Інформаційна безпека та методи захисту інформації

Ефективне функціонування підприємства неможливе без управління ресурсами, що використовуються для досягнення мети. Згідно з поширеними нині в управлінській літературі поглядами поняття ресурси охоплює не лише людей, капітал, сировину, а й інформацію. Саме тому інформація, як і решта ресурсів, потребує особливого захисту.

Під інформаційною безпекою слід розуміти захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести нанесенням шкоди власникам або користувачам інформації і підтримуючої інфраструктури.

Впровадження обчислювальної техніки і різних інформаційних систем в діяльність і життя сучасних людей має безліч позитивних моментів. Але разом з користю з'явилося і безліч різного роду загроз.

Виділимо найпоширеніші види потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій:

– відсутність регламентованого доступу до файлів даних;

– вільне втручання в програмне забезпечення;

– відсутність протоколювання змін у програмному забезпеченні;

– відсутність регламентації користувачів інформації;

– відсутність дублювання важливих документів на документальних носіях даних;

– часті удосконалення одного і того ж програмного забезпечення різними особами;

– відсутність схем інформаційного забезпечення рівнів управління;

– наявність непідзвітних посадових осіб у системі управління тощо.

Однією з найбільш нагальних проблем інформаційного суспільства є захист інформації, оскільки всілякі дані, що обробляються і накопичуються

обчислювальною технікою, стали останнім часом визначати напрямок діяльності і багато інших аспектів життя сучасного соціального організму.

За допомогою незаконного володіння інформацією можна здійснювати найрізноманітніші протиправні діяння, наприклад, виробляти незаконний оборот фінансових коштів, отримувати доступ до секретної комерційної інформації і ін.

Слід зазначити, що конфіденційна інформація представляє величезний інтерес для конкуруючих фірм. Саме вона стає причиною посягань з боку зловмисників.

З інформаційною безпекою тісно пов'язане і таке поняття, як комерційна таємниця.

Комерційна таємниця — інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Статтею 420 Цивільного кодексу України визначено, що комерційна таємниця є одним з об'єктів інтелектуальної власності. Відповідно майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором.

Умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих

мотивів і завдало істотної шкоди суб'єкту господарської діяльності передбачає кримінальну відповідальність.

Законом переслідується не лише розголошення комерційної таємниці, але й приховування її (або надання недостовірної інформації) у тих випадках, коли надання такої інформації передбачено законом.

Багато проблем інформаційної безпеки пов'язані з недооцінкою важливості такої загрози, як конфіденційність інформації. В результаті для підприємства це може обернутися банкрутством. Навіть одиничний випадок халатності персоналу підприємства може принести йому багатомільйонні збитки, втрату репутації фірми і довіри клієнтів.

Щоб цього уникнути, фахівці служби безпеки підприємства використовують спеціальне обладнання, яке виробляє аналіз електромагнітних випромінювань, одержуваних під час роботи на комп'ютері.

Іноді співробітники підприємства можуть спеціально провокувати внутрішню витік інформації, показуючи цим своє невдоволення зарплатою, роботою або колегами. Вони запросто можуть передати всю цінну інформацію підприємства його конкурентам, спробувати знищити її або навмисне внести в комп'ютери вірус.

Технології забезпечення інформаційної безпеки можна поділити на дві групи:

I-а група - захищають програмні і апаратні засоби для обробки і зберігання інформації від відмов, порушень, здатних виникнути в результаті випадкової помилки;

II-а група - захищають програмні і апаратні засоби обробки інформації від всіляких навмисних загроз, які заздалегідь плануються зловмисниками.

Зауважимо, що існує безліч причин відмови техніки, яка обробляє інформацію, які є наслідком діяльності зловмисників або іншої дії.

Відзначимо найбільш поширені з них:

- старіння і знос деталей апаратного забезпечення, в результаті чого відбувається пошкодження даних;

- комп'ютерні ресурси використовуються некоректним чином;

- в структурі даних з часом накопичується велика кількість різноманітних помилок, що може привести до їх пошкодження.

Захистити інформацію від різних дефектів апаратної частини просто: слід лише своєчасно здійснювати її діагностику і ремонт.

Часто трапляється, що дані пошкоджуються через неправильне використання апаратної частини комп'ютера. Причин тому може бути досить багато, наприклад, недостатня кваліфікація фахівця.

Нерідко причиною псування інформації стає неправильно налаштоване програмне забезпечення. Найбільш часто грає роль саме людський фактор. Так, неправильне налаштування систем обробки інформації нерідко призводить до її псування, втрату або розкрадання.

Виходом із ситуації може стати робота тільки висококваліфікованого фахівця, що має великий досвід роботи в області інформаційних технологій.

Повноцінне забезпечення інформаційної безпеки на підприємстві повинно бути стандартизовано і перебувати під повним контролем цілий рік, в реальному часі, в цілодобовому режимі. При цьому система враховує весь життєвий цикл інформації, починаючи з моменту появи і до повного її знищення або втрати значущості для підприємства.

Якісні системи інформаційної безпеки враховують всілякі об'єкти загроз, їх джерела, цілі зловмисників, способи оволодіння інформацією, а також варіанти і засоби захисту. Вони забезпечують повне збереження інформаційного середовища, підтримують функціонування робочих комплексів, вдосконалюють його в інтересах робітничого персоналу.

Для збереження і запобігання втрати даних в індустрії інформаційної безпеки розробляються системи захисту. Їх робота заснована на складних програмних комплексах з широким набором опцій, що запобігають будь-які втрати даних.

Відзначимо, що специфікою програм є те, що для правильного їх функціонування потрібно розбірлива і налагоджена модель внутрішнього обороту даних і документів. Аналіз безпеки всіх кроків при використанні інформації ґрунтується на роботі з базами даних.

Існує п'ять рівнів захисту інформації: 1 - законодавчий; 2 - адміністративний; 3 - апаратно-програмний; 4 - фізичний; 5 - морально-етичний.

Тільки в комплексі всі ці рівні спрямовані на усунення загрози безпеки і утворюють систему захисту інформації.

Слід зауважити, що з метою захисту інформації кожен користувач зобов'язаний знати і здійснювати наступні заходи:

1) контролювати доступ як до інформації в комп'ютері, так і до прикладних програм. Необхідно мати гарантії того, що тільки авторизовані користувачі зможуть мати доступ до інформації і додатків;

2) процедури авторизації. Адміністратору слід розробити процедури авторизації, що визначають, хто з користувачів може мати доступ до тих чи інших прикладних програм та інформації, і передбачити відповідні заходи щодо впровадження в організацію таких процедур;

3) захист файлів. Слід розробити процедури по обмеженню доступу до файлів: для вказівки типу інформації, що міститься в файлах, і необхідного рівня безпеки використовувати зовнішні та внутрішні мітки; обмежувати доступ в ті приміщення, в яких зберігаються архіви, файли і бібліотеки даних; для обмеження доступу до файлів тільки авторизованих користувачів використовувати організаційні заходи і програмно-апаратні засоби;

4) захист цілісності інформації. Вводиться інформацію слід піддавати перевіркам на помилки, вона повинна бути авторизованої, повною і точною. Точність інформації необхідно перевіряти за допомогою процедур порівняння отриманих результатів обробки з передбачуваними;

5) захист системних програм. При розробці програм заходи захисту повинні включати в себе процедури щодо внесення змін до програми, її приймання і тестування до введення в експлуатацію;

6) становлення заходів захисту більш адекватними за рахунок залучення спеціалізованих організацій;

7) розгляд питання про комунікаційної безпеки. Дані, що передаються по незахищених лініях, можуть бути перехоплені.

Безсумнівно, для боротьби з тенденцією зростання злочинних злочинів в IT-сфері необхідна злагоджена й цілеспрямована організація процесу захисту інформаційних ресурсів. У цьому процесі повинні активно брати участь фахівці, адміністрація, співробітники і користувачі. Це визначає підвищену значимість організаційної сторони питання.

До захисту інформації пред'являються певні вимоги. Такий захист має бути:

- безперервної. Так як зловмисники постійно шукають можливість для обходу захисту їх цікавить;

- планової. Кожна служба здійснює планування шляхом розробки детальних планів захисту інформації в сфері її компетенції і з урахуванням загальних цілей організації;

- цілеспрямованої. Має захищатися не всі підряд, а певні об'єкти, що відповідають конкретним цілям;

- конкретною. Захищаються дані, об'єктивно що підлягають охороні, при втраті яких може бути завдано певної шкоди організації;

- активною. Інформацію необхідно захищати з достатнім ступенем наполегливості;

- надійної. Незалежно від форми подання охоронюваних даних, мови їх вираження і виду фізичного носія, на якому вони закріплені, методи і форми захисту повинні надійно перекривати можливі шляхи неправомірного доступу до цих даних;

- універсальної. Незалежно від характеру, форми і види інформації необхідно розумними і достатніми засобами перекривати будь-які види каналів витоку, де б вони не проявлялися;

- комплексної. Неприпустимо застосовувати лише окремі форми або технічні засоби для захисту інформації. Всі види і форми захисту повинні застосовуватися в повному обсязі у всьому різноманітті структурних елементів.

Відзначимо, що правовий захист інформації як ресурсу визнана на міжнародному та державному рівнях і визначається міждержавними договорами, конвенціями, деклараціями і реалізується патентами, ліцензіями і авторським правом.

На державному рівні правовий захист регулюється державними та відомчими актами.

У нашій країні регуляторами є: Конституція, закони України, цивільне, адміністративне і кримінальне право. Відомчі нормативні акти визначаються наказами, інструкціями, положеннями та інструкціями, які видаються самими відомствами, організаціями, а також підприємствами, що діють в рамках певних структур.

З усього вище сказаного слід зробити висновок, що захист інформації від неправомірного оволодіння нею відводиться далеко не останнє місце. При цьому цілями захисту інформації є:

- запобігання розголошенню, витоку і несанкціонованого доступу до охоронюваним відомостями;

- запобігання протиправних дій з модифікації, знищення, перекручення, блокування і копіювання інформації;

- запобігання інших форм протизаконного втручання в інформаційні системи та інформаційні ресурси;

- забезпечення для документованої інформації правового режиму як для об'єкта власності;

- захист прав громадян, забезпечених конституцією, на збереження особистої таємниці та конфіденційність персональних даних, які є в інформаційних системах;

- забезпечення конфіденційності документованої інформації і збереження державної таємниці відповідно до чинного законодавства;

- забезпечення прав суб'єктів в усіх інформаційних процесах, а також при розробці, виробництві і використанні інформаційних технологій, систем і засобів їх забезпечують.

Найважливішими на практиці є три аспекти IT-безпеки (рис.):

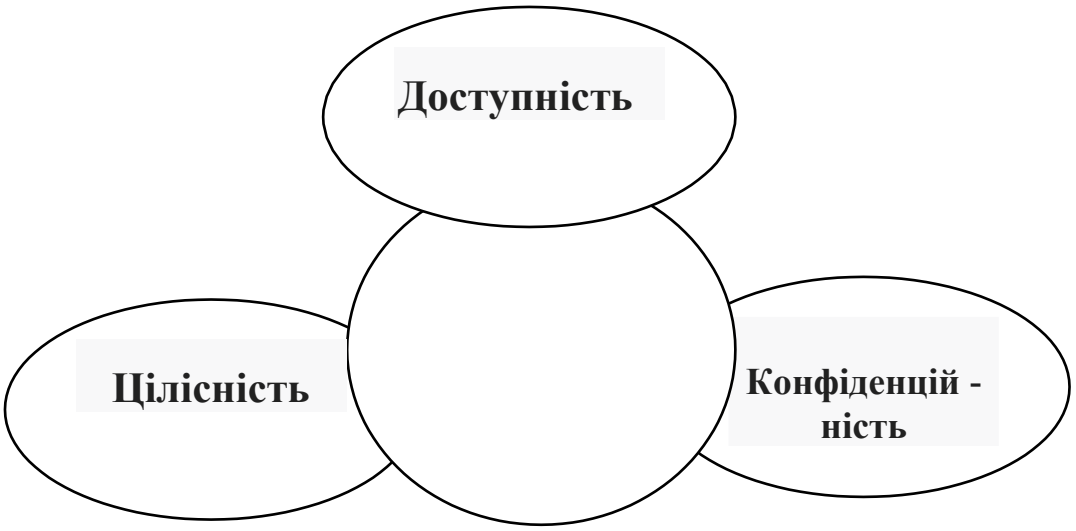

Рис. Складові інформаційної безпеки

- цілісність - захищеність системи від несанкціонованих змін і руйнування;

- доступність - можливість швидко отримати необхідну інформаційну послугу;

- конфіденційність - захищеність від несанкціонованого прочитання.

Створюючи системи захисту на підприємстві, необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різноманітних заходів, які можна розподілити на три групи: юридичні, організаційно-економічні й технологічні. По-друге, хоча

розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту. Аналіз поглядів і концептуальних підходів до формування сучасних ефективних систем інформаційної безпеки підприємства дозволив сформулювати основні функції та завдання і намітити організаційні основи функціонування відповідних підрозділів інформаційної безпеки. У сучасному поданні рольових функцій служби інформаційної безпеки можна виділити чотири напрями:

1) розробка методології та методик аналізу загроз, оцінки рівня інформаційної безпеки підприємства і системи її забезпечення;

2) організація і здійснення конкретних видів діяльності із захисту інформації;

3) експлуатація технічних засобів захисту інформації;

4) аудит і контроль функціонування системи інформаційної безпеки підприємства.

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням.

Технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті. Сьогодні використовується шість основних способів захисту: перешкода, маскування, регламентація, управління, примус, спонукання.

Усі перераховані методи націлені на побудову ефективної технології захисту інформації, при якій виключено витрати через недбалість і успішно відображено різні види загроз. Під перешкодою розуміється спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.

Маскування – способи захисту інформації, що передбачає перетворення даних у форму, не придатну для сприйняття сторонніми особами. Для розшифровки потрібне знання принципу.

Управління – способи захисту інформації, при яких здійснюється управління над всіма компонентами інформаційної системи.

Регламентація – найважливіший метод захисту інформаційних систем, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з даними, що охороняються.

Примус – методи захисту інформації, тісно пов'язані з регламентацією, що припускають введення комплексу заходів, при яких працівники змушені виконувати встановлені правила. Коли використовуються способи впливу на працівників, за яких вони виконують інструкції з етичних і особистісним міркувань, то йдеться про спонукання.

Інформаційні системи повинні використовуватися відповідно до чинного законодавства.

У більшості випадків законодавство відстає від потреб практики, і це створює в суспільстві певну напруженість. Для інформаційних технологій подібне відставання законів, нормативних актів, національних та галузевих стандартів виявляється особливо болючим.

Отже, у сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. Своєю чергою, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити

ефективну систему управління інформаційною безпекою.