ЛЕКЦІЯ 1. Тема. Вступ. Основні завдання захисту інформації. Об’єкти захисту інформації.

План викладу матеріалу теми

1. Вступ.
2. Основні завдання захисту інформації.
3. Об’єкти захисту та їхні властивості.

1. Вступ.

Інформація цінувалася у всі часи. Щоб володіти нею відбувалися вбивства, війни. В наші дні вона має не меншу цінність. Ця цінність може визначатися не тільки кількістю праці витраченої на її створення, але і кількістю прибутку, отриманого від її можливої реалізації.

Проблема захисту інформації: надійне забезпечення її збереження і встановлення статусу використовування - є однією з найважливіших проблем сучасності.

Цілями системи захисту інформації підприємства є:

- запобігання витоку, розкраданню, втраті, спотворенню, підробці інформації;
- запобігання погрозам безпеці особи, підприємства, суспільства, держави;
- запобігання несанкціонованим діям із знищення, модифікації, спотворення, копіювання, блокування інформації;
- запобігання іншим формам незаконного втручання в інформаційні ресурси і системи, забезпечення правового режиму документованої інформації як об'єкту власності;
- захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, наявних в інформаційних системах;
- збереження, конфіденційності документованої інформації відповідно до законодавства.

Причини втрати і пошкодження інформації можуть бути різними. Найчастіше це зараження вірусами. Сьогодні нікого не здивуєш існуванням комп'ютерних вірусів. Якщо звернутися до історії, то можна побачити, що одним з перших був створений вірус, який розповсюджувався по глобальній мережі, був створений в 1988 році. Його написав аспірант факультету інформатики Корнелльського університету Роберт Моррисан. У перебігу декількох годин 2 листопада 1988 року були заражені більше 6000 комп'ютерів.

Подібні програми створюються і зараз. І для розповсюдження, також використовують проломи в системах захисту серверів. Окрім програм, які

займаються псуванням, знищенням даних, псуванням апаратного забезпечення, уповільненням роботи комп'ютера, існують віруси, які стараються нічим не видати своєї присутності, а потихеньку збирають інформацію, наприклад, паролі, ведуть контроль за натисненням клавіш користувача ПЕВМ, а потім передають знайдену інформацію на заздалегідь певну адресу, або здійснюють які-небудь певні дії. Ці віруси відносяться до так званих “троянским коням”.

Основним засобом захисту від вірусів можна вважати використання антивірусів, краще якщо це буде дві незалежні програми, наприклад Dr.Web, AVP. Антивірусні засоби рекомендується встановити на ЄОМ і на поштовому сервері, або змусити сканувати весь трафік, а також правильна політика безпеки, що включає оновлення використовуваних програм і антивірусних засобів, оскільки антивірусні засоби пасивні і не в змозі гарантувати 100 % захист від невідомих вірусів, допоможе уникнути вірусного зараження.

На сьогоднішній день найменш контрольована область – це інформація, що надсилається за допомогою електронної пошти. Цим активно користуються інсайдери і несумлінні працівники, і левова частка конфіденційної або небажаної інформації витікає саме через Інтернет, за допомогою повідомлень електронної пошти. Наприклад, такі системи, як E-NIGMA, Secure, Altell використовують в своїх програмах методи розмежування прав доступу до e-mail повідомлень, за допомогою яких дотримується інформаційна безпека підприємства. Контроль за якістю роботи співробітників є важливим процесом в організації роботи цілого підприємства. Однією з складових цього контролю є моніторинг листування співробітників. Використовуючи одну з програм приведених вище систем можна легко відстежувати листування кожного із співробітників, не вмонтовуючи собі їх ящики, оскільки вона перехоплює всю пошту на рівні протоколу.

Радіовипромінювання монітора. Перехоплення зображення монітора достатньо поширений спосіб розкрадання інформації. Це стає можливим у зв'язку з його паразитним випромінюванням, прийом якого можливий до 50 м. Основним захистом можна вважати екранування приміщення, металевий корпус ПЕВМ, а також використання пристроїв тих, що маскують побічне електромагнітне випромінювання, наприклад, генератор радіошуму ГШ-1000, який зашумляє діапазон частот від 0,1 до 1000 Мгц.

Сьогодні існують пристрої, здатні розкодувати факс-модемную передачу, із запису її на магнітофон, або безпосередньо з телефонної лінії. Заборонити це не можливо, оскільки підключитися до телефонної лінії можна на будь-якій ділянці проходження телефонного з'єднання. Єдиний захист - це не передавати за допомогою подібного устаткування відомостей не бажаних для розголошування.

Забезпечення інформаційної безпеки традиційно розглядається як сукупність чисто оборонних заходів. Характерними прикладами оборонних заходів, використовуваних для захисту комунікаційних мереж, є міжмережеві

екрани, шифрування і системи виявлення вторгнень (Intrusion Detection Systems, IDS). Стратегія будується на класичній парадигмі забезпечення безпеки "захищай, виявляй, виправляй". При такому підході виникає проблема, пов'язана з тим, що ініціатива належить атакуючому, який завжди виявляється на крок попереду. За останні декілька років стає все більш очевидним, що традиційні прийоми мережевого захисту ефективні лише в певних межах. Відповідно необхідні нові методи посилення захисту мереж. Одним з перспективних підходів є використовування приманок - комп'ютерних ресурсів, що знаходяться під постійним спостереженням, які ми дозволяємо випробовувати на міцність, атакувати і зламувати. Точніше кажучи, приманка є "елементом інформаційної системи, цінність якого полягає у тому, що він дозволяє вести моніторинг несанкціонованого або протиправного використовування даного елементу". Моніторинг даних, що поступають на приманку і покидають її, дозволяє зібрати відомості, які не можна добути за допомогою IDS. Приманки можуть працювати під управлінням будь-якої операційної системи і на будь-якій кількості серверів. За допомогою налаштувань задаються доступні супротивнику способи злому або перевірки стійкості системи. Приманки володіють двома додатковими перевагами: масштабованістю і легкістю в обслуговуванні.

Таким чином, на сьогоднішній день пропонується безліч способів забезпечення безпеки інформації, але не всі вони є ефективними. Відомо, що тільки «комплексна система може гарантувати досягнення максимальної ефективності захисту інформації, оскільки системність забезпечує необхідні складові захисту і встановлює між ними логічний і технологічний зв'язок, а комплексність, що вимагає повноти цих складових, всеосяжності захисту, забезпечує її надійність»

Будь-яка інформація, незалежно від того, чи є вона власністю держави, всього суспільства або окремих організацій чи фізичних осіб, становить певну цінність. Відтак інформаційні ресурси потребують захисту від різних впливів, які можуть призвести до зниження їхньої цінності.

Здавна люди розв’язували питання захисту інформації, переважно – державних і військових таємниць. Завдання захисту були досить типовими і не змінювалися протягом тисячоліть – забезпечити передавання інформації від достовірного джерела вповноваженій особі так, щоб вона не потрапила до інших осіб. Для цього використовували різні методи захисту. Деякі з них із незначними змінами застосовують і зараз, коли, наприклад, підтверджують справжність документа особистою печаткою. Були й такі методи, що сьогодні виглядають досить дивними і жорстокими, – відсікання голови посланцю, який передав усне повідомлення, щоб той не міг в подальшому переповісти його будь-кому. Вже тодіпочали винаходити способи таємного записування інформації, щоб лише

уповноважені особи могли зрозуміти зміст надісланих їм повідомлень.

У XX столітті правила роботи з таємною інформацією, способи її зберігання, передавання, а також методи ведення розвідки з метою здобуття такої інформації не уповноваженими (ворожими) особами зазнали суттєвих змін через бурхливий розвиток технічних засобів, що використовували як для захисту інформації, так і для подолання цього захисту. Наприкінці XX століття було здійснено чергову технічну революцію, яка стосувалася саме технологій підготовки, зберігання, пошуку, оброблення та розповсюдження інформації. Йдеться про масове застосування комп'ютерної техніки, що стала загальнодоступною, а також про об'єднання комп'ютерів у мережі, які досягли глобального масштабу. В результаті виникли і набули поширення розподілені інформаційні системи, які дістали назву інформаційно-комунікаційних систем.

Можна було б припустити, що питання захисту цифрової інформації можна вирішувати тими самими методами, що застосовували для захисту традиційних (паперових) носіїв інформації. Певною мірою це дійсно так.

Але є й інший бік проблеми. Комп'ютерна технологія оброблення інформації несе в собі певні загрози, які можуть призвести до небажаних втрат або тимчасової недоступності важливих даних. Зрештою, будь-яка нова технологія приховує небезпеку, яка не завжди очевидна. Можна навести безліч прикладів з історії розвитку техніки, коли під час бурхливого впровадження певної технології питання безпеки спочатку не дуже цікавили людство, а потім ставали пріоритетними (це стосується автомобільного та авіаційного транспорту), а в деяких випадках навіть критичними для його існування (наприклад, атомна енергетика, хімічна промисловість).

У контексті інформаційно-комунікаційних систем слід згадати системи зберігання даних, надійність яких власники інформації інколи переоцінюють. Але є й менш очевидні проблеми. Зокрема, це можливість (на жаль, реалізована на практиці) існування шкідливого і навіть руйнівного програмного забезпечення. Передумовою його існування є унеможливлення або суттєве ускладнення перевірки всіх функції програмного забезпечення. Це означає, що програми можуть містити так звані не документовані функції – приховані функції, реалізовані програмістами та навмисно або через їхню недбалість долучені до програмного продукту і не описані в документації. Такі функції можуть бути активізовані випадково (за збігу обставин, внаслідок помилок чи збоїв) або навмисно (за певних умов). Одним із найпоширеніших і найнебезпечніших різновидів шкідливого програмного забезпечення є комп'ютерні віруси, здатні розмножуватись і розповсюджуватись.

З усього цього можна зробити один важливий висновок – без застосування спеціальних заходів захисту існує дуже висока ймовірність пошкодження

інформації в інформаційно-комунікаційній системі, що може завдати збитків її власнику.

Отже, задачі захисту інформації в інформаційно-комунікаційній системі є суперпозицією задач двох головних напрямів:

- захист важливої інформації, зокрема державної, військової або комерційної таємниці, від цілеспрямованих дій порушників;
- захист інформації від впливів, спричинених некоректним функціонуванням комп'ютерної системи через відмови обладнання, збої програмного забезпечення, помилки в реалізації апаратних або програмних засобів, або наявність програмних засобів з прихованими руйнуючими властивостями.

Захист інформації на підприємстві починається з визначення самої інформації, втрата, порушення цілісності або доступності якої можуть призвести до непередбачених фінансових витрат та завдати моральної чи фізичної шкоди.

Організацією процесу визначення інформації на підприємстві повинен займатися підрозділ, на якого покладено функції з адміністрування процесами управління підприємством, та який має організаційно-розпорядчий вплив на всі структурні підрозділи підприємства (як приклад служба забезпечення діяльності керівника підприємства).

Вихідними даними даного етапу є аналітична інформація про інформаційну систему підприємства, що використовується підрозділом захисту інформації підприємства у подальшому, при створенні комплексної системи захисту інформації.

2. Основні завдання захисту інформації.

Далі зосереджуємо увагу на термінах, безпосередньо пов'язаних із питаннями захисту інформації, при цьому будемо користуватися термінологією згідно з НД ТЗІ 1.1-093-99 [2] та ДСТУ 3396.2-97 «Захист інформації. …» (НД ТЗІ – нормативний документ технічний захист інформації, ДСТУ – державний стандарт України). Зрозуміло, що захист інформації без чіткого визначення завдань захисту не має сенсу.

Наведемо приклад неадекватного застосування заходів щодо захисту інформації. Уявіть собі веб-сайт, який містить загальнодоступну інформацію рекламного характеру. Для доступу на цей сайт користувачі мусять проходити попередню процедуру реєстрації з отриманням персонального пароля, який необхідно змінювати щонайменше щотижня. Під час навігації по сайту користувачі отримуватимуть попередження про реєстрацію всіх їхніх дій. Чи буде такий сайт популярним (адже саме це потрібно його власникам)? Усі ці заходи були б цілком прийнятні та навіть необхідні, якби сайт містив, наприклад, конфіденційну корпоративну інформацію.

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, оброблення, зберігання, пошуку та надання користувачам. Ці технології мають ураховувати особливості інформації, які й роблять її цінною, а також давати змогу користувачам різних категорій працювати з інформаційними ресурсами (створювати, знаходити, копіювати, узагальнювати, порівнювати, модифікувати, перетворювати, знищувати тощо).

Передусім слід усвідомлювати, що не реалізація інформаційно-комунікаційної системи дає можливість користувачам різних категорій звертатися до певних інформаційних ресурсів, а зовнішні чинники, до яких насамперед належать Закони України (або іншої держави, відповідно до того правового поля, в якому функціонуватиме система). З усього цього випливає найважливіше для визначення мети захисту інформації поняття – політика безпеки.

Політика безпеки інформації –це сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок оброблення інформації в ІКС. Таким чином, саме політика безпеки інформації обумовлює вживання тих чи інших заходів захисту, які дають змогу підтримувати безпеку інформації.

Безпека інформації – це стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. Багаторічний досвід захисту інформації в ІКС дозволив визначити головні властивості інформації, збереження яких дає змогу гарантувати збереження цінності інформаційних ресурсів. Це конфіденційність, цілісність і доступність інформації.

Конфіденційність – властивість інформації, завдяки якій лише вповноважені користувачі мають змогу її отримувати (тобто ознайомлюватися з інформацію

Цілісність – властивість інформації, яка дає можливість лише вповноваженим користувачам її модифікувати.

Доступність – властивість інформації, завдяки якій уповноважені користувачі можуть використовувати її згідно з правилами, встановленими політикою безпеки, не очікуючи довше заданого (невеликого) проміжку часу. Тобто інформаційний ресурс має необхідний користувачу вигляд, знаходиться в тому місці, де це потрібно користувачу, і тоді, коли це йому потрібно.

3. Об’єкти захисту та їхні властивості

До цього ми розглядали систему як ціле, хоча й згадували окремі її складові та ресурси. Далі ми розглядатимемо окремі підсистеми і об’єкти

системи, а також їх взаємодію.

Комплекс засобів захисту (КЗЗ) – сукупність програмно-апаратних засобів, що забезпечують реалізацію політики безпеки інформації. Тобто КЗЗ є складовою обчислювальної системи (див. рис.).

Рис. 1.1. Структура автоматизованої системи

КЗЗ може бути локалізованим у системі у вигляді одного чи кількох апаратних і програмних компонентів, а може бути розпорошеним по різноманітних програмних засобах. Безперечно, перший варіант має суттєві переваги, проте другий – також іноді використовують у достатньо надійних, перевірених часом рішеннях (наприклад, саме такий вигляд має архітектура КЗЗ ОС UNIX).

Об'єкт системи – це елемент ресурсів обчислювальної системи, який знаходиться під керуванням КЗЗ і характеризується визначеними атрибутами й поводженням.

Розрізняють такі види об'єктів:

- пасивні об'єкти;
- об'єкти-користувачі;
- об'єкти-процеси.

Об'єкти-користувачі й об'єкти-процеси є активними об'єктами. Активні об'єкти можуть виконувати дії над пасивними об'єктами.

У більшості зарубіжних стандартів, зокрема й у сучасному міжнародному стандарті ISO 15408 [8-10], пасивні об'єкти називають *об'єктами*, а активні об'єкти – *суб'єктами*. Потрібно розуміти, що, як правило, суб'єкт – це об'єкт-процес, який діє від імені певного об'єкта-користувача.

Об'єкт-користувач – це подання фізичного користувача в обчислювальній системі, яке утворюється під час його входження в систему і характеризується своїм контекстом (обліковий запис, псевдонім, ідентифікаційний код, повноваження тощо).

Об'єкт-процес – задача, процес, потік, що виконується в поточний момент (абстракція програми, що виконується) і повністю характеризується своїм контекстом (стан регістрів, адресний простір, повноваження тощо).

З міркувань безпеки інформації в ІКС виняткове значення має спроможність об'єктів взаємодіяти. Для цього використовують поняття доступу.

Доступ – це взаємодія двох об'єктів обчислювальної системи, коли один із них (той, що здійснює доступ) виконує дії над іншим (тим, до якого здійснюється доступ). Результатом такого доступу є змінення стану системи (наприклад, запуск програми на виконання) і (або) утворення інформаційного потоку від одного об'єкта до іншого (наприклад, читання або записування інформації). У випадку, коли утворюється інформаційний потік, кажуть, що здійснюється ***доступ до інформації***. Для забезпечення захисту інформації доступ до об'єктів, які містять інформацію, що підлягає захисту, слід здійснювати з дотриманням визначених правил.

Правила розмежування доступу (ПРД) – складова політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів.

Несанкціонований доступ (НСД) – доступ, який здійснюють з порушенням політики безпеки, тобто з порушенням ПРД. Цей термін є найбільш уживаним, переважно до систем, в яких обробляють таємну інформацію, тому його винесено в назви деяких нормативних документів системи технічного захисту інформації (НД ТЗІ) [2, 11-13]. Разом із тим навіть у цих документах зазначено, що захист інформації не обмежується захистом від НСД.

Щоб можна було реалізувати розмежування доступу, система має розпізнавати об'єкти.

Ідентифікація – процес розпізнавання об'єктів системи за їхніми мітками, або ідентифікаторами.

Ідентифікатор – це унікальний атрибут об'єкта, який дає змогу вирізнити об'єкт з-поміж інших. Ідентифікацією називають процедуру присвоєння ідентифікаторів об'єктам. Стосовно ідентифікації користувачів системи процедура може полягати у введенні унікального ідентифікатора користувача, наприклад його кодового імені. Є також застаріле визначення ідентифікатора як послідовності латинських літер і цифр, яка починається з літери.

Автентифікація – перевірка запропонованого ідентифікатора на відповідність об'єкту, пересвідчення в його справжності. Стосовно автентифікації користувачів системи процедура передбачає введення додаткової інформації, яка дає змогу системі пересвідчитися, що користувач справді є тим, за кого себе видає. Наприклад, у найпростішому і найпоширенішому випадку це введення таємного кодового слова – пароля. Вважається, що якщо користувач знає пароль, то він справді той, за кого себе видає.

Авторизація – це процедура надання користувачу визначених повноважень у системі. У захищених системах авторизації користувача обов'язково передують його ідентифікація й автентифікація. Наприклад, в операційних системах авторизація полягає у створенні програмного середовища, яке дає змогу користувачу виконувати дозволені йому функції, зокрема запускати в системі процеси від свого імені. Іноді ідентифікацію і автентифікацію розглядають як складові процесу авторизації. Також для повідомлення (пасивного об'єкта) авторизацією називають процедуру визначення його джерела (користувача або процесу, тобто активного об'єкта).

Відмова від авторства – це заперечення причетності до створення або передавання якого-небудь документа чи повідомлення.

Відмова від одержання – це заперечення причетності до отримання якого-небудь документа чи повідомлення.

Контрольні запитання

1. Назвіть основні цілі системи захисту інформації підприємства.
2. Перелічіть причини втрати і пошкодження інформації.
3. Задачі захисту інформації в інформаційно-комунікаційній системі є суперпозицією задач двох головних напрямів, перерахуйте їх.
4. Назвіть мету захисту інформації.
5. Дайте визначення поняттю «Політика безпеки інформації».
6. Безпека інформації це?
7. Дайте визначення наступним понятям: «Конфіденційність», «Цілісність», «Доступність».
8. Комплекс засобів захисту це?
9. Дайте визначення поняттю «Об'єкт системи».
10. Які є види об'єктів? Дайте визначення кожного з них.
11. Доступ це? Несанкціонований доступ це?
12. Правила розмежування доступу це?
13. Дайте визначення наступним понятям: «Ідентифікація», «Ідентифікатор».
14. Чим на Вашу думку відрізняється «Ідентифікація» від «Ідентифікатора»?
15. Дайте визначення наступним понятям: «Автентифікація», «Авторизація».
16. Чим на Вашу думку відрізняється «Автентифікація» від «Авторизації».
17. Чим на Вашу думку відрізняється «Відмова від авторства» від «Відмова від одержання»