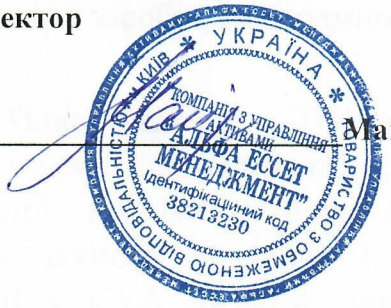
ЗАТВЕРДЖЕНО
Рішенням Загальних зборів Учасників
ТОВ «КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ»

протокол № 31 від "27" червня 2014 р.
Директор



_____ Майборода В.В.

ПЛАН ЗАХИСТУ ІНФОРМАЦІЇ В ТОВ «КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ»

Київ, 2014

Захист інформації в АС - єдина сукупність правових і морально-етичних норм, організаційних мір, фізичних мір і засобів, програмно-технічних засобів.

План захисту інформації (далі – План захисту) в ТОВ «КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ» (далі – КУА) розробляється на підставі проведеного аналізу технології обробки інформації, аналізу ризиків, сформульованої політики безпеки інформації. План захисту визначає і документально закріплює об'єкт захисту інформації в КУА, основні завдання захисту, загальні правила обробки інформації в КУА, мету побудови та функціонування заходів із захисту інформації. План захисту має фіксувати на певний момент часу склад АІС, перелік оброблюваних відомостей, технологію обробки інформації, склад комплексу засобів захисту інформації, склад необхідної документації та ін.

План захисту повинен регулярно переглядатися та при необхідності змінюватись.

План захисту інформації повинен складатись з наступних розділів:

- завдання захисту інформації в АІС;
- класифікація інформації, що обробляється в АІС;
- опис компонентів АІС та технології обробки інформації;
- загрози для інформації в АІС;
- політика безпеки інформації в АІС;
- система документів з забезпечення захисту інформації в АІС.

На підставі Плану захисту складається календарний план робіт з захисту інформації в АІС.

1. *ЗАВДАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АІС.*

Повинні бути визначені основні завдання і мета захисту інформації, об'єкти захисту.

Завданнями захисту інформації можуть бути:

- забезпечення визначених політикою безпеки властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації АІС;
- своєчасне виявлення та знешкодження загроз для ресурсів АІС, причин та умов, які спричиняють (можуть привести до) порушення її функціонування та розвитку;
- створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні АІС;
- ефективне знешкодження (попередження) загроз для ресурсів АІС

шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;

- керування засобами захисту інформації, керування доступом користувачів до ресурсів АІС, контроль за їхньою роботою з боку персоналу КУА;

- реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;

- створення умов для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними (несанкціонованими) діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками, зменшення негативного впливу наслідків порушення безпеки на функціонування АІС.

2. *КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ, ЩО ОБРОБЛЯЄТЬСЯ В АІС.*

Повинні бути класифіковані всі відомості за режимом доступу, за правовим режимом, а також за типом їхнього представлення в АІС. Класифікація є підставою для визначення методів і способів захисту кожного окремого виду інформації.

За режимом доступу інформація в АІС поділена на:

- відкриту;

- з обмеженим доступом.

Відкриту інформацію поділяється на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, яка такого захисту потребує. До другої слід відносити інформацію, важливу для КУА, важливі для КУА відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків.

За правовим режимом інформація з обмеженим доступом повинна бути поділена на таємну та конфіденційну.

До таємної інформації має бути віднесена інформація, що містить відомості, які становлять державну, а також іншу, передбачену законом таємницю.

Конфіденційну інформацію необхідно класифікувати, поділивши її на декілька категорій за ступенем цінності (критерії розподілу можуть бути визначені під час оцінки ризиків).

Для встановлення правил взаємодії активних і пасивних об'єктів АІС інформація повинна бути класифікована за типом її представлення в АІС (для кожної з визначених категорій встановлюються типи пасивних об'єктів комп'ютерної системи, якими вона може бути представлена).

3. *ОПИС ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ В АІС КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ».*

Повинна бути проведена інвентаризація усіх компонентів АІС і

зафіксовані всі активні і пасивні об'єкти, які беруть участь у технологічному процесі обробки і тим чи іншим чином впливають на безпеку інформації. Для кожного активного об'єкту АІС має бути визначено перелік пасивних об'єктів, які з ним взаємодіють.

До об'єктів, що підлягають інвентаризації, відносяться:

- обладнання - ЕОМ та їхні складові частини (процесори, монітори та ін.), периферійні пристрої;
- програмне забезпечення - вихідні, завантажувальні модулі, утиліти, операційні системи та інші системні програми, діагностичні і тестові програми тощо;
- дані - тимчасового і постійного зберігання, на магнітних носіях, друковані, архівні і резервні копії, системні журнали, технічна, експлуатаційна і розпорядча документація та ін.;
- персонал і користувачі АІС.

Окрім компонентів АІС, необхідно дати опис технології обробки інформації в АІС, що потребує захисту, тобто способів і методів застосування засобів обчислювальної техніки під час виконання функцій збору, зберігання, обробки, передачі і використання даних, або алгоритмів окремих процедур. Опис (як в цілому, так і для окремих компонентів) може бути неформальним або формальним.

При цьому доцільно розробити структурну схему інформаційних потоків в АІС, яка б відображала інформаційну взаємодію між основними компонентами АІС (завданнями, об'єктами) з прив'язкою до кожного елемента схеми категорій інформації та визначених політикою безпеки рівнів доступу до неї.

4. *ЗАГРОЗИ ДЛЯ ІНФОРМАЦІЇ В АІС.*

Основою для проведення аналізу ризиків є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в АІС:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні та інші канали;
- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
- несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних

вірусів.

Загрози для інформації, що обробляється в АІС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АІС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

- збої і відмови у роботі обладнання та технічних засобів АІС;

- наслідки помилок під час проектування та розробки компонентів АІС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

- помилки персоналу (користувачів) АІС під час експлуатації;

- навмисні дії (спроби) потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережливості та керованості АІС.

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

- дії, що призводять до відмови АІС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);

- ненавмисне пошкодження носіїв інформації;

- неправомірна зміна режимів роботи АІС (окремих компонентів, обладнання, тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

- неумисне зараження комп'ютерними вірусами;

- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

- наслідки некомпетентного застосування засобів захисту;

- інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АІС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу

до її ресурсів, можуть бути:

- порушення фізичної цілісності АІС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АІС (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.);

- порушення режимів функціонування АІС (обладнання, тощо);

- впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

- використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;

- використання (шантаж, підкуп тощо) з корисливою метою персоналу АІС;

- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

- несанкціоноване копіювання носіїв інформації;

- читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

- неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

- інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити:

-на порушення яких властивостей інформації або АІС вона спрямована (порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережливості та керованості АІС);

-джерела виникнення (які суб'єкти АІС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

-можливі способи здійснення загроз.

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної АІС.

Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і та ін. По відношенню до АІС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника повинна визначати:

- можливу мету порушника та її градацію за ступенями небезпечності для АІС;
- категорії осіб, з числа яких може бути порушник.;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Необхідно класифікувати порушників за рівнем можливостей, що надаються їм засобами АІС, наприклад, поділити на чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей ведення діалогу з АІС — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням АІС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
- четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АІС, аж до включення до складу АІС власних засобів з новими функціями обробки інформації.

За рівнем знань про АІС усіх порушників можна класифікувати як таких, що:

- володіють інформацією про функціональні особливості АІС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;
- володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;
- володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АІС;
- володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників можна класифікувати як таких, що:

- використовують виключно агентурні методи одержання відомостей;
- використовують пасивні технічні засоби перехоплення інформаційних

сигналів;

- використовують способи і засоби активного впливу на АІС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, тощо).

За місцем здійснення дії можуть класифікуватись:

- без одержання доступу на контрольовану територію КУА (АІС);
- з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АІС;
- з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АІС;
- з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);
- з одержанням доступу до засобів адміністрування АІС;

5. *ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ В АІС.*

Як було сказано раніше **Політика безпеки інформації** – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок накопичення, обробки, зберігання інформації. Термін "політика безпеки" може бути застосовано щодо АІС в цілому, окремого її компонента, послуги захисту, що реалізується системою і т. ін.

Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, фізичного середовища та інші чинники. В АІС може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки в АІС мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів АІС), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів АІС політика безпеки стосується, а яких – ні).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування в АІС кожного з цих видів.

Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;

- гнучкості керування системою захисту, простоти і зручності її використання;

- відкритості алгоритмів і механізмів захисту.

Політика безпеки повинна доказово давати гарантії того, що:

- в АІС (в кожній окремій складовій частині, в кожному функціональному завданні і т. ін.) забезпечується адекватність рівня захисту інформації рівню її критичності;

- реалізація заходів захисту інформації є рентабельною;

- в будь-якому середовищі функціонування АІС забезпечується оцінюваність і перевіряємість захищеності інформації;

- забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів АІС), звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування АІС;

- персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;

- всі критичні з точки зору безпеки інформації технології (функції) АІС мають відповідні плани забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій;

- враховані вимоги всіх документів, які регламентують порядок захисту інформації в АІС, та забезпечується їхнє суворе дотримання.

Методологія розроблення політики безпеки включає в себе наступні роботи:

- розробка концепції захисту інформації в ТОВ «КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ»;

- аналіз ризиків;

- визначення вимог до заходів, методів та засобів захисту;

- вибір основних рішень з забезпечення безпеки інформації;

- організація виконання відновлювальних робіт і забезпечення неперервного функціонування АІС;

- документальне оформлення політики безпеки.

Концепція захисту інформації в КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ» (далі – Концепція) повинна визначати основи політики КУА в сфері захисту інформації, забезпечувати єдність принципів побудови інформації, що збирається, накопичується, обробляється, використовується та збирається в КУА при виконанні покладених на неї функцій.

Концепція повинна формулювати основні загрози безпеці інформації і цілі впровадження захисту інформації, визначати пріоритетні напрями її впровадження в КУА.

Концепція повинна забезпечувати єдність принципів формування і проведення політики захисту інформації в усіх сферах діяльності КУА і служить підставою для створення короткострокових та довгострокових програм розвитку сфери захисту інформації.

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в КУА. Під час проведення аналізу ризиків необхідним є виконання наступних робіт.

Визначення компонентів і ресурсів АІС, які необхідно враховувати при аналізі: повинні бути визначені критичні з точки зору безпеки компоненти і ресурси АІС, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення безпеки інформації (об'єкти захисту).

Ідентифікація загроз з об'єктами захисту: встановлюється відповідність моделі загроз і об'єктів захисту, тобто складається матриця загрози/компоненти (ресурси) АІС. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс АІС. У процесі упорядкування матриці може уточнюватися список загроз і об'єктів захисту, внаслідок чого коригуватись модель загроз.

Оцінка ризиків: повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози необхідно вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту податкової інформації. На практиці для більшості загроз неможливо одержати достатньо об'єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо.

Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока).

У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

Вибір основних рішень з забезпечення безпеки інформації

Комплекс заходів з забезпечення безпеки інформації повинен розглядатися на трьох рівнях:

- правовому;
- організаційному;
- технічному.

На правовому рівні забезпечення безпеки інформації повинні бути

вироблені підходи щодо:

- системи нормативно-правового забезпечення робіт з захисту інформації в АІС КУА;

- підтримки керівництвом заходів з забезпечення безпеки інформації в АІС КУА, виконання правових вимог з захисту інформації, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподілу обов'язків співробітників системи захисту інформації;

- процедур доведення до персоналу і користувачів АІС основних положень політики безпеки інформації, їхнього навчання і підвищення кваліфікації з питань безпеки інформації;

- системи контролю за своєчасністю, ефективністю і повнотою реалізації в АІС рішень з захисту інформації, дотриманням персоналом і користувачами положень політики безпеки.

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

- застосування режимних заходів на об'єктах АІС;

- забезпечення фізичного захисту обладнання АІС, носіїв інформації, інших ресурсів;

- проведення обстеження середовищ функціонування АІС КУА;

- виконання робіт з модернізації АІС (окремих компонентів);

- регламентації доступу сторонніх користувачів до ресурсів АІС;

- регламентації доступу власних користувачів і персоналу до ресурсів АІС;

- здійснення профілактичних заходів (наприклад, попередження ненавмисних дій, що призводять до порушення політики безпеки, попередження появи вірусів та ін.);

- реалізації окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до АІС, використання мереж передачі даних загального користування, зокрема Internet, використання несертифікованого ПЗ та ін.).

На технічному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації. Під час розгляду різних варіантів реалізації необхідно враховувати наступні аспекти:

- інженерно-технічне обладнання виділених приміщень, в яких розміщуються компоненти АІС, експлуатація і супроводження засобів блокування технічних каналів витоку інформації;

- реєстрація санкціонованих користувачів АІС, авторизація користувачів в системі;

- керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів і адміністраторів;

- виявлення і реєстрація небезпечних подій з метою здійснення повсякденного контролю або проведення службових розслідувань;

- перевірка і забезпечення цілісності критичних даних на всіх стадіях

їхньої обробки в АІС;

- забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів;

- резервне копіювання критичних даних, супроводження архівів даних і ПЗ;

- відновлення роботи АІС після збоїв, відмов, особливо для систем із підвищеними вимогами до доступності інформації;

- захист ПЗ, окремих компонентів і АІС в цілому від внесення несанкціонованих доповнень і змін;

- забезпечення функціонування засобів контролю, у тому числі засобів виявлення технічних каналів витоку інформації.

Організація проведення відновлювальних робіт і забезпечення неперервного функціонування АІС

Повинні бути вироблені підходи щодо планування і порядку виконання відновлювальних робіт після збоїв, аварій, інших непередбачених ситуацій (надзвичайних ситуацій) з метою забезпечення неперервного функціонування АІС в захищеному режимі. Під час планування цих робіт необхідно враховувати наступні питання:

- виявлення критичних з точки зору безпеки процесів у роботі АІС;

- визначення можливого негативного впливу надзвичайних ситуацій на роботу АІС;

- визначення й узгодження обов'язків персоналу і користувачів, а також порядку їхніх дій у надзвичайних ситуаціях;

- підготовка персоналу і користувачів до роботи в надзвичайних ситуаціях.

План проведення відновлювальних робіт і забезпечення неперервного функціонування АІС повинен описувати дії щодо улагодження інциденту, дії щодо резервування, дії щодо відновлення. Він включає в себе:

- опис типових надзвичайних ситуацій, які потенційно найбільш можливі в АІС внаслідок наявності вразливих місць, або які реально мали місце під час роботи;

- опис процедур реагування на надзвичайні ситуації, які слід вжити відразу після виникнення інциденту, що може призвести до порушення політики безпеки;

- опис процедур тимчасового переводу АІС або окремих її компонентів на аварійний режим роботи;

- опис процедур поновлення нормальної виробничої діяльності АІС або окремих її компонентів;

- порядок тестування плану, тобто проведення тренувань персоналу в умовах імітації надзвичайних ситуацій.

План проведення відновлювальних робіт і забезпечення неперервного функціонування АІС підлягає перегляду у разі виникнення істотних змін в АІС. Такими змінами можуть бути:

- встановлення нового обладнання або модернізація існуючого,

включення до складу АІС нових компонентів;

- встановлення нових систем життєзабезпечення АІС (сигналізації, вентиляції, пожежогасіння, кондиціонування та ін.);

- проведення будівельно-ремонтних робіт;

- організаційні зміни у структурі АІС, виробничих процесах, процедурах обслуговування АІС;

- зміни у технології обробки інформації;

- зміни у програмному забезпеченні;

- будь-які зміни у складі і функціях КСЗІ.

Найважливішу частину політики безпеки, яка регламентує доступ користувачів і процесів до ресурсів АІС, складають **правила розмежування доступу (ПРД).** ПРД - є певним абстрактним механізмом, який виступає посередником при будь-яких взаємодіях об'єктів АІС і є найбільш суттєвим елементом політики безпеки.

Як приклад, загальні ПРД можуть бути наступними (за припущення, що в АІС визначено такі ієрархічні ролі – адміністратор безпеки АІС, адміністратор мережі, користувач):

- відповідальність за працездатність робочого місця користувача та за дотримання всіх вимог і процедур, пов'язаних з обробкою інформації та її захистом, повинне бути покладено на користувача, при цьому, користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;

- для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів АІС, керування механізмами захисту здійснюється адміністратором безпеки АІС;

- для попередження поширення комп'ютерних вірусів відповідальність за дотримання правил використання ПЗ несуть: на АРМ – користувачі, адміністратор мережі, в АІС - адміністратор безпеки АІС. Використовуватись повинно тільки ПЗ, яке дозволено політикою безпеки (ліцензійне, яке має відповідні сертифікати, експертні висновки тощо);

- за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор безпеки АІС. Такі роботи виконуються за його дозволом;

- кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору мережі. Атрибути для адміністраторів мережі надає адміністратор безпеки АІС. Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача. Користувачам забороняється спільне використання персональних атрибутів;

- користувачі проходять процедуру автентифікації для отримання доступу до ресурсів АІС;

- атрибути користувачів періодично змінюються, а невикористовувані і скомпрометовані – видаляються;

- процедури використання активного мережевого обладнання, а також окремих видів ПЗ, яке може суттєво впливати на безпеку (аналізатори трафіку,

аналізатори безпеки мереж, засоби адміністрування та ін.), авторизовані і здійснюються під контролем адміністратора безпеки АІС;

- адміністратор безпеки АІС і адміністратори мережі повсякденно здійснюють перевірку працездатності засобів захисту інформації, ведуть облік критичних з точки зору безпеки подій і готують звіти щодо цього.

Загальні ПРД мають бути конкретизовані на рівні вибору необхідних функціональних послуг захисту (профілю захищеності) та впровадження організаційних заходів захисту інформації.

КАЛЕНДАРНИЙ ПЛАН РОБІТ З ЗАХИСТУ ІНФОРМАЦІЇ В АІС

На підставі Плану захисту інформації в АІС складається календарний план робіт з реалізації заходів захисту інформації в АІС, який може мати такі розділи:

- організаційні заходи;
- контрольно-правові заходи;
- профілактичні заходи;
- інженерно-технічні заходи.
- робота з кадрами.

Організаційні заходи з захисту інформації - це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення захисту інформації. До плану можуть включатись заходи щодо:

- розробки документів (інструкцій, методик, правил, розпоряджень тощо) з різних напрямів захисту інформації в АІС;
- внесення змін та доповнень до чинних в АІС документів з урахуванням зміни умов (обставин);
- розробки та впровадження нових організаційних заходів з захисту інформації;
- обгрунтування необхідності застосування та впровадження нових засобів захисту інформації;
- координації робіт та взаємодії з іншими підрозділами органу ДПС або зовнішніми організаціями на всіх етапах життєвого циклу АІС;
- розгляду результатів виконання затверджених заходів та робіт з захисту інформації;
- інші.

До контрольно-правових заходів можуть бути віднесені:

- контроль за виконанням персоналом (користувачами) вимог відповідних інструкцій, розпоряджень, наказів;
- контроль за виконанням заходів, розроблених за результатами попередніх перевірок;
- контроль за станом зберігання та використання носіїв інформації на

робочих місцях;

- інші.

До ***профілактичних*** слід відносити заходи, спрямовані на формування у персоналу (користувачів) мотивів поведінки, які спонукають їх до безумовного виконання у повному обсязі вимог режиму, правил проведення робіт та ін., а також на формування відповідного морально-етичного стану в колективі.

До ***інженерно-технічних*** слід відносити заходи, спрямовані на налагодження, випробування і введення в експлуатацію, супроводження і технічне обслуговування апаратних і програмних засобів захисту інформації від НСД, засобів захисту інформації від загроз її витоку технічними каналами, інженерне обладнання споруд і приміщень, в яких розміщуються засоби обробки інформації, у тому числі в процесі капітального будівництва тощо.

Планування роботи з кадрами включає заходи з підбору та навчання персоналу (користувачів) встановленим правилам безпеки інформації, новим методам захисту інформації, підвищення їхньої кваліфікації. Навчання персоналу (користувачів) може здійснюватись власними силами, з залученням спеціалістів зовнішніх організацій або в інших організаціях. Навчання повинно здійснюватися згідно з програмою, затвердженою керівництвом КУА. Навчальні програми повинні мати теоретичний і практичний курси. Доцільність і необхідність включення до програм окремих розділів визначається особливостями АІС і технологіями захисту інформації, що використовуються в ній, функціональними завданнями спеціалістів, що входять до складу навчальних груп та іншими чинниками.

Нормативна база України в сфері технічного захисту інформації

Ліцензування в галузях технічного і криптографічного захисту інформації та у галузі голографічного захисту

ЗАКОН УКРАЇНИ **"Про ліцензування певних видів господарської діяльності"**

Стаття 9. Види господарської діяльності, що підлягають ліцензуванню

Відповідно до цього Закону ліцензуванню підлягають такі види господарської діяльності:

13) розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівля спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації;

14) розроблення, виробництво, використання, експлуатація, сертифікаційні випробування, тематичні дослідження, експертиза, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівля криптосистемами і засобами криптографічного захисту інформації;

15) розроблення, виробництво, впровадження, сертифікаційні випробування, ввезення, вивезення голографічних захисних елементів;

16) розроблення, виробництво, впровадження, обслуговування, дослідження ефективності систем і засобів технічного захисту інформації, надання послуг в галузі технічного захисту інформації;

Криптографічний захист інформації.

Види робіт, що зазначені в "Ліцензійних умовах провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації (КЗІ), надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного захисту інформації", затверджених наказом Державного комітету України з питань регуляторної політики та підприємництва, Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України 29.12.2000 № 88/66 та зареєстрованих в Міністерстві юстиції України 20 січня 2001 р. за № 49/5240.

1. Розробка апаратних, апаратно-програмних засобів КЗІ та криптосистем.
2. Розробка програмних засобів КЗІ та криптосистем.
3. Виробництво апаратних, апаратно-програмних засобів КЗІ та криптосистем.
4. Виробництво програмних засобів КЗІ та криптосистем.
5. Використання, експлуатація засобів КЗІ та криптосистем.
6. Сертифікаційні випробування, експертиза криптосистем та засобів КЗІ.
7. Тематичні дослідження засобів КЗІ та криптосистем.
8. Надання послуг в галузі КЗІ.
9. Ввезення, вивезення засобів КЗІ та криптосистем.
10. Торгівля засобами КЗІ та криптосистемами.

Прошнуровано, пронумеровано
та скріплено відбитком печатки
та підписом керівника 16
(шістнадцять) аркушів