповідними дозволами та ліцензіями.

Атестація виділених приміщень – комплекс робіт, спрямованих на реалізацію заходів з ТЗІ, метою яких є приведення виділених приміщень відповідно до вимог нормативних документів з ТЗІ та визначення відповідності захищеності виділеного приміщення встановленій категорії.

Порушення з ТЗІ – невиконання вимог нормативно-правових актів з питань ТЗІ, яке створює умови або реальну можливість порушення конфіденційності, цілісності або доступності інформації.

Інші терміни використовуються згідно з:

– НД ТЗІ 1.1–003–99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»;

– ДСТУ 3396.2 «Захист інформації. Технічний захист інформації. Терміни та визначення»;

– «Термінологічний довідник з технічного захисту інформації на об’єктах інформаційної діяльності».

1.2 Сутність та задачі комплексної системи захисту інформації

1.2.1 Основні підходи до створення комплексної системи захисту інформації

Існує думка, що проблеми захисту інформації стосуються виключно інформації, що обробляється комп'ютером. Це, мабуть, пов'язано з тим, що комп'ютер і, зокрема, персональний комп'ютер є «ядром», центром зберігання інформації. Об'єкт інформатизації, стосовно до якого спрямовані дії щодо

захисту інформації, видається більш широким поняттям порівняно з персональним комп'ютером.

У реальному житті всі ці окремі “об'єкти інформатизації” розташовані в межах одного підприємства і являють собою єдиний комплекс компонентів, пов'язаних спільними цілями, завданнями, структурними відносинами, технологією інформаційного обміну і т. д.

Сучасне підприємство – велика кількість різнорідних компонентів, об'єднаних в складну систему для виконання поставлених цілей, які в процесі функціонування підприємства можуть модифікуватися. Різноманіття та складність впливу внутрішніх та зовнішніх чинників, які часто не піддаються чіткому кількісному оцінюванню, призводять до того, що ця складна система може набувати нові якості, не властиві її складовим компонентів.

Характерною особливістю подібних систем є насамперед наявність людини в кожній з складових підсистем і віддаленість людини від об'єкта її діяльності. Це відбувається у зв'язку з тим, що безліч компонентів, які складають об'єкт інформатизації, інтегрально може бути подано сукупністю трьох груп систем: 1) люди (біосоціальні системи); 2) техніка (технічні системи та приміщення, в яких вони розташовані); 3) програмне забезпечення, яке є інтелектуальним посередником між людиною і технікою (інтелектуальні системи). Сукупність цих трьох груп утворює соціотехнічну систему. Таке уявлення про соціотехнічну систему є досить поширеним і може стосуватися багатьох об'єктів. Коло наших інтересів обмежується дослідженням безпеки систем, призначених для обробки вхідної на їх вхід інформації і видачі результату.

Якщо звернутися до історії цієї проблеми, то можна умовно виділити три періоди розвитку засобів захисту інформації (ЗІ):

– перший ми відносимо до того часу, коли обробка інформації здійснювалася за традиційними (ручними, паперовими) технологіями;

– другий – коли для обробки інформації на регулярній основі застосовувалися засоби електронної обчислювальної техніки перших поколінь;

– третій – коли використання засобів електронно-обчислювальної техніки набрав масового і повсюдний характер (поява персональних комп'ютерів).

У зв’язку з тим, що КСЗІ впроваджують, як правило, на підприємствах, то треба і розглянути підприємство як предметне середовище.

Сучасне підприємство являє собою складну систему, в рамках якої здійснюється захист інформації.

Розглянемо основні особливості сучасного підприємства:

– складна організаційна структура;

– багатоаспектність функціонування;

– висока технічна оснащеність;

– широкі зв'язки з кооперації;

– необхідність розширення доступу до інформації;

– зростаюча питома вага цифрової технології обробки інформації;

- зростаюча питома вага автоматизованих процедур в загальному обсязі процесів обробки даних;

- важливість і відповідальність рішень, прийнятих в автоматизованому режимі, на основі автоматизованої обробки інформації;

- висока концентрація в автоматизованих системах інформаційних ресурсів;

- велике територіальне розподілення компонентів автоматизованих систем;

- накопичення на технічних носіях величезних обсягів інформації;

- інтеграція в єдиних базах даних інформації різного призначення і різної належності;

- довгострокове зберігання великих обсягів інформації на машинних носіях;

- безпосередній і одночасний доступ до ресурсів (також і до інформації) автоматизованих систем великого числа користувачів різних категорій і різних установ;

- інтенсивна циркуляція інформації між компонентами автоматизованих систем, також і віддалених один від одного.

Таким чином, створення індустрії переробки інформації, з одного боку, створює об'єктивні передумови для підвищення рівня продуктивності праці та життєдіяльності людини, з іншого боку, породжує цілий ряд складних і великомасштабних проблем. Однією з них є забезпечення збереження і встановленого статусу інформації, що циркулює і оброблюється на підприємстві, в організації.

1.2.2 Поняття комплексної системи захисту інформації

Роботи з захисту інформації у нас в країні ведуться досить інтенсивно і вже тривалий час. Накопичено значний досвід. Зараз вже ніхто не вважає, що досить провести на підприємстві ряд організаційних заходів, ввести до складу автоматизованих систем деякі технічні і програмні засоби – і цього буде достатньо для забезпечення безпеки.

Головний напрямок пошуку нових шляхів захисту інформації полягає не просто в створенні відповідних механізмів, а являє собою реалізацію регулярного процесу, здійснюваного на всіх етапах життєвого циклу систем обробки інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи і заходи, які використовуються для ЗІ, найбільш раціональним чином об'єднуються в єдиний цілісний механізм – причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також позаштатних ситуацій технічного характеру.

Основною проблемою реалізації систем захисту є:

– з одного боку, забезпечення надійного захисту ідентифікації, що знаходиться в системі інформації: унеможливлення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації та обслуговувального персоналу;

– з іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи.

Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякої сукупності наукових, науково-технічних і організаційних заходів і застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів із ЗІ .

На основі теоретичних досліджень і практичних робіт у сфері ЗІ сформульований системно-концептуальний підхід до захисту інформації.

Під системністю як основною частиною системно-концептуального походу розуміється:

– системність цільова, захищеність інформації розглядається як основна частина загального поняття якості інформації;

– системність просторова, яка пропонує взаємопов'язані рішення всіх питань захисту на всіх компонентах підприємства;

– системність тимчасова, що означає безперервність робіт із ЗІ, що здійснюються відповідно до планів;

– системність організаційна, що означає єдність організації всіх робіт по ЗІ і управління ними.

Концептуальність підходу передбачає розробку єдиної концепції як повної сукупності науково обґрунтованих поглядів, положень і рішень, необхідних і достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також цілеспрямованої організації всіх робіт щодо ЗІ.

Комплексний (системний) підхід до побудови будь-якої системи містить в собі: перш за все, вивчення об'єкта впроваджуваної системи; оцінювання загроз безпеки об'єкта; аналіз засобів, якими будемо оперувати при побудові системи; оцінку економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх і зовнішніх чинників; можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця.

Комплексний (системний) підхід – це принцип розгляду проекту, при якому аналізується система в цілому, а не її окремі частини. Його завданням є оптимізація всієї системи в сукупності, а не поліпшення ефективності окремих частин. Це пояснюється тим, що, як показує практика, поліпшення одних параметрів часто призводить до погіршення інших, тому необхідно намагатися забезпечити баланс протиріч вимог і характеристик.

Комплексний (системний) підхід не рекомендує приступати до створення системи до тих пір, поки не визначені такі її компоненти:

1. Вхідні елементи. Це ті елементи, для обробки яких створюється система. Як вхідні елементи виступають види загроз безпеки, можливі на даному об'єкті;

2. Ресурси. Це кошти, які забезпечують створення та функціонування системи (наприклад, матеріальні витрати, енергоспоживання, допустимі

розміри і т. д.). Зазвичай рекомендується чітко визначати види і допустиме споживання кожного виду ресурсу як в процесі створення системи, так і в ході її експлуатації;

3. Навколишнє середовище. Слід пам'ятати, що будь-яка реальна система завжди взаємодіє з іншими системами, кожен об'єкт пов'язаний з іншими об'єктами. Дуже важливо встановити межі сфер інших систем, які не підкоряються керівнику даного підприємства і не входять в сферу його відповідальності.

Характерним прикладом важливості вирішення цього завдання є розподіл функцій із захисту інформації, переданої сигналами в кабельній лінії, що проходить територіями різних об'єктів. Як би не встановлювались межі системи, не можна ігнорувати її взаємодію з навколишнім середовищем, бо в цьому випадку прийняті рішення можуть виявитися марними;

4. Призначення і функції. Для кожної системи повинна бути сформульована мета, до якої вона (система) прагне. Ця мета може бути описана як призначення системи, як її функція. Чим точніше і конкретніше вказано призначення або перераховані функції системи, тим швидше і правильніше можна вибрати кращий варіант її побудови. Так, наприклад, мета, сформульована в найзагальнішому вигляді як забезпечення безпеки об'єкта, змусить розглядати варіанти створення глобальної системи захисту. Якщо уточнити її, визначивши, наприклад, як забезпечення безпеки інформації, що передається по каналах зв'язку всередині будівлі, то коло можливих рішень істотно звузиться. Слід мати на увазі, що, як правило, глобальна мета досягається через досягнення безлічі менш загальних локальних цілей. Побудова такого «дерева цілей» значно полегшує, прискорює і здешевлює процес створення системи;

5. Критерій ефективності. Необхідно завжди розглядати кілька шляхів, що ведуть до мети, зокрема декілька варіантів побудови системи, що забезпечують задані цілі функціонування. Для того, щоб оцінити, який із шляхів краще, необхідно мати інструмент порівняння – критерій ефективності. Він повинен: характеризувати якість реалізації заданих функцій; враховувати витрати ресурсів, необхідних для виконання функціонального призначення системи; мати ясний і однозначний фізичний зміст; бути пов'язаним з основними характеристиками системи і допускати кількісне оцінювання на всіх етапах створення системи.

Таким чином, з огляду на різноманіття потенційних загроз інформації на підприємстві, складність його структури, а також участь людини в технологічному процесі обробки інформації, цілі захисту інформації можуть бути досягнуті тільки шляхом створення СЗІ на основі комплексного підходу.

1.2.3 Призначення комплексної системи захисту інформації

Головна мета створення системи захисту інформації – забезпечення надійності ЗІ. Система ЗІ - це організована сукупність об'єктів і суб'єктів ЗІ, використовуваних методів і засобів захисту, а також здійснюваних захисних заходів.

Але компоненти ЗІ, з одного боку, є складовою частиною системи, з іншого – самі організовують систему, здійснюючи захисні заходи.

Оскільки система може бути визначена як сукупність взаємопов'язаних елементів, то призначення СЗІ полягає в тому, щоб об'єднати всі складові захисту в єдине ціле, в якому кожен компонент, виконуючи свою функцію, одночасно забезпечує виконання функцій іншими компонентами та пов'язаний з ними логічно і технологічно.

Надійність захисту інформації прямо пропорційна системності. При неузгодженості між собою окремих складових ризик «проколів» в технології захисту збільшується.

По-перше, необхідність комплексних рішень полягає в об'єднанні в одне ціле локальних СЗІ, при цьому вони повинні функціонувати в єдиній «зв'язці». Як локальні СЗІ можуть бути розглянуті, наприклад, види захисту інформації (правова, організаційна, інженерно-технічна).

По-друге, необхідність комплексних рішень обумовлена призначенням самої системи. Система повинна об'єднати логічно і технологічно всі складові захисту. Але з її сфери випадають питання повноти цих складових, вона не враховує всіх факторів, які забезпечують або можуть впливати на якість захисту. Наприклад, система охоплює якісь об'єктів захисту, а всі вони внесені до неї чи ні – це вже поза межами системи.

Тому якість, надійність захисту залежать не тільки від видів складових системи, але і від їх повноти, яка забезпечується при врахуванні всіх чинників і обставин, що впливають на захист. Саме повнота всіх складових системи захисту, що базується на аналізі таких факторів і обставин, є другим призначенням комплексності.

При цьому повинні враховуватися всі параметри уразливості інформації, потенційно можливі загрози її безпеці, охоплюватися всі необхідні об'єкти захисту, використовуватися всі можливі види, методи і засоби захисту та необхідні для захисту кадрові ресурси, здійснюватися все, виходячи з цілей і завдань захисту заходу.

По-третє, тільки при комплексному підході система може забезпечувати безпеку всієї сукупності інформації, що підлягає захисту, і при будь-яких обставинах. Це означає, що повинні захищатися всі носії інформації, в всіх місцях її збирання, зберігання, передачі і використання, весь час і при всіх режимах функціонування систем обробки інформації.

У той же час комплексність не усуває, а, навпаки, передбачає диференційований підхід до захисту інформації, залежно від складу її носіїв, видів таємниці, до яких віднесена інформація, ступеня її конфіденційності, засобів зберігання і обробки, форм і умов прояву уразливості, каналів і методів несанкціонованого доступу до інформації.

Таким чином, значимість комплексного підходу до захисту інформації полягає у:

– інтеграції локальних систем захисту;

– забезпеченні повноти всіх складових системи захисту;

– забезпеченні всеосяжність захисту інформації.

Виходячи з цього, можна сформулювати таке означення:

«Комплексна система захисту інформації – система, що повно і всебічно охоплює всі предмети, процеси і фактори, які забезпечують безпеку всієї захищуваної інформації».

1.3 Основні стратегії захисту інформації

Усвідомлення необхідності розробки стратегічних підходів до захисту формувалося в міру усвідомлення важливості, натхнення і проблеми захисту, а також неможливості ефективного її здійснення простим використанням деякого набору засобів захисту.

Під стратегією взагалі розуміється загальна спрямованість в організації відповідної діяльності, що розробляється з урахуванням об'єктивних потреб в даному виді діяльності, потенційно можливих умов її здійснення і можливостей організації.

Відомий канадський фахівець у сфері стратегічного управління Г. Мінцберг запропонував визначення стратегії в рамках системи «5-Р». На його думку, вона містить:

1) план (Plan) - заздалегідь намічені в деталях і контрольовані дії на певний термін, що переслідують конкретні цілі;

2) прийом, або тактичний хід (Ploy), що є короткочасною стратегією, яка має обмежені цілі, спроможна змінюватися та маневруввати з метою використати їх проти противника;

3) модель поведінки (Patten of behaviour) – часто спонтанну, неусвідомлену, що не має конкретних цілей;

4) позицію щодо до інших (Position in respect to others);

5) перспективу (Perspective).

Завдання стратегії полягає в створенні конкурентної переваги, усунення негативного ефекту нестабільності навколишнього середовища, забезпеченні прибутковості, врівноваженні зовнішніх вимог і внутрішніх можливостей. Через її призму розглядаються всі ділові ситуації, з якими організація стикається в повсякденному житті.

Здатність компанії, організації проводити самостійну стратегію в усіх сферах робить її більш гнучкою, стійкою, дозволяє адаптуватися до вимог часу і обставин.

Стратегія формується під впливом внутрішнього і зовнішнього середовищ, постійно розвивається, бо завжди виникає щось нове, на що потрібно реагувати.

Фактори, які можуть мати для фірми вирішальне значення в майбутньому, називаються стратегічними. На думку одного з провідних західних фахівців Б. Карлофа, вони, впливаючи на стратегію будь-якої організації, надають і специфічні властивості. До таких факторів належать:

1) мета, яка відображає філософію фірми, організації її призначення. При перегляді мети, що відбувається в результаті зміни суспільних пріоритетів;

2) конкурентні переваги, якими організація має в своїй сфері діяльності в порівнянні з суперниками або до яких прагне (вважається, що вони

найбільше впливають на стратегію). Конкурентні переваги будь-якого типу забезпечують більш високу ефективність використання ресурсів підприємства;

3) характер продукції, що випускається, особливості її збуту, післяпродажного обслуговування, ринки та їх межі;

4) організаційні чинники, серед яких виділяється внутрішня структура компанії та її очікувані зміни, система управління, ступінь інтеграції і диференціації внутрішніх процесів;

5) наявні ресурси (матеріальні, фінансові, інформаційні, кадрові та ін.). Чим вони більші, тим масштабнішими можуть бути інвестиції в майбутні проекти. Сьогодні для розробки і реалізації стратегії велике значення мають, перш за все, структурні, інформаційні та інтелектуальні ресурси. Порівнюючи значення параметрів готівки і потрібних ресурсів, можна визначити ступінь їх відповідності стратегії;

6) потенціал розвитку організації, вдосконалення діяльності, розширення масштабів, зростання ділової активності, інновацій;

7) культура, філософія, етичні погляди і компетентність управлінців, рівень їх домагань і підприємливості, здатність до лідерства, внутрішній клімат в колективі.

На стратегічний вибір впливають: ризик, на який готова йти фірма; досвід реалізації чинних стратегій, позиції власників, наявність часу.

Розглянемо особливості стратегічних рішень. За ступенем регламентованості вони належать до контурних (надають широку свободу виконавцям стосовно тактики), а за ступенем обов'язковості проходження головним установкам – директивним.

За функціональним призначенням такі рішення найчастіше бувають організаційними або розпорядчими способами здійснення в певних ситуаціях тих чи інших дій. З точки зору визначеності, це рішення запрограмовані. Вони приймаються в нових, неординарних обставинах, коли необхідні кроки важко заздалегідь точно розписати. З точки зору важливості, стратегічні рішення кардинальні: стосуються основних проблем і напрямків діяльності фірми, визначають основні шляхи розвитку її в цілому, окремих підрозділів або видів діяльності на тривалу перспективу (не менше 5–10 років). Вони випливають насамперед із зовнішніх, а не з внутрішніх умов, повинні враховувати тенденції розвитку ситуації і інтереси безлічі суб'єктів. Практична незворотність стратегічних рішень обумовлює необхідність їх ретельної та всебічної підготовки. Стратегічним рішенням притаманна комплексність. Стратегія зазвичай являє собою не одне, а сукупність взаємопов'язаних рішень, об'єднаних спільною метою, узгоджених між собою за термінами виконання та ресурсами. Такі рішення визначають пріоритети і напрямки розвитку фірми, її потенціалу, ринків, способи реакції на непередбачені події. Практика сформувала нижченаведені вимоги до стратегічних рішень:

1. Реальність, що передбачає її відповідність ситуації, цілям, технічному та економічному потенціалу підприємства, досвіду і навичками працівників і менеджерів, культурі, існуючій системі управління;

2. Логічність, зрозумілість, прийнятність для більшості членів організації, внутрішня цілісність, несуперечність окремих елементів, підтримка ними один одного, що породжує синергетичний ефект;

3. Своєчасність (реалізація рішення повинна встигнути призупинити негативне розвиток ситуації або не дозволити упустити вигоду);

4. Сумісність із середовищем, що забезпечує можливість взаємодії з нею (стратегія перебуває під впливом змін в оточенні підприємства і сама може формувати ці зміни);

5. Спрямованість на формування конкурентних переваг;

6. Збереження свободи тактичного маневру;

7. Усунення причин, а не наслідків існуючої проблеми;

8. Чіткий розподіл за рівнями організації роботи з підготовки та прийняття рішень, а також відповідальності за них конкретних осіб;

9. Облік прихованих і явних, бажаних і небажаних наслідків, які можуть виникнути при реалізації стратегії або відмову від неї для фірми, її партнерів; в зв'язку з існуючим законодавством, етичною стороною справа, допустимим рівнем ризику та інше.

Розробка науково обґрунтованої системи стратегій організації як ключової умови її конкурентоспроможності та довгострокового успіху є однією з основних функцій її менеджерів, перш за все вищого рівня. Від них вимагається:

– виділяти, відстежувати і оцінювати ключові проблеми;

– адекватно і оперативно реагувати на зміни всередині і в оточенні організації;

– вибирати оптимальні варіанти дій з урахуванням інтересів основних суб'єктів, причетних до її діяльності;

– створювати сприятливий морально-психологічний клімат, заохочувати підприємницьку і творчу активність низових керівників і персоналу.

Вихідний момент формування стратегії – постановка глобальних якісних цілей і параметрів діяльності, які організація повинна досягти в майбутньому. В результаті ув'язки цілей і ресурсів формуються альтернативні варіанти розвитку, оцінювання яких дозволяє вибрати кращу стратегію. Єдиних рецептів вироблення стратегій не існує. В одному випадку доцільно стратегічне планування (програмування) в іншому – ситуаційний підхід.

Виходячи з великої різноманітності умов, при яких може виникнути необхідність захисту інформації, загальна цільова установка на вирішення стратегічних питань полягала в розробці безлічі стратегій захисту, і вибір такого мінімального їх набору, який дозволяв би раціонально забезпечувати необхідний захист в будь-яких умовах.

Відповідно до найбільш реальних варіантів поєднань значень розглянутих факторів виділено три стратегії захисту:

– оборонна – захист від вже відомих загроз здійснюваний автономно, тобто без надання істотного впливу на інформаційно - керувальну систему;

– наступальна – захист від усієї множини потенційно можливих загроз, при здійсненні якої в архітектурі інформаційно - керувальної системи і технології її функціонування повинні враховуватися умови, продиктовані потребами захисту;

– упереджувальна – створення інформаційного середовища, в якому загрози інформації не мали б умов для прояву.

1.4 Розробка політики безпеки

Перш ніж пропонувати будь-які рішення щодо організації системи захисту інформації, належить розробити політику безпеки. Політика безпеки – набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Політика безпеки реалізується за допомогою організаційних заходів та програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту. Для конкретної організації політика безпеки повинна бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації і т. д.

Організаційно політика безпеки визначає порядок подання та використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки. Система захисту інформації виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки. Етапи побудови організаційної політики безпеки – це внесення в опис об'єкта структури цінностей і проведення аналізу ризику, і визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності. Перш за все необхідно скласти детальний опис загальної мети побудови системи безпеки об'єкта, що виражається через сукупність факторів або критеріїв, які уточнюють мету. Сукупність факторів є базисом для визначення вимог до системи (вибір альтернатив). Фактори безпеки, в свою чергу, можуть поділятися на правові, технологічні, технічні та організаційні.

Розробка політики безпеки організації, як формальної, так і неформальної, – безумовно, нетривіальне завдання. Експерт повинен не тільки знати відповідні стандарти і добре розбиратися в комплексних підходах до забезпечення захисту інформації організації, але й, наприклад, проявляти детективні здібності при виявленні особливостей побудови інформаційної системи та існуючих заходів з організації захисту інформації. Аналогічна проблема виникає в подальшому при необхідності аналізу відповідності рекомендацій політики безпеки реальному стану речей: необхідно за деяким критерієм відібрати свого роду «контрольні точки» і порівняти їх практичну реалізацію з еталоном, що задається політикою безпеки.

У загальному випадку можна виділити наступні процеси, пов'язані з розробкою і реалізацією політики безпеки.

1. Комплекс заходів, пов'язаних з проведенням аналізу ризиків. До цієї групи можна віднести:

– облік матеріальних або інформаційних цінностей;

– моделювання загроз інформації системи;

– власне аналіз ризиків з використанням того чи іншого підходу – наприклад, вартісний аналіз ризиків.

2. Заходи з оцінювання відповідності заходів щодо забезпечення захисту інформації системи деякого еталонного зразка: стандарт, профіль захисту тощо.

3. Дії, пов'язані з розробкою різного роду документів, зокрема звітів, діаграм, профілів захисту, заданої з безпеки.

4. Дії, пов'язані зі збиранням, зберіганням і обробкою статистики щодо подій безпеки для організації.

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назву політики безпеки.

Для вивчення властивостей способу управління доступом, створюється його формальний опис – математична модель. При цьому модель повинна відображати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в сенсі даного управління. Без цього говорити про які-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно. Відзначимо лише, що для розробки моделей застосовується широкий спектр математичних методів (моделювання, теорії інформації, графів і ін.).

В даний час найкраще вивчені два види політики безпеки: виборча і повноважна, засновані, відповідно, на виборчому і повноважному способах керування доступом.

Крім того, існує набір вимог, що підсилюють дію цих політик і призначені для управління інформаційними потоками в системі. Слід відзначити, що засоби захисту, призначені для реалізації будь-якого з названих способів управління доступом, тільки дають можливості надійного управління доступом або інформаційними потоками.

Основою виборчої політики безпеки є виборче керування доступом, що має на увазі, що

• всі суб'єкти і об'єкти системи повинні бути ідентифіковані;

• права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого управління доступом застосовується модель системи на основі матриці доступу, іноді її називають матрицею контролю доступу. Така модель отримала назву матричної. Матриця доступу являє собою прямокутну матрицю, в якій об'єкту системи відповідає рядок, а суб'єкту – стовпець. На перетині рядка і стовпця матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Зазвичай виділяють такі типи доступу суб'єкта до об'єкта, як «доступ на читання», «доступ на запис», «доступ на виконання» та ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують в даній системі. Визначення і зміна цих правил також є завданням матриці доступу.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеного у відповідній клітинці матриці доступу. Зазвичай виборче управління доступом реалізує принцип «що не дозволено, то заборонено», який передбачає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу – найбільш простий підхід до моделювання систем доступу.

Виборча політика безпеки найбільш широко застосовується в комерційному секторі, оскільки її реалізація на практиці відповідає вимогам комерційних організацій щодо розмежування доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

Основу повноважної політики безпеки складає повноважне управління доступом, що має на увазі, що

– всі суб'єкти і об'єкти системи повинні бути однозначно ідентифіковані;

– кожному об'єкту системи привласнена мітка критичності, що визначає цінність, яка міститься в ньому;

– кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

Коли сукупність міток має однакові значення, кажуть, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру, і, таким чином, в системі можна реалізувати ієрархічно висхідний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливіше об'єкт чи суб'єкт, тим вища його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності.

Кожен суб'єкт, крім рівня прозорості має поточне значення рівня безпеки, яке може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Основне призначення повноважної політики безпеки – регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії в нижні, а також блокування можливого проникнення з нижніх рівнів в верхні. При цьому вона функціонує на тлі виборчої політики, надаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Вибір політики безпеки – це прерогатива керівника системи захисту інформації. Але якою б вона не була, важливо, щоб впроваджена система захисту інформації відповідала ряду вимог.