ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ СОЗДАНИЯ И РАЗВИТИЯ ПЕРСПЕКТИВНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 681.3.06:519.248.681

М. Ф. БОНДАРЕНКО, д-р. техн. наук , О. В. ПОТІЙ, канд. техн. наук, В. Г. ЛАВРІНЕНКО, Ю. І. ГОРБЕНКО

ВИЗНАЧЕННЯ ТА ОБҐРУНТУВАННЯ СУТІ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Фундаментальну роль у забезпеченні безпеки інформаційних технологій (ІТ-безпеки) відіграє політика безпеки інформації (ПБ). Політика безпеки це основа створення та ефективного функціонування комплексної системи захисту інформації (КСЗІ). Відсутність сильної, добре продуманої політики безпеки приводить до відсутності методологічного та організаційного фундаменту забезпечення безпеки інформації та інших цінних ресурсів, інформаційної інфраструктури систем інформаційних технологій (ІТ-систем), комп'ютерних та автоматизованих систем, а також до безсистемності розв'язання задач захисту інформації. Реальність показує, що на сьогодні інформаційні технології настільки глибоко інтегровані в телекомунікаційні системи, комп'ютерні та автоматизовані системи, що у практику впроваджується термін інформаційно-телекомунікаційні системи (ІТС). У подальшому ми будемо використовувати саме цей термін.

Згідно з уже майже усталеними поглядами політика безпеки розробляється на основі моделі забезпечення безпеки інформації. Проведений аналіз та практичний досвід показують, що в якості базової змістовної моделі забезпечення безпеки інформації необхідно використовувати модель, що визначається міжнародним стандартом ISO/IEC 15408 «Єдині критерії оцінки безпеки систем інформаційних технологій» [1 – 3].

Згідно з даною моделлю, при розгляданні проблеми забезпечення безпеки інформації в ІТС необхідно виходити з того, що існують дві основні протиборчі (конфліктуючі) сторони – *власник* ресурсів ІТС, що мають певну цінність і вимагають свого захисту, і *порушник(зловмисник)*, який має мотиви і можливість для незаконного використання ресурсів ІТС, що може привести до нанесення збитку (морального, матеріального, економічного і т. ін.) власнику ресурсів. Третьою, незалежною стороною є арбітр (система арбітражу), основними задачами якого є розгляд суперечок між користувачами ІТС, перш за все коли один із них є внутрішнім зловмисником, а також між користувачами та власниками інформації та ресурсів. Крім того, арбітр може бути як довіреною стороною, так і зловмисником.

За збереження ресурсів відповідає їх власник, для якого ці ресурси мають цінність. У такому випадку ресурси можуть розглядатися як активи. Безпека ІТС пов'язана перш за все із захистом інформаційних ресурсів системи. Необхідно чітко розуміти, що інформація (інформаційний ресурс) – це найбільш цінний актив власника ІТС.

Зловмисник або агент погроз розглядається як джерело погроз безпеці інформації та ресурсам. Під погрозою будемо розуміти можливі події, дії (впливи), процеси чи явища, реалізація яких може привести до нанесення збитку (втрат) власнику та користувачам ресурсів. Агенти погроз (порушники) мають певну зацікавленість у несанкціонованому використанні ресурсів ІТС і прагнуть їх використати, незважаючи на інтереси власника. Власник ресурсів повинен сприймати подібні погрози як потенціал впливу на ресурси, що призводить до пониження їх цінності і до різних видів збитків для власника. Основними загрозами в ІТС є:

– втрата (порушення) конфіденційності інформації та ресурсів, тобто розкриття змісту інформаційного ресурсу несанкціонованим користувачем;

– втрата (порушення) цілісності інформації та ресурсів внаслідок впливів як природного, так і штучного характеру;

– втрата або неякісна доступність до інформації та ресурсів користувачів, а також можливість доступу до інформації зловмисників;

– неякісна спостережність власників та/або користувачів за інформацією та ресурсами.

Власник автоматизованої системи аналізує можливі погрози з метою виявлення, які з них дійсно мають місце у середовищі експлуатації автоматизованої системи. Як результат такого аналізу визначаються ризики інформаційної безпеки. Аналіз може допомогти при виборі контрзаходів для протистояння погрозам та зниженню ризиків до придатного рівня.

Контрзаходи застосовуються для зменшення вразливості та реалізації політики безпеки власника ресурсів. Однак і після введення таких контрзаходів можуть зберігатися залишкові вразливості. Такі вразливості можуть використовуватися агентами погроз (порушниками), становлячи рівень залишкового ризику для активів. Власник ресурсів повинен мінімізувати цей ризик, задаючи додаткові обмеження.

Під ресурсами слід розуміти, в широкому розумінні, все, що має цінність з точки зору власника автоматизованої системи. Виділяють наступні класи ресурсів:

– обладнання автоматизованої системи (фізичні ресурси);

– інформаційні ресурси (бази даних, файли, всі види документів, дані, що передаються каналами зв'язку);

– програмне забезпечення (системне, прикладне, утиліти, інші допоміжні програми);

– сервіс та підтримуюча інфраструктура (обслуговуючі засоби обчислювальної техніки, енергопостачання, забезпечення необхідних умов експлуатації і т.ін.).

Традиційно під *політикою безпеки розуміють низку правил безпеки, котрі регламентують порядок обробки інформації та направлені на захист інформації від визначеної множини погроз безпеці* [4 – 8]. На наш погляд, з точки зору системного підходу таке визначення не повністю відображає сутність політики безпеки. Зокрема при такому визначенні не враховується діяльнісний аспект політики безпеки. Метою даної статті є уточнення самого визначення політики безпеки, з'ясування її змісту та сутності, а також формулювання підходу до розробки політики безпеки на основі діяльнісного підходу як альтернативи традиційному (морфологічному).

1 Сутність традиційного підходу до визначення політики безпеки

Морфологічний підхід до визначення політики безпеки відображає традиційні, класичні погляди на сутність політики безпеки і зручний для її аналізу з точки зору складу та змісту правил безпеки, тобто які конкретно правила безпеки повинні бути включені до політики, на основі яких принципів здійснюється забезпечення безпеки інформації в ІТС, які основні напрямки захисту інформації обрані у системі. Таким чином, з позиції морфологічного підходу політика безпеки повинна розглядатися як деяка організована сукупність правил безпеки, а саме *політика безпеки – це система взаємопов'язаних та погоджених правил безпеки, що регламентують порядок обробки інформації в ІТС, і направлених на відвертання визначеної множини погроз безпеці.* Принциповою відмінністю сформульованого визначення від раніше наведених є те, що правила безпеки повинні являти собою не просто деякий набір, а систему з усіма системними властивостями. Такий погляд на політику безпеки дозволяє нам сформулювати загальний підхід до розробки змісту політики безпеки і визначити властивості, які повинна мати політика безпеки як сукупність правил безпеки.

Політика безпеки може бути подана у вигляді дворівневої моделі. Перший рівень моделі – множина цілей безпеки і задач захисту, тобто цільова множина $T \in T_0$, де T_0 – вихідна множина задач захисту та цілей безпеки. Другий рівень – це множина правил безпеки $R \in R_0$,

де R_0 – вихідна множина правил захисту безпеки. Вихідна множина правил безпеки та вихідна множина задач захисту міститься у нормативних документах та стандартах зі інформаційної безпеки, наприклад у таких документах як [7 – 9]. Множина правил безпеки R розробляється для досягнення цілей безпеки шляхом розв'язання задач захисту, а їх сукупність є унікальною для конкретної автоматизованої системи.

Морфологічна модель політики безпеки розглядає правила безпеки з позиції вимог власника об'єкту захисту (інформації), тобто політика безпеки визначає, що необхідно зробити для задоволення потреб у захисті інформації. В основу формування правил безпеки закладаються загальноприйняті принципи забезпечення безпеки ІТС, які застосовуються незалежно від призначення системи, її розмірів та критичності.

Необхідно як мінімум виділити вісім основоположних принципів, на яких будь-яка організація базує свою програму щодо забезпечення безпеки інформації [10, 11].

1. Система безпеки інформації повинна підтримувати головну мету власника ІТС. Мета забезпечення безпеки інформації полягає у захисті ресурсів ІТС (активів власника ІТС) шляхом вибору та застосування відповідних заходів безпеки.
2. Забезпечення безпеки інформації – це елемент єдиного управління. В цьому виявляється ієрархічність управління інформаційною безпекою, підпорядкованість єдиній меті управління.
3. Рентабельність та ефективність процесів забезпечення безпеки інформації. Необхідно відмітити, що впровадження заходів безпеки інформації потребує виділення додаткових коштів. Рівень безпеки повинен відповідати і бути пропорційним цінності ресурсів, що захищаються, та рівню можливого збитку, який може бути нанесено у випадку порушення цілісності, конфіденційності або доступності інформації.
4. Відповідальність власника ІТС за безпеку ресурсів перед зовнішніми сторонами. Якщо в системі циркулює інформація, яка належить стороннім організаціям, то власник ІТС повинен забезпечувати адекватний захист цієї інформації і нести відповідальність за порушення конфіденційності, цілісності та доступності даної інформації під час її обробки засобами ІТС.
5. Попередній розподіл та встановлення відповідальності всіх сторін (власників та користувачів) за фактичний стан безпеки інформації. Даний принцип передбачає, що в ІТС на всіх рівнях чітко визначені права, обов'язки та відповідальність усіх осіб, що приймають участь у процесі обробки інформації, відносно розв'язання задач захисту інформації. З одного боку це означає визначення правових та адміністративних норм, які регулюють взаємовідношення та обов'язки різних учасників відносно забезпечення безпеки інформації. З іншого боку це передбачає реалізацію спеціальних заходів нагляду (спостережності), що дозволяють визначити порушення політики безпеки та ідентифікувати особу, що причетна до дій, які привели до порушення безпеки.
6. Комплексний підхід до розв'язання задач безпеки, за якого реалізація заходів захисту здійснюється на правовому, адміністративному, процедурному, програмно-технічному рівнях з комплексним застосуванням засобів захисту інформації, взаємодії всіх елементів та служб ІТС.
7. Безперервність забезпечення режиму інформаційної безпеки передбачає реалізацію заходів безпеки на постійній основі, періодичну переоцінку рівня захищеності ІТС, адаптацію системи безпеки ІТС до умов експлуатації, що змінюються.
8. Дотримання вимог та положень існуючого національного та міжнародного законодавства, врахування соціальних чинників, у тому числі тих, що впливають на обслуговуючий персонал та користувачів. Експлуатація систем забезпечення інформаційної безпеки повинна бути психологічно сприйнятною і не викликати напруги власників та користувачів ІТС.

З точки зору морфологічної моделі або моделі складу політика безпеки повинна задовольняти наступним вимогам та наступним властивостям:

1. Узгодженість та несуперечність головної мети функціонування ІТС та цілей безпеки і задач захисту, що направлені на досягнення головної мети функціонування ІТС за рахунок впровадження політики безпеки.
2. Повнота сукупності правил безпеки (необхідність та достатність). Тут необхідно врахувати, що умова достатності є важко досяжною. Достатність можна забезпечити тільки на деякому проміжку часу функціонування системи захисту інформації. У ході функціонування системи захисту будуть відбуватися зміни зовнішніх умов функціонування ІТС, зміни моделі погроз безпеці, що потягне за собою необхідність внесення змін до політики безпеки. Умова необхідності передбачає включення до політики безпеки мінімально необхідної множини правил безпеки, що як мінімум відображає вимоги нормативних документів щодо забезпечення безпеки інформації. Умова необхідності передбачає реалізацію базового рівня захищеності об'єкта захисту.
3. Відповідність положень політики безпеки вимогам законодавства та нормативних документів, що регламентують порядок забезпечення безпеки інформації в ІТС (національних та міжнародних стандартів, рекомендації органів державного управління, відомчих нормативних документів).
4. Законність розробки та прийняття політики безпеки.
5. Взаємна узгодженість цілей безпеки, задач захисту та правил безпеки.

2 Сучасне визначення політики інформаційної безпеки

Згідно з новітніми поглядами, подальше вдосконалення суті політики безпеки може бути виконане на основі використання моделі практичної діяльності власника ІТС із забезпечення інформаційної безпеки. Використання моделі практичної діяльності власника ІТС щодо забезпечення безпеки інформації є суттю діяльнісного підходу до визначення політики безпеки Забезпечення безпеки інформації в ІТС, з точки зору практичної діяльності власника, є видом організаційно-управлінської діяльності, котра буде підпорядковуватися загальним законам здійснення такої діяльності з акцентом на особливості і специфіку розв'язання задач забезпечення безпеки інформаційних технологій. З цих позицій *політика безпеки це систематична, стабільна, організована та цілеспрямована ДІЯЛЬНІСТЬ власника ІТС відносно розв'язання проблем забезпечення безпеки інформації в ІТС, яка здійснюється або безпосередньо самим власником ІТС, або непрямо – через відповідні механізми і органи управління, і має вплив на функціонування ІТС і на управління підприємством (технологічними процесами, бізнес-процесами і т. ін.) в цілому.* Така діяльність дозволяє за виділених фінансових та матеріально-технічних затратах мінімізувати витрати в конкретних умовах функціонування ІТС.

Політика безпеки в цілому це не тільки сукупність правил безпеки – це план високого рівня, в якому описуються цілі та задачі заходів щодо забезпечення безпеки інформації в ІТС. Вона забезпечує планування і виконання програми безпеки.

Після розробки правил безпеки виникає проблема впровадження, реалізації цих правил у конкретній системі, на конкретному об'єкті. Тут виникає безліч питань, а саме: яким чином можна оцінити ступінь рішення проблем безпеки інформації, чи є питання політики безпеки адекватним даній ситуації, яким чином можна оцінити альтернативні стратегії забезпечення безпеки інформації. Відповіді на ці та подібні питання можна одержати лише за розгляду політики безпеки з позиції діяльнісного підходу.

Аналіз низки джерел та проведені дослідження показали, що сучасна ефективна ПБ може бути здійснена на базі таких базових принципів.

1. Принцип цілеспрямованості, який передбачає, що в основу забезпечення безпеки закладені конкретні цілі безпеки, на досягнення яких направлена практична діяль-

ність власника ІТС. Уся діяльність власника ІТС має основний системостворюючий чинник – спрямування до основної мети щодо забезпечення безпеки.

2. Принцип цілісності (інтегрованості) вимагає внутрішню єдність складових елементів політики безпеки. Всі правила політики безпеки повинні неухильно виконуватись усіма об'єктами та суб'єктами процесу забезпечення безпеки інформації, у противному випадку це порушує цілісність політики.
3. Принцип структурованості передбачає чіткість та суворість взаємного розподілення функцій, задач, прав, обов'язків та відповідальності між усіма учасниками процесів забезпечення безпеки інформації.
4. Принцип організованості вимагає, щоб діяльність здійснювалась систематично, підпорядковувалась визначеному порядку виконання практичних робіт, залучені до процесу особи діяли у відповідності з раніше встановленими планами (спланованість діяльності). Крім того, ця діяльність піддається постійному контролю за результативністю і управляємістю.
5. Принцип узгодженості (координованості) діяльності передбачає гармонійне поєднання всіх видів діяльності і заходів щодо забезпечення безпеки інформації, взаємну зумовленість та взаємозв'язок практичних робіт.
6. Принцип мотивованості та усвідомленості передбачає формування активного, усвідомленого, зацікавленого та діяльнісного відношення всіх учасників процесів забезпечення безпеки інформації на всіх рівнях і напрямках до виконання правил безпеки.
7. Принцип стабільності, який передбачає стабільність рівня вимог, правил безпеки та зусиль власника щодо реалізації правил безпеки в часі.
8. Принцип безперервності, що передбачає здійснення практичної діяльності на постійній основі й протягом усього життєвого циклу ІТС.

Використання діяльнісного підходу до визначення політики безпеки дозволяє ввести практичні критерії оцінки політики безпеки. Ці критерії дозволяють оцінити та порівняти різні альтернативи здійснення політики безпеки з точки зору її впливу на функціонування ІТС у цілому, на досягнення поставлених цілей безпеки і розв'язання задач захисту, а також оцінити діяльність власника стосовно впровадження у життя положень політики безпеки і реалізації принципів забезпечення безпеки інформації. В якості таких критеріїв необхідно використовувати:

- критерій результативності;
- критерій ефективності;
- критерій адекватності;
- критерій реагованості (гнучкості);
- критерій доцільності;
- критерій здійснюваності:
- критерій простоти в адміністративному забезпеченні.

Критерій результативності та критерій ефективності є самостійними оціночними критеріями, останні можуть бути віднесені до практичних.

Критерій результативності визначає, в якій мірі може і чи може взагалі впровадження політики безпеки й окремих її положень або правил привести до досягнення поставлених цілей безпеки та розв'язання визначених задач захисту. Основною проблемою використання даного критерію на сьогодні є визначення показників результативності політики безпеки. Бажано мати в розпорядженні кількісні показники результативності, однак цілком можливо

застосування і якісних показників. Використовуючи показники результативності можна ввести *шкалу результативності*, яка буде показувати рівень досягнення цілей безпеки.

Під ефективністю політики безпеки будемо розуміти співвідношення результатів, досягнутих за впровадження політики безпеки, і витрат, необхідних для досягнення цих результатів. Таким чином, у даному випадку ефективність є синонімом економічної раціональності політики безпеки. Ефективність в основному вимірюється грошовим еквівалентом. Основним підходом до визначення ефективності є підрахунок витрат на реалізацію сукупності правил безпеки, направлених на забезпечення розв'язання визначеної задачі захисту. Кожне правило безпеки, що прописане у нормативній політиці безпеки, має на увазі виконання комплексу організаційних заходів, проведення технічних робіт, закупку технічних та інших засобів, які мають безпосереднє відношення до захисту інформації. Усе це вимагає вкладання коштів, що і дає підставу на введення та використання критерію ефективності політики безпеки.

При визначенні показників ефективності виникає ряд проблем, а саме:

- відсутність показників результативності політики безпеки;
- різноманітність варіантів реалізації політики безпеки;
- наявність широкого спектру технічних засобів захисту інформації, що володіють різною технічною ефективністю;
- необхідність обліку побічних витрат, що виникають як при розробці самої політики безпеки, так і при впровадженні її у повсякденну практику.

Політика безпеки є ефективною, якщо вона досягає максимальної результативності за мінімальних затрат.

Таким чином, критерії результативності й ефективності тісно взаємопов'язані і є базовими оціночними критеріями політики безпеки.

Розглянемо практичні критерії оцінки політики безпеки.

Критерій адекватності визначає, що даний рівень результативності дійсно відповідає ситуації, яка склалася відносно існуючих погроз безпеці і задовольняє потребам власника інформаційних ресурсів відносно забезпечення безпеки інформації. Політика безпеки є адекватною, якщо правила безпеки і рівень їх реалізації адекватні погрозам безпеки для даного об'єкту захисту і сприяє надійному запобіганню виявлених погроз та зниженню ризиків до придатного рівня.

Критерій доцільності пов'язаний із визначенням, чи є протиріччя між задачами і основними положеннями політики безпеки та загальними задачами об'єкту захисту. Критерій доцільності уточнює питання, чи необхідні цілі безпеки і задачі захисту в конкретній системі, чи нема протиріч між загальними задачами, що стоять перед нею.

Для оцінки політики безпеки за даним критерієм необхідно врахувати всі критерії одночасно, виразити відношення між їхніми кількісними формами. Використання для розробки політики безпеки стандартів безпеки або залучання для її розробки і оцінки експертів – це один з основних доводів доцільності політики безпеки. Таким чином, політика безпеки – доцільна, якщо положення безпеки і задачі захисту не мають протиріч між основними задачами об'єктів захисту, узгоджені з цілями функціонування об'єкту.

Критерій гнучкості (реагованості) пов'язаний з оцінкою здатності політики безпеки задовольнити потреби власника інформаційних ресурсів у відношенні безпеки інформації в умовах обстановки, що змінюється. Іншими словами, політика безпеки повинна бути здатною адекватно реагувати на зміни умов функціонування об'єкту інформації, зміни цілей і задач функціонування, інтересів і потреб власника інформаційних ресурсів. Політика безпеки називається гнучкою, якщо вона здатна задовольнити потреби в безпеці інформації у будь-яких умовах функціонування ІТС.

Критерій здійсненності пов'язаний з визначенням умов здійсненності конкретної політики безпеки в конкретних умовах при заданих обмеженнях у конкретній ІТС. Даний критерій враховує умови здійсненності політики безпеки і впровадження її на різних рівнях

забезпечення безпеки інформації і у зв'язку з цим має різні аспекти. Безпека інформації забезпечується на чотирьох рівнях – законодавчому (правовому), адміністративному, процедурному і програмно-технічному. Таким чином, необхідно розглядати здійсненність політики безпеки на цих рівнях.

На правовому рівні необхідно оцінювати політику безпеки з точки зору її легітимності. Чи можуть конкретні положення політики безпеки бути реалізовані на даному об'єкті з точки зору правового поля держави в області захисту інформації. Чи має право керівництво приймати такого роду рішення? Чи відповідають положення політики безпеки нормам законів та інших нормативних актів в області захисту інформації.

Здійсненність політики безпеки на адміністративному рівні залежить від ступеню розуміння керівництвом цілей безпеки і задач захисту, усвідомлення реальності погроз безпеці, реалізація яких може нанести збиток, рівня сформованості потреб у розв'язанні таких задач захисту.

На процедурному рівні здійсненність політики безпеки залежить від ступеня технологічної і організаційної готовності об'єкта інформатизації до впровадження правил безпеки. Тут важливе місце набуває готовність персоналу виконувати вимоги безпеки. Така готовність залежить від багатьох чинників: розуміння персоналом необхідності виконання цих вимог, рівня усвідомлення і дисциплінованості персоналу, рівня його професійної підготовленості.

Іншими чинниками, що мають істотний вплив на здійсненність політики безпеки, це якість системи менеджменту (управління) безпекою на об'єкті інформатизації. Якість практичних робіт щодо реалізації положень політики безпеки і досягнення цілей безпеки залежить не тільки від придбання ефективних засобів захисту інформації, але й від ефективного управління безпекою на об'єкті, планування захисту, визначення конкретного переліку робіт щодо реалізації правил безпеки, впровадження системи контролю та оцінки виконання цих робіт.

На програмно-технічному рівні на здійсненність політики безпеки має вплив можливість закупки необхідних заходів захисту і технічні можливості їх застосування на об'єкті інформатизації. На здійсненність впливають розмір фондів, що виділяються на реалізацію програми забезпечення безпеки інформації і планів захисту, наявність на ринку відповідних засобів захисту потрібної якості, технологічний рівень процесів обробки інформації на об'єкті інформатизації (стан парку обчислювальної та іншої спеціалізованої техніки, рівень комп'ютеризації та інформатизації технологічних процесів і т. ін.).

Таким чином, політика безпеки є здійсненною, якщо на правовому, адміністративному, процедурному та програмно-технічному рівнях забезпечення безпеки інформації створені всі умови для здійснення правил безпеки.

Критерій простоти в адміністративному забезпеченні розглядає політику безпеки з точки зору її придатності для адміністрування, тобто враховує наявність достатнього адміністративного персоналу для впровадження політики безпеки, рівень професіоналізму, організаторських здібностей та навичок персоналу, що відповідає за реалізацію політики безпеки і організацію ефективного захисту інформації. Політика безпеки є простою в адміністративному забезпеченні, якщо вона потребує мінімальних витрат на організаційно-штатні зміни в структурі організації.

Таким чином, з точки зору діяльності політика безпеки повинна бути цілеспрямованою, стабільною, неперервною, організованою, керованою, узгодженою та мотивованою, забезпечувати максимальну результативність і ефективність при досягненні цілей безпеки і розв'язанні задач захисту, бути адекватною погрозам безпеки, доцільною та гнучкою в реалізації, здійсненною на різних рівнях забезпечення безпеки інформації, достатньо простою у адміністративному забезпеченні. З позиції діяльнісного підходу від політики безпеки вимагається значно більше, ніж це передбачається за традиційного підходу до аналізу політики безпеки.

3 Взаємозв'язок морфологічного та діяльнісного підходу. Системне визначення політики безпеки

Викладене в першому та другому розділах дозволяє стверджувати, що політика безпеки має двоякі властивості. З одного боку це сукупність документів, що містять систематизоване викладення цілей безпеки, задач захисту та правил безпеки. З іншого – це практична діяльність власника ІТС, яка здійснюється у відповідності до правил безпеки і спрямована на досягнення цілей безпеки. Таким чином, політика безпеки складається з двох складових – пасивної та активної. Пасивна складова – це нормативна (документальна) частина політики безпеки, тобто взаємопов'язана сукупність правил безпеки, які визначають, що повинно бути захищеним і які обмеження накладаються на управління процесами забезпечення безпеки інформації. У подальшому для позначення пасивної складової політики безпеки будемо використовувати термін *нормативна політика безпеки.*

Активна складова політики безпеки – це діяльність власника інформаційних ресурсів, що спрямована на досягнення цілей безпеки на основі і через реалізацію встановлених правил безпеки. По суті це *практична політика безпеки.*

Аналіз показує, що обидві складові знаходяться у тісній взаємодії і не можуть розглядатися у відриві одна від одної. Якщо формувати нормативну частину політики безпеки без підтримки власника ІТС, без урахування можливостей наступної реалізації, то політика безпеки виродиться у мертві документи.

Здійснення ж практичної діяльності без нормативного забезпечення перетвориться в латання дірок у системі захисту, у вирішення окремих задач, які не позв'язані єдиним задумом, концепцією і планом. У результаті не буде досягнуто необхідний рівень захищеності всієї інформаційно-телекомунікаційної системи.

Узагальнена системна модель політики безпеки подана на рис. 1.

Таким чином, сформулюємо визначення політики безпеки. **Політика безпеки це систематична, стабільна, організована та цілеспрямована ДІЯЛЬНІСТЬ власника ІТС відносно розв'язання проблем забезпечення безпеки інформації, що здійснюється на основі і через реалізацію встановлених правил безпеки і впливає на функціонування ІТС у цілому.**

Тісний внутрішній зв'язок пасивної та активної складових політики безпеки і обумовлює взаємопов'язаність властивостей, критеріїв та показників цих складових. Цей взаємозв'язок представлено на рис. 2.

Подана модель дозволяє визначити наступні базові елементи політики безпеки, які складають стратегію забезпечення безпеки інформації (рис. 3):

- створення організаційно-методологічних основ забезпечення безпеки інформації, що виражається у розробці Концепції безпеки інформації в АСУ і стратегічної програми щодо забезпечення інформаційної безпеки у результаті створюється організаційно-методологічні основи забезпечення ІБ в ІТС;
- здійснення ефективного менеджменту в області безпеки інформації;
- здійснення практичної діяльності щодо реалізації правил політики безпеки (інжиніринг безпеки);
- створення ефективної системи аудиту безпеки (контролю ефективності комплексної системи захисту інформації).

Реалізація всіх перелічених вище елементів політики безпеки дійсно дозволяє сформувати і проводити в життя ефективну політику безпеки.

Рис. 1

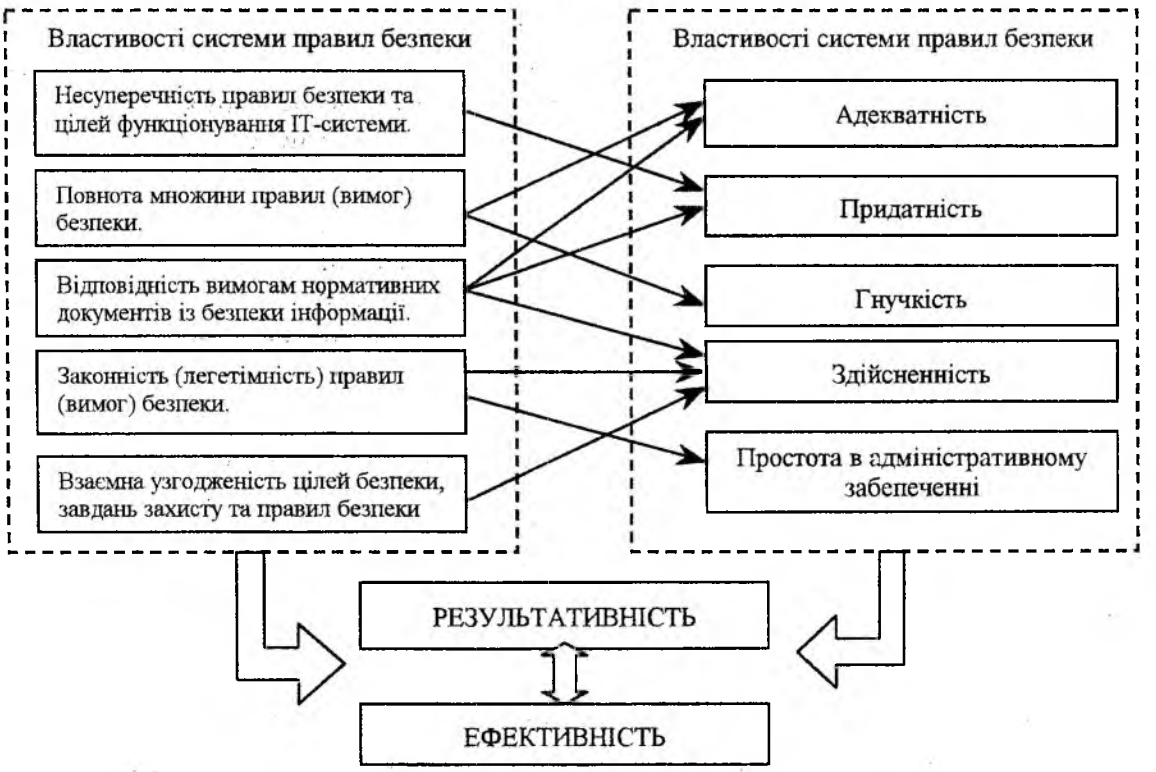

Рис. 2

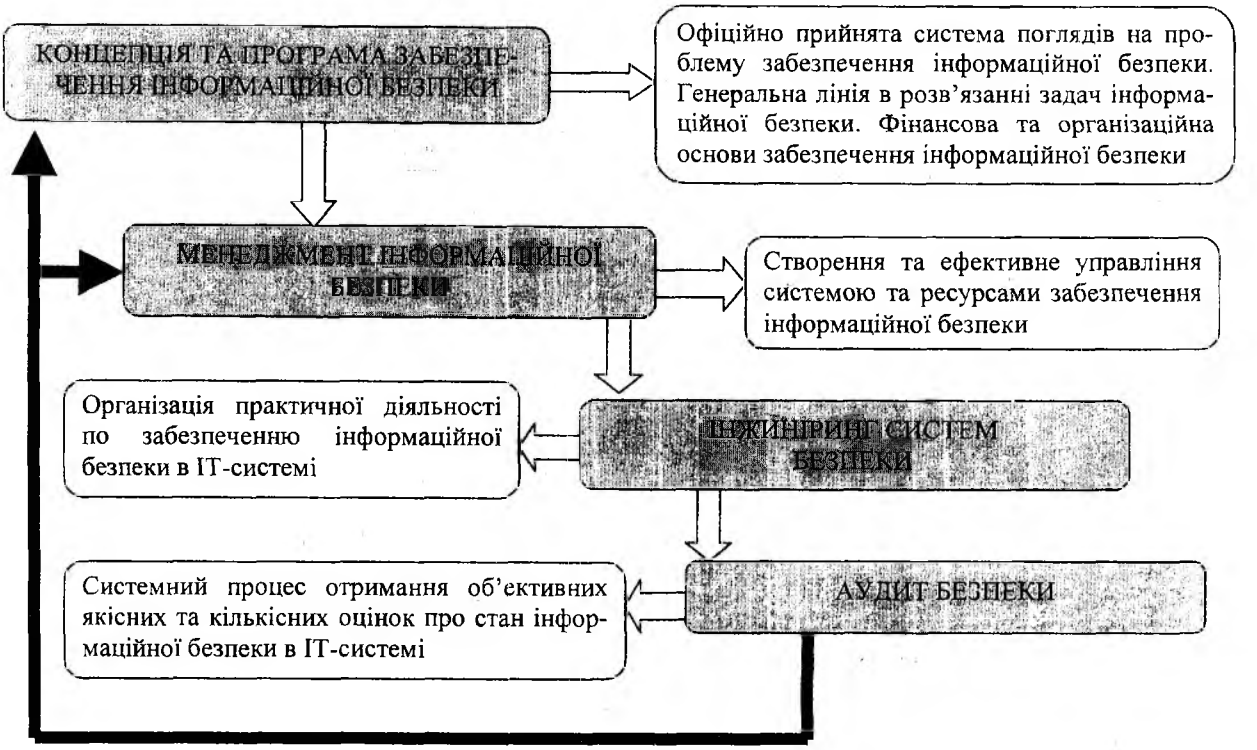

Рис. 3

4 Загальний порядок розробки політики безпеки

З практичної точки зору під час розробки змісту політики безпеки (ПБ) важливо чітко уявляти склад і зміст вихідних даних для її розробки (рис. 4).

Вихідними даними, що безпосередньо впливають на зміст ПБ є:

- характеристика об'єкту застосування ПБ. Політика безпеки як нормативний документ застосовується тільки до конкретного об'єкту. Об'єктами застосування політики безпеки можуть бути організації в цілому, окрема проблема забезпечення інформаційної безпеки і конкретна система;
- сукупність вимог, що містяться в законах і нормативних актах держави, міжнародних, національних та промислових стандартах у галузі інформаційної безпеки, нормативних документах державного і відомчого характеру. Політика безпеки повинна розроблятися у відповідності до нормативно-правової бази, що діє на території держави (держав) і відомства (відомств), у рамках якого існує, здійснює діяльність (функціонує) об'єкт застосування політики безпеки;
- групи осіб, для яких призначена політика безпеки. Цілі, задачі, структура та зміст ПБ суттєво залежать від того, для якого рівня керівників та фахівців об'єкта застосування розробляється політика.

Перелічені вище категорії інформації визначають наступні практичні аспекти розробки політики безпеки:

- визначення цілей і задач політики безпеки;
- розробка структури і конкретного змісту політики безпеки (розробка правил безпеки);
- визначення шляхів проведення в життя і реалізації положень, правил, норм та вимог політики безпеки, ступінь відповідальності за порушення вимог ПБ і контроль за їх виконанням.

Наостанку, не можна забувати про те, що розробка ПБ і діяльність щодо реалізації її положень можуть бути ефективними лише в умовах реального взаємозв'язку з іншими документами і діяльністю організації в області забезпечення ефективного функціонування і безпеки.

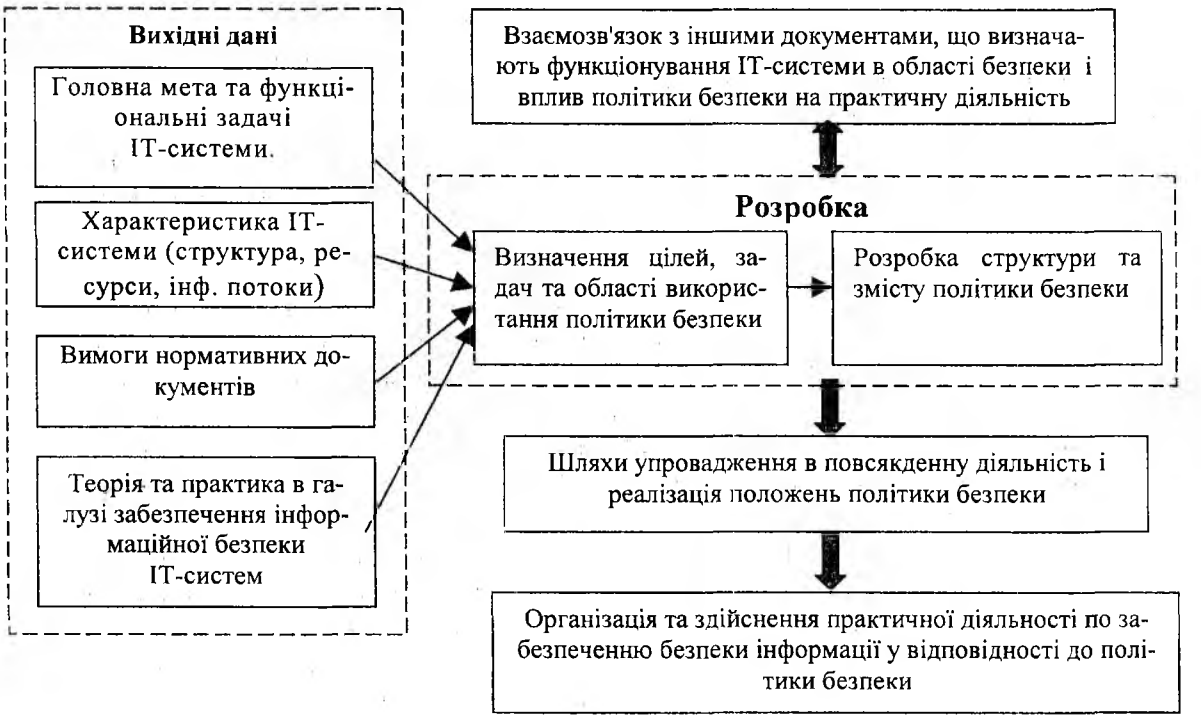

Рис. 4

Нормативна політика безпеки це сукупність документів, які охоплюють досить широке коло питань і є документами загального характеру. Для опису правил безпеки розроблюються і використовуються різні документи:

- методичні вказівки щодо здійснення практичної діяльності;
- порядок робіт, інструкції, керівництва;
- міжнародні, національні, галузеві та промислові стандарти;
- настанови, розпорядження, директиви, накази;
- регламенти (технічні регламенти) та інші документи.

Розробка вищеперелічених документів повинна здійснюватися на єдиній методологічній основі із забезпеченням наслідування і не мати протиріч із правилами та вимогами, що містяться у нормативних документах різного рівня.

5 Типи політики безпеки

Сьогодні розрізняють три основні типи політики безпеки [8, 12]:

- програмна політика безпеки;
- проблемно-орієнтована політика безпеки;
- політика безпеки конкретної системи чи об'єктова політика безпеки.

Програмна політика безпеки

Програмна політика безпеки це політика верхнього рівня. Об'єктом застосування програмної політики безпеки є відомство (організація) в цілому як систематизоване і свідоме об'єднання по місцю та часу дій людей, що мають досягти визначених цілей. За організацію і здійснення розробки програмної політики безпеки безпосередню відповідальність несе керівник. Програмна політика безпеки розробляється з метою визначення (реструктуризації)

основних компонентів і реалізації (впровадження в дію) програми забезпечення інформаційної безпеки (ПЗІБ) відомства.

Програмна політика безпеки визначає:

- цілі і задачі ПЗІБ, сферу її діяльності всередині відомства;
- осіб, що відповідають за реалізацію різних напрямків ПЗІБ.

Таким чином, програмна політика безпеки визначає множину стратегічних напрямків забезпечення інформаційної безпеки, види і обсяг ресурсів, які виділяються для реалізації ПЗІБ. У даному випадку програмна політика безпеки визначає стратегію керівництва в області забезпечення інформаційної безпеки. Саме тому цей документ розробляється на довгий строк (5 і більше років).

Основними компонентами програмної політики безпеки є:

1. Ціль і призначення. Програмна політика безпеки визначає, встановлює і на адміністративному рівні закріплює стратегічний напрямок діяльності керівництва відомства в області забезпечення інформаційної безпеки. Вона містить обґрунтування необхідності реалізації програми забезпечення інформаційної безпеки, визначає цілі програми. В даній частині визначається і обґрунтовується потреба в забезпеченні цілісності, доступності, конфіденційності ресурсів. Ці потреби формулюються у формі основних (базових) цілей (задач) захисту, котрі встановлюються політикою безпеки.

2. Область та об'єкт застосування положень політики безпеки. Програмна політика повинна чітко визначати, які ресурси, включаючи обладнання, апаратуру, апаратне та програмне забезпечення, інформацію та персонал, охоплює програма із забезпечення безпеки. У більшості випадків програма буде охоплювати всю систему і весь персонал організації. Іноді область застосування програми може бути обмеженою.

3. Встановлення прав та обов'язків. Програмна політика безпеки повинна створювати організаційно-технічну основу формування відповідних структур (служб, підрозділів), що повинні здійснювати управління та контроль над процесами забезпечення режиму інформаційної безпеки в організації. Документ повинен чітко визначати права та обов'язки керівників різного рівня, технічного персоналу, користувачів та інших осіб у відношенні підтримки, реалізації цілей та задач забезпечення інформаційної безпеки. Визначення змісту прав та обов'язків повинно здійснюватись у відповідності до принципів конкретності (призначається конкретна особа, яка несе відповідальність за конкретні дії) і принципу відповідності вимогам чинного законодавства та інших нормативних документів.

4. Визначення принципів контролю (нагляду) за підтриманням режиму інформаційної безпеки. В програмній політиці приділяється увага двом основним задачам забезпечення контролю. По-перше, здійснення загального контролю за реалізацією вимог безпеки, що визначаються програмою із забезпечення безпеки і керівниками різних підрозділів організації. З цією метою може бути призначений генеральний інспектор, який відповідає за здійснення постійного моніторингу стану інформаційної безпеки в організації, включаючи перевірку якості здійснення процесів управління безпекою і реалізації положень програми щодо забезпечення інформаційної безпеки. Іншою задачею є визначення штрафів та дисциплінарних стягнень. Оскільки політика безпеки – це документ високого рівня, то визначення конкретного змісту покарань за різні порушення в документі не деталізується. Політика безпеки може встановити необхідність створення контролюючої структури (служби), яка відповідає за розробку конкретного переліку порушень і визначення стягнень за них. Даний розділ політики безпеки повинен ураховувати норми законодавства в даній сфері і бути узгодженим із ними. Покарання, що передбачені за визначені дії законами, не повинні дублюватися у внутрішніх документах організації. Але з метою навчання та інформованості персоналу перелік цих дій і форми відповідальності за них можуть наводитися в політиці безпе-

ки. Розробник даної частини політики безпеки повинен пам'ятати, що порушення політики можуть бути і не навмисними.

Проблемно-орієнтована політика безпеки

Об'єктом застосування проблемно-орієнтованої політики безпеки є окрема проблема або задача в області забезпечення безпеки інформації в організації. Частіше за все проблемно-орієнтована політика безпеки розробляється для розв'язання знову виникаючих проблем, наприклад для реалізації і обліку нових вимог, що вводяться прийняттям нового закону чи іншого нормативного документа. Необхідність розробки проблемно-орієнтованої політики безпеки часто вимагає у відповідь як на появу та використання в організації нових технологій, так і на виникнення нових погроз та слабкостей. Проблемно-орієнтована політика безпеки може часто піддаватися перегляду в залежності від змін, які відбуваються в технологіях, законодавстві країни, структурі організації, та інших чинників. Звідси витікає одна з її властивостей – змінність.

Серед галузей діяльності організації, для яких повинна розроблятися проблемно-орієнтована політика безпеки, є політика здійснення Internet-доступу в організації; політика захисту електронної пошти; управління ризиками та планування безперебійної роботи; правила використання неавторизованого програмного забезпечення; організація виконання робіт з використанням мобільних та стаціонарних засобів обчислювальної техніки; правила використання засобів зберігання даних та систем резервного копіювання і т. ін.

У залежності від вирішуваної проблеми проблемно-орієнтована політика безпеки може бути подана у вигляді як окремого, інколи досить об'ємного документа, так і у вигляді окремих правил безпеки. Частіше за все проблемно-орієнтована політика безпеки уточнює, конкретизує положення програмної політики безпеки чи об'єктової політики безпеки.

Основними компонентами проблемно-орієнтована політика безпеки є:

1. Формулювання та опис роботи. Чітке визначення проблеми, що підлягає розв'язанню, її системний опис повинні передувати безпосередній розробці правил безпеки. Розробник політики повинен визначити важливість, відмінні ознаки та умови існування проблеми. Усвідомлення проблеми дозволить сформулювати цілі проблемно-орієнтованої політики безпеки і обґрунтувати необхідність її розробки.

2. Формулювання позиції організації. Даний компонент містить чітке та прозоре викладення позиції організації у відношенні до даної проблеми.

3. Обґрунтованість застосування. Правила, які вводяться проблемно-орієнтованою політикою безпеки, повинні містити обґрунтування свого застосування. Це означає, що положення політики повинні містити пояснення що, де, як, коли та ким конкретно застосовується правило.

4. Повноваження та відповідальність. Як і будь-яка політика безпеки, проблемно-орієнтована політика безпеки повинна чітко формулювати повноваження та відповідальність осіб, що мають відношення до реалізації положень політики.

5. Порядок взаємодії. У будь-якій проблемній політиці безпеки називаються конкретні посадові особи в організації, які уповноважені вирішувати ті чи інші проблеми, що виникли при реалізації конкретних положень політики безпеки. Оскільки позиція організації з даного питання змінюється не частіше, ніж конкретні співробітники, то краще вказати посаду (роль) співробітника, якому впроваджено вирішення таких проблем посадовими обов'язками. Для вирішення практичних проблем в реалізації конкретних положень політики (правил) користувачі можуть контактувати з керівниками різного рангу, економістами, інженерно-технічним складом, системними адміністраторами і т.ін. Співробітник повинен знати, до кого звернутися з питаннями і за додатковою інформацією – до безпосереднього начальника, системного адміністратора чи співробітника служби захисту інформації.

Проблемно-орієнтована політика безпеки часто супроводжується керівництвами, настановами та інструкціями. Наприклад, політика використання неофіційного ПЗ може включати в себе керівництва з перевірки дисків, їх реєстрації та обліку і т.ін.

Системно-орієнтована політика безпеки

Системно-орієнтована політика безпеки перш за все визначає напрямок, методи та процедури забезпечення інформаційної безпеки у конкретній ІТС. Даний тип політики обмежений рамками окремої ІТС, а також областю взаємодії самої системи і середовища її експлуатації. Політика безпеки ІТС – це частина програмної політики безпеки, яка наслідує основні принципи політики інформаційної безпеки організації (відомства). Системна політики безпеки розробляється з одного боку для керівників старшої ланки, які приймають фінансові та технічні рішення відносно використання в тій чи іншій ІТС. З іншого боку вимоги політики безпеки доводяться до відома всіх робітників, які мають безпосереднє відношення до закупівлі обладнання та експлуатації ІТС, а також до інформації, котра обробляється в даній системі.

В самому загальному випадку для опису системної політики безпеки можна використовувати дворівневу модель: цілі (задачі) захисту та практичні правила безпеки. Для розробки пов'язаного та повного набору правил безпеки розробник повинен використовувати спеціальні прийоми, за допомогою яких на основі аналізу задач захисту формулюються правила безпеки.

Визначення цілей безпеки та формулювання задач захисту є важливим етапом розробки системної політики безпеки. Крім того, даний етап – неперервний, тобто спеціалісти служби захисту інформації ІТС здійснюють постійний моніторинг актуальності сформульованих та уточнених задач захисту в процесі експлуатації системи. Відносно безпеки ІТС задачі захисту повинні бути конкретно та прозоро сформульовані. Тут краще застосовувати вимоги міжнародних стандартів ISO/IEC 15408 «Єдині критерії оцінки безпеки IT-систем» та ISO/IEC 15446 «Керівництво з розробки профілю захисту та проекту безпеки». Останній стандарт досить докладно описує методику визначення цілей безпеки та формулювання задач захисту IT-систем. Задачі захисту містять послідовність тверджень, які описують чіткі цілеспрямовані дії над конкретними ресурсами. В цілому задачі захисту допомагають точно визначити, що повинно бути захищеним у IT-системі.

Після того як будуть визначені задачі захисту, необхідно сформулювати правила безпеки. Загальна модель типового правила – хто, що і за яких умов. Тобто хто (особа, категорія осіб, організація) має право здійснювати будь-які дії (записати, модифікувати, купувати, знищити, увійти і т.ін.) і за яких умов ця дія може бути здійснена. При розробці правил політики безпеки основною перешкодою є забезпечення необхідного рівня деталізації правила. Необхідно пам'ятати, що політики безпеки не є ні директива, ні норматив, ні інструкція. Вона описує безпеку в узагальнених термінах без специфічних деталей. У правилах безпеки описано, що повинно бути захищеним і які обмеження накладаються на управління. Надмірна деталізація правил безпеки на рівні системи приведе до істотного адміністративного тягаря, негнучкості політики безпеки, яка розробляється на досить тривалий строк і повинна давати можливість використовувати широкий спектр різних методів та засобів захисту для забезпечення вимог безпеки.

Основними компонентами системно-орієнтованої політики безпеки є:

1. Концепція інформаційної безпеки ІТС, яка відображає систему поглядів, основних принципів та основних направлень забезпечення режиму інформаційної безпеки в системі. В концепції на основі аналізу сучасного досягнутого рівня і динаміки розвитку інформаційних технологій, очікуваних погроз інформаційній безпеці, джерел цих погроз та чинників, що сприяють їх реалізації, подається систематизоване викладання цілей, задач та принципів досягнення рівня безпеки, що вимагається. Концепція визначає генеральну лінію у вирішенні проблем інформаційної безпеки та викладає шляхи досягнення поставлених цілей безпеки.

2. Опис процесів управління ризиками. Даний компонент містить результати аналізу погроз, аналізу ризиків та вразливість і оцінку ризиків. Управління ризиками передбачає вивчення моделі погроз і моделей джерел погроз, оцінку можливих наслідків від реалізації погроз, формування моделі захисту інформації в ІТС і прийняття рішення на знешкодження ризиків. Основними елементами управління ризиками є визначення компонентів і ресурсів (активів) ІТС, ідентифікація погроз та зв'язок їх з об'єктом захисту, оцінка ризиків та величини можливого збитку, вибір варіанту побудови системи захисту інформації, оцінка витрат на реалізацію засобів захисту та створення системи захисту.

3. Загальні вимоги до безпеки інформації та рішення щодо забезпечення режиму інформаційної безпеки. Тут безпосередньо містяться правила безпеки відносно фізичної безпеки, автентифікації, ідентифікації та управління доступом, правила застосування криптографічних засобів, правила забезпечення антивірусного захисту та інші питання.

4. Обов'язки в області інформаційної безпеки розробляються з метою одержати ясне розуміння ролей та обов'язків окремих осіб у відношенні до безпеки ІТС.

5. План забезпечення безперебійної роботи ІТС містить опис процедур реагування на нештатні та надзвичайні ситуації, процедур переходу системи в аварійний режим функціонування, процедури відновлення функціонування системи після збоїв та інших ситуацій.

Тут наведені основні компоненти політики безпеки, перелік яких може бути збільшено. Структура та зміст системної політики безпеки визначаються у кожному конкретному випадку.

Політика безпеки повинна бути активним компонентом всієї діяльності щодо створення, реалізації, виготовленню, експлуатації ІТС. Вона буде і повинна впливати на різні аспекти організаційно-технічної діяльності з організації циклу управління підприємством. На рис.5 подано взаємозв'язок політики безпеки з різними аспектами експлуатації ІТС.

Рис. 5

Висновки

1. Політика безпеки має складну двояку природу та має пасивну і активну складові. З одного боку політика безпеки – це система взаємопов'язаних та узгоджених правил безпеки, які регламентують порядок обробки інформації в ІТС і направлені на запобігання визначеної множини погроз безпеці (пасивна складова). З цих позицій політика безпеки повинна мати властивості не протиріччя цілей безпеки та головної цілі функціонування ІТС, повноти вимог безпеки, не протиріччя правил безпеки вимогам нормативних документів і стандартів, законності, узгодженості. Пасивна складова відповідає за формування правил безпеки і по суті відповідає за формальне формування політики безпеки. Правила безпеки не замінюють інструкції та стандарти, не є директивами і засобами управління, описують безпеку в загальних термінах і не дають вказівки, яким чином здійснюються конкретні заходи безпеки.

З іншого боку політика безпеки – це систематична, стабільна, організована та цілеспрямована ДІЯЛЬНІСТЬ власника ІТС відносно розв'язання проблем забезпечення безпеки інформації, що здійснюється або безпосередньо самим власником, або через відповідні механізми і органи управління та впливає на функціонування ІТС у цілому (активна складова). З позиції діяльнісного підходу політика безпеки повинна бути цілеспрямованою, стабільною, неперервною, організованою, керованою, узгодженою, мотивованою, забезпечувати максимальну результативність і ефективність при досягненні цілей безпеки і розв'язанні задач захисту, бути адекватною погрозам безпеки, придатною та гнучкою в реалізації, здійснюваною на різних рівнях забезпечення безпеки інформації, досить простою в адміністративному забезпеченні.

2. Основними складовими політики безпеки є: концепція і програма забезпечення безпеки інформації в ІТС, менеджмент, інжиніринг та аудит безпеки.

3. Правила безпеки важливі для забезпечення якісного управління безпекою, вибору номенклатури засобів захисту інформації, демонстрації активної підтримки власником процесів забезпечення безпеки інформації в ІТС, знищення організаційних і економічних перешкод створенню комплексної системи захисту інформації в ІТС, забезпечення послідовного і повного захисту інформаційних ресурсів на систематичній основі.

4. Загальний порядок розробки пасивної складової політики безпеки включає обробку вихідних даних відносно об'єкта захисту і середовища його експлуатації, визначення цілей і задач політики безпеки, розробку структури і конкретного змісту політики безпеки, визначення шляхів впровадження в життя та реалізації положень, правил, норм та вимог політики безпеки, а також визначення ступеня відповідальності за порушення вимог ПБ та контроль за їх виконанням.

5. Загальними задачами, на вирішення яких направлена політика безпеки, є:

- забезпечення конфіденційності, цілісності та доступності інформації в ІТС;
- безпечне функціонування ІТС із придатним рівнем ризику;
- управління інформацією та ресурсами з метою вдоволення експлуатаційних вимог до ІТС;
- здіснення цілеспрямованої та структурованої діяльності з тестування й оцінки безпеки за реалізації розроблюваних та запропонованих до застосування функцій та механізмів безпеки;
- здійснення аудиту безпеки, сертифікації та акредитації компонентів ІТС для прийняття рішення про можливість функціонування системи в захищеному режимі з вимагаємим рівнем ризику.

Список літератури: 1. *ISO/IEC 15408:2000* – Information technology – Security techniques – Evaluation criteria for IT security. – Part 1: Introduction and general model. 2. *ISO/IEC 15408:2000* – Information technology – Security techniques – Evaluation criteria for IT security. – Part 2: Security functional requirements. 3. *ISO/IEC 15408:2000* – Information technology – Security techniques – Evaluation criteria for IT security. – Part 3: Security assurance requirements. 4. *Бондаренко М.Ф., Черных С.П., Горбенко И.Д., Замула А.А., Ткач А.А.* Методологические основы концепции и политики безопасности информационных технологий // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С. 5 – 17. 5. *НД ТЗИ 1.1 – 003 –99.* Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. 6. *НД ТЗІ 2.5 – 004 – 99.* Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа. 7. *НД ТЗИ 3.7. – 001 – 99.* Методические указания по разработке технического задания на создание комплексной системы защиты информации в автоматизированной системе. 8. *NIST SP 800-12.* An Introduction to Computer Security: The NIST Handbook. 1998. 9. *ISO/IEC 17799:2001* – Information technology. – Information Security Management – Code of Practice for Information Security Management. 10. *OECD* Guidelines for Security of Information Systems and Networks. – OECD, 2002. 11. *NIST SP 800-14.* Generally Accepted Principles and Practices for securing Information Technology Systems (Principles and Practices). 2000. 12. *Потий А.В.* Политика безопасности: её типы и оценка // Служба безопасности. 2002. № 4, 5, 6. С. 18 – 20, 23 – 25, 27 – 31.

Харківський національний
університет радіоелектроніки
Державне управління справами
АО «Інститут інформаційних технологій»

Надійшла до редколегії 15.05.2003