ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

Факультет цивільного захисту
Кафедра організації та технічного забезпечення
аварійно-рятувальних робіт

ЗАТВЕРДЖУЮ

Начальник кафедри організації
та технічного забезпечення
аварійно-рятувальних робіт,
к.т.н., доцент
Віталій СОБИНА
«___» _____ 2024 р.

КОНСПЕКТ ЛЕКЦІЙ
з дисципліни

«ІНФОРМАЦІЙНА БЕЗПЕКА У СФЕРІ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ»

циклу обов’язкової професійної підготовки за другим (магістерським) рівнем вищої освіти за освітньо-професійною програмою «Управління пожежною безпекою»

Розробник(и):
старший викладач кафедри організації та технічного забезпечення аварійно-рятувальних робіт факультету цивільного захисту, к.ю.н., доцент
Лариса БОРИСОВА

2024 рік

Лекція 1. Забезпечення інформаційної безпеки в системі ДСНС України

План

Вступ

1. Інформаційна безпека: поняття, структура, зміст.
2. Державна таємниця як особливий вид інформації, що захищається.
3. Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій.
4. Організація діяльності підрозділів технічного захисту інформації в системі Державної служби України з надзвичайних ситуацій.

Література

1. Богуш В. М. Інформаційна безпека держави : навч. посіб. / В. М. Богуш, О. К. Юдін. – К. : МК-Прес, 2005. – 432 с.
2. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. –412 с.
3. Лизанчук В. В. Інформаційна безпека України: теорія і практика : підручник / Львів. нац. ун-т ім. Івана Франка, Львів. шк. журналістики. Львів : ЛНУ ім. Івана Франка, 2017. – 725 с.
4. Борисова Л. В. Правові засади захисту інформації : навч. посіб. / Л. В. Борисова, М. Ф. Логвиненко. МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2013. – 212 с.

Вступ

Безпека звичайно пов’язується зі станом нормального функціонування суспільних інститутів та інших форм соціальної діяльності, зі станом захищеності об’єкта (системи) від зовнішніх та внутрішніх негативних впливів, загроз, небезпек тощо. При цьому основними об’єктами, на які направлені заходи із забезпечення безпеки, тобто передусім захисні заходи, є людина і громадянин, суспільство і держава.

1. Поняття інформації

Першу спробу уточнити термін «інформація» зробив у 1921 р. Р. Фішер, який хотів підвести інформацію під імовірність; через сім років Р. Хартлі вводить поняття «логарифмічна міра кількості інформації»; у 1929 р. Л. Сциллард пов’язує інформацію з ентропією. У кінці 1940-х рр. К. Шенон математично обґрунтував поняття кількості інформації як міри зменшення невизначеності, що перевело слово «інформація» в ряд наукових термінів. Теорія інформації, створена К. Шеноном, була першою науковою дисципліною, безпосередньо зв’язаною з переосмисленням феномена інформації.

Ідея про те, що інформацію можна розглядати як щось самостійне, виникла разом з новою наукою – кібернетикою, яка вивчає закономірності управління системами з перероблення інформації (кібернетичними системами), довівши, що інформація має безпосереднє відношення до процесів управління і розвитку, забезпечуючи стійкість і виживання будь-яких систем.

Інформація і є інформація, а не матерія і не енергія. Інформація, за визначенням В. М. Бехтерєва, – «це нематеріальна субстанція, на відміну від речовини або енергії, але від них невід'ємна, як від своїх носіїв» .

Першим сформулював поняття «інформація» математик Н. Вінер: «Інформація – це визначення змісту, отриманого із зовнішнього світу в процесі нашого пристосування до нього і пристосування до нього наших почуттів. Процес отримання та використання інформації є процесом нашого пристосування до випадковостей зовнішнього середовища нашої життєдіяльності в цьому середовищі».

У. Р. Ешбі пов'язує інформацію з різноманітністю, а також з процесами відображення, котрі завжди супроводжують будь-які взаємодії матеріальних систем; це є підґрунтям уважати, що інформація може існувати там, де є різноманіття.

Дж. Хопфілд під «комунікацією» розуміє створенням порядку з безладдя або, збільшення ступені тієї упорядкованості, яка існувала до одержання повідомлення.

Згідно зі ст. 1 Закону України «Про інформацію», під інформацією розуміють «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді».

Інформація є не прямою фізичною дією, а є опосередкованою, тобто відбувається за допомогою сигналів, що припускають у об'єктів наявності хоч би простої системи зворотного зв'язку, яка кодує і декодує сигнали.

2. Інформаційна безпека: поняття, структура, зміст

За останні десятиліття інформація стала настільки потужним фактором розвитку суспільства, який сприяє внутрішньодержавній і світовій інтеграції та реінтеграції.

Актуальність проблеми правового регулювання суспільних відносин у сфері інформаційної безпеки зумовлена підвищенням ролі інформації в усіх сферах і видах діяльності особистості та держави в умовах впливу зовнішніх і внутрішніх загроз, а також розвитком нових інформаційних відносин, котрі вимагають дотримання і захисту прав, законних інтересів суб'єктів в інформаційній сфері.

Національні інтереси України в інформаційній сфері полягають у розвитку сучасних електронних комунікаційних технологій, захисті державних інформаційних ресурсів від несанкціонованого доступу.

Під національним інформаційним простором розуміють усю сукупність інформаційних потоків як національного походження, так і іноземних, що доступні на території держави.

Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання, і розвиток в інтересах громадян, організацій, держави.

Під *інформаційним середовищем* розуміють сферу діяльності суб'єктів, пов'язану із створенням, перетворенням і споживанням інформації.

Інформаційне середовище умовно поділяється на *три основні складові*:

створення і розповсюдження вихідної та похідної інформації;

формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;

споживання інформації;

та дві *забезпечувальні предметні складові*:

створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;

створення і застосування засобів і механізмів інформаційної безпеки.

Із врахуванням складових інформаційного середовища *інформаційна безпека – це стан захищеності потреб особистості, суспільства і держави, при якому забезпечуються їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх загроз.*

Безпека інформаційної сфери – це ужиття комплексних заходів щодо захисту свого інформаційного простору та входження України у світовий інформаційний простір.

Безпека в інформаційній сфері передбачає:

забезпечення інформаційного суверенітету України;

удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері;

активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;

забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Основою *правового регулювання захисту та обмеження доступу до інформації* є:

норми ч. 1 ст. 32 Конституції України, згідно з якими не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини;

норми ч. 2 ст. 34 Конституції України, якими передбачено можливість обмеження свободи інформації на основі закону в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Важливе місце у вирішенні проблеми забезпечення інформаційної безпеки займає *реалізація системи комплексного захисту інформації*, котра є поєднанням у єдине ціле окремих елементів, механізмів, процесів, явищ, заходів і програм захисту інформації, взаємозв'язок яких сприяє реалізації цілей, концептуального підходу до питань тимчасового функціонування і структурної побудови системи інформаційного забезпечення і захисту.

Згідно зі ст. 1 Закону України «Про інформацію» від 2 жовтня 1992 р. № 2657-XII, під *інформацією* розуміють «*будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді*».

Стаття 21 цього Закону визначає режим доступу до інформації як передбачений правовими нормами порядок отримання, використання, поширення і зберігання інформації і поділяє інформацію на відкриту та інформацію з обмеженим доступом.

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну, таємну та службову інформацію.

Конфіденційною інформацією є відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умовах.

До *таємної інформації* належить інформація, що містить відомості, які становлять державну таємницю, а також іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі (службова, військова, комерційна, банківська, лікарська, адвокатська, досудового слідства та дізнання тощо).

2. Державна таємниця як особливий вид інформації, що захищається

VI – середина XVI ст.	Початковий період захисту інформації за часів Київської Русі пов'язаний з потребами князів у захисті інформації. Відомості, що потребували захисту, стосувалися військової справи або питань державної політики: про військо племінного князя, дислокацію війська під час походу, зміст невигідно укладених договорів; розташування, укріплення і забезпечення продовольством та оснащення княжого граду. Передача військової інформації ворогу

	або втеча з поля бою з метою передання інформації (зрада) були державним злочином і теж жорстоко каралися звичаєвим правом1 та законами Київської Русі.
Князювання Володимира та Ярослава Мудрого	За князювання Ярослава Мудрого зібрання грамот і договорів Русі з іншими країнами розміщувалося в Михайлівському приділі Софійського собору. Одним із найбільш відомих сховищ важливих документів на території України був також Києво-Печерський монастир. Зазначений порядок, по суті, можна віднести до перших режимних заходів, які забезпечували охорону важливих документів (відомостей).
Княгиня Ольга	Складаються традиції діловодства, накопичується досвід документування, оброблення і зберігання документів, захисту від підробки. Одним із методів захисту інформації стала криптографія, котра виникла разом із появою писемності, коли для шифрування писемної інформації слов'янські літери почали замінювати грецькими або латинськими. У давньоруській писемності для визначення таємного письма вживали терміни «хвіоть», або «фіоть», та «еффата». Відомі два методи шифрування: перший полягає в переміщенні літер у тексті, що веде до зміни їхнього порядку при написанні; другий метод залишає порядок літер попереднім, але вони замінюються умовними знаками (іншими літерами, цифрами, знаками).
Литовсько-польське панування	З'являється новий вид інформації – державна таємниця, формується нормативна база, що регулює охорону державної таємниці, набуває значення інформація про внутрішньополітичне становище і зовнішню політику. Наприклад, у артикулі 3 розд. 1 Литовського статуту Великого князівства Литовського 1588 р., що діяв на значній території України, за злочини проти маєстату (престолу), за листування з ворогом і повідомлення йому відомостей, котрі могли б завдати шкоди державі, передбачалася страта.
Запорізька січ	У Запорізькій Січі система діловодства була розвиненою: при головній військовій канцелярії та при канцеляріях у паланках існували власні архіви. Є дані, що кількісний склад військової канцелярії Січі у XVIII ст. нараховував 48 чоловік. Важливою посадою військових служителів є посада військового тлумача (драгомана), який, окрім іншомовних перекладів документів та переговорів з іноземцями, очолював розвідку та контррозвідку Січі та для виконання цих обов'язків виїздив сам або направляв розвідників у сусідні держави, входив до складу посольств, що відряджалися із Січі до іноземних країн. Гетьман шляхом дезінформації застосовував принципи ведення «психологічної війни», що започаткувало процес становлення в Україні служби внутрішньої безпеки, створено елементи контролю з боку уряду за діяльністю дипломатів.
Гетьман П. Орлик	Шифрував свої листи до короля Швеції, представників інших країн, а також до Запорізького Війська. У листуванні П. Орлика застосовувалася передова для початку XVIII ст. технологія шифрування – для зашифрування числових даних використовувалися кодові позначення цифр і чисел.
Середина XVII ст.	На українських землях у складі російської імперії увага приділяється захисту інформації, що регламентується правовими

	джерелами, у яких закріплюється кримінальна відповідальність за розголошення державної таємниці (Соборне уложення 1649 р., Генеральний регламент (Статут державних колегій) 1720 р., Права, за якими судиться малоросійський народ 1722 р., Уложення про покарання кримінальні і виправні 1743 р., Кримінальне уложення 1845 р., Закон Російської імперії «Про зміну чинних законів про державну зраду шляхом шпигунства» 1912 р.).
Друга половина XVIII ст.	Розробкою та розкриттям шифрів займався один із підрозділів Секретної експедиції Колегії іноземних справ. у 1802 р. було організовано Міністерство внутрішніх справ з особливою канцелярією, яка займалася політичними справами. 28 січня 1811 р. було видано «Загальне заснування міністерств» – законодавчий акт, який визначав усю систему міністерського устрою, включаючи діловодство.
XX ст.	Прийняті: «Перелік відомостей, які становлять таємницю і не підлягають поширенню» (1921 р.); Постанова «Про порядок збереження і руху секретних документів» (1922); Інструкція з ведення секретного і шифрувального діловодства, Інструкція про порядок підготовки і конвертування кореспонденції, яка надсилається дипломатичною поштою у 1928 р. – Інструкція із секретного діловодства та Інструкція із шифрувального діловодства.
1924-1925 р.р.	Органам Державного політичного управління УРСР ввірявся контроль за додержанням режиму таємності та веденням шифрувальної справи.
1926 р.	Перелік відомостей, що є за своїм змістом спеціально охоронюваною державною таємницею, у якому всі відомості були розділені на три групи: відомості військового характеру, відомості економічного характеру і відомості іншого характеру, а також введені три категорії таємності: «Цілком таємно», «Таємно», «Не підлягає оголошенню».
1940 р.	Інструкцію з ведення секретних і мобілізаційних робіт і діловодства в установах і на підприємствах, метою якої було посилення режиму секретності, вироблення єдиної системи секретного діловодства та забезпечення охорони секретної інформації в установах і на підприємствах СРСР та УРСР.
40-80 р.р. XX ст.	Про встановлення переліку відомостей, що складають державну таємницю, розголошення яких карається законом» (1947 р.), «Про відповідальність за розголошення державної таємниці й за втрату документів, що містять державну таємницю» (1947 р.), Інструкція із забезпечення охорони державної таємниці в установах і на підприємствах СРСР у якій визначено допуск осіб до документів та інформації «Особливої важливості», «Цілком таємної», «Таємної», чітко визначено ступінь таємності (1954 р.).

Закон «Про державну таємницю» від 21 січня 1994 р., № 3855-XII, який регулює суспільні відносини, пов'язані з віднесенням певних відомостей до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці в інтересах національної безпеки України, уперше визначив основні поняття у сфері захисту інформації.

Державна таємниця (секретна інформація) – вид таємної інформації, що охоплює відповідні відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визначені в порядку, встановленому цим законом, державною таємницею і підлягають охороні державою.

Охорона державної таємниці – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

Режим секретності – встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці.

Ступінь секретності («Особливої важливості», «Цілком таємно», «Таємно») – категорія, що характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

Технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Строк дії режиму таємності залежить від ступеня таємності інформації. Згідно зі ст. 13 Закону «Про державну таємницю», строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України.

Технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Строк дії режиму таємності залежить від ступеня таємності інформації. Згідно зі ст. 13 Закону «Про державну таємницю», строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються СБ України.

Інформація, що може бути віднесена до державної таємниці, визначається відповідно до норм ст. 8 Закону «Про державну таємницю» і викладена у Зводі відомостей, що становлять державну таємницю України (ЗВДТ), який «є єдиною формою реєстрації цих відомостей в Україні. З моменту опублікування ЗВДТ держава забезпечує захист і в правову охорону відомостей, які зареєстровані в ньому».

Звід відомостей є систематизованим переліком відомостей, що становлять державну таємницю, котрі упорядковані за чотирма великими групами (статті) відповідно до сфери державної діяльності:

сфера оборони;

сфера економіки, науки і техніки;

сфера зовнішніх відносин;

сфера державної безпеки і охорони правопорядку.

Відомості, що належать до цих груп, класифікуються на окремі пункти та підпункти за основними характеристиками:

зміст відомостей, які становлять державну таємницю;

ступінь секретності («Особливої важливості», «Цілком таємно», «Таємно»);

строк дії рішення про віднесення інформації (30 років, 10 років, 5 років).

Реєстрація відомостей у Зводі є підставою для надання документу, виробу чи іншому матеріальному носію інформації, що містить ці відомості, грифа секретності, який відповідає ступеню секретності, встановленому для них у Зводі. Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю.

Перелік відомостей, котрі становлять державну таємницю, у рамках визначених Законом «Про державну таємницю» і Зводу чотирьох основних сфер умовно класифікуються за напрямками та видами інформації.

Відомості щодо цивільного захисту, що становлять державну таємницю, відносяться до сфери оборони (пп. 1.4.2, 1.12.1 – 1.12.3).*

*Про затвердження Зводу відомостей, що становлять державну таємницю: наказ Служби безпеки України від 23. 12. 2020 р. № 383.

Основним нормативно-правовим актом, на основі якого здійснюється регулювання питань службової інформації, є:

*Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформаці*ю, затверджена постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893. Згідно з цією Інструкцією переліки відомостей, які містять службову (конфіденційну) інформацію, що є власністю держави;

Наказ від 13 вересня 2013 р. № 600 у Державній службі України з надзвичайних ситуацій затверджено і введено в дію Перелік відомостей, що становлять службову інформацію у ДСНС, якій надається гриф обмеженого доступу «Для службового користування».

У зв’язку з рішенням Ради національної безпеки і оборони України Указом Президента України від 28.12.2021 р. № 685/20211 затверджено *Стратегію інформаційної безпеки України* (Указ Президента України), в якій зазначено, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави.

Відповідно до Закону України «Про Національну програму інформатизації» Національна програма інформатизації формується з урахуванням світових напрямів розвитку та досягнень у сфері інформатизації і спрямована на розв’язання найважливіших загальносуспільних проблем та створення умов для інтеграції України у світовий інформаційний простір відповідно до сучасних тенденцій інформаційної геополітики.

Таблиця 1

Напрям	Система заходів
Інформатизація в галузі екології та використання природних ресурсів	Створення на основі картографічних баз даних багатоцільової інформаційно-технологічної бази з використанням геоінформаційних технологій збирання, зберігання, аналізу всієї сукупності відомостей для моделювання і подальшого прогнозування екологічного стану територій, створення комплексу програмно-апаратних засобів для вирішення питань прогнозування забруднення навколишнього середовища, аналізу та оцінки ризику еколого-економічних конфліктів, прогнозування наслідків техногенного впливу і природних катастроф для надійного захисту екологічного простору України, раціонального використання природних ресурсів на основі підвищення узгодженості управління різними видами виробничої діяльності

3. Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій

Найбільш уразливими об'єктами забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій є система прийняття рішень з оперативних дій (реакцій), пов'язаним із розвитком таких ситуацій і ходом ліквідації їхніх наслідків, а також система збору й обробки інформації про можливе виникнення надзвичайних ситуацій.

Широке використання систем ПЕОМ і розробка різного плану інформаційних систем підвищують ефективність прийняття групових рішень, алгоритмічні та програмні засоби яких є елементами моделювання деревовидних структур рішень аналізу ризику, прогнозування, містять засоби зв'язку та системи управляння даними із загальним та індивідуальним доступом, стандартні засоби аналізу даних і управління інформацією.

Основою функціонування систем інформаційної підтримки прийняття колективних рішень (за міжнародною термінологією – brain storm – мозковий штурм) є застосування інтерактивної обчислювальної мережі та відповідних методів аналізу, що використовуються для отримання інформації та опрацюванні різних аспектів і шляхів вирішення поставленої проблеми.

Особливе значення для нормального функціонування зазначених об'єктів має *забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах*.

Приховування, затримка надходження, перекручування та руйнування оперативної інформації, несанкціонований доступ до неї окремих осіб чи груп осіб можуть призвести як до людських жертв, так і до виникнення різних утруднень при ліквідації наслідків надзвичайної ситуації, пов'язаних з особливостями інформаційного впливу в екстремальних умовах швидкого виникнення та поширення серед людей паніки та помилкової чи недостовірної інформації.

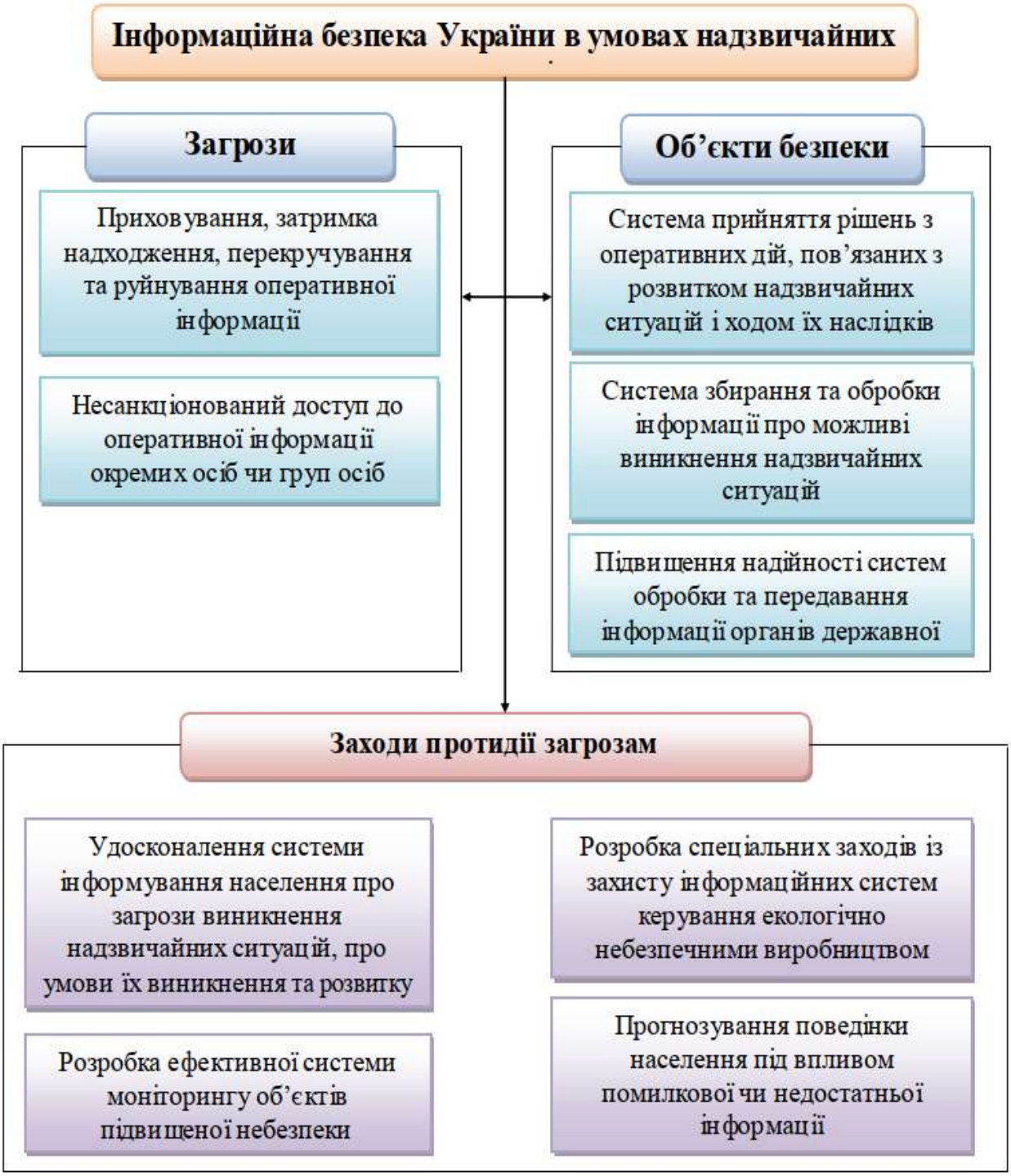

Рис. 1 – Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій

До специфічних для даних умов напрямів забезпечення інформаційної безпеки належать:

розробка ефективної системи моніторингу об'єктів підвищеної небезпеки, порушення функціонування яких може призвести до виникнення надзвичайних ситуацій, і прогнозування надзвичайних ситуацій;

удосконалення системи інформування населення про загрози виникнення

надзвичайних ситуацій, про умови їхнього виникнення і розвитку;

підвищення надійності систем обробки та передачі інформації, які забезпечують діяльність органів державної виконавчої влади; прогнозування поведінки населення під впливом помилкової чи недостовірної інформації про можливі надзвичайні ситуації і розробка заходів щодо надання допомоги великим масам людей в умовах таких ситуацій;

розробка спеціальних заходів із захисту інформаційних систем, які забезпечують керування екологічно небезпечними й економічно важливими виробництвами.

4. Організація діяльності підрозділів технічного захисту інформації в системі Державної служби України з надзвичайних ситуацій

Порядок організації діяльності підрозділів технічного захисту інформації в системі ДСНС України відповідно до наказу Міністерства України з надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи «Про організаційні засади діяльності підрозділів технічного захисту інформації у структурі МНС» від 5 листоп. 2010 р. № 977 визначає правові та організаційні засади діяльності підрозділів ДСНС, яким надано повноваження на проведення відповідних видів робіт з технічного захисту інформації в урядових органах державного управління, територіальних органах управління ДСНС, підприємствах, установах та організаціях, що належать до сфери управління ДСНС.

У затвердженому Порядку організації діяльності підрозділів технічного захисту інформації у системі ДСНС наведено посилання на такі нормативні документи:

1. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 р. № 1229/99 (1229/99) .

2. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

3. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб, затверджене наказом ДСТСЗІ СБ України від 23.02.2002 № 9 (z0245-02) , зареєстроване у Міністерстві юстиції України 13 березня 2002 р. за № 245/6533.

4. Положення про державну експертизу в сфері ТЗІ, затверджене наказом Держспецзв’язку України від 16.05.2007 № 93 (z0820-07) , зареєстроване у Міністерстві юстиції України 16 липня 2007 р. за N 820/14087.

5. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

6. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.

7. НД ТЗІ 3.3-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

8. НД ТЗІ 2.1-002-07. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ.

9. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

10. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

11. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

12. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

13. Типовий порядок створення комплексних систем захисту інформації в автоматизованих системах класу 1 у структурі МНС України, погоджений з Держспецзв’язку 22.05.2007 і затверджений наказом МНС від 08.08.2007 № 539дск.

Розв’язання завдань із захисту населення і територій від надзвичайних ситуацій неможливе без сучасної системи зв’язку, оповіщення та інформатизації ДСНС.

Розпорядження Кабінету міністрів України «Про затвердження Комплексної програми розвитку системи зв’язку, оповіщення та інформатизації МНС на 2004-2010 роки» від 4 березня 2004 р. № 109-р визначає *основні завдання із захисту інформації*:

утворення підрозділів технічного захисту інформації (в тому числі в автоматизованих системах), регіональних лабораторій спеціальних досліджень, отримання у встановленому порядку ліцензій на виконання робіт у сфері криптографічного і технічного захисту інформації;

забезпечення територіальних органів, підрозділів сил ДСНС спеціальною апаратурою, обладнанням і технічними засобами захисту;

упровадження засобів захисту інформації з обмеженим доступом від просочення технічними каналами, програмних засобів антивірусного захисту в автоматизованих системах, програмно-апаратних засобів захисту від несанкціонованого доступу в автоматизованих системах, програмно-апаратних засобів криптографічного захисту в телекомунікаційних мережах;

використання можливостей Національної системи конфіденційного зв’язку;

проведення атестації комплексів технічного захисту інформації на об’єктах інформаційної діяльності;

проектування комплексних систем захисту інформації в автоматизованих системах усіх рівнів;

забезпечення захисту автоматизованих робочих місць, транспортних

мереж передачі даних локальних обчислювальних мереж; впровадження програмно-апаратних засобів криптографічного захисту інформації в локальних обчислювальних мережах усіх рівнів;

створення захищених систем електронного документообігу;

проведення тестування комплексних систем захисту інформації з метою виявлення їх вразливості;

проведення державної експертизи комплексних систем захисту інформації в автоматизованих системах.

Законом України «Про державну службу спеціального зв'язку і захисту

інформації України» від 23 лютого 2006 р. № 3475-IV у ст. 3 визначені основні задачі серед яких забезпечення у встановленому порядку урядовим зв'язком у мирний час, в умовах надзвичайного і воєнного положення, а також у випадках виникнення надзвичайних ситуацій.

Згідно з наказом адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Положення про державний контроль за станом технічного захисту інформації» від 16 травня 2007 р. № 87, визначаються порядок організації та здійснення державного контролю за станом технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Організаційно-технічні принципи, порядок здійснення заходів із технічного захисту інформації, порядок контролю в цій сфері, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, порядок атестації та експертизи комплексів технічного захисту інформації визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами.

Захист інформації від несанкціонованого доступу, а також криптографічний захист під час її передачі каналами системи зв'язку ДСНС здійснюється комплексно з урахуванням як новітніх технологій у телекомунікаційних системах, так і засобів (систем) несанкціонованого отримання інформації, її спотворення або знищення.

Комплексні системи захисту інформації на об'єктах інформаційної діяльності від витоку технічними каналами створюються власними силами та із залученням організацій, що мають відповідні ліцензії (дозволи).

Типове положення, про підрозділ, який виконує роботи з технічного захисту інформації в системі ДСНС визначає, що підрозділ технічного захисту інформації (підрозділ ТЗІ) є структурним підрозділом урядового органу державного управління, територіального органу управління ДСНС, а також підприємства, установи та організації, що належить до сфери управління ДСНС.

До *об'єктів ТЗІ* належить інформація, вимога щодо захисту якої встановлена законом. До об'єктів захисту в телекомунікаційних системах та інформаційних технологіях відноситься програмне забезпечення, що призначене для обробки цієї інформації.

До *об'єктів захисту в електронних комунікаційних системах та*

інформаційних технологіях відноситься програмне забезпечення, що призначене для обробки цієї інформації.

Організаційно-технічні принципи, порядок здійснення заходів щодо ТЗІ, порядок контролю у цій сфері, характеристики загроз для інформації, норми та вимоги з ТЗІ визначаються нормативно-правовими актами з питань ТЗІ.

Підрозділ ТЗІ – підрозділ Установи, призначений для виконання робіт з технічного захисту інформації у системі ДСНС відповідно до повноважень, наданих Міністерством згідно з Дозволом на проведення робіт з технічного захисту інформації для власних потреб.

Види робіт з ТЗІ, які можуть виконуватися підрозділами ТЗІ:

1. Розроблення, впровадження, випробування, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля.

2. Розроблення, впровадження, випробування, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали.

3. Розроблення, впровадження, випробування, супроводження комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу.

4. Виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об’єктах інформаційної діяльності.

Дія Положення про технічний захист інформації у Державній службі України з надзвичайних ситуацій не поширюється на системи і засоби, що базуються на криптографічних методах захисту інформації.

Організація заходів протидії технічним розвідкам у ДСНС України регламентується нормативними документами Державної служби спеціального зв’язку та захисту інформації України. Комплекси системи захисту інформації на об’єктах інформаційної діяльності від витоку технічними каналами створюються власними силами та із залученням організацій, що мають відповідні ліцензії (дозволи).

Під час розроблення і впровадження заходів з ТЗІ використовуються засоби, дозволені Державною службою спеціального зв’язку та захисту інформації України для застосування та включені до відповідних переліків.

Підрозділи ТЗІ органів та підрозділи ДСНС здійснюють організацію, методичне забезпечення та контроль за впровадженням в органах та підрозділах ДСНС заходів ТЗІ. Типове положення, про *підрозділ, який виконує роботи з технічного захисту інформації в системі ДСНС* визначає, що підрозділ технічного захисту інформації (підрозділ ТЗІ) є структурним підрозділом урядового органу державного управління, територіального органу управління ДСНС, а також підприємства, установи та організації, що належить до сфери управління ДСНС.

Напрями розвитку ТЗІ обумовлюються необхідністю своєчасного вжиття заходів, адекватних масштабам загроз для інформації, і ґрунтуються на засадах правової демократичної держави відповідно до прав суб’єктів інформаційних

відносин на доступ до інформації та її захист. Розв'язання завдань із захисту населення і територій від надзвичайних ситуацій неможливе без сучасної системи зв'язку, оповіщення та інформатизації ДСНС:

стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;

систем управляння об'єктами критичної інфраструктури;

розробку та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав – членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність.

Лекція 2. Загрози інформаційній безпеці

План

Вступ

1. Основні характеристики інформаційної системи як об'єкта захисту.
2. Класифікація загроз інформаційній безпеці.
3. Ієрархічна класифікація загроз інформаційній безпеці.
4. Джерела загроз інформаційній безпеці.

Література

1. Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 5 лип. 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.
2. Про науково-технічну інформацію: закон України від 25 черв. 1993 р. № 3322-XII // Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345.
3. Захист інформації: навч. посіб. / О. В. Глоба, С. В. Білецький, А. А. Чубар. – Київ: НАУ, 2016. – 184 с.
4. Гончарова Л. Л., Возненко А. Д., Стасюк О. І., Коваль Ю. О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. Київ, 2013. – 435 с.
5. Мехед Д. Б., Базилевич В. М., Ткач Ю. М., Петренко Т. А. Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11. Захист інформації. Київ, 2015. Т. 17, № 4. С. 274-278.

Вступ

Основними об'єктами забезпечення інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах є:

інформаційні ресурси, що містять державну таємницю, та іншу інформацію обмеженого доступу;

засоби та системи інформатизації (засоби обчислювальної техніки, інформаційно-обчислювальні комплекси, мережі та системи), програмні засоби (операційні системи, системи керування базами даних, інше загальносистемне та прикладне програмне забезпечення), автоматизовані системи керування, системи зв'язку та передачі даних, що здійснюють приймання, обробку, зберігання та передачу інформації обмеженого доступу, їхні інформативні фізичні поля;

технічні засоби та системи, що обробляють відкриту інформацію, але розміщені в приміщеннях, де обробляється інформація обмеженого доступу;

приміщення, призначені для проведення закритих переговорів, під час яких озвучується інформація обмеженого доступу.

1. Основні характеристики інформаційної системи як об'єкта захисту

Для інформаційних систем як об'єктів безпеки властиві наступні такі характеристики як конфіденційність, доступність та цілісність інформації (даних) в інформаційній системі.

Конфіденційність інформації (даних) в інформаційній системі – це властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом інформаційної системи. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Доступність у загальному смислі представляється як можливість проникнення куди-небудь. Для інформаційної системи – це властивість ресурсу системи, яка полягає в тому, що користувач і (або) процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, і в той час, коли він йому необхідний.

Доступність даних в інформаційній системі – це властивість даних, що полягає у можливості їхнього читання користувачем або програмою. Визначається рядом факторів: можливістю працювати за терміналом, володінням паролем, знанням мови запитів і т.ін.

Цілісність – це внутрішня єдність, зв'язаність усіх частин чого-небудь, єдине ціле. В інформаційній системі – це стан даних або інформаційної системи системи, в якій дані та програми використовуються встановленим чином, що забезпечує:

стійку роботу системи;

автоматичне відновлення у випадку виявлення системою потенційної помилки;

автоматичне використання альтернативних компонентів замість тих, що

вийшли з ладу.

Забезпечення безпеки інформації повинно носити комплексний характер, засновуватися на всебічному аналізі можливих негативних наслідків і при якому важливо не упустити будь-які суттєві аспекти. Виникає наступний ланцюжок: *джерело загрози – фактор (уразливість) загроза (дія) – наслідки (атака)*.

2. Класифікація загроз інформаційній безпеці

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері.

Загрози інформаційній безпеці реалізуються через порушення інфраструктури, вільного обігу інформації, неправомірні дії щодо інформації, через невідповідність інформаційної політики, засобів інформування громадськості. Відповідно до критичних сфер міжнародного співробітництва класифікуються *загрози для інформаційної безпеки*. Існують різні типології загроз, але, узагальнюючи, можна виділити такі види загроз:

інформаційно-технологічні;

інформаційно-комунікаційні;

інформаційно-психологічні.

Загрози інформаційній безпеці України можна розділити на три групи:

загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);

загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і майнову власність на документовану інформацію; праву на особисту таємницю;

праву на захист честі і достоїнства і т.ін.).

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні.

Під основними *політичними факторами загроз інформаційній безпеці* розуміють:

зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;

інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів з метою здобуття односторонніх переваг;

становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;

порушення інформаційних зв'язків унаслідок утворення на території колишнього СРСР нових держав.

Економічними факторами загроз безпеці інформації є:

перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур – виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;

критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;

розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними *організаційно-технічними факторами загроз інформаційній безпеці* є:

недостатньо узгоджена нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;

недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;

зростання обсягів інформації, яка передається відкритими каналами зв'язку;

загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

3. Ієрархічна класифікація загроз інформаційній безпеці

Глобальні фактори загроз інформаційній безпеці:

недружня політика іноземних держав у галузі глобального інформаційного моніторингу;

діяльність іноземних розвідувальних та спеціальних служб;

діяльність іноземних політичних та економічних структур, спрямована проти інтересів держави;

злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці:

невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами;

недопустимо високий рівень технологічної залежності держави від зарубіжних держав у зв'язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій;

розвиток зарубіжних технічних засобів розвідки та промислового шпіонажу для одержання несанкціонованого доступу до конфіденційної

інформації, у тому числі такої що складає державну таємницю;

зростання злочинності в інформаційній сфері;

широке розповсюдження комп'ютерних вірусів, призначених для ураження систем управління та зв'язку;

відсутність ефективної системи забезпечення цілісності інформації, у тому числі такої, що є інтелектуальною власністю.

Локальні фактори загроз інформаційній безпеці:

перехоплення електронних випромінювань;

застосування підслуховуючих пристроїв або закладок;

дистанційне фотографування;

розкрадання носіїв інформації та промислових відходів;

копіювання носіїв інформації з подоланням заходів захисту; – незаконне приєднання до апаратури та ліній зв'язку;

упровадження та використання комп'ютерних вірусів тощо.

4. Джерела загроз інформаційній безпеці

Джерело загрози **–** це потенційні антропогенні, техногенні або стихійні носії загрози безпеці.

Загроза (дія) – це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), яке наносить збиток власнику або користувачу, що проявляється як небезпека спотворення або втрати інформації.

Фактор (уразливість) – це властиві об'єкту інформатизації причини, які призводять до порушення безпеки інформації на конкретному об'єкті та зумовлені вадами

Атака – це завжди пара «джерело-фактор», що реалізує загрозу та приводить до збитків.

Виділяють три основні види загроз безпеці інформації: загрози безпеці інформації при забезпеченні конфіденційності, доступності та цілісності.

Загрози безпеці інформації при забезпеченні конфіденційності:

крадіжка (копіювання) інформації та засобів її оброблення;

втрата (ненавмисна втрата, витік) інформації та засобів її оброблення.

Загрози безпеці інформації при забезпеченні доступності:

блокування інформації;

знищення інформації та засобів її оброблення.

Загрози безпеці інформації при забезпеченні цілісності:

модифікація (спотворення) інформації;

заперечення автентичності інформації;

нав'язування фальшивої інформації.

Ранжування джерел загроз безпеці інформації

Носіями загроз безпеці інформації є джерела загроз.

Джерелами загроз можуть бути як суб'єкти (особистість), так і об'єктивні прояви. Джерела загроз можуть знаходитися як усередині організації – внутрішні джерела, так і ззовні її – зовнішні джерела. Поділ джерел на суб'єктивні та об'єктивні виходить з міркувань стосовно вини або ризику збитку інформації.

Усі джерела загроз безпеці інформації діляться на три групи: – обумовлені діями суб'єкта (антропогенні джерела загроз);

обумовлені технічними засобами (*техногенні джерела загроз*);

обумовлені стихійними джерелами.

Антропогенним джерелом загроз можна вважати суб'єкта, який має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта, що підлягає захисту.

Антропогенними джерелами загроз виступають суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини. Ця група джерел загроз найбільш численна та представляє найбільший інтерес із точки зору організації захисту, так як дії суб'єкта завжди можна оцінити, спрогнозувати та прийняти адекватні заходи. Методи протидії у цьому випадку керовані й залежать від волі організаторів захисту інформації. Суб'єкти, дії яких можуть привести до порушення безпеки інформації, можуть бути як внутрішніми, так і зовнішніми.

Внутрішні джерела (суб'єкти) це – висококваліфіковані спеціалісти у галузі розробки та експлуатації програмного забезпечення та технічних засобів, знайомі зі специфікою завдань, що вирішуються, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного обладнання та технічних засобів мережі.

Кваліфікація антропогенних джерел загроз безпеці інформації відіграє важливу роль для оцінки їхнього впливу та враховується при ранжируванні джерел загроз.

Зовнішні джерела можуть бути випадковими або навмисними та мати різний рівень кваліфікації.

Друга група містить джерела загроз, що визначаються технократичною діяльністю людини, є особливо актуальною в сучасних умовах, очікується різке зростання числа техногенних катастроф, викликаних фізичним та моральним старінням існуючого обладнання.

Технічні засоби, що є джерелами потенційних загроз безпеці інформації, можуть бути зовнішніми та внутрішніми.

Третя група джерел загроз об'єднує обставини, що складають непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер, що розповсюджується на всіх.

До непереборної сили в законодавстві та договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або їм запобігти або можливо передбачити, але не можливо запобігти їм при сучасному рівні знань і можливостей людини. Стихійні джерела потенційних загроз (природні катаклізми) інформаційній безпеці є зовнішніми по

відношенню до об'єкта захисту.

Усі джерела загроз мають різну міру небезпеки, яку можна оцінити, якщо провести їхнє ранжирування. При цьому, оцінка міри небезпеки здійснюється за непрямими показниками.

Критеріями порівняння (показників) може бути:

можливість виникнення джерела, визначаючи міру доступності до можливості використати фактор (уразливість) (для антропогенних джерел), віддаленість від фактора (уразливості) (для техногенних джерел) або особливості обстановки (для випадкових джерел);

готовність джерела, що визначає міру кваліфікації та привабливість здійснення діяння зі сторони джерела загрози (для антропогенних джерел) або наявність необхідних умов (для техногенних та стихійних джерел).

фатальність визначає міру непереборності наслідків реалізації загрози.

Кожний показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Причому, 1 відповідає мінімальній мірі впливу показника, який оцінюється на небезпеку використання джерела, а 5 – максимальній.

Результати ранжирування відносно конкретного об'єкта захисту зводяться в таблицю, яка дозволяє визначити найбільш небезпечні для даного об'єкта джерела загроз безпеці інформації.

Лекція 3. Захист інформації як інтегральна проблема та шляхи її вирішення

План

Вступ
1. Умови безпеки інформації.
2. Державна політика і система ТЗІ в Україні.
3. Нормативно-правова база України в сфер ТЗІ.
4. Кіберзахист та організація протидії кіберзагрозам.
5. Структура системи захисту інформації.

Література

1. Рибальський О. В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації: посібник для курсантів ВНЗ МВС України. Київ: Вид-во Національної академії внутрішніх справ, 2012. 104 с.
2. Державна служба спеціального зв'язку та захисту інформації України. URL: www.dsszzi.gov.ua/.
3. Перелік нормативно-методичних документів в галузі захисту інформації. URL: nics.com.ua/ images/price/price09_10.doc.

1. Ланде, Д. В., Субач, І. Ю., Бояринова, Ю. Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки. – К. : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. 300 с.
2. Захист інформації: навч. посіб. / О. В. Глоба, С. В. Білецький, А. А. Чубар. – Київ: НАУ, 2016. 184 с.
3. Браіловський, М. М., Зибін, С. В., Пискун, І. В. та ін. Технології захисту інформації. – К: ЦП «Компринт», 2021. 296 с.

Вступ

Організація захисту інформації забезпечується правовими, організаційними і інженерно-технічними заходами. Організаційні інженерно-технічні заходи складають зміст технічного захисту інформації. Правові заходи інформації є базисом, на який спирається організаційні та інженерно-технічні заходи по захисту інформації.

1. Умови безпеки інформації

Інформація – це зафіксоване на носію уявлення про предмети, процеси, явища та інше.

Під фіксацією розуміється закріплення будь-чого у визначеному положенні або вигляді. Інформація для свого існування завжди потребує наявність носія.

В якості носія інформації може виступати: поле, речовина, людина.

У процесі інформаційних відносин носії можуть бути носіями-джерелами (джерелами) або носіями-утримувачами (утримувачі) в залежності від напрямку переміщення інформації.

Закон України «Про інформацію» під джерелом інформації визначає передбачені чи установлені законом носії інформації: документи чи інші носії інформації, які представляють собою матеріальні об’єкти, які зберігають інформацію.

У загальному випадку утримувачі сприймають інформацію через сенсор (датчик, вимірювальний перетворювач). Процес сприйняття інформації складається із отримання і перетворення інформації, забезпечуючи відображення об’єктивної реальності і орієнтировку в навколишньому світі.

Сприйняття може включати в себе:

знаходження об’єкта в полі сприйняття;

відмежування окремих ознак в об’єкті;

виділення в ньому інформативного змісту, адекватної мети дії;

формування образу сприйняття.

Інформація володіє деякими суттєвими з точки зору її захисту властивостями:

конфіденційність – властивість інформації бути захищеною від

несанкціонованого ознайомлення;

цілісність – властивість інформації бути захищеною від несанкціонованого викривлення, роз рушення або знищення;

доступність – властивості інформації бути захищеною від несанкціонованого блокування.

Отже, *технічний захист інформації – це діяльність, направлена на забезпечення організаційні і інженерно-технічні заходи конфіденційності, цілісності, доступності інформації, яка визначена власником або уповноваженою особою як об'єкт захисту.*

Подія, яка потенційно може порушити одну із властивостей інформації називають *загрозами* порушення конфіденційності, цілісності та доступності інформації.

До *таємної* (особливо важлива – ОВ, цілком таємна – ЦТ, таємна – Т) відноситься інформація, що містить відомості, які складають державну або іншу, передбачену законом таємницю, розголошення якої наносить шкоду суспільству(державі).

Конфіденційна інформація – це відомості, які знаходяться у власності, використанні чи розпорядженні окремих фізичних чи юридичних осіб і розповсюдження за їхнім бажанням у відповідності з передбаченими ними умовами.

Таємна і конфіденційна інформація підлягають захисту від загрози порушення конфіденційності, цілісності і доступності, а відкрита інформація, яка важлива для особи, суспільства і держави – захист від загрози порушення цілісності і доступності.

Інформація вважається захищеною, якщо при переміщенні інформації зберігається режимна адекватність та комунікабельність носіїв інформації.

Порушення інформаційної безпеки можливе лише при переміщення інформації.

У процесі переміщення може проходити заміна її носія. Носіями інформації при її переміщення може бути:

матеріальне середовище (повітря, вода, метал, і др.);

сенсори або датчики;

перетворювачі і інші об'єкти живої і не живої природи, які несуть функцію проміжних носіїв інформації.

Режимна адекватність носіїв – це відповідність режимів доступу носіїв інформації (джерела дотримувача) при їх взаємодії.

Загрози цілісності інформації направлені на заборону режимом доступу (порядок отримання, використання, розповсюдження і зберігання) її зміни або викривлення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена умисно, а також в результаті об'єктивних дій зі сторони середовища, яке окружає носія інформації.

Інформація зберігає доступність, якщо зберігається комунікабельність носіїв інформації при їх взаємодії.

2. Державна політика і система ТЗІ в Україні

Нормативними документами в сфері ТЗІ визначенні основні загрози безпеки інформації в Україні:

діяльність інших держав, направлена на отримання переваги в внутрішньополітичній, економічній, воєнній і інших сферах;

недосконаліть організації в Україні міжнародних виставок апаратури різного призначення (особливо рухомих) і заходів екологічного моніторингу, які можуть використовуватися для отримання інформації розвідувального характеру;

діяльність політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, направлена на отримання переваги в політичній боротьбі і конкуренції;

злочинна діяльність, направлена на протизаконне отримання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним або фізичним особам;

використання інформаційної системи низького рівня, які приводять до залучення небездоганних технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ і засобів ТЗІ;

недостатність документації на засоби забезпечення ТЗІ іноземного виробництва, а також кваліфікація технічного персоналу.

Система ТЗІ визначається як:

суб'єктами, об'єднаних цілями і задачами інформації організаційними і інженерно-технічними заходами;

нормативно-правової бази;

матеріально-технічної бази.

Державна політика у сфері ТЗІ формується з урахуванням таких принципів:

дотримання балансу інтересів особистості, суспільства і держави, їх взаємна відповідальність;

єдині підходи до забезпечення ТЗІ, які визначаються загрозами безпеки інформації і режимів доступу до неї;

комплектність, повнота та безперервність заходів ТЗІ;

відкритість нормативно-правових актів і нормативних документів з питань ТЗІ, які не містять відомостей, що складають державну таємницю;

узгодженість нормативно-правових актів і нормативних документів з питань ТЗІ з відповідними міжнародними договорами України;

Обов'язковість використання інженерно-технічних заходів для захисту інформації:

інформації, яка складає державну та іншу передбачену законом таємницю;

конфіденційної інформації, що є власністю держави;

відкритої інформації, важливої для держави, незалежно від того, де вказана інформації циркулює;

відкритої інформації, важливої для особистості та суспільства, якщо ця інформація циркулює в державних органах, підприємств, установ, організаціях;

виконання на свій розсуд суб'єктами інформаційних відносин потреб відносно технічного захисту;

конфіденційної інформації, яка не належить державі і відкритої інформації, яка важлива для особи і суспільства, якщо інформація циркулює не в межах державних органів, підприємств, установ і організацій;

покладання відповідальності за формування і реалізацію державної політики у сфері ТЗІ за спеціально уповноважений центральний орган виконавчої влади;

ієрархічна побудова організаційної структури системи ТЗІ і керівництво їх діяльності у межах повноважень, визначених нормативно-правовими актами;

методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;

координації дій і розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації і системами інформаційної і національної безпеки;

фінансове забезпечення системи ТЗІ за рахунок державного бюджету України, бюджету Автономної Республіки Крим, місцевих бюджетів і інших джерел.

У якості суб'єктів в системі ТЗІ України виступають:

Держспецзв'язок – спеціально уповноважений центральний орган виконавчої влади, на який покладена відповідальність за формування і реалізації державної політики у сфері ТЗІ;

органи, у відношенні яких здійснення ТЗІ;

державні наукові, науково-дослідницькі і науково-виробничі підприємства, установи і організації, які належать системі СБУ і виконують задачі технічного захисту інформації;

військові частини, підприємства, установи і організації всіх форм власності і громадяни-підприємці, які здійснюють діяльність з технічного захисту інформації по відповідним дозволам або ліцензіям;

навчальний заклад з підготовки, перепідготовки і підвищення

кваліфікації спеціалістів з технічного захисту інформації.

3. Кіберзахист та організація протидії кіберзагрозам

Об'єктами кіберзахисту в ДСНС є інформаційні системи та інформаційно-комунікаційні мережі, поштові та загальносистемні сервери.

Суб'єктами, які здійснюють у межах компетенції заходи із забезпечення кібербезпеки в ДСНС, є фахівці кібербезпеки, технічного захисту інформації, користувачі та інші.

За координацію забезпечення кібербезпеки відповідає керівник установи. Здійснення заходів із забезпечення кібербезпеки покладається на відповідний

структурний підрозділ (фахівців) установи, а за його відсутністю – на підрозділ(и), відповідальний (ні) за адміністрування телекомунікаційних мереж, загальносистемних серверів та/або технічний захист інформації. Структурні підрозділи (фахівці) установи, які відповідають у межах компетенції за забезпечення кібербезпеки на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління:

здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

забезпечують проведення контролю виконання заходів та функціонування засобів інформаційної безпеки;

здійснюють адміністрування телекомунікаційних мереж, поштових та загальних серверів;

надають дозвіл, контролюють та підтримують функціонування системи контролю та управління доступу до внутрішньої мережі, мережі Інтернет тощо;

беруть участь у заходах щодо створення, впровадження та забезпечення функціонування системи управління інформаційною безпекою;

забезпечують інформування про кіберінциденти керівництва установи, ДСНС та взаємодіють із іншими органами відповідно до чинного законодавства.

Закон України «Про основні засади забезпечення кібербезпеки України» не поширюється на діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення».

4. Структура системи захисту інформації

В якості конкретних об'єктів захисту, як правило, виступають нерозрізнені носії інформації, а об'єднана загальними задачами упорядкована їх сукупність.

Під *об'єктом захисту* розуміється інформаційна система (ІС), яка реалізує автоматизований збір, обробку і маніпулювання даними, що включає (Рис. 2):

технічні засоби;

програмне забезпечення;

відповідний персонал;

допоміжні засоби.

Рисунок 2 – Носії інформації

Систему захисту інформації (СЗІ) для конкретних об'єктів(інформаційних систем) можна представити у вигляді:

основ побудови системи захисту інформації;

направлень по захисту інформації;

етапів побудови СЗІ.

Основою побудови системи захисту інформації є:

1) Законодавча, нормативно-правова, наукова і методична база забезпечення захисту інформації.

2) Структура і задачі органів (підрозділів), що забезпечують безпеку інформаційних технологій.

3) Організаційно-технічні і режимні заходи і методи захисту інформації.

4) Програмно-технічні способи і засоби, що використовуються для захисту інформації.

Напрямки захисту інформації формуються виходячи із конкретних особливостей інформаційної системи як об'єкту захисту. Виходячи з типової структури ІС і історично складених висновків робіт по захисту інформацією, можна виділити наступні напрямки:

1) Захист об'єктів інформаційних систем.

2) Захист процесів, процедур і програм обробки інформації.

3) Захист каналів зв'язку.

4) Пригнічення побічних електромагнітних наведень.

5) Управління системою захисту.

Етапи побудови СЗІ необхідно пройти в рівній кількості для всіх і кожного окремо напрямків(з врахуванням всіх основ).

У загальному випадку можна виділити наступні етапи побудови СЗІ:

визначення інформаційних ресурсів (ІР), які підлягають захисту;

виявлення всієї кількості загроз безпеки ІР, які підлягають захисту;

проведення оцінки чутливості і ризиків для ІР, які підлягають захисту, при виявленні великої кількості загроз;

розробка проекту (плану) системи захисту інформації, знижаючого за вибраним критерієм ризику для ІР, які підлягають захисту, при виявленні великої кількості загроз;

реалізація проекту (плану) захисту інформації;

визначення якості реалізації системи захисту;

здійснення контролю функціонування і управління системою захисту.

Проходження етапів необхідно в тій чи іншій мірі здійснювати безперервно і по замкнутому циклу, з проведенням відповідного аналізу стану СЗІ та уточнюючою вимогою до неї після кожного кроку (Рис. 3).

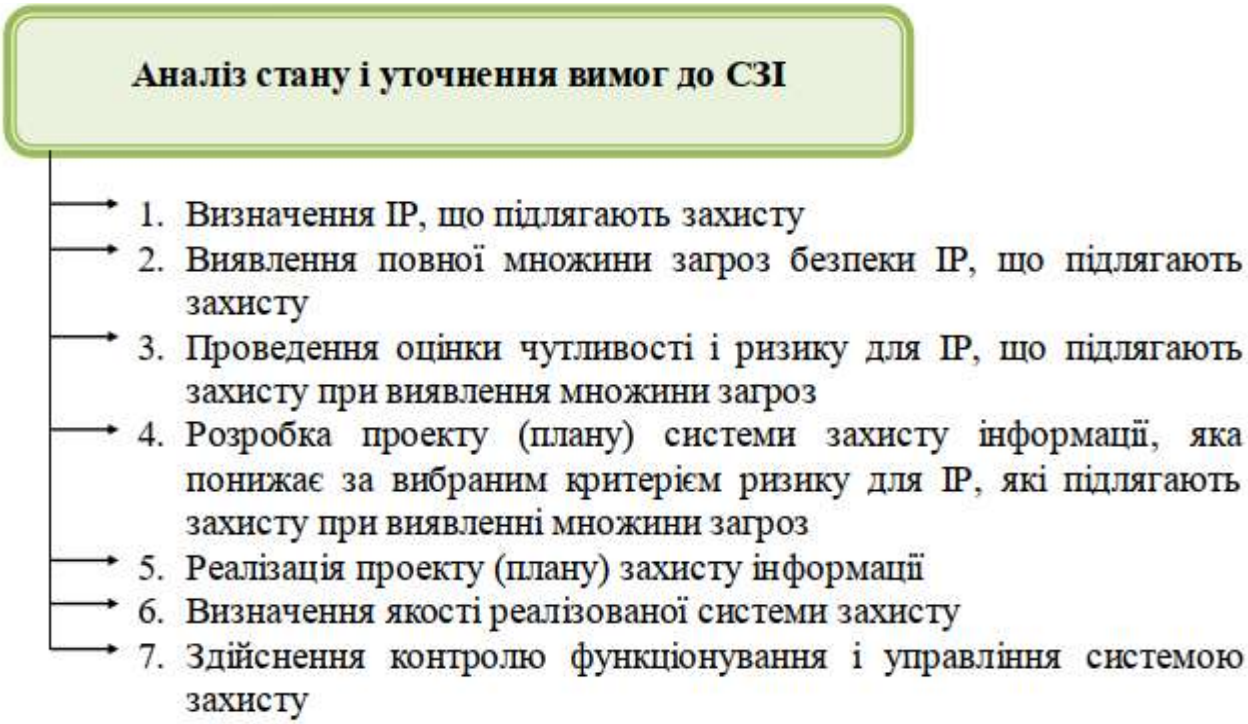

Рисунок 3 – Аналіз стану і уточнення вимог до СЗІ

Для описання логічних зв'язків і більш повного представлення процесу захисту інформації для кожної ІС формують матрицю знань інформаційної безпеки (ІБ). Матриця знань ІБ логічно об'єднує складові блоків «основи», «напрями» і «етапи» за принципом кожен із кожним.

Аналіз стану і уточнення вимог до СЗІ об'єднує складові блоків основи, напрямки, етапи за принципом один з одним.

У загальному випадку кількість елементів матриці може бути визначена із співвідношення

$$K = O_i H_j M_k$$

де K – кількість елементів матриці;

O_i – кількість складових блоку основи;

H_j – кількість складових блоку напряму;

M_k – кількість складових блоку.

Зміст кожного з елементів матриці описує взаємозв'язок складових створюваної СЗІ. Комплекс питань створення й оцінювання СЗІ розглядається

шляхом аналізу різних груп елементів матриці й залежно від вирішуваних завдань.

Використовуючи міжнародний стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій», можна показати (Рис.4) динаміку побудови системи захисту інформації й процеси, що відбуваються при цьому.

Тут:

контрзаходи – комплекс засобів захисту;

загрози події, які потенційно можуть порушити одне із властивостей інформації, що захищають;

порушник – людина, діяльність якого може привести до реалізації загроз, тобто він є джерелом;

уразливості – властивості носіїв інформації, які можуть сприяти реалізації загроз безпеки інформації;

ризик – величина, що характеризує можливість зазнати шкоди через порушення режиму інформаційної безпеки

керуванням ризиками – процес ідентифікації й зменшення ризиків, які можуть впливати на інформаційну систему.

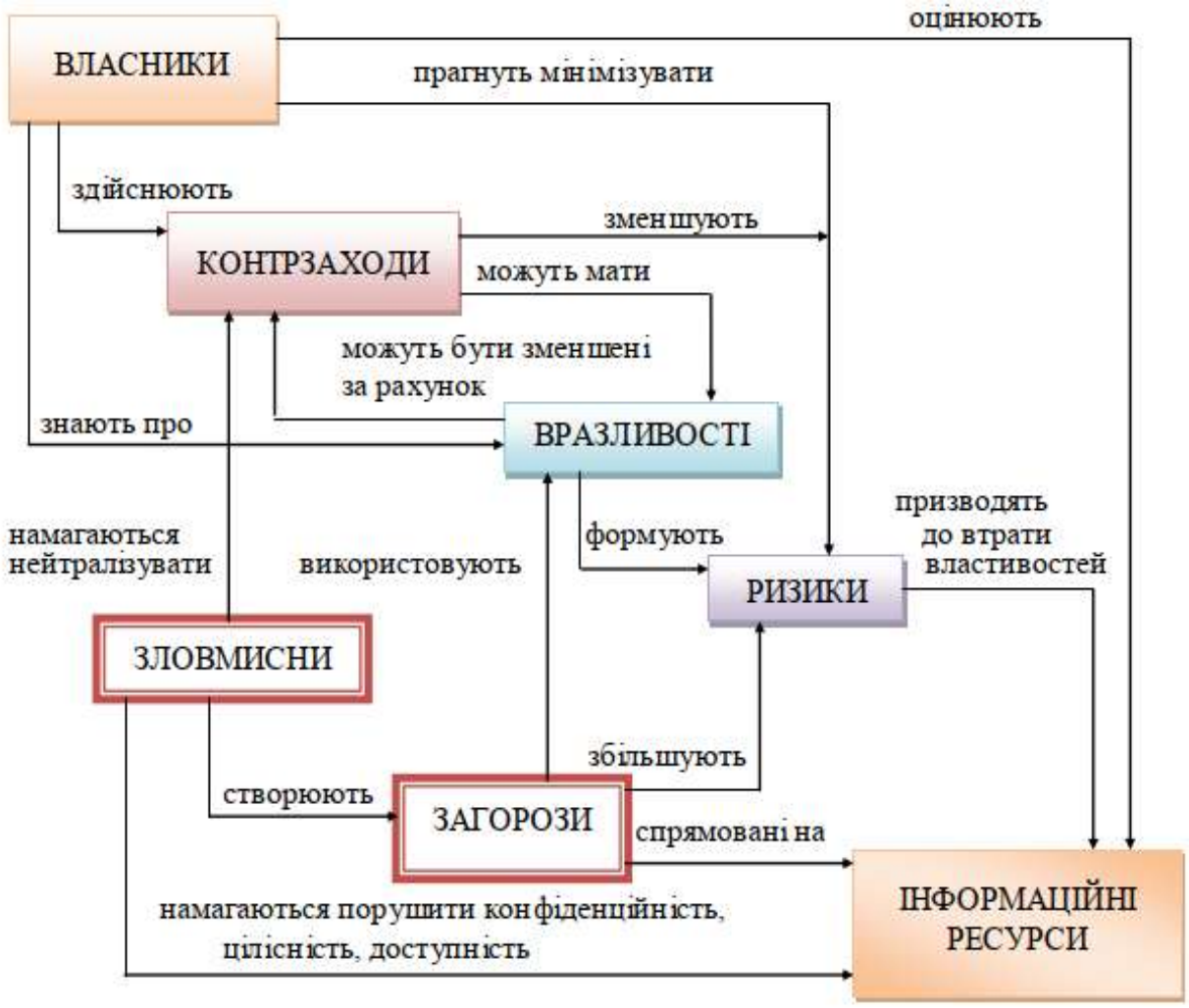

Рисунок 4 – Динаміка побудови системи захисту інформації

Загрози створюють потенційну небезпеку для об'єкта або предмета захисту. Зміни в інформації або її викрадення виникають при реалізації загроз. *Загрози* представляють собою стан або дію взаємодіючих з носіями інформації суб'єктів і об'єктів матеріального світу, які можуть привести до зміни, знищення, викрадення і блокування інформації.

По *виду реалізації загрози* можна розділити на дві групи:

фізичний вплив зовнішніх сил на джерела інформації, в результаті якого можливі її зміни, знищення, викрадення і блокування;

несанкціоноване поширення носія з захищеною інформацією від її джерела до зловмисника, який призводить до викрадення інформації.

Загрози, при реалізації яких відбувається вплив різних сил (механічних, електричних, магнітних) на джерело інформації, називаються *загрозами впливу на джерело інформації*, а загрози, що призводять до несанкціонованого поширення носія до зловмисника, – загрозами витоку інформації.

Основні форми і способи забезпечення інформаційної безпеки утворюють інструмент, через який сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави.

Лекція 4. Класифікація та характеристика технічних каналів витоку інформації

План

Вступ

1. Загальна характеристика технічного каналу витоку інформації.
2. Класифікація та характеристика технічних каналів витоку інформації, що обробляється ТЗПІ.
3. Електромагнітні канали витоку інформації.
4. Електричні канали витоку інформації.
5. Параметричний канал витоку інформації.

Література

1. Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 5 лип. 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.
2. Про науково-технічну інформацію: закон України від 25 черв. 1993 р. №3322XII // Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345.
3. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. : ДСТСЗІ СБ України, 1999. 41 с.

4. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов – Київ : НТУУ «КПІ», 2016. 101с.
5. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К. : Видавництво Ліра-К, 2021. 412 с.
6. Лизанчук В. В. Інформаційна безпека України: теорія і практика : підручник / Львів. нац. ун-т ім. Івана Франка, Львів. шк. журналістики. Львів : ЛНУ ім. Івана Франка, 2017. 725 с.

Вступ

Згідно з Державним стандартом України (ДСТУ 3396.2-96) «Технічний захист інформації. Терміни та визначення», *технічний канал витоку інформації* – сукупність носіїв інформації, середовища їх поширення та засобів технічної розвідки (ЗТР).

1. Загальна характеристика технічного каналу витоку інформації

ТКВІ – це спосіб одержання за допомогою ТЗР розвідувальної інформації про об’єкт. Під розвідувальною інформацією звичайно розуміються відомості або сукупність даних про об’єкти розвідки незалежно від форми їхнього подання.

Сигнали є матеріальними носіями інформації. По своїй фізичній природі *сигнали* бувають *електричними, електромагнітними, акустичними*, і т.д. Тобто *сигналами є електромагнітні, механічні й інші види коливань (хвиль),* причому інформація втримується в їхніх параметрах, що змінюються.

Залежно від природи сигнали поширюються в певних фізичних середовищах. У загальному випадку середовищем поширення можуть бути газові (повітряні), рідинні (водні) і тверді середовища. Наприклад повітряний простір, конструкції споруд, сполучні лінії й струмопровідні елементи, ґрунт (земля) і т.п. Технічні засоби розвідки служать для прийому й вимірювання параметрів сигналів.

2. Класифікація та характеристика технічних каналів витоку інформації, що обробляється ТЗПІ

Канал витоку інформації (КВІ) – неконтрольований фізичний шлях від джерела інформації за межі організації чи кола осіб, що володіють оволодіння зловмисником інформацією.

З технічних каналів витоку інформації найбільшу небезпеку представляє такий НСД, як знімання інформації за рахунок побічних електромагнітний

випромінювань і наведень (ПЕМВН).

Для перехоплення, обробки й аналізу інформації в КВІ можуть використовуватися різноманітні технічні засоби (ТЗ), а також люди (порушники). Тоді існуючі КВІ в залежності від джерел і одержувачів інформації утворять чотири основних типи каналів:

1. *«людина – людина»;*
2. *«людина – ТЗ»;*
3. *«ТЗ – ТЗ»;*
4. *«ТЗ – людина».*

Сказане визначає напрямок потоків інформації. Якщо інформаційний потік поширюється в напрямку від носія до одержувача, то утвориться *узагальнений канал витоку*, якщо ж інформаційний потік у виді явного чи схованого впливу спрямований по вищевказаним чотирьох типах каналів від порушника до носія інформації, то виникає так називаний *узагальнений канал інформаційного впливу* на носій інформації.

У залежності від того, на який параметр носія інформації задумано здійснити вплив, порушником можуть бути застосовані психічні, фізичні, програмно-математичні, радіоелектронні й інші способи і засоби. Параметрами, на які задумано здійснити вплив можуть мати різні характеристики матеріальних носіїв, у тому числі й особистісні характеристики головного прямого носія інформації на об’єкті захисту – людини.

Найбільший потенціал інформативності мають КВІ, у яких для добування конфіденційної інформації використовуються різні технічні засоби. Такі канали одержали назву технічних (ТКВІ). Структура будь-якого ТКВІ, що утворюється в результаті перехоплення, може бути представлена у вигляді системи передачі інформації (рис. 5). При цьому процес передачі повідомлень розбивається на три основні етапи.

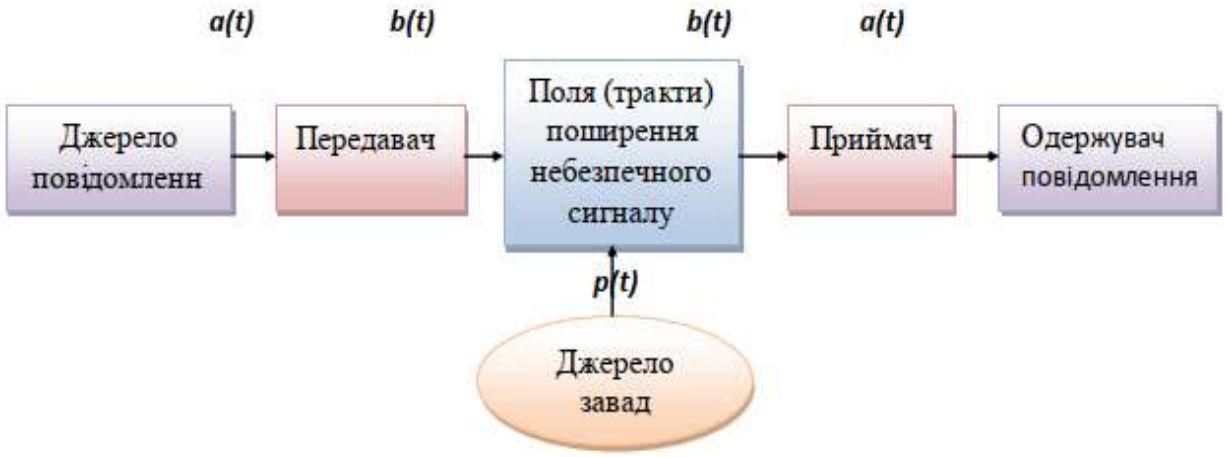

Рисунок 5 – Структура ТКВІ

На початку кожне повідомлення *a(t)* перетворюється передавачем у небезпечний (інформаційний) сигнал *b(t)*. Небезпечний сигнал переміщується

по тракту його поширення, де на нього діє завада *p(t)*, внаслідок чого він частково затухає.

Далі одержаний на приймальній стороні небезпечний сигнал *b'(t)* перетворюється приймачем порушника в повідомлення *a'(t)*.

Оскільки завади в загальному випадку мають випадковий характер, сигнал на вході приймача *b'(t)* буде випадковим чином відрізнятися від *b(t)* і повідомлення *a(t)* може відрізнятися від *a'(t)*.

ТКВІ може бути утворений як за допомогою спеціальних закладних пристроїв (мініатюрні передавачі) та приймачів, так і з допомогою тільки приймачів, які приймають небезпечні сигнали, утворені несанкціонованим перетворенням сигналів з ІПЗ у технічних засобах обробки інформації.

Залежно від використовуваних фізичних полів (трактів) ТКВІ можна класифікувати:

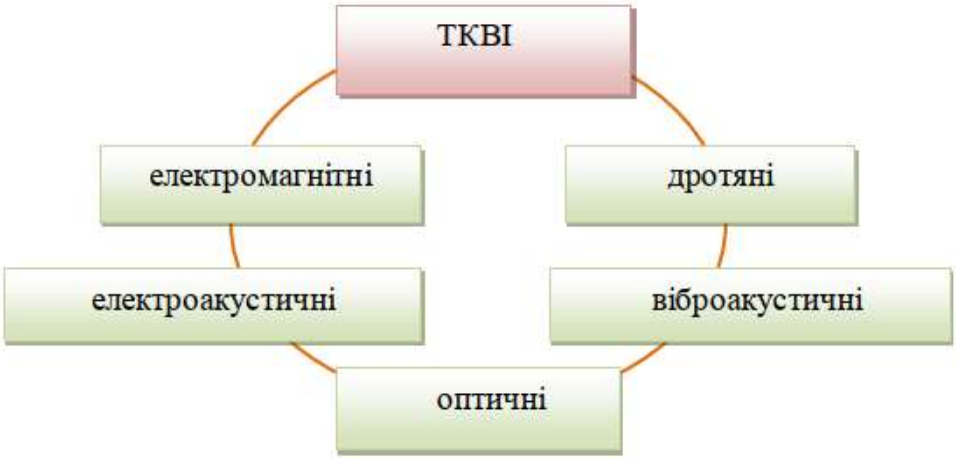

Рисунок 6 – Класифікація ТКВІ

Виходячи з фізичної природи утворення, технічні канали витоку інформації класифікують як:

візуально-оптичні канали – це, як правило, візуальне спостереження: безпосереднє чи віддалене із застосуванням технічних засобів. Переносником інформації виступає світло, що випускається джерелом конфіденційної інформації, або відбите від нього у видимому, інфрачервоному чи ультрафіолетовому діапазонах;

віброакустичні канали. В акустичних каналах переносником інформації (мова, шуми) виступає звук, що лежить у смузі ультразвуку (понад 20000 Гц), чутного та інфразвукового (до 16 Гц) діапазонів. Діапазон звукових частот, які чує людина, лежить у межах від 16 до 20000 Гц, а як таких, що містяться в людському мовлені, – від 100 до 6000 Гц. Середовищем поширення звуку є повітря, земля, вода, будівельні конструкції (цегла, залізобетон, металева арматура та ін.);

радіоелектронний канал. Переносником інформації є або електромагнітні хвилі в радіочастотному діапазоні, або струм, що проходить через загальне

джерело живлення або по колу заземлення;

матеріально-дійсними каналами витоку виступають найрізноманітніші матеріали у твердому, рідкому чи газоподібному або корпускулярному (радіоактивні елементи) вигляді.

Пошуки шляхів підвищення дальності добування мовної інформації призвели до появи складених каналів витоку інформації, що містять в собі сполучення вищевказаних каналів, наприклад *радіоакустичний, акустооптичний* тощо.

Технічні засоби прийому, обробки, зберігання й передачі інформації (ТЗПІ) – це технічні засоби, що безпосередньо обробляють конфіденційну інформацію.

До таких засобів відносяться:

електронно-обчислювальна техніка, режимні АТС;

системи оперативно-командного й гучномовного зв'язку;

системи звукопідсилення;

звукового супроводу і звукозапису і т.д.

При виявленні технічних каналів витоку інформації ТЗПІ необхідно розглядати як систему, що включає основне (стаціонарне) устаткування, кінцеві пристрої, сполучні лінії (сукупність проводів і кабелів, що прокладаються між окремими ТЗПІ і їхніми елементами), розподільні й комутаційні пристрої, системи електроживлення, системи заземлення.

Окремі технічні засоби або група технічних засобів, призначених для обробки конфіденційної інформації, разом із приміщеннями, у яких вони розміщаються, становлять *об'єкт ТЗПІ.*

Під *об'єктами ТЗПІ* розуміють також виділені приміщення, призначені для проведення закритих заходів.

Поряд із ТЗПІ в приміщеннях установлюються технічні засоби й системи, що безпосередньо не беруть участь в обробці конфіденційної інформації, але використовуються разом із ТЗПІ і перебувають у зоні електромагнітного поля, створюваного ними. Такі технічні засоби й системи називаються *допоміжними технічними засобами й системами (ДТЗС*).

До них відносяться:

технічні засоби відкритого телефонного, гучномовного зв'язку;

системи пожежної й охоронної сигналізації, електрофікації,

радіофікації, часофікації, електропобутові прилади і т.д.

Як канал витоку інформації найбільший інтерес представляють ДТЗС, що мають вихід за межі контрольованої зони (КЗ), тобто зони, у якій виключена поява осіб і транспортних засобів, які не мають постійних або тимчасових пропусків.

Крім з'єднувальних ліній ТЗПІ й ДТЗС за межі контрольованої зони можуть виходити кабелі, які для цих ліній не застосовуються, але проходять через приміщення, де встановлені технічні засоби, а також металеві труби систем опалення, водопостачання й інші струмопровідні металоконструкції. Такі з'єднувальні лінії, кабелі й струмопровідні елементи називаються

сторонніми провідниками.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їхнього поширення й способів перехоплення, технічні канали витоку інформації можна розділити на електромагнітні, електричні й параметричний.

Основні технічні заходи спрямовані на блокування каналів витоку інформації і ґрунтуються на одному з принципів показаних на рис. 7.

Успіх реалізації вказаних принципів захисту залежить від багатьох чинників. Основними з них є:

механізм утворення конкретного ТКВІ;

принцип дії та технічні характеристики спеціальних засобів знімання інформації;

особливості побудови і функціонування елементів ІС та їх територіального розташування;

обраний критерій ефективність/вартість захисту.

Рисунок 7 – Принципи блокування ТКВІ

Спеціальні засоби ТЗІ, використовувані під час реалізації основних технічних заходів, можна розділити на засоби ТЗІ і засоби спеціального контролю (рис. 8).

Рисунок 8 – Класифікація спеціальних засобів ТЗІ

Основні технічні заходи передбачають:

1. Заходи щодо блокування ТКВІ з використанням *пасивних засобів*:

контроль і обмеження доступу на об'єкти ТСПІ та у виділені приміщення:

установка на об’єктах ТСПІ та у виділених приміщеннях технічних засобів і систем обмеження і контролю доступу;

локалізація випромінювань:

екранування ТСПІ та їх сполучних ліній;

заземлення ТСПІ та екранів їх сполучних ліній; звукоізоляція виділених приміщень.

розв’язування інформаційних сигналів:

встановлення смугових фільтрів у допоміжних технічних засобах і системах, у яких спостерігається «мікрофонний ефект» і які мають вихід за межі контрольованої зони;

установка спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалювання, водопостачання і каналізації, що мають вихід за межі контрольованої зони;

установка автономних або стабілізованих джерел електроживлення ТСПІ;

установка пристроїв гарантованого живлення ТСПІ (наприклад, генераторів мотора);

установка в ланцюгах і лініях електроживлення ТСПІ та виділених приміщень спеціальних фільтрів, що заглушують.

2. Заходи щодо блокування ТКВІ з використанням *активних засобів*:

просторове зашумлення:

просторове електромагнітне зашумлення з використанням

генераторів шуму або створення прицільних завад (у випадках виявлення і визначення частоти випромінювання закладного пристрою або побічних електромагнітних випромінювань ТСПІ) з використанням засобів створення прицільних завад;

створення акустичних і вібраційних завад з використанням генераторів акустичного шуму;

заглушення диктофонів у режимі запису з використанням відповідних пристроїв;

лінійне зашумлення:

лінійне зашумлення ліній електроживлення;

лінійне зашумлення сторонніх провідників і сполучних ліній ДТСЗ, що мають вихід за межі контрольованої зони;

знищення закладних пристроїв:

знищення закладних пристроїв, підключених до лінії, з використанням спеціальних генераторів імпульсів (випалювачів «жучків»).

3. Електромагнітні канали витоку інформації

Електромагнітні канали витоку інформації виникають за рахунок різного виду побічних електромагнітних випромінювань (ЕМВ) ТЗПІ:

випромінювань елементів ТЗПІ;

випромінювань на частотах роботи високочастотних (ВЧ) генераторів ТЗПІ;

випромінювань на частотах самозбудження підсилювачів низької частоти (ПНЧ) ТЗПІ.

Електромагнітні випромінювання елементів ТЗПІ. У ТЗПІ носієм інформації є електричний струм, параметри якого (сила струму, напруга, частота й фаза) змінюються за законом інформаційного сигналу. При проходженні електричного струму по струмопровідних елементах ТЗПІ навколо них (у навколишньому просторі) виникає електричне й магнітне поле. У силу цього елементи ТЗПІ можна розглядати як випромінювачі електромагнітного поля, модульованого за законом зміни інформаційного сигналу.

Електромагнітні випромінювання на частотах роботи ВЧ- генераторів ТЗПІ й ДТЗС.

До складу ТЗПІ й ДТЗС можуть входити різного роду високочастотні генератори, а саме:

генератори тактової частоти;

генератори стирання й підмагнічування магнітофонів;

гетеродини радіоприймальних і телевізійних пристроїв;

генератори вимірювальних приладів і т.д.

У результаті зовнішніх впливів інформаційного сигналу (наприклад, електромагнітних коливань) на елементах ВЧ-генераторів наводяться електричні сигнали. Приймачем магнітного поля можуть бути котушки індуктивності коливальних контурів, дроселі в ланцюгах електроживлення і т.п. Приймачем електричного поля є проводи високочастотних ланцюгів і інші елементи. Наведені електричні сигнали можуть викликати ненавмисну модуляцію власних ВЧ-коливань генераторів. Ці промодельовані ВЧ-коливання випромінюються в навколишній простір.

Електромагнітні випромінювання на частотах самозбудження ПНЧ ТЗПІ. Самозбудження ПНЧ ТЗПІ (наприклад, підсилювачів систем звукопідсилення й звукового супроводу, магнітофонів, систем гучномовного зв'язку т.п.) можливо за рахунок випадкових перетворень негативних зворотних зв'язків (індуктивних або ємнісних) у паразитні позитивні, що приводить до переведення підсилювача з режиму посилення в режим автоматичної генерації сигналів. Частота самозбудження лежить у межах робочих частот нелінійних елементів ПНЧ (наприклад, напівпровідникових приладів, електровакуумних ламп і т.п.). Сигнал на частотах самозбудження, як правило, виявляється інформаційним сигналом, який промодульований. Самозбудження спостерігається, в основному, при перекладі ПНЧ у нелінійний режим роботи, тобто в режим перевантаження.

Перехоплення побічних електромагнітних випромінювань ТЗПІ здійснюється засобами радіо-, радіотехнічної розвідки, розміщеними поза контрольованою зоною.

Зона, у якій можливі перехоплення (за допомогою розвідувального приймача) побічних електромагнітних випромінювань і наступна розшифровка інформації, що міститься в них (тобто зона, у межах якої відношення «інформаційний сигнал/перешкода» перевищує припустиме нормоване значення), називається (небезпечної) зоною 2.

4. Електричні канали витоку інформації

Причинами виникнення електричних каналів витоку інформації можуть бути:

наведення електромагнітних випромінювань ТЗПІ на сполучні лінії ДТЗС і сторонні провідники, що виходять за межі контрольованої зони;

витік інформаційних сигналів у ланцюги електроживлення ТЗПІ;

витік інформаційних сигналів у ланцюги заземлення ТЗПІ.

Наведення електромагнітних випромінювань ТЗПІ виникають при випромінюванні елементами ТЗПІ (у тому числі і їхніми сполучними лініями) інформаційних сигналів, а також при наявності гальванічного зв'язку з'єднувальних ліній ТЗПІ та сторонніх провідників або ліній ДТЗС. Рівень сигналів, що наводяться, у значній мірі залежить від потужності випромінюваних сигналів, відстані до провідників, а також довжини спільного

пробігу сполучних ліній ТЗПІ й сторонніх провідників.

Простір навколо ТЗПІ, у межах якого на випадкових антенах наводиться інформаційний сигнал вище припустимого (нормованого) рівня, називається (небезпечної) зоною 1.

Випадковою антеною є ланцюг ДТЗС або сторонні провідники, здатні приймати побічні електромагнітні випромінювання.

Випадкові антени можуть бути зосередженими й розподіленими. *Зосереджена випадкова антена* являє собою компактний технічний засіб, наприклад телефонний апарат, гучномовець радіотрансляційної мережі й т.д. До *розподілених випадкових антен* відносять випадкові антени з розподіленими параметрами: кабелі, проводи, металеві труби й інші струмопровідні комунікації .

Витік інформаційних сигналів у ланцюзі електроживлення можливо при наявності магнітного зв'язку між вихідним трансформатором підсилювача (наприклад, ПНЧ) і трансформатором випрямного пристрою. Крім того, струми посилюваних інформаційних сигналів замикаються через джерело електроживлення, створюючи на його внутрішньому опорі спад напруги, що при недостатньому загасанні у фільтрі випрямного пристрою може бути виявлене в лінії електроживлення. Інформаційний сигнал може проникнути в ланцюги електроживлення також у результаті того, що середнє значення споживаного струму в кінцевих каскадах підсилювачів у більшому або меншому ступені залежить від амплітуди інформаційного сигналу, що створює нерівномірне навантаження на випрямляч і приводить до зміни споживаного струму за законом зміни інформаційного сигналу.

Витік інформаційних сигналів у ланцюги заземлення. Крім заземлюючих провідників, що служать для безпосереднього з'єднання ТЗПІ з контуром заземлення, гальванічний зв'язок із землею можуть мати різні провідники, що виходять за межі контрольованої зони. До них відносять нульовий провід мережі електроживлення, екрани (металеві оболонки) сполучних кабелів, металеві труби систем опалення і водопостачання, металеві арматури залізобетонних конструкцій і т.д. Усі ці провідники разом із заземлюючим пристроєм утворять розгалужену систему заземлення, на яку можуть наводитися інформаційні сигнали. Крім того, у ґрунті навколо заземлюючого пристрою виникає електромагнітне поле, що також є джерелом інформації.

Перехоплення інформаційних сигналів по електричних каналах витоку можливе шляхом безпосереднього підключення до сполучних ліній ДТЗС і стороннім провідникам, що проходять через приміщення, де встановлені ТЗПІ, а також до їхніх систем електроживлення й заземлення. Для цих цілей використовуються спеціальні засоби радіо- і радіотехнічної розвідки, а також спеціальна вимірювальна апаратура.

Знімання інформації з використанням апаратних закладок. В останні роки почастішали випадки знімання інформації, оброблюваної в ТЗПІ, шляхом установки в них електронних пристроїв перехоплення інформації – закладних пристроїв.

Електронні пристрої перехоплення інформації, установлювані в ТЗПІ, іноді називають *апаратними закладками*. Вони являють собою міні-передавачі, випромінювання яких модулюється інформаційним сигналом. Найбільше часто закладки встановлюються в ТЗПІ іноземного виробництва, однак можлива їхня установка й у вітчизняних засобах.

Перехоплена за допомогою закладних пристроїв інформація або безпосередньо передається по радіоканалі, або спочатку записується на спеціальний запам'ятовувальний пристрій, а вже потім по команді передається на об'єкт, що її запросив.

5. Параметричний канал витоку інформації

Для перехоплення інформації з даного каналу необхідні спеціальні високочастотні генератори з антенами, що мають вузькі діаграми спрямованості і спеціальні радіо пристрої. Схема параметричного каналу витоку інформації представлена на рис. 9.

Рисунок 9 – Технічні канали витоку інформації, що обробляється ТЗПІ

Перехоплення оброблюваної в технічних засобах інформації може здійснюватися шляхом їх «високочастотного опромінення». При взаємодії електромагнітного поля, що опромінює, з елементами ТЗПІ відбувається перевипромінювання електромагнітного поля. У ряді випадків це вторинне випромінювання модулюється інформаційним сигналом. При зніманні інформації для виключення взаємного впливу випромінюваного й перевипроміненого сигналів може використовуватися їх тимчасова або частотна розв'язка.

При перевипромінюванні параметри сигналів змінюються. Тому даний канал витоку інформації часто називають параметричним.

Поряд із ТЗПІ в приміщеннях встановлюються технічні засоби й системи, що безпосередньо не беруть участі в обробці конфіденційної інформації, але використовуються разом із ТЗПІ і перебувають у зоні електромагнітного поля, створюваного ними. Такі технічні засоби й системи називаються *допоміжними технічними засобами й системами (ДТЗС).*

Лекція 5. Класифікація та характеристика технічних каналів витоку інформації (2)

План

Вступ

1. Особливості витоку інформації технічними каналами.
2. Типова структура та види технічних каналів витоку інформації.
3. Класифікація методів та засобів захисту інформації від витоку технічними каналами.

Література

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов – Київ : НТУУ «КПІ», 2016. 101с.
2. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. : ДСТСЗІ СБ України, 1999. 41 с.
3. Захист інформації в інформаційних системах: навчальний посібник / С.В. Шахов, А.В. Жуков, В.В. Безкоровайний. – Київ : ВПЦ «Київський Університет», 2012. 324 с.
4. Охорона інформації в системах зв'язку та інформаційних технологій: навчальний посібник / Л.І. Герасимова, В.П. Бакланов, Л.А. Торба та ін. – Київ : НАУ, 2012. 364 с.

Вступ

Під *витоком інформації* розуміється несанкціоноване перенесення інформації від її джерела до зловмисника.

1.Особливості витоку інформації технічними каналами

Витік інформації має ряд особливостей, які треба враховувати при організації захисту інформації:

не виконується закон збереження матерії, в наслідок чого витік не може бути виявлений в результаті зменшення кількості інформації джерела;

витік інформації може відбуватися лише при потраплянні до зацікавленого в ній несанкціонованого одержувача (зловмисника);

внаслідок розширення кола її споживачів ціна інформації зменшується.

При витоку інформації можуть бути відсутні явні ознаки її розкрадання:

документи в наявності, відбитки печаток на сейфі не порушенні, слідів проникнення в приміщення сторонніх осіб немає. Однак поява непрямих ознак (раптова поява на ринку конкурентного товару з ідентичними споживчими властивостями, зрив з незрозумілих причин виконання договору) змушує причину цих подій розглядати, як витік інформації. Через істотне запізнення виявлення ознак по відношенню до часу витоку інформації завдання хоча б часткової нейтралізації її наслідків стає вельми проблематичною;

самі по собі факти втрати документу, розголошення відомостей, поширення носіїв за межі контрольованої зони та інші дії далеко не завжди призводять до витоку інформації.

У загальному випадку можна говорити про витік інформації, як факту порушення її безпеки тільки в тому випадку, якщо вона потрапляє до зловмисника незалежно від того, знає або не знає про це власник інформації.

Під *витоком* слід розуміти не процес поширення носія інформації, а *варіант розповсюдження, що закінчується потраплянням інформації до зловмисника.* Вихід же носія інформації за межі заданої області створює передумови для її витоку і підвищує загрозу її безпеці.

Можливість витоку інформації характеризується *ризиком витоку,* а цілеспрямована діяльність зі зміни можливості витоку називається *управлінням ризиком.*

Часто розкрадання і витік інформації розглядають, як автономні процеси. Якщо під розкраданням і витоком інформації розуміти умисне привласнення чужої власності без дозволу її законного власника, то несанкціоноване отримання інформації в результаті її витоку являє собою один із способів її розкрадання. Коли зловмисник знаходить загублений документ з грифом «таємно» і продасть його зарубіжній спецслужбі, то він може бути притягнутий до кримінальної відповідальності за розкрадання держтаємниці.

2. Типова структура та види технічних каналів витоку інформації

Узагальнена структура типового технічного каналу витоку інформації наведена на рис. 10.

Рисунок 10 – Узагальнена структура типового технічного каналу витоку інформації

Фізичний шлях несанкціонованого розповсюдження носія інформації до зловмисника утворює канал витоку інформації.

Інформація, що переноситься, може міститися як на носіях, що є одночасно її джерелами, так і носіях-переносниках, на яких вона переписується з джерел. Тому канал витоку інформації на макротілах містить джерело інформації, середовище поширення носія і несанкціонованого одержувача. Інформація, що переноситься динамічними носіями у вигляді полів (акустичних і електромагнітних) і електричного струму, заздалегідь переписується в джерелі сигналів в їх інформаційні параметри.

Середовище її поширення і приймач сигналу утворюють в сукупності канал зв'язку. Завдання каналу зв'язку полягає в передачі вхідної інформації санкціонованому одержувачеві з мінімальними змінами, тимчасовими, енергетичними і іншими витратами.

Канал витоку інформації на носіях у вигляді нулів і елементарних часток містить ті ж елементи, що і канал зв'язку. І відмінність між ними умовна – залежно від одержувача формації. *У каналі зв'язку одержувач інформації санкціонований, у каналу витоку – несанкціонований.*

На вхід каналу зв'язку поступає інформація у вигляді первинного сигналу або саме джерело може бути джерелом інформації. Первинний сигнал є носієм з інформацією від джерела або з виходу попереднього каналу. В якості джерел сигналів можуть бути:

об'єкт спостереження, що відбиває електромагнітні хвилі, у тому числі світло;

об'єкт спостереження, випромінюючий власні електромагнітні хвилі в оптичному і радіодіапазонах, викликані тепловим рухом електронів;

механізми, що рухаються, і машини, створюють акустичні сигнали;

передавачі функціональних каналів зв'язку;

ретранслятори, наприклад заставні пристрої;

джерела побічних електромагнітних випромінювань і наведень (ПЕМВН);

радіоактивні матеріали.

Більшість джерел сигналу є одночасно джерелами інформації про видові, сигнальні або речові ознаки. Тільки у разі, коли передається семантична інформація, вона поступає на вхід джерела сигналу на носії у вигляді первинного сигналу.

Вказані на рис. 10 стрілками шляху входу і виходу інформації означають вхід і вихід первинних сигналів з інформацією. Оскільки інформація від джерела поступає на вхід каналу на мові джерела (у вигляді буквено-цифрового тексту, символів, знаків, звуків, сигналів і т.д.), то передавач робить перетворення цієї форми представлення інформації у форму, що забезпечує запис її на носій інформації, що відповідає середовищу поширення.

У загальному випадку джерело сигналу виконує наступні функції:

створює (генерує) поле (акустичне, електромагнітне) або електричний струм, які переносять інформацію;

робить запис інформації на носій (модуляцію інформаційних параметрів носія);

посилює потужність сигналу (носія з інформацією);

забезпечує передачу (випромінювання) сигналу в середовище поширення в заданому секторі простору.

Запис інформації робиться шляхом зміни параметрів носія відповідно до рівня первинного сигналу, що поступає на вхід.

Якщо носіями інформації є суб’єкти і матеріальні тіла (мікрочастки), то передавач відповідає первинному значенню цього слова – передавати або переносити, тобто виконує функцію носія. У разі коли інформацію переносять сигнали(поля, електричний струм і елементарні частки), то передавачі є джерелами сигналів.

Приймач сигналу виконує функцію, зворотну функції передавача, а саме:

вибір (селекцію) носія з потрібною одержувачеві інформацією;

посилення прийнятого сигналу-носія до значень, що забезпечують знімання інформації;

знімання інформації з носія (демодуляцію, декодування);

перетворення інформації у форму сигналу, доступну одержувачеві (людині, технічному пристрою), і посилення первинних сигналів до значень, необхідних для їх сприйняття людиною і технічним пристроєм.

Якщо одержувач інформації людина, то інформація з виходу приймача має бути представлена на мові спілкування людей. Якщо технічний пристрій, то форма представлення інформації має бути зрозуміла цьому пристрою.

У середовищі можуть поширюватися носії з іншою інформацією, які по відношенню до носія з даною інформацією є перешкодами. Чим ближче ознаки носія з інформацією, що захищається, і перешкод, тим складніше приймачу їх розрізнити і тим сильніше вплив перешкод на інформацію.

Наприклад, якщо частоти перешкоди і радіосигналу відрізняються на

величину більше за смугу пропускання приймача, то перешкода буде пригнічена селективними ланцюгами приймача. Якщо їх частоти перетинаються, то після демодуляції перешкода накладається на сигнал, що приведе до зміни інформаційних параметрів сигналу, аж до повного руйнування інформації. Постійно зростаюча кількість сигналів в радіодіапазоні породила серйозну проблему їх електромагнітної сумісності.

Для санкціонованих джерел ця проблема вирішується організаційними заходами: законодавчим розподілом шкали радіодіапазону між різними джерелами; контролем за дисципліною зв'язку. Ці заходи погано працюють стосовно джерел перешкод. Класифікація каналів витоку інформації за різними класифікаційними ознаками дана на рис. 11.

Рисунок 11 – Класифікація технічних каналів витоку інформації за різними класифікаційними ознаками

Основною класифікаційною ознакою технічних каналів витоку інформації є фізична природа носія. За цією ознакою вони діляться на: оптичні; радіоелектронні; акустичні; речові.

Носієм інформації в *оптичному каналі* є електромагнітне поле (фотони) в діапазоні 0,46-0,76 мкм (видиме світло) і 0,76-13 мкм (інфрачервоні випромінювання).

У *радіоелектронному каналі* носіями витоку інформації є електричні, магнітні і електромагнітні поля в радіодіапазоні, а також електричний струм, що поширюється по металевих дротах. Діапазон коливань носія цього виду

надзвичайно великий: від звукового діапазону до десятків ГГц. Відповідно до видів носіїв інформації радіоелектронний канал доцільно розділити на 2 підвиди:

електромагнітний *канал, носіями* інформації в якому є електричне, магнітне і електромагнітне поля;

електричний *канал, носій* інформації в якому – електричний струм. Носіями інформації в *акустичному каналі* є пружні акустичні хвилі в інфразвуковому (менше 16 Гц), звуковому (16 Гц – 20 кГц) і ультразвуковому (понад 20 кГц) діапазонах частот, що поширюються в атмосфері, воді і твердому середовищі.

У *речовому каналі* витік інформації здійснюється шляхом несанкціонованого поширення носіїв з інформацією, що захищається, у вигляді речовини, чернеток документів і використаного копіювального паперу, забракованих деталей і вузлів, що передусім викидаються, демаскуючих речовин та ін.

Демаскуючі речовини у вигляді твердих, рідких і газоподібних відходів або проміжних продуктів дозволяють визначити склад, структуру і властивості нових матеріалів або відновити технологію їх отримання. До витоку по цьому каналу віднесено несанкціоноване поширення продуктів розпаду радіоактивних речовин, виявлення і розпізнавання яких зловмисником забезпечують можливість визначення наявності і ознак радіоактивних речовин.

Коли йдеться про поширення за межі організації відходів виробництва, слід відрізняти технічний канал витоку від агентурного, у рамках якого винесення носія з інформацією робиться зловмисником, що проник до джерела, завербованим співробітником організації або співробітником, прагнучим продати інформації будь-якому її покупцеві.

Межа між агентурним і каналом витоку досить умовна, проте у разі витоку інформації в агентурному каналі носієм інформації є особа, свідома виконуюча протиправні дії, а в технічному речовому каналі носії вивозяться з організації з метою звільнення її від відходів або відходи поширюються в результаті дії природних сил. У якості таких сил можуть бути повітряні потоки, що розносять газоподібні відходи, що викидаються трубами, або водні потоки річок або водойм, куди скидаються недостатньо очищені рідкі або зважені у воді тверді частки демаскуючих речовин.

Кожен з технічних каналів має свої особливості, які необхідно знати і враховувати для забезпечення ефективного захисту інформації від її витоку.

Технічний канал витоку інформації складається з передавача, середовища поширення і приймача, є простим або одноканальним.

Проте можливі варіанти, коли витік інформації відбувається складнішим шляхом – по декількох послідовних або паралельних каналах. У цьому випадку канал можна назвати складним. При цьому використовується властивість інформації переписуватися з одного носія на інший. У двох останніх варіантах утворюється складний канал, створений з послідовно сполучених акустичного і оптичного (на лазерному промені) або акустичного і радіоелектронного

(радіозакладка). Такі канали коректно назвати *акустооптичним* і *акусторадіоелектронним* відповідно.

Для підвищення дальності каналу витоку може також використовуватися ретранслятор, що поєднує функції приймача одного каналу витоку інформації і передавача наступного каналу. Наприклад, для підвищення дальності підслуховування з використанням радіозакладки можна розмістити ретранслятор слабкого сигналу заставного пристрою в портфелі, що здається нібито на зберігання в камеру схову закритого підприємства, а приймати і реєструвати потужніший сигнал ретранслятора на видаленні в декілька кілометрів у безпечному місці. Такий складний канал називається *акустично-радіо, електронно-радіоелектронний*.

По *частоті прояву канали* діляться на постійні і епізодичні. У *постійному каналі* витік інформації носить регулярний характер.

До *епізодичних каналів* відносяться канали, витік інформації в яких має короткочасний, часто випадковий характер.

За *способом створення канали витоку* можуть бути спеціально організовані і випадкові.

Організовані канали створюються зловмисником для регулярного добування інформації. Наприклад, для підслуховування на великій відстані від джерела мовної інформації організовується канал витоку з приміщення шляхом розміщення в нім заставного пристрою. Характеристики (частота випромінювання, вид модуляції, потужність передавача та ін.) цього каналу відомі зловмисникові, що дозволяє йому безперервно або в певний час прослуховувати усі розмови, що ведуться в приміщенні.

Побічні електромагнітні випромінювання і наведення створюють передумови для утворення випадкових каналів витоку інформації, параметри яких апріорі зловмисникові не відомі. Якщо вдасться настроїти свій приймач на частоту побічного випромінювання, то виникає випадковий канал витоку інформації. Такий канал може бути дуже інформативним, але випадковий характер його утворення і часу роботи (коли включений випромінюючий технічний засіб) знижує його корисність для зловмисника.

По технічному каналу витоку інформація може передаватися не лише у відкритому виді, вона може бути і закритою. З метою підвищення скритності сигнал на виході перспективних заставних пристроїв закривається, а канал витоку, що використовує ці пристрої, є технічно закритим. При перехопленні функціональних каналів зв’язки, по яких передається шифрована інформація, утворюється шифрований канал просочування інформації.

Випадкові небезпечні сигнали створюють такі електричні прилади, в тому числі:

засоби охоронної сигналізації; засоби пожежної сигналізації; засоби системи електрочасофікації;

засоби розмноження документів;

засоби системи кондиціонування і вентиляції повітря;

побутові прилади, оргтехніка та інше виробниче устаткування; елементи

перетворення акустичної інформації в електричні сигнали (акусто-електричні перетворювачі);

електропровідні комунікації будівлі, що проходять через контрольовану зону.

Характеристики небезпечних випадкових сигналів радіоелектронних засобів та електричних приладів апріорі невідомі ні зловмисникові, ні їх користувачеві. Для їх виявлення і уточнення характеристик проводять спеціальні перевірки та дослідження засобів і приладів.

У залежності від приналежності циркулюючої (оброблюваної, що зберігається, переданої) в технічних засобах та системах інформації до секретної (конфіденційної) або несекретний ці засоби і системи діляться на *основні технічні засоби й системи (ОТЗС)* і *допоміжні технічні засоби та системи (ДТЗС).*

До основних технічних засобів і систем відносяться засоби (системи) і їх комунікації (лінії зв'язку), забезпечуючи обробку, зберігання та передачу інформації, що захищається. З цього не випливає, що ОТЗС повинні обробляти тільки захисну інформацію. В умовах ринку це економічно недоцільно. У загальному випадку ОТЗС можуть використовуватися для розв'язання завдань, не пов'язаних зі збереженням таємниці, але в них вжиті заходи щодо захисту інформації. Якщо в технічних засобах (системах) прийому, обробки, зберігання і передачі інформації такі заходи відсутні, то вони відносяться до допоміжних.

Допоміжні технічні засоби й системи ДТЗС не призначені для обробки інформації, що захищається, але можуть розміщуватися спільно з ОТЗС в контрольованій зоні. Останнє зауваження має принципове значення, оскільки саме близькість розміщення ДТЗС до ОТЗС змушує розглядати допоміжного засоби і системи як потенційні джерела небезпечних сигналів.

З порівняння призначення ОТЗС і ДТЗС випливає, що безлічі ОТЗС і ДТЗС перетинаються. Дійсно, в одному приміщенні можуть розміщуватися засоби, наприклад, подібні комп'ютери, частина з яких є основними, другі – допоміжні. Допоміжний комп'ютер може бути підключений до інтегральної мережі загального користування, наприклад до Internet, що не можна робити для комп'ютера, що відноситься до основного засобу обробки інформації.

До *ДТЗС* віднесені:

різного роду телефонні засоби і системи;

засоби та системи передачі даних в системі радіозв'язку;

засоби та системи охоронної та пожежної сигналізації;

засоби та системи оповіщення та сигналізації;

засоби та системи кондиціонування;

засоби та системи дротового радіотрансляційної мережі та приймання програм радіомовлення та телебачення (абонентські гучномовці, системи радіомовлення та радіоприймачі і т. д.);

засоби електронної оргтехніки;

засоби та системи електрочасофікації;

інші технічні засоби і системи.

3. Класифікація методів та засобів захисту інформації від витоку технічними каналами

1. Організаційні методи захисту.

2. Технічні методи захисту.

1. *Організаційний захід* – це захід захисту інформації, проведення якого не вимагає застосування спеціально розроблених технічних засобів. Захист інформації від витоку по технічних каналах досягається проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням портативних електронних пристроїв перехоплення інформації(заставних пристроїв).

До основних організаційних і режимних заходів відносяться:

залучення до проведення робіт по захисту інформації організацій, що мають ліцензію на діяльність в області захисту інформації, видану відповідними органами;

категоріювання і атестація об'єктів ТСПІ і виділених для проведення закритих заходів приміщень (далі виділених приміщень) по виконанню вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідної міри секретності;

використання на об'єкті сертифікованих ТСПІ у ВТСС;

встановлення контрольованої зони навколо об'єкту;

залучення до робіт по будівництву, конструкції об'єктів ТСПІ, монтажу апаратури організацій, що мають ліцензію на діяльність в області захисту інформації за відповідними пунктами;

організація контролю і обмеження доступу на об'єкти ТСПІ і у виділені приміщення;

введення територіальних, частотних, енергетичних, просторових і тимчасових обмежень в режимах використання технічних засобів, що підлягають захисту;

відключення на період закритих заходів технічних засобів, що мають елементи, що виконують роль електроакустичних перетворювачів, від ліній зв'язку і так далі.

2. *Технічний захід* – це захід по захисту інформації, який передбачає застосування спеціальних технічних засобів, а також реалізацію технічних рішень.

Технічні заходи спрямовані на закриття каналів витоку інформації шляхом послаблення рівня інформаційних сигналів або зменшенням відношення сигнал/шум в місцях можливого розміщення портативних засобів розвідки або їх датчиків до величин, що забезпечують неможливість виділення інформаційного сигналу засобом розвідки, і проводяться з використанням активних і пасивних засобів.

До *технічний заходам з використанням пасивних засобів* відносяться: *контроль і обмеження доступу на об'єкти ТСПІ та у виділені приміщення***:**

встановлення на об’єктах ТСПІ і у виділених приміщеннях технічних засобів і систем обмеження і контролю доступу.

локалізація випромінювань **:**

екранування ТСПІ та їх ліній з’єднання;

заземлення ТСПІ і екранів їх ліній з’єднання;

звукоізоляція виділених приміщень.

розв’язування інформаційних сигналів:

встановлення спеціальних засобів захисту типу «Граніт» у

допоміжних технічних засобах і системах, що мають «мікрофонний ефект» та вихід за межі контрольованої зони;

встановлення спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалювання, водопостачання і каналізації що мають вихід за межі контрольованої зони;

встановлення автономних або стабілізованих джерел електроживлення ТСПІ;

встановлення облаштувань гарантованого живлення ТСПІ (наприклад, мотор-генераторів);

встановлення в ланцюгах електроживлення ТСПІ, а також в лініях освітлювальної і розеткової мереж виділених приміщень перешкодоподавляючих фільтрів типу Ф11.

До технічних заходів з використанням активних засобів відносяться:

*просторове зашумлення***:**

просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних перешкод (при виявленні і визначенні частоти випромінювання заставного пристрою або побічних електромагнітних випромінювань) з використанням засобів створення прицільних перешкод;

створення акустичних і вібраційних перешкод з використанням генераторів акустичного шуму;

пригнічення диктофонів в режимі запису з використанням пригнічувачів диктофонів;

лінійне зашумлення:

лінійне зашумлення ліній електроживлення;

лінійне зашумлення сторонніх провідників і сполучних ліній ВТСС, що мають вихід за межі контрольованої зони;

знищення закладних пристроїв, підключених до лінії, з використанням спеціальних генераторів імпульсів (спалювачів жучків).

Виявлення портативних електронних облаштувань перехоплення інформації (заставних пристроїв) здійснюється проведенням спеціальних обстежень, а також спеціальних перевірок об'єктів ТСПІ і виділених приміщень.

Спеціальні обстеження об’єктів ГСІІ і виділених приміщень проводяться шляхом їх візуального огляду без застосування технічних засобів.

Спеціальна перевірка проводиться з використанням технічних засобів. При цьому здійснюється:

виявлення закладних пристроїв з використанням пасивних засобів:

пошук заставних пристроїв з використанням індикаторів поля, інтерцепторів, частотомірів, приймачів і програмно-апаратних комплексів контролю;

організація радіоконтролю (постійно або на час проведення конфіденційних заходів) і побічних електромагнітних випромінювань ТСПІ.

виявлення заставних пристроїв з використанням активних засобів:

спеціальна перевірка виділених приміщень з використанням нелінійних локаторів;

спеціальна перевірка виділених приміщень, ТСПІ і допоміжних технічних засобів з використанням рентгенівських комплексів;

установка у виділених приміщеннях засобів і систем виявлення лазерного опромінення (підсвічування) вікон;

установка у виділених приміщеннях стаціонарних шукачів диктофонів.

Розвідка технічними каналами витоку інформації забезпечує добування інформації, що знаходиться в телефонних, телеграфних, телеметричних і т.п. повідомленнях і документах (текстах, таблицях, малюнках, картах, знімках і т.п.) з використанням радіоелектронної спеціальної апаратури, яка реєструє ненавмисні (первинні) електромагнітні випромінювання (ЕМВ) і електричні сигнали, що наводять первинними ЕМВ, у струмопровідних ланцюгах і середовищах різних технічних засобів обробки, зберігання й передачі інформації (ТЗПІ), струмопровідних елементах конструкцій будинків, споруджень (системи заземлення, мережі електроживлення ТЗПІ, ланцюга зв'язку в тому ж кабелі, лінії зв'язку з паралельними пробігами, лінії зв'язку в сусідніх приміщеннях і т.п.).

Лекція 6. Методи і засоби захисту інформації в комп'ютерних системах

План

Вступ

1. Загальна характеристика організаційних методів захисту інформації в комп'ютерних системах.
2. Захист інформації в комп'ютерних системах від випадкових загроз.
3. Методи і засоби захисту від електромагнітних випромінювань і наведень.
4. Захист інформації в комп'ютерних системах від несанкціонованого доступу.
5. Захист інформації в розподілених системах.

Література

1. Браіловський, М. М., Зибін, С. В., Пискун, І. В. та ін. Технології захисту інформації. – К: ЦП «Компринт», 2021. – 296 с.
2. Козюра, В. Д., Ткач, Ю. М., Шелест, М. Є. та ін. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах. – Ніжин: ФОП Лук'яненко В.В., 2019. – 144 с. 8.
3. Захист інформації: навч. посіб. / О. В. Глоба, С. В. Білецький, А. А. Чубар. – Київ: НАУ, 2016. – 184 с. 9.
4. Охорона інформації в системах зв'язку та інформаційних технологій: навчальний посібник / Л.І. Герасимова, В.П. Бакланов, Л.А. Торба та ін. – Київ: НАУ, 2012. – 364 с. 11. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. : ДСТСЗІ СБ України, 1999. – 41 с.

Вступ

Методи захисту інформації включають заходи і дії, які повинні виконувати посадові особи в процесі створення і експлуатації комп'ютерних систем для забезпечення заданого рівня безпеки інформації.

1. Загальна характеристика організаційних методів захисту інформації

На *організаційному* рівні вирішуються завдання забезпечення безпеки інформації в комп'ютерних системах:

розмежування доступу до ресурсів комп'ютерної системи;
планування заходів;
організація робіт по розроблення системи захисту інформації;
навчання обслуговуючого персоналу і користувачів;
сертифікація засобів захисту інформації;
ліцензування діяльності із захисту інформації;
атестація об'єктів захисту;
удосконалення комп'ютерної системи;
оцінка ефективності функціонування системи захисту інформації;
контроль виконання встановлених правил роботи в комп'ютерній системі.

За допомогою цих заходів є можливим об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації єдину комплексну систему.

2. Захист інформації в комп'ютерних системах від випадкових загроз

Для блокування випадкових загроз безпеці інформації в комп'ютерних системах доцільно вирішити комплекс завдань.

Рисунок 12 – Завдання захисту інформації в комп'ютерних системах від випадкових загроз

Дублювання інформації є ефективним способом забезпечення цілісності інформації як від випадкових загроз, так і від навмисні дій. У залежності від цінності інформації, особливостей побудови і режимів функціонування комп'ютерної системи можуть такі методи дублювання.

За часом відновлювання інформації методи дублювання поділені на:

оперативні;

неоперативні.

До *оперативних методів* відносяться методи дублювання інформації, котрі дозволяють використовувати дублюючу інформацію в реальному масштабі часу.

Тобто, перехід до використання дублюючої інформації здійснюється за час, який дає змогу виконати запит на використання інформації в режимі реального часу для даної комп'ютерної системи.

Усі методи, що не забезпечують виконання цих умов, відносяться до *неоперативних методів дублювання*.

За засобами, які використовуються для цілей дублювання, методи дублювання можна поділити на методи, що використовують:

додаткові зовнішні запам'ятовуючі пристрої (блоки);

змінні носії інформації.

За числом копій методи дублювання діляться на:

однорівневі;

багаторівневі, але не більше трьох.

За ступенем просторової віддаленості носіїв основної і дублюючої інформації методи дублювання можуть бути:

зосередженого дублювання;

розосередженого дублювання.

Методами зосередженого дублювання доцільно вважати такі методи, для яких носії з основною і дубльованою інформацією знаходяться в одному приміщенні. Всі інші методи відносяться до розосереджених.

У відповідності з процедурою дублювання розрізняють методи:

повного копіювання;

дзеркального копіювання;

часткового копіювання;

комбінованого копіювання.

При *повному копіюванні* дублюються всі файли.

При *дзеркальному копіюванні* будь-які зміни основної інформації супроводжуються таким ж змінами дубльованої інформації (інформація і дубль завжди ідентичні).

Часткове дублювання передбачає створення дублів певних файлів, наприклад, файлів користувача (метод створення дублів файлів, які змінені з часу останнього копіювання).

Комбіноване копіювання допускає комбінації повного і часткового копіювання з різною періодичністю проведення.

По *виду дублювання інформації* методи дублювання такі:

методи із стиканням інформації;

методи без стискання інформації.

У комп'ютерних системах, до яких пред'являються високі вимоги щодо збереження інформації, як правило, використовуються два резервних диски, підключених до окремих контролерів і блоків живлення.

3. Методи і засоби захисту від електромагнітних наведень

Усі методи захисту від електромагнітних випромінювань і наводок можна поділити на активні та пасивні.

Пасивні методи захисту забезпечують зменшення рівня небезпечного сигналу або зниження інформативності сигналів.

Активні методи захисту направлені на створення перешкод в каналах побічних електромагнітних випромінювань і наведень, які ускладнюють прийом і виділення корисної інформації сигналів із перехоплених зловмисником.

Пасивні методи захисту від побічних електромагнітних випромінювань і наведень можна розділити на три групи.

1. Екранування.

Під екрануванням розуміється розміщення елементів комп'ютерної системи, які створюють електричні, магнітні і електромагнітні поля, в просторово замкнених конструкціях.

У залежності від типу утвореного електромагнітного поля розрізняють такі види екранування:

екранування електричного поля;

екранування магнітного поля;

екранування електромагнітного поля.

Екранування електричного поля заземленням металевого екрану забезпечує нейтралізацію електричних зарядів, які стікають по заземленому контуру.

При екрануванні магнітних полів розрізняють низькочастотні магнітні поля (до 10 кГц) і високочастотні. Поглинаюча здібність екрану залежить від частоти побічного випромінювання і від матеріалу, з якого виготовлений екран.

Низькочастотні магнітні поля закриваються екраном за рахунок направленості силових ліній впродовж стінок екрану, що досягається значнішою магнітною проникливістю матеріалу у порівнянні із повітрям.

Високочастотне магнітне поле зумовлює виникнення в екрані перемінних індукційних вихрових токів, які утвореним ними магнітним полем перешкоджають розповсюдженню побічного магнітного поля.

Електромагнітні випромінювання блокуються методами високочастотного електромагнітного і магнітного екранування. Екранування здійснюється на п’яти рінях:

рівень елементів схеми;

рівень блоків; рівень пристроїв;

рівень кабельних ліній;

рівень приміщень.

Вибір числі рівнів і матеріалів екранування здійснюється із врахуванням:

характеристик випромінювання (тип, частота, потужність);

вимог до рівнів випромінювання за межами контрольованої зони і розмірів зони;

наявності або відсутності інших методів захисту від побічних електромагнітних випромінювань і наведень;

мінімізація витрат на екранування.

2. Зниження потужності випромінювання і наведень.

Способи захисту від побічних електромагнітних випромінювань і наведень, об’єднаних в цю групу, реалізуються з метою зниження рівня випромінювання і взаємного впливу елементів комп’ютерної системи. До даної групи відносяться такі методи:

зміна електричних схем;

використання оптичних каналі зв’язку;

зміна конструкції;

використання фільтрів;

гальванічне розв’язування.

Зміна електричних схем здійснюється для зменшення потужності побічних випромінювань.

Оптичні канали зв’язку не утворюють побічних електромагнітних випромінювань і наведень, забезпечуючи високу швидкість передачі, не потрапляючи під вплив електромагнітних перешкод.

Зміна конструкції зводиться до зміни взаємного роз положення окремих вузлів, кабелів, блоків, скороченню довжини шин.

Використання фільтрів є одним із основних способів захисту від побічних електромагнітних випромінювань і наведень. Фільтри усувають розповсюдження і можливе підсилення наведених побічних електромагнітних сигналів на виході із об’єктів ліній зв’язку, сигналізації та електроживлення.

Наявність генераторів живлення, які забезпечують гальванічну розв’язку між первинним і вторинним ланцюгом, повністю виключають потрапляння побічних наведених сигналів у зовнішні ланцюги електроживлення.

3. Зниженні інформативності сигналів.

Зниження інформативності сигналів побічних електромагнітних випромінювань і наведень, що ускладнює їх використання при перехопленні, здійснюється у такі способи:

спеціальні схемні рішення;

кодування інформації.

Для попередження витоку інформації застосовується кодування.

Активні методи захисту від побічних електромагнітних випромінювань і наведень передбачають:

використання генераторів шумів, які різняться принципами формування маскуючи перешкод;

просторове зашумлення за рахунок випромінювання за допомогою антен електромагнітних сигналів у простір;

лінійне зашумлення генераторами прицільних перешкод передбачає підключення до електроліній для утворення в них електричних перешкод, які не дають змогу зловмисником виділяти наведені сигнали.

4. Захист інформації в комп’ютерних системах від несанкціонованого доступу

Отримати несанкціонований доступ до інформації при наявності системи розмежування доступу можливо:

при збої та відмові комп’ютерної системи;

використанні слабких місць в комплексній системі захисту інформації.

Для захисту інформації від несанкціонованого доступу створюється система розмежування доступу до інформації.

1. Система розмежування доступу до інформації в комп’ютерних системах управління доступом.

Вихідною інформацією для створення системи управління доступом є рішення власника (адміністратора) щодо доступу користувачів до певних інформаційних ресурсів комп’ютерної системи.

Так, як інформація в комп'ютерних системах зберігається, обробляється і передається файлами (частинами файлів), то доступ до інформації регламентується на рівні файлів (об'єктів доступу).

Складніше організовується доступ в базах даних, в яких він може регламентуватися до окремих її частин за певними правилами. При визначені повноважень доступу адміністратор встановлює операції, котрі дозволено виконувати користувачу (суб'єкту доступу).

Розрізняють наступні операції з файлами:

читання (*R*);

записування;

виконання програм (*E*).

Як приклад спеціальних схемних рішень, можна навести такі, як заміна послідовного коду паралельним, збільшення розрядності паралельних кодів, зміни черговості розвертки строк на моніторі, що при перехопленні електромагнітного поля і використанні стандартної розвертки зловмисником не буде відповідати вихідному.

Операція записування в файл має дві модифікації:

суб'єкту доступу може надаватися право здійснювати запис із зміна змісту файлу (*W*);

організація записування в файл передбачає тільки дописування в файл, без зміни попереднього змісту (*A*).

У комп'ютерній системі застосовується два підходи до організації розмежування доступу:

матричний;

повноважний (мандатний).

Матричне управління доступом передбачає використання матриць доступу, тобто максимальну деталізацію встановлення права суб'єкта на доступ для виконання дозволених операцій над об'єктами доступу.

Повноважний (мандатний) метод базується на багаторівневій моделі захисту, а саме такий підхід побудований по аналогії з «ручним» конфіденційним (секретним) діловодством.

Суб'єктам доступу встановлюється рівень доступу, який визначає максимальний для даного суб'єкта рівень конфіденційності документа, до якого дозволений допуск.

Суб'єкту доступу встановлюються категорії, які пов'язані з мітками документа.

Правило розмежування доступу полягає в тому, що особа допускається до роботи з документом тільки у випадку, коли рівень допуску суб'єкта дорівнює або вище рівня конфіденційності документа, а в наборі категорій, присвоєних даному суб'єкту доступу, наявні всі категорії, визначені для даного документа.

У комп'ютерній системі всі права доступу фіксуються в його мандаті.

Об'єкти доступу мають мітки, в яких записані ознаки конфіденційності.

Права доступу кожного суб’єкта і характеристики конфіденційності кожного об’єкта відображаються як сукупність рівня конфіденційності і набору категорій конфіденційності.

2. Склад системи розмежування доступу.

Система розмежування доступу до інформації повинна складатися із чотирьох функціональних блоків:

блоку ідентифікації і автентифікації суб’єктів доступу;

диспетчеру доступу;

блоку криптографічного перетворення інформації при її зберіганні і передаванні;

блоку очищення пам’яті.

У комп’ютерній системі всі права доступу фіксуються в його мандаті. Об’єкти доступу мають мітки, в яких записані ознаки конфіденційності. Права доступу кожного суб’єкта і характеристики конфіденційності кожного об’єкта відображаються як сукупність рівня конфіденційності і набору категорій конфіденційності.

Автентифікація –

1) перевірка належності суб’єктові доступу пред’явленого ним ідентифікатора; процес установлення достовірності ідентифікаційної інформації;

2) процедура перевірки відповідності пред’явленого ідентифікатора об’єкта комп’ютерної системи на предмет належності його цьому об’єктові;

установлення або підтвердження автентичності.

Ідентифікація і автентифікація суб’єктів здійснюються в момент їх доступу до пристроїв, в тому числі й дистанційного доступу.

Диспетчер доступу реалізується як апаратно-програмний механізм і забезпечує необхідну дисципліну доступу суб’єктів до об’єктів доступу (в тому числі і до апаратних блоків, вузлам, пристроям).

Диспетчер доступу розмежовує доступ до внутрішніх ресурсів комп’ютерної системи суб’єктів, які вже отримали доступ до цих систем.

Необхідність використання диспетчеру доступу виникає тільки в багато користувальницьких комп’ютерних системах.

Система розмежування доступу повинна реалізовувати функцію очищення оперативної пам’яті і робочих областей на зовнішніх запам’ятовуючих пристроях після завершення виконання, що обробляє конфіденційні дані. Очищення повинно проводитися шляхом запису у вільні ділянки пам’яті у певній послідовності двоїчних кодів, а не вилученням тільки облікової інформації про файли із таблиць Оперативної системи, як це має місце у разі стандартного вилучення засобами операційної системи.

3. Концепція побудови систем розмежування доступу.

В основі побудови системи розмежування доступу лежить концепція розробки захищеної універсальної операційної системи на базі ядра безпеки.

Під ядром безпеки розуміють локалізовану, мінімізовану, чітко обмежену і надійно ізольовану сукупність програмно-апаратних механізмів, що доказово вірно реалізують функції диспетчера доступу.

Для апаратної підтримки захисту і ізоляції ядра в архітектурі ЕОМ доцільно передбачити:

багаторівневий режим виконання команд;

використання ключів захисту і сегментування пам'яті;

реалізацію механізму віртуальної пам'яті з поділом адресних просторів;

апаратну реалізацію частини функцій операційної системи;

зберігання програм ядра в постійному запам'ятовуючому пристрої;

використання нової архітектури ЕОМ, відмінної від фоннеймановської архітектури (архітектури з реалізацією абстрактних типів даних, тегові архітектури з привілеями.

Існує два шляхи отримання *захищених від несанкціонованого доступу комп'ютерних систем*:

створення спеціалізованих комп'ютерних систем;

оснащення універсальних систем додатковими засобами захисту.

Найчастіше захист комп'ютерних систем здійснюється шляхом використання додаткових програмних або апаратно-програмних засобів.

5. Захист інформації в розподілених комп'ютерних системах

1. Архітектура розподілених комп'ютерних систем

Розподілена комп'ютерна – це множина зосереджених комп'ютерних систем, зв'язаних в єдину систему за допомогою комунікаційної підсистеми.

Зосередженими комп'ютерними системами можуть бути окремі ПЄОМ, обчислювальні системи і комплекси, а також локальні обчислювальні мережі. Розподілені комп'ютерні системи будуються по мережевим технологіям і представляють собою обчислювальні мережі. Комутаційна підсистема включає в себе:

комунікаційні модулі (КМ);

канали зв'язку;

концентратори;

межмережні шлюзи (мости).

Основною функцією комунікаційних модулів є передача отриманого пакету до іншої комп'ютерної мережі або абонентському пункту у відповідності з маршрутом передачі. Комунікаційний модуль називають також центром комутації пакетів.

Канали зв'язку об'єднують елементи мережі в єдину мережу.

Концентратори використовуються для ущільнення передачі інформації перед передаванням її по високошвидкісним каналам.

Межмережні шлюзи і мости використовуються для зв'язку мережі з локальними обчислювальними мережами і для зв'язку сегментів мережі з однаковими мережевими протоколами.

Будь-яка розподілена комп'ютерна система у відповідності з функціональними призначенням має три підсистеми:

користувальницька підсистема;

підсистема управління;

комунікаційна підсистема.

Користувальницька (абонентська) підсистема включає в себе комп'ютерні системи користувачів (абонентів) і призначена для задоволення потреб користувачів у зберіганні, обробленні і отриманні інформації.

Підсистема управління дозволяє об'єднувати всі елементи розподіленої комп'ютерної системи в єдину, в якій взаємодія елементів здійснюється за єдиними правилами.

Підсистема забезпечує взаємодію елементів системи шляхом збирання і аналізу службової інформації і впливу на елементи з метою створення оптимальних умов для функціонування всієї мережі.

Комунікаційна підсистема забезпечує передачу інформації в мережі в інтересах користувачів і управління розподіленою комп'ютерною системою.

2. Особливості захисту інформації в розподілених комп'ютерних системах

При побудові системі захисту в будь-якій розподіленій комп'ютерній системі необхідно враховувати:

складність системи, яка визначається як кількістю підсистем, так і різноманіттям їх типів і виконуваних функцій;

неможливість забезпечення ефективного контролю за доступом до ресурсів, розподілених на значних відстанях, можливо і за межами держави можливість належності ресурсів мережі різним власникам.

Аналіз особливостей потенційних активних і пасивних загроз безпеці інформації в розподілених комп'ютерних системах показує, що наряду з мірами, які вживаються для забезпечення безпеки інформації в зосереджених комп'ютерних системах, реалізується ряд механізмів для захисту інформації при передаванні її каналами зв'язку, а також для захисту від несанкціонованого впливу на інформацію комп'ютерної системи з використанням каналів зв'язку.

Усі методи і засоби, що забезпечують безпеку інформації в обчислювальній системі, що захищається, розподіляються на групи:

забезпечення безпеки інформації в користувальницькій підсистемі і спеціалізованих комунікаційних комп'ютерних системах;

захист інформації на рівні підсистеми управління мережею;

захист інформації в каналах зв'язку;

забезпечення контролю справжності взаємодіючих процесів.

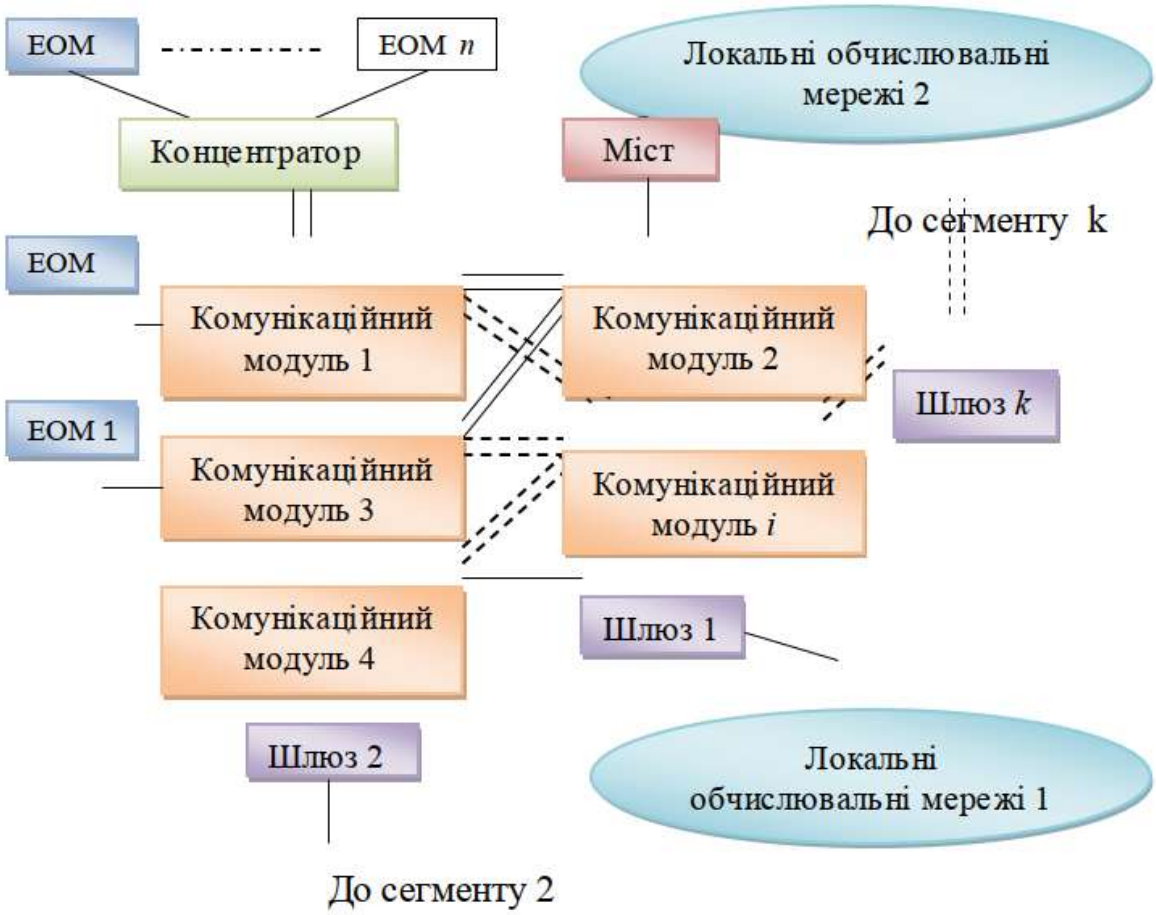

Рисунок 13 – Фрагмент розподіленої комп'ютерної системи

3. Забезпечення безпеки інформації в користувальницькій підсистемі і спеціалізованих комунікаційних комп'ютерних системах

Особливістю захисту об'єктів розподілених комп'ютерних систем є

необхідність підтримки механізмів автентифікації і розмежування доступу віддалених процесів до ресурсів об'єкта, а також наявність в мережі спеціальних комунікаційних комп'ютерних систем.

Усі елементи комунікаційної підсистеми, за винятком каналів зв'язку, розглядаються як спеціалізовані комунікаційні комп'ютерні системи.

У закритих системах робоча інформація в межах комунікаційної підсистеми циркулює в зашифрованому виді.

Розрізняють два види шифрування в комп'ютерних системах:

шифрування в комунікаційній підсистемі – лінійне;

межкінцеве шифрування – абонентське.

Надійним є спосіб управління ключами, коли вони невідомі ні адміністратору, ні абонентам. Ключ генерується датчиком випадкових чисел і записується в спеціальний асоціативний запам'ятовуючий пристрій, і всі дії з ним проводяться в замкнутому просторі, в який оператор комп'ютерної системи не може потрапити з метою ознайомлення зі змістом пам'яті.

Необхідні ключі вибираються із спеціальної пам'яті для відправлення або

перевірки у відповідності з ідентифікатором абонента або адміністратора.

4. Особливості захисту інформації в базах даних.

Бази даних знаходяться:

в комп'ютерній системі користувача;

в спеціально виділеній ЕОМ (сервері).

Захист інформації в базах даних має такі особливості:

необхідність обліку функціонування системи управління базою

даних при виборі механізмів захисту;

розмежування доступу до інформації реалізацією не тільки на рівні файлів, але й на рівні частин баз даних.

Протидія загрозам здійснюється наступними методами:

блокуванням відповіді у разі невірного числа запитів;

перекрученням відповіді шляхом округлення та іншої навмисної корекції даних;

розділом баз даних;

випадковим вибором запису для обробки;

контекстно-орієтированим захистом;

контролем запитів, що поступають.

Метод блокування відповіді при невірній кількості запитів передбачає відмову у виконанні запиту, якщо він вміщує більше певного числа співпадаючих записів із попередніх запитів, чим забезпечується принцип мінімального взаємозв'язку запитань.

Метод корекції полягає в незначній зміні точної відповіді на запит користувача. Для того, щоб зберегти можливу точність статистичної інформації, використовується свопинг даних. Суть його полягає у взаємному обміні значень полів запису, в результаті чого всі статистики *i*-го порядку, включаючи і атрибути, будуть захищеними для всіх, менших або рівних деякому числу.

Метод розділення баз даних на групи полягає в тому, що в кожну групу може бути включено визначену кількість записів.

Сутність контекстно-орієнтированого захисту заключається в призначенні атрибутів доступу (читання, вставка, обновлення, управління тощо) елементами бази даних (записам, полям, групам полів) в залежності від попередніх запитів користувача. Найефективнішим методом захисту інформації в базах даних є

контроль запитів, що поступають на наявність «підозрюваних» запитів або комбінації запитів. Аналіз подібних спроб дозволяє виявити можливі канали отримання несанкціонованого доступу до закритих даних.

Найефективнішим методом захисту інформації в базах даних є контроль запитів, що поступають на наявність «підозрюваних» запитів або комбінації запитів. Аналіз подібних спроб дозволяє виявити можливі канали отримання несанкціонованого доступу до закритих даних.

Лекція 7. Побудова комплексних систем захисту інформації

План

Вступ

1. Концепція організації захищених комп'ютерних систем.
2. Етапи створення комплексної системи захисту комп'ютерних систем.
3. Науково-дослідницька розробка комплексної системи захисту інформації.
4. Вибір показників ефективності та критеріїв оптимальності комплексної системи захисту інформації.
5. Розробка політики безпеки.

Література

1. Браіловський, М. М., Зибін, С. В., Пискун, І. В. та ін. Технології захисту інформації. – К: ЦП «Компринт», 2021. 296 с.
2. Козюра, В. Д., Ткач, Ю. М., Шелест, М. Є. та ін. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах. – Ніжин: ФОП Лук'яненко В.В., 2019. 144 с.
3. Методи та засоби захисту інформації в комп'ютерних системах та мережах / С.В. Шахов, А.В. Жуков, В.В. Безкоровайний. – Київ: ВПЦ «Київський університет», 2007. 300 с.
4. Захист інформації: навч. посіб. / О. В. Глоба, С. В. Білецький, А. А. Чубар. – Київ: НАУ, 2016. 184 с.
5. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. : ДСТСЗІ СБ України, 1999. 41 с.

Вступ

Захист інформації повинен бути системним, що містить в собі різні взаємопов'язані компоненти, найважливішим із яких є об'єкти захисту. Склад об'єктів захисту визначають методи, засоби захисту і склад захисних заходів.

Будь-яка система інформаційної безпеки з розподіленою інформаційною системою, або система, що являє собою один міжмережевий екран, повинна бути мати адекватний вибір рівня захисту, правильний вибір технологій і засобів захисту.

1. Концепція організації захищених комплексних систем захисту інформації

Концептуальність підходу передбачає розробку єдиної концепції як повної сукупності науково обґрунтованих поглядів, положень і рішень,

необхідних і достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також цілеспрямованої організації всіх робіт щодо ЗІ.

Комплексний (системний) підхід до побудови будь-якої системи містить в собі:

вивчення об'єкта впроваджуваної системи;

оцінювання загроз безпеки об'єкта;

аналіз засобів, якими будемо оперувати при побудові системи;

оцінку економічної доцільності;

вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності;

співвідношення всіх внутрішніх і зовнішніх чинників;

можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця.

Система ЗІ – це організована сукупність об'єктів і суб'єктів ЗІ, використовуваних методів і засобів захисту, а також здійснюваних захисних заходів.

1.1.Об'єкти захисту КСЗІ

Захист інформації повинен бути системним, що містить в собі різні взаємопов'язані компоненти, найважливішим із яких є об'єкти захисту. Склад об'єктів захисту визначають методи, засоби захисту і склад захисних заходів.

Інформація є предметом захисту, але захищати її як таку неможливо, оскільки вона не існує сама по собі, а фіксується (відображається) в певних матеріальних об'єктах або пам'яті людей, які виступають в ролі її носіїв і складають основний, базовий об'єкт захисту.

Для запису як секретної, так і несекретної інформації використовуються одні й ті ж носії.

Як правило, носії інформації з обмеженим доступом (ІзОД) охороняються власником цієї інформації.

Особливим носієм інформації є людина, мозок якої являє виключно складну систему, що зберігає і переробляє інформацію, що надходить із зовнішнього світу. Людина, як носій інформації, володіє позитивними та негативними рисами.

Позитивні – без згоди суб'єкта-носія інформація, що захищається, не може бути вилучена з його пам'яті.

Негативні – суб'єкт-носій інформації може помилятися щодо істинності споживача, інформації, що захищається, або навмисно не зберігати довірену йому інформацію: зрада чи просто поширення.

Поширеними видами носіїв конфіденційної інформації є:

паперові носії;

магнітні носії; магнітооптичні та оптичні носії (лазерні диски, компакт-диски);

продукція, що випускається (вироби); технологічні процеси виготовлення продукції;

фізичні поля.

Носії ІзОД як об’єкти захисту захищатися залежно від:

їх видів;

несанкціонованого доступу до них;

втрати;

витоку вміщуваної інформації.

Щоб забезпечити захист, необхідно захищати і об’єкти, які є підступами до носіїв, і їх захист виступає в ролі певних рубежів захисту носіїв.

Об’єктами захисту повинні бути:

засоби відображення, обробки, відтворення і передачі конфіденційної інформації, в тому числі ЕОМ, які повинні захищатися від несанкціонованого підключення, побічних електромагнітних випромінювань, зараження вірусом, електронних закладок, візуального спостереження, виведення з ладу, порушення режиму роботи;

копіювально-розмножувальна техніка, що захищається від візуального спостереження і побічних електромагнітних випромінювань під час обробки інформації;

засоби відео-, звукозаписувальної та відтворювальної техніки, які вимагають захисту від прослуховування, візуального спостереження і побічних електромагнітних випромінювань;

засоби транспортування носіїв конфіденційної інформації, що підлягають захисту від проникнення сторонніх осіб до носіїв або їх знищення під час транспортування;

засоби радіо- і кабельного зв’язку, радіомовлення і телебачення, які використовуються для передачі конфіденційної інформації, що повинні захищатися від прослуховування, виведення з ладу, порушення режиму роботи;

системи забезпечення функціонування підприємства (електро-, водопостачання, кондиціонування та ін.), які повинні захищатися від використання їх для виведення з ладу засобів обробки і передачі інформації прослуховування конфіденційних розмов, візуального спостереження за носіями;

технічні засоби захисту інформації та контролю за ними, що вимагають захисту від несанкціонованого доступу з метою виведення їх з ладу.

1.2. Суб’єкти КСЗІ

До процесу створення КСЗІ залучаються такі сторони:

організація, для якої здійснюється побудова КСЗІ (Замовник);

організація, що здійснює заходи з побудови КСЗІ (Виконавець);

Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) (орган контролю);

організація, що здійснює державну експертизу КСЗІ (Організатор експертизи);

організація, у разі необхідності, залучена Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник).

1.3. Основні вимоги до комплексної системи захисту інформації:

система захисту інформації повинна забезпечувати виконання АС своїх основних функцій без істотного погіршення характеристик останньої;

бути економічно доцільною, оскільки вартість системи захисту інформації входить у вартість АС;

захист інформації в АС повинен забезпечуватися на всіх етапах життєвого циклу, при всіх технологічних режимах обробки інформації, в тому числі при проведенні ремонтних і регламентних робіт;

у систему захисту інформації повинні бути закладені можливості її вдосконалення і розвитку відповідно до умов експлуатації та конфігурації АС.

відповідно до встановлених правил КСЗІ повинна забезпечувати розмежування доступу до ІзОД з відволіканням порушника на помилкову інформацію, тобто мати властивості активного і пасивного захисту;

при взаємодії захищеної АС з незахищеними АС система захисту повинна забезпечувати дотримання встановлених правил розмежування доступу;

система захисту повинна дозволяти проводити облік і розслідування випадків порушення безпеки інформації в АС;

застосування системи захисту не повинно погіршувати екологічну обстановку, не бути складною для користувача, не викликати психологічної протидії та бажання обійтися без неї.

1.4. Завдання комплексної системи захисту інформації:

управління доступом користувачів до ресурсів АС з метою її захисту від неправомірного випадкового або навмисного втручання в роботу системи та несанкціонованого (з перевищенням наданих повноважень) доступу до її інформаційних, програмних і апаратних ресурсів з боку сторонніх осіб, а також осіб з числа персоналу організації та користувачів;

захист даних, що передаються по каналах зв’язку;

реєстрація, збір, зберігання, обробка і видача відомостей про всі події, що відбуваються в системі і які стосуються її безпеки;

контроль роботи користувачів системи з боку адміністрації та оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

контроль і підтримку цілісності критичних ресурсів системи захисту та середовища виконання прикладних програм;

забезпечення замкнутого середовища перевіреного програмного забезпечення з метою захисту від безконтрольного впровадження в систему потенційно небезпечних програм (у яких можуть міститися шкідливі закладки або небезпечні помилки) і засобів подолання системи захисту, а також від впровадження і розповсюдження комп’ютерних вірусів;

управління засобами системи захисту.

1.5. Основні принципи організації КСЗІ в АС:

системність;

комплексність;

безперервність захисту;

розумна достатність;

гнучкість управління і застосування;

відкритість алгоритмів і механізмів захисту;

простота застосування захисних заходів і засобів.

Системи захисту інформації відносяться до класу складних систем і для їх побудови можуть використовуватися основні принципи побудови складних систем із врахуванням специфіки завдань, що вирішуються:

паралельна розробка комп'ютерної системи і системи захисту інформації;

системний підхід до побудови захищеної комп'ютерної системи;

багаторівнева структура системи захисту інформації;

блочна архітектура захищеної комп'ютерної системи;

можливість розвитку системи захисту інформації;

дружній інтерфейс захищеної комп'ютерної системи з користувачами і обслуговуючим персоналом.

Принцип системності є одним із основних концептуальних і методологічних принципів побудови захищених комп'ютерних систем, а саме:

аналіз усіх можливих загроз безпеки інформації;

забезпечення захисту на всіх життєвих циклах комп'ютерних систем;

захист інформації у всіх ланцюгах комп'ютерної системи;

комплексне використання механізмів захисту.

Система захисту інформації повинна мати декілька рівнів, що перекривають один одного, тобто, щоб добратися до закритої інформації, зловмиснику необхідно «зруйнувати» усі рівні захисту.

Наприклад, для окремого об'єкта комп'ютерної системи можна виділити 6 рівнів захисту:

охорона по периметру території об'єкта;

охорона по периметру будівлі;

охорона приміщення;

захист апаратних засобів;

захист програмних засобів;

захист інформації.

Використання принципів блочної архітектури при побудові захищених комп'ютерних систем має ряд переваг:

спрощена розробка, наладка, контроль, і верифікація пристроїв (програм, алгоритмів);

допускається паралельність розробки блоків;

використовуються уніфіковані стандартні блоки;

спрощується модернізація система;

зручність і простота експлуатації.

Комплексна система захисту інформації повинна бути дружньою по відношенню до користувачів і обслуговуючого персоналу, а саме:

повинна бути максимально автоматизованою і не вимагати від користувача виконання значного об'єму дій, пов'язаних з системою захисту інформації;

не створювати обмежень у виконанні користувачем своїх службових обов'язків;

доцільним є передбачення заходів щодо зняття інформації з пристроїв, які відмовили для відновлення їх робото здатності.

2. Етапи створення комплексної системи захисту інформації

У залежності від особливостей комп'ютерної системи, умови її експлуатації і вимог до захисту інформації процес створення комплексної системи захисту може не вміщувати окремих етапів, або зміст їх може частково відрізнятися від загальноприйнятих норм при розробці складних апаратно-програмних систем. Розробка таких систем включає наступні етапи:

розробка технічного завдання (науково-дослідна розробка);

ескізне проектування;

технічне проектування;

робоче проектування;

виробництво дослідного зразка.

Одним із основних етапів розробки комплексної системи захисту інформації є етап розробки технічного завдання.

3. Науково-дослідна розробка комплексної системи захисту інформації

Науково-дослідна розробка починається з аналізу загроз безпеці інформації, аналізу комп'ютерної системи, що захищається і аналізу конфіденційності та важливості інформації, яка повинна оброблятися, зберігатися і передаватися в комп'ютерній системі. На основі аналізу інформації визначаються вимоги до її захищеності. Вимоги створюються шляхом присвоєння визначеного рівня конфіденційності, встановлення правил розмежування доступу.

Комплексна система захисту інформації є підсистемою комп'ютерної системи, то взаємодія системи захисту з комп'ютерною системою можна визначити як внутрішню, а взаємодію із зовнішнім середовищем – як зовнішню.

Внутрішні умови взаємодії визначаються архітектурою комп'ютерної системи. При цьому враховуються:

географічне положення комп'ютерної системи;

тип комп'ютерної системи (розподілений або зосереджений);

структура комплексної системи (технічна, програмна, інформаційна тощо);

надійність та продуктивність;

типи апаратних і програмних засобі, які використовуються, і режими їх роботи;

загрози безпеці інформації, які виникають всередині комп'ютерної системи (відмови апаратних і програмних засобів, алгоритмічні помилки тощо).

Враховуються наступні зовнішні умови:

взаємодія із зовнішн

іми умовами;

випадкові і умисні загрози.

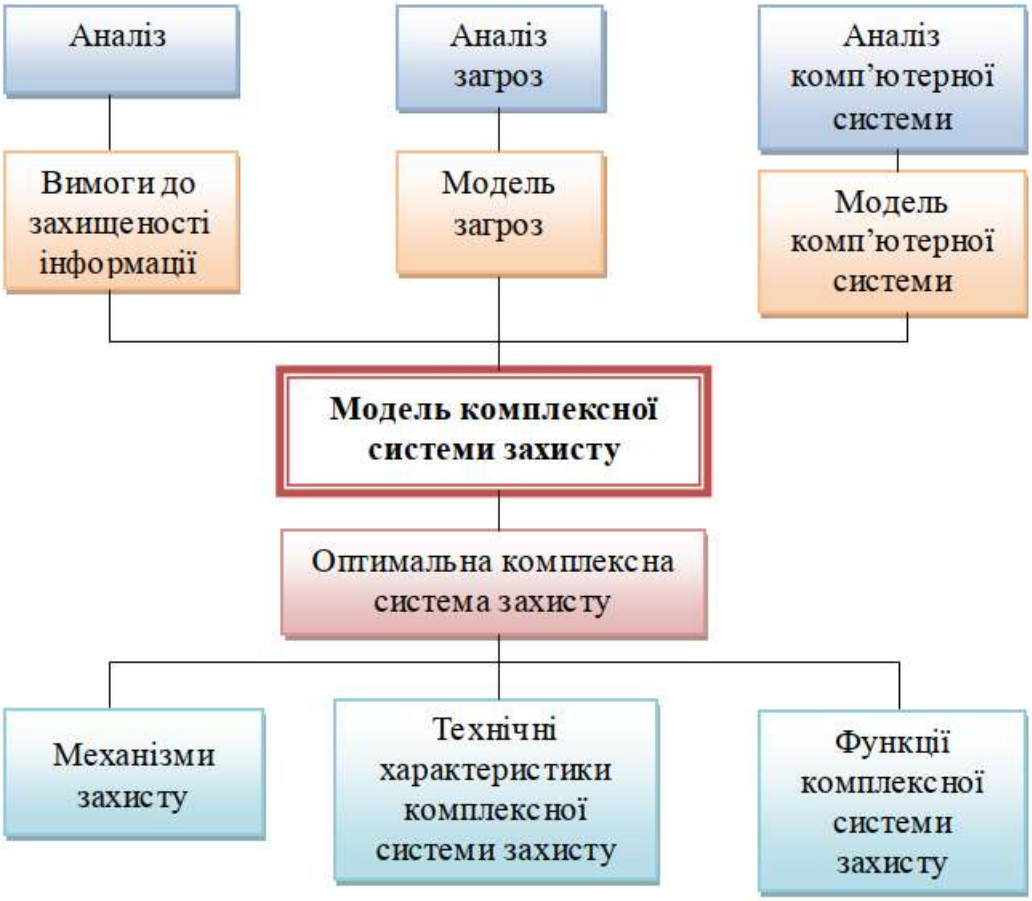

Рис. 14 – Послідовність і зміст науково-дослідної розробки комплексної системи захисту інформації

Модель загроз розглядається і як композиція моделі загроз злочинця і моделі випадкових загроз.

Моделі надаються у вигляді таблиць, графів або на вербальному рівні. При побудові моделі зловмисника використовуються два підходи:

модель орієнтується тільки на висококваліфікованого зловмисника-професіонала, який має легальний доступ на всіх рубежах захисту;

модель враховує кваліфікацію зловмисника, його можливості та офіціальний статус в комп'ютерній системі.

Другий підхід відрізняється гнучкістю і дає змогу враховувати особливості комп'ютерної системи в повній мірі. Градація зловмисників за їх кваліфікацією ділиться на три класи:

висококваліфікований зловмисник-професіонал;

кваліфікований зловмисник-професіонал;

некваліфікований зловмисник-непрофесіонал.

Модель зловмисника і модель випадкових загроз дає змогу отримати повний спектр загроз та їх характеристик. У сукупності із вихідними даними, отриманими в результаті аналізу інформації, особливостей архітектури комп'ютерної системи, що проектується, моделі загроз безпеці інформації дають змогу отримати вихідні дані для побудови моделі комплексної системи захисту інформації.

4. Вибір показників ефективності та критеріїв оптимальності комплексної системи захисту інформації

Ефективність систем оцінюється за допомогою показників ефективності.

Показник ефективності характеризує ступінь відповідності оцінюваної системи своєму призначенню.

Використовуються кількісні та якісні характеристики. Кількісні характеристики систем мають числове значення (їх називають також параметрами). Якісні характеристики визначають наявність (відсутність) певних режимів, захисних механізмів або порівняльний ступінь властивостей систем (добре, задовільно, краще, гірше).

Щоб оцінити ефективність системи захисту інформації або порівняти системи за їх ефективністю, необхідно задати деяке правило переваг. Таке правило або відношення, засноване на використанні показників ефективності, називають критерієм ефективності. Для отримання критеріїв ефективності при використанні деякої множини *k* показників використовують ряд підходів.

1. Вибираємо один головний показник, і оптимальною називається система, для якої цей показник досягає максимуму, за умови, що інші показники задовольняють систему обмежень, заданих у виді нерівностей.

2. Методи, засновані на ранжуванні показників за важливістю. При порівнянні систем однойменні показники ефективності співпадають в порядку зменшення їх важливості за визначеними алгоритмами. Прикладами таких методів можуть бути лексикографічний метод і метод послідовних поступок.

3. Мультиплікативні і адитивні методи отримання критеріїв ефективності ґрунтуються на об'єднанні усіх або частини показників за допомогою операцій множення або складання в узагальненні показники.

4. Система захисту інформації може здійснюватися методом Парето, сутність якого полягає в тому, що при використанні n показників ефективності системі відповідає точка *n*-мірному просторі.

В *n*-мірному просторі будується область парето-оптимальних рішень, в якій для не зрівняльних показників покращення будь-якого параметру неможливо без погіршення інших показників ефективності.

Організаційна система захисту інформації призначена для виконання:

організаційних способів захисту;

експлуатації технічних, програмних і криптографічних засобів захисту;

контролю за виконанням встановлених правил експлуатації комп'ютерної системи обслуговуючим персоналом і користувачами.

Такі структури входять до складу служб безпеки відомств, корпорацій, організацій.

5. Розробка політики безпеки

Політика безпеки – набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі.

Політика безпеки повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях.

Політика безпеки реалізується за допомогою організаційних заходів та програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту.

Для конкретної організації політика безпеки повинна бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації і т. д.

Організаційно політика безпеки визначає порядок подання та використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки.

Система захисту інформації виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки.

Етапи побудови організаційної політики безпеки:

внесення в опис об'єкта структури цінностей і проведення аналізу ризику,

визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності.

Необхідно скласти детальний опис загальної мети побудови системи безпеки об'єкта, що виражається через сукупність факторів або критеріїв, які уточнюють мету.

Сукупність факторів є базисом для визначення вимог до системи (вибір альтернатив). Фактори безпеки, в свою чергу, можуть поділятися на правові, технологічні, технічні та організаційні.

Процеси, пов'язані з розробкою і реалізацією політики безпеки.

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

облік матеріальних або інформаційних цінностей;

моделювання загроз інформації системи;

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

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

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

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

Результати виконаного на певному етапі аналізу і прийняті на їх підставі рішення нарівні з уточненими вимогами слугують вихідними даними для аналізу на наступному етапі.

Загрози мають бути визначені в термінах ймовірності їх реалізації і величини можливих збитків.

Ризик являє собою функцію ймовірності реалізації певної загрози, виду і величини завданих збитків. Величина ризику може бути виражена в грошовому вимірі або у вигляді формальної оцінки (високий, низький і т. п.).

На підставі виконаної роботи виробляються заходи захисту, втілення яких дозволило б знизити рівень остаточного ризику до прийнятного. Підсумком даного етапу робіт повинна стати сформульована або скоригована політика безпеки.

На підставі проведеного аналізу ризиків сформованої політики безпеки розробляється план захисту, який містить опис послідовності і змісту всіх стадій та етапів життєвого циклу КСЗІ, що мають відповідати стадіям і етапам життєвого циклу КС.

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

Для вивчення властивостей способу управління доступом, створюється його формальний опис – математична модель. При цьому модель повинна відображати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в сенсі даного управління. Для розробки моделей застосовується широкий спектр математичних методів (моделювання, теорії інформації, графів і ін.).

Застосовуються *два види політики безпеки*: виборча і повноважна, засновані на виборчому і повноважному способах керування доступом.

Існує набір вимог, що підсилюють дію цих політик і призначені для управління інформаційними потоками в системі.

Засоби захисту, призначені для реалізації будь-якого з названих способів управління доступом, тільки дають можливості надійного управління доступом або інформаційними потоками.

Основою виборчої політики безпеки є *виборче керування доступом*, тобто:

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

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

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

Об’єкти і типи доступу до них суб’єкта може змінюватися відповідно до деяких правил, що існують в даній системі. Визначення і зміна цих правил також є завданням матриці доступу.

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

Основу повноважної політики безпеки складає *повноважне управління доступом*:

усі суб’єкти і об’єкти системи повинні бути однозначно ідентифіковані;

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

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

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

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

Основне *призначення повноважної політики безпеки* – регулювання доступу суб’єктів системи до об’єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії в нижні, а також блокування можливого проникнення з нижніх рівнів в верхні. При цьому вона

функціонує на тлі виборчої політики, надаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Лекція 8. Порядок здійснення захисту інформації на об'єктах інформаційної діяльності

План

Вступ

1. Методика виявлення способів впливу на інформацію.
2. Сутність та класифікація методів захисту інформації в комп'ютерних системах та мережах.
3. Антивірусні програми та програми-архіватори. Використання архівів.
4. Застосування шифрування інформації та програмне забезпечення для шифрування.
5. Утиліти знищення вилученої інформації та очищення диска.

Література

1. Браіловський, М. М., Зибін, С. В., Пискун, І. В. та ін. Технології захисту інформації. – К: ЦП «Компринт», 2021. 296 с.
2. Козюра, В. Д., Ткач, Ю. М., Шелест, М. Є. та ін. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах. – Ніжин: ФОП Лук'яненко В.В., 2019. 144 с.
3. Методи та засоби захисту інформації в комп'ютерних системах та мережах / С.В. Шахов, А.В. Жуков, В.В. Безкоровайний. – Київ: ВПЦ «Київський університет», 2007. 300 с.
4. Захист інформації: навч. посіб. / О. В. Глоба, С. В. Білецький, А. А. Чубар. – Київ: НАУ, 2016. 184 с.
5. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. : ДСТСЗІ СБ України, 1999. 41 с.

Вступ

В інформаційних системах є велике число лазівок для несанкціонованого доступу до інформації. Ніякий окремо взятий спосіб захисту не може забезпечити адекватну безпеку. Надійний захист може бути гарантований лише при створенні механізму комплексного забезпечення безпеки як засобів обробки інформації, так і каналів зв'язку.

1. Методика виявлення способів впливу на інформацію

Залежно від джерела і виду спосіб впливу на інформацію, що захищається може бути безпосереднім або опосередкованим, через інше джерело впливу.

З боку людей можливі такі види впливу:

1. Безпосередній вплив на носії інформацію, що захищається.

2. Несанкціоноване розповсюдження конфіденційної інформації.

3. Вихід з ладу технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку.

4. Порушення режиму роботи перерахованих засобів та технології обробки інформації.

5. Вихід з ладу і порушення режиму роботи систем забезпечення функціонування названих засобів.

Способами безпосереднього впливу на носії інформації, що захищається можуть бути:

фізичне руйнування носія (поломка, руйнування і ін.);

створення аварійних ситуацій для носіїв (підпал, штучне затоплення, вибух і т. д.);

видалення інформації з носіїв;

створення штучних магнітних полів для розмагнічування носіїв;

внесення фальсифікованої інформації у носії.

Дестабілізуючий вплив на інформацію, що захищається, призводить до реалізації трьох форм прояву уразливості інформації: знищення, спотворення, блокування.

Несанкціоноване розповсюдження ІзОД може здійснюватися шляхом:

словесної передачі (повідомлення) інформації;

передачі копій (знімків) носіїв інформації;

показу носіїв інформації;

введення інформації в обчислювальні мережі;

опублікування інформації в пресі;

використання інформації у відкритих публічних виступах, в тому числі по радіо, телебаченню.

До *способів виведення з ладу* технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку відносять:

неправильний монтаж засобів;

поломку (руйнування) засобів, в тому числі розрив (пошкодження) кабельних ліній зв'язку;

створення аварійних ситуацій для засобів (підпал, штучне затоплення, вибух та ін.);

відключення засобів від систем;

виведення з ладу або порушення режиму роботи систем забезпечення функціонування технічних засобів;

вмонтування в ЕОМ радіо- і програмних закладних пристроїв.

Способами порушення режиму роботи технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації, засобів зв'язку і технології обробки інформації можуть бути:

пошкодження окремих елементів засобів;

порушення правил експлуатації засобів;

внесення змін до порядку обробки інформації;

зараження програм обробки інформації шкідливими програмами;

видача неправильних програмних команд;

перевищення розрахункового числа запитів;

створення завад у радіоефірі за допомогою додаткового звукового або шумового фону, зміни (накладення) частот передачі інформації;

передача хибних сигналів;

порушення (зміна) режиму роботи систем забезпечення функціонування засобів.

Даний вид дестабілізуючого впливу також призводить до знищення, перекручення і блокування інформації.

До способів виведення з ладу і порушення режиму роботи систем забезпечення, функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації слід віднести:

неправильний монтаж систем;

поломку (руйнування) систем або їх елементів;

створення аварійних ситуацій для систем (підпал, штучне затоплення, вибух і т. д.);

відключення систем від джерел живлення;

порушення правил експлуатації систем.

Цей вид дестабілізуючого впливу призводить до тих же результатів, що і два попередні види.

До видів дестабілізуючого впливу на інформацію, що захищається, *з боку іншого джерела впливу* – технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку – відносять:

1. Виведення засобів з ладу;
2. Збої в роботі засобів;
3. Створення електромагнітних випромінювань.

Вихід засобів з ладу, що призводить до неможливості виконання операцій, може відбуватися шляхом:

технічної поломки, аварії (без втручання людей);

загоряння, затоплення (без втручання людей);

виходу з ладу систем забезпечення функціонування засобів;

впливу природних явищ;

впливу зміненої структури навколишнього магнітного поля;

зараження програм обробки інформації шкідливими програмами (шляхом розмноження останніх або з заражених дискет);

руйнування або пошкодження носія інформації, в тому числі розмагнічування магнітного шару диска (стрічки) через осипання магнітного порошку.

Цей вид дестабілізуючого впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, перекручення, блокування.

Збої в роботі засобів, що призводять до неправильного виконання операцій (помилок), можуть відбуватися в зв'язку з:

виникненням технічних несправностей елементів засобів;

зараженням програм обробки інформації шкідливими програмами (шляхом розмноження останніх або з заражених дискет);

впливом природних явищ;

впливом навколишнього магнітного поля;

частковим розмагнічування магнітного шару диска (стрічки) через осипання магнітного порошку;

порушенням режиму функціонування засобів.

Даний вид дестабілізуючого впливу призводить до реалізації чотирьох форм прояву уразливості інформації: знищення, перекручення, блокування, розголошенню (наприклад, телефонне з'єднання не з тим абонентом, який набирався, або чутність розмови інших осіб через несправність в ланцюгах комунікації телефонної станції).

Електромагнітні випромінювання, в тому числі побічні, що утворюються в процесі експлуатації засобів, призводять до розкрадання інформації.

Наступне джерело дестабілізуючого впливу на інформацію – *системи забезпечення функціонування* технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації – має два види впливу:

1. Вихід систем з ладу.
2. Збої в роботі систем.

Вихід систем з ладу може відбуватися шляхом:

поломки, аварії (без втручання людей);

загоряння, затоплення (без втручання людей);

виходу з ладу джерел живлення;

впливу природних явищ.

Цей вид дестабілізуючого впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, блокування, викривлення.

Збої в роботі систем можуть здійснюватися за допомогою:

появи технічних несправностей елементів систем;

впливу природних явищ;

порушення режиму роботи джерел живлення.

Результатом дестабілізуючого впливу також є знищення, блокування, спотворення інформації.

Видом дестабілізуючого впливу на інформацію з боку технологічних процесів окремих промислових об'єктів є *зміна структури навколишнього середовища*. Це вплив здійснюється шляхом:

зміни природного радіаційного фону навколишнього середовища, що відбуваються при функціонуванні об’єктів ядерної енергетики;

зміни хімічного складу навколишнього середовища, що відбувається при функціонуванні об’єктів хімічної промисловості;

зміни локальної структури магнітного поля, що відбуваються внаслідок діяльності об’єктів радіоелектроніки і з виготовлення деяких видів озброєння і військової техніки.

Цей вид дестабілізуючого призводить до розкрадання ІзОД.

Останнє джерело дестабілізуючого впливу на інформацію – *природні явища, що охоплюють стихійні лиха і атмосферні явища (коливання).*

До стихійних лих і одночасно видів впливу слід віднести: землетруси, повені, шторми, зсуви, лавини, виверження вулканів; до атмосферних явищ (видів впливу): грозу, дощ, сніг, перепади температури і вологості повітря, магнітні бурі.

Способами впливу з боку стихійних лих і атмосферних явищ можуть бути руйнування (поломки), землетруси, загоряння носіїв інформації засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку, систем забезпечення функціонування цих засобів, порушення режиму роботи засобів і систем, а також технології обробки інформації, створення паразитних наведень (грозові розряди).

Ці види впливу призводять до п’яти форм прояву уразливості інформації: втрати, знищення, перекручення, блокування і розкрадання.

Наявність джерел, видів, способів, причин і обставин (передумов) дестабілізуючого впливу на інформацію є потенційно існуючою небезпекою, яка може бути реалізована при наявності певних умов для цього.

2. Сутність та класифікація методів захисту інформації в комп’ютерних системах та мережах

Об’єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Одним з напрямків захисту інформації в інформаційних системах є ТЗІ. Питання ТЗІ розбиваються на два великих класи завдань:

захист інформації від несанкціонованого доступу (НСД);

захист інформації від витоку технічними каналами.

НСД – це доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу.

Захист від НСД може здійснюватися в різних складових інформаційної системи:

прикладному та системному ПЗ;

апаратній частині серверів і робочих станцій;

комунікаційному устаткуванні та каналах зв'язку;

периметрі інформаційної системи.

Для захисту інформації на рівні прикладного й системного ПЗ використовуються:

системи розмежування доступу до інформації;

системи ідентифікації й аутентифікації;

системи аудита й моніторингу;

системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

апаратні ключі;

системи сигналізації;

засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовуються наступні засоби мережевого захисту інформації:

міжмережеві екрани (Firewall) – для блокування атак із зовнішнього середовища. Вони управляють проходженням мереженого трафіка відповідно до правил політики безпеки. Міжмережеві екрани встановлюються на вході мережі й розділяють внутрішні (частки) і зовнішні (загального доступу) мережі;

системи виявлення вторгнень (IDS – Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу «відмова в обслуговуванні». Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки й витрати на підтримку працездатності мережі;

засоби створення віртуальних приватних мереж (VPN – Virtual Private Network) – для організації захищених каналів передачі даних через незахищене середовище. Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування;

засоби аналізу захищеності – для аналізу захищеності корпоративної мережі й виявлення можливих каналів реалізації погроз інформації. Їхнє застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Для захисту периметра інформаційної системи створюються:

системи охоронної й пожежної сигналізації;

системи цифрового відеоспостереження;

системи контролю й керування доступом (СККД).

Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами й заходами:

використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях;

установкою на лініях зв'язку високочастотних фільтрів;

побудовою екранованих приміщень («капсул»);

використанням екранованого устаткування;

установкою активних систем зашумлення.

Програмні засоби захисту інформації – це спеціально розроблені програми, що реалізують функції безпеки обчислювальної системи (антивірусні програми, системи розмежування повноважень, програмні засоби контролю доступу, криптографічний захист інформації).

Програмно-апаратні засоби захисту засновані на використанні різних електронних пристроїв і спеціальних програм, що входять до складу ІС і виконують (самостійно або в комплексі з іншими засобами) функції захисту (ідентифікацію й аутентифікацію користувачів, розмежування доступу до ресурсів, реєстрацію подій, криптографічне закриття інформації і т.д.).

Характерною рисою *засобів криптографічного захисту* (ЗКЗІ) є те, що вони забезпечують найвищий захист інформації від несанкціонованого доступу. Крім цього, ЗКЗІ забезпечують захист інформації від модифікації.

Програмні засоби захисту реалізують наступні основні функції:

ідентифікацію й аутентифікацію суб'єктів у комп'ютерній системі (КС) на основі паролів і додаткових ідентифікаційних номерів чи міток, роз-міщених на електронних чи магнітних картках;

криптографічний захист інформації на гнучких або твердих дисках на основі реалізації різних алгоритмів шифрування, у тому числі прозорого шифрування (непомітно для користувача);

аутентифікацію суб'єктів у мережах і забезпечення цілісності при передачі повідомлень з використанням цифрових підписів, для створення яких також використовується шифрування.

Програмний напрямок найбільш розвивається, він використовує безліч різноманітних засобів, що дозволяють запобігти витоку інформації чи НСД. Без додаткової підтримки спеціальними апаратними засобами захисту від НСД неможливо забезпечити реальний захист комп’ютерної системи від дій програм-порушників.

Засоби захисту інформації повинні бути уніфіковані і сертифіковані, тобто вони повинні давати гарантію визначеного рівня захищеності.

3. Антивірусні програми та програми-архіватори. Використання архівів

Інтернет-атаки організовані і використовують загальний інтелектуальний потенціал для розробки нових стратегій нападу і нового функціонала в шкідливих програмах, що дозволяє проникати їм непоміченими.

Двадцять років тому сигнатурні антивіруси чудово захищали від шкідливого коду. Сучасний шкідливий код сильно відрізняється.

Визначення комп’ютерного вірусу полягає в тому, що він самовідтворюється і найчастіше наносить шкоду або знищує щось. Шкідливий код непомітний, має цільову аудиторію і може або не може поширюватися.

Приклад, як поширюється антивірусний захист. З появою нового вірусу процес створення сигнатури складається з наступних етапів:

виявлення вірусу;

розробка сигнатури і її випуск;

установка сигнатури.

На найпершому етапі вірус легко знаходить свій спосіб поширення, проникає в мережу і починає виконуватися, оскільки сигнатура ще не готова. Чим більше заявляє про себе цей вірус, тим швидше він буде виявлений і наступить другий етап, коли антивірусна компанія одержує код вірусу і розробляє сигнатуру, що потім буде закачана клієнтами. Процес розробки сигнатури може тривати декілька годин або навіть днів – ви все ще незахищені від погрози.

Сьогоднішні погрози порушують сформовану практику. По-перше, вони можуть відтягнути або навіть уникнути свого виявлення. Використовуючи технології свого приховання або атакуючи спеціально обрані системи, цей код може взагалі не потрапитися антивірусним вендорам, оскільки він не заразив настільки багато систем, щоб стати помітним.

По-друге, активно використовуються технології створення численних варіацій вірусу або багатокомпонентних вірусів. Сучасний шкідливий код – це утиліта типу все-в-одному: руткіт, і троян, і хробак. Для свого поширення шкідливий код використовує різні вразливості операційних систем, помилки конфігурацій, паролі, що легко угадуються, автозапуск із флешек.

Через сучасні технологічні можливості та безліч шляхів поширення, корпоративні системи повинні використовувати кілька рівнів захисту, щоб знизити ризики багатокомпонентних атак. При зростаючому числі атак, що використовують кілька компонентів, завжди існує загроза, що один з цих методів спрацює, якщо ви не підготувалися до нього.

4. Застосування шифрування інформації та програмне забезпечення для шифрування

Шифрування – це чудовий засіб захисту інформації будь-якого типу. Текстові файли, файли програм і навіть графічних файлів можуть бути зашифровані для збереження або для наступної передачі.

У залежності від ситуацій, можуть знадобитися різні засоби шифрування файлів на жорсткому диску. Звичайного парольного захисту файлу або його приховування за допомогою зміни атрибутів може виявитися недостатньо.

Програмне забезпечення для шифрування.

Існує декілька як безкоштовно, так і комерційно розповсюджуваних програм, яки використовуються при шифруванні даних.

Цифровий підпис – унікальний ідентифікуючий рядок символів, використовуваний як засіб перевірки й ідентифікації поштових повідомлень. З початку повідомлення хешується, при цьому кожному символу привласнюється

числове значення. Потім, на основі цього набору значень за складним математичним алгоритмом генерується інший рядок чисел, причому відновити вихідний набір символів практично неможливо. Ці числа додаються до повідомлення у вигляді цифрового підпису та зберігаються системою, що надалі, в разі необхідності, використовує їх для порівняння.

Файли відкритого ключа та підпису, можна створювати за алгоритмами RSA, DES, PGP та іншими. Один зі способів поширення відкритого ключа – його додавання після електронного підпису наприкінці кожного повідомлення.

Віртуальний диск – логічний диск, інформація на якому зберігається в зашифрованому вигляді. Віртуальний диск стає доступним користувачу тільки після того, як він введе пароль або вкаже файли ключа та таблиці.

Для створення віртуальних дисків використовуються призначені для цього програмні засоби.

Система захисту конфіденційної інформації для широкого кола користувачів комп'ютерів.

При установці системи Secret Disk у комп'ютері з'являється новий віртуальний логічний диск (один або декілька). Все, що на нього записується, автоматично шифрується, а при читанні – розшифровується. Зміст цього логічного диска знаходиться в спеціальному контейнері – зашифрованому файлі. Файл секретного диска може знаходитися на жорсткому диску ПК, на сервері, на знімних носіях типу Zip, Jaz, CD-ROM або магнітооптиці.

Secret Disk забезпечує захист даних навіть у випадку вилучення такого диску або самого комп'ютера. Використання секретного диску рівнозначно вбудовуванню функцій шифрування у всі додатки, що запускаються.

Підключення секретного диску та робота з зашифрованими даними можливі тільки після апаратної аутентифікації користувача та введення правильного пароля. Для аутентифікації використовується електронний ідентифікатор – смарткартка, електронний ключ або брелок (апаратні ключі). Після підключення секретного диску, він стає «видний» операційній системі Windows як ще один жорсткий диск, а записані на ньому файли доступні будь-яким програмам.

Не маючи електронного ідентифікатора і не знаючи пароля, підключити секретний диск не можна: для сторонніх він залишиться просто зашифрованим файлом з довільним ім'ям.

Як будь-який фізичний диск, захищений диск може бути наданий для спільного використання в локальній мережі. Після відключення диску всі записані на ньому файли та програми стають недоступними.

Програмно-апаратний комплекс «Захисник» для операційної системи Windows, який реалізує функції обмеження доступу, всебічного захисту інформації та шифрування даних, що знаходяться на жорсткому диску комп'ютера. Комплекс сертифікований в департаменті спецтелекомунікаційних систем захисту інформації СБ України.

Комплекс «Захисник» дозволяє створювати захищені від НСД персональні робочі місця, захищати електронні документи та інформаційні потоки при

використанні найсучасніших і могутніх технологій криптозамін і захисту інформації.

Програмно-апаратний комплекс «Захисник» є спеціалізованою надбудовою над операційною системою, доповнюючи її функціями із захисту інформації від несанкціонованого доступу на окремо розташованому комп'ютері. Даний комплекс дозволяє створити замкнуте захищене середовище обробки даних з обмеженим колом користувачів, що володіють різними повноваженнями доступу до інформаційних ресурсів комп'ютера. Замкнутість системи забезпечується тим, що всі захисні функції працюють як у безпосередньо Windows графічному інтерфейсі, так і при перевантаженні комп'ютера в режимі DOS.

Апаратно-програмний комплекс «Захисник» являє собою функціонально закінчену систему, що виконує:

1. Антивірусний захист, включаючи і захист від новітніх вірусів, що знищують BIOS комп'ютера.
2. Захист інформації, що знаходиться на жорсткому диску, від доступу сторонніх осіб.
3. Приховання інформації від стороннього погляду.
4. Шифрування інформації, як додатковий ступінь захисту особливо важливих файлів.
5. Обмеження доступу до комп'ютера.

Апаратно-програмний комплекс «Захисник»:

працює у власному захищеному режимі процесора;

забезпечує захист на всіх рівнях операційної системи Windows, включаючи ядро системи;

має спеціально розроблені файлові функції, файловий кеш та екстендер, що робить спроби зламу системи нерентабельними, тому що у зловмисника відсутня можливість використання стандартних інструментів для перехоплення та аналізу викликів системи захисту.

5. Утиліти знищення вилученої інформації та очищення диска

Для повного знищення вилучених з диска файлів, необхідно щось записати в ті сектори, де знаходився вилучений файл. Цю процедуру називають *обнуліннам секторів, оскільки більшість утиліт записують у ці сектори двійкові нулі.* Деякі утиліти заповнюють ці сектори випадковими числами, причому можуть робити це кілька разів. Відповідно до вимог Міністерства оборони США, для видалення файлу з диска потрібно цілком стерти його вміст три рази.

Не застосовуючи спеціальних утиліт, не можна перезаписувати або іншим способом змінити дані у необхідному секторі диска.

Утиліти очищення диска є відносно новими програмами. Програми такого типу призначені для видалення тимчасових і інших непотрібних файлів,

що залишаються після роботи різних додатків, а також для допомоги в деінсталяції програм.

Такі утиліти допоможуть видалити тимчасові файли різних типів. Вони також можуть виконувати чергові операції з регулярного очищення диску від непотрібних файлів.

Лекція 9. Захист інформації в комп'ютерній системі організації

План

1. Порядок створення, впровадження, супроводу та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
2. Організація захисту інформації в комп'ютерній системі від витоку каналами ПЕМВН.
3. Рекомендації з захисту інформації від перехоплення випромінювань технічних засобів ОІД.
4. Рекомендації щодо захисту інформації від перехоплення наводок на незахищені технічні засоби та додаткові технічні засоби, що мають вихід за межі контрольованої території.
5. Рекомендації із захисту інформації від витоку колами заземлення.
6. Рекомендації із захисту інформації від витоку колами заземлення.
7. Рекомендації стосовно застосування системи просторового зашумлення ОІД.
8. Основні рекомендації щодо обладнання та застосування екранувальних конструкцій.
9. Захист програмного забезпечення в інформаційних системах.

9.1. Безпека програмного забезпечення.

9.2. Життєвий цикл програмного забезпечення.

9.3. Загрози безпеці програмного забезпечення.

9.4. Комп'ютерні віруси.

9.5. Алгоритмічні і програмні закладки.

Вступ

Згідно з Положенням про технічний захист інформації в Україні в комп'ютерних системах (КС), де обробляється інформація, яка є власністю держави або захист якої гарантується державою, повинні використовуватись засоби ТЗІ, які мають документ, що засвідчує їх відповідність вимогам нормативних документів з питань технічного захисту інформації (експертний висновок та/або сертифікат відповідності).

1. Порядок створення, впровадження, супроводу та модернізації засобів технічного захисту інформації від несанкціонованого доступу

Склад засобів ТЗІ, що використовуються під час створення комплексу засобів захисту інформації, визначають власники КС, де обробляється інформація, яка підлягає захисту, або уповноважені ними суб'єкти системи ТЗІ, з урахуванням того, що ці засоби повинні мати рівень гарантій коректності реалізації послуг безпеки (НД ТЗІ 2.5-004-99) не нижчий від рівня гарантій створюваного комплексу засобів захисту (КЗЗ).

Дозволяється в КС класів «1» та «2» (НД ТЗІ 2.5-005-99) використання засобів ТЗІ з рівнем гарантій на один нижче від рівня гарантій створюваного КЗЗ, за умов реалізації в цих КС необхідного обсягу організаційних заходів. Обсяг цих заходів визначається моделями загроз та порушника, умовами експлуатації КС тощо.

Засоби криптографічних перетворень, які є складовою частиною засобів ТЗІ, повинні відповідати вимогам нормативних документів з питань криптографічного захисту інформації.

Створення та впровадження засобів ТЗІ здійснюють підприємства, установи та організації всіх форм власності, за умови наявності у них відповідної ліцензії на право провадження господарської діяльності в галузі ТЗІ.

Виробництво та впровадження апаратних і програмно-апаратних засобів ТЗІ здійснюється за наявності технічних умов (ТУ), які розробляються, оформляються та реєструються відповідно до вимог ДСТУ 1.3-98, ГОСТ 2.114-95.

Створення програмних засобів ТЗІ здійснюється з урахуванням вимог ДСТУ 3918-99, ГОСТ 19.101-77.

Впровадження програмних засобів ТЗІ здійснюється за наявності формуляру, який розробляється відповідно до вимог ГОСТ 19.501-78.

З метою досягнення певного рівня гарантій реалізації функціональних послуг безпеки інформації розробники (впроваджувальні організації) засобів ТЗІ повинні взаємодіяти з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

Експертне оцінювання засобів ТЗІ на відповідність нормативних документів з питань ТЗІ, здійснюється в порядку, визначеному Положенням про державну експертизу в сфері технічного захисту інформації.

Рівень гарантії реалізації функціональних послуг безпеки визначається в процесі експертного оцінювання з урахуванням вимог цих НД ТЗІ.

Для забезпечення можливості досягнення 3-7 рівнів гарантій реалізації функціональних послуг безпеки розробник (впроваджувальна організація) повинен здійснювати супровід засобу ТЗІ. Для цього розробник (впроваджувальна організація) укладає з користувачем договір на супровід засобу ТЗІ.

Модернізація засобів ТЗІ в комп'ютерних системах здійснюється згідно окремим ТЗ або доповненням до основного ТЗ на створення засобу ТЗІ. ТЗ (доповнення до основного ТЗ) розробляється та оформляється відповідно до чинних ДСТУ з урахуванням вимог НД ТЗІ 3.7–001–99.

2. Організація захисту інформації в комп'ютерній системі від витоку каналами ПЕМВН

Роботи з технічного захисту інформації в ІС і ЗОТ передбачають:

категоріювання об'єктів електронно-обчислювальної техніки (ЕОТ);

внесення до технічних завдань на монтаж ІС і ЗОТ розділу з ТЗІ;

монтаж ІС і ЗОТ відповідно до рекомендацій відповідних документів;

обстеження (в тому числі технічний контроль) об'єктів ЕОТ;

установлення (при необхідності) атестованих засобів захисту;

технічний контроль за ефективністю вжитих заходів.

Для об'єктів ЕОТ, що обробляють ІзОД, проводиться обов'язкове категоріювання згідно з чинним Положенням про категоріювання. Обсяг і зміст робіт із захисту цієї інформації визначаються присвоєною категорією.

Обстеження ІС і ЗОТ відповідно до рекомендацій проводиться структурними підрозділами ТЗІ, у віданні яких знаходиться об'єкт, або підприємствами, установами, організаціями і громадянами, що одержали в установленому порядку відповідні ліцензії Державної служби України з питань технічного захисту інформації.

Рекомендований такі *алгоритм обстеження містить процедури*:

аналіз у технічних засобах ЕОТ потоків інформації з обмеженим доступом;

визначення складу ОТЗ і ДТЗ на ОІД;

визначення складу кабельних ліній, що виходять за межі КТ і розміщенні паралельно з кабелями ІС і ЗОТ;

виявлення комунікацій, що проходять через територію ОІД і мають вихід за межі КЗ;

інструментальне вимірювання інформативних побічних електромагнітних випромінювань та наводок;

оцінювання відповідності рівнів сигналів і параметрів полів, які є носіями ІзОД, нормам ефективності захисту.

За результатами обстеження складається акт, в якому відбиваються:

категорія ОІД;

перелік ОТЗ (найменування, тип, заводський номер);

перелік ДТЗ і комунікацій, що знаходяться на ОІД;

оцінка відповідності монтажу цим рекомендаціям;

пропозиції щодо застосування додаткових заходів захисту (при необхідності).

До акта додаються:

схема розміщення технічних засобів ОІД і проходження комунікацій на ньому;

протоколи вимірювань.

3. Рекомендації з захисту інформації від перехоплення випромінювань технічних засобів ОІД

Навколо ОТЗ повинна забезпечуватися контрольована територія, за межами якої відношення «інформативний сигнал/шум» не перевищує норм. З цією метою ОТЗ рекомендується розташовувати у внутрішніх приміщеннях об'єкта, бажано, на нижніх поверхах.

У випадку неможливості забезпечення цієї умови необхідно:

замінити ОТЗ на захищені;

провести часткове або повне екранування приміщень чи ОТЗ;

установити системи просторового зашумлення;

замінити незахищені ТЗ на захищені;

застосувати завадозаглушувальні фільтри.

В екранованих приміщеннях (капсулах) рекомендується розміщувати високочастотні (ВЧ) ОТЗ. Як правило, до них відносять процесори, запам'ятовувальні пристрої, дисплеї тощо.

4. Рекомендації щодо захисту інформації від перехоплення наводок на незахищені технічні засоби та додаткові технічні засоби, що мають вихід за межі контрольованої території

У незахищених каналах зв’язку, лініях, проводах та кабелях ОТЗ і ДТЗ, що мають вихід за межі КТ, установлюються завадозаглушувальні фільтри.

Проводи і кабелі прокладаються в екранованих конструкціях.

Монтаж кіл ТЗ, що мають вихід за межі КТ, рекомендується проводити екранованим або прокладеним в екранувальних конструкціях симетричним кабелем.

Кабелі ОТЗ прокладаються окремим пакетом і не повинні утворювати петлі. Перехрещення кабелів ОТЗ і ДТЗ, що мають вихід за межі КТ, рекомендується проводити під прямим кутом, забезпечуючи відсутність електричного контакту екранувальних оболонок кабелів у місці їх перехрещення.

Незадіяні проводи і кабелі демонтуються або закорочуються та заземляються.

5. Рекомендації із захисту інформації від витоку колами заземлення

Система заземлення технічних засобів ОІД не повинна мати вихід за межі КТ і повинна розміщуватися на відстані не менше 10-15 м від них.

Заземлювальні проводи повинні бути виконані з мідного дроту (кабеля) з перехідним опором з'єднань не більше 600 мкОм. Опір заземлення не повинен перевищувати 4 Ом.

Не рекомендується використовувати для системи заземлення ТЗ ОІД природні заземлювачі (металеві трубопроводи, залізобетонні конструкції будинків тощо), які мають вихід за межі КТ.

Для усунення небезпеки витоку інформації металевими трубопроводами, що виходять за межі КТ, рекомендується використовувати струмонепровідні вставки (муфти) довжиною не менше 1 м.

За наявності в ТЗ ОІД «схемної землі» окреме заземлення для них створювати не потрібно. Шина «схемна земля» повинна бути ізольованою від захисного заземлення та металоконструкцій і не повинна утворювати замкнену петлю.

При неможливості провести заземлення ТЗ ОІД допускається їх «занулення».

6. Рекомендації із захисту інформації від витоку колами заземлення

Найбільш ефективно гальванічну та електромагнітну розв'язку кабелів електроживлення ТЗ ОІД від промислової мережі забезпечує їх розділова система типу «електродвигун-генератор». Електроживлення допускається також здійснювати через завадозаглушувальні фільтри.

Електроживлення повинно здійснюватись екранованим (броньованим) кабелем.

Кола електроживлення ТЗ ОІД на ділянці від ОТЗ до розділових систем чи завадозаглушувальних фільтрів рекомендується прокладати у жорстких екранувальних конструкціях.

Не допускається прокладання в одній екранувальній конструкції кабелів електроживлення, розв'язаних від промислової мережі, з будь-якими кабелями, що мають вихід за межі КТ.

Забороняється здійснювати електроживлення технічних засобів, що мають вихід за межі КТ, від захищених джерел електропостачання без установлення завадозаглушувальних фільтрів.

Для об'єктів 2-ої - 4-ої категорій допускається не проводити роботи із захисту кіл електроживлення, якщо всі пристрої і кабелі електропостачання ОІД, також трансформаторна підстанція низької напруги із заземлювальним пристроєм, розміщені у межах КТ.

7. Рекомендації стосовно застосування системи просторового зашумлення ОІД

Пристрої просторового зашумлення застосовуються у випадках, коли пасивні заходи не забезпечують необхідної ефективності захисту ОІД.

Установленню підлягають тільки сертифіковані Державною службою України з питань технічного захисту інформації засоби просторового зашумлення, до складу яких входять:

надширокосмугові генератори електромагнітного поля шуму (генератор шуму);

система рамкових антен;

пульт сигналізації справності роботи системи.

Установлення генераторів шуму, монтаж антен, а також їх обслуговування в процесі експлуатації здійснюють підприємства, установи й організації, що мають відповідну ліцензію ДСТЗІ.

Живлення генераторів шуму повинно здійснюватися від того ж джерела, що і живлення ТЗ ОІД. Антени рекомендується розташовувати поза екранованим приміщенням.

8. Основні рекомендації щодо обладнання та застосування екранувальних конструкцій

Екранувальні кабельні конструкції разом з екранувальними конструкціями ТЗ ОІД повинні створювати екранувальний замкнений об’єм.

Виведення кабелів з екранувальних конструкцій і введення в них необхідно здійснювати через завадозаглушувальні фільтри.

Екранувальні кабельні конструкції можуть бути жорсткими і гнучкими. Основу жорстких конструкцій становлять труби, короби та коробки; основу гнучких конструкцій – металорукави, взяті в обплетення, і сітчасті рукави.

Для екранування проводів і кабелів застосовуються водогазопровідні труби. Рекомендується застосовувати сталеві тонкостінні оцинковані труби або сталеві електрозварені.

З’єднання нероз’ємних труб здійснюється зварюванням, роз’ємних – за допомогою муфти та контргайки.

Для екранування проводів і кабелів застосовуються короби прямокутного перерізу. Їх переваги порівняно з трубами – можливість прокладання кабелю з роздільними роз’ємами.

Короби виготовляються з листової сталі. На кінцях секцій короба повинні бути фланці для з’єднання коробів між собою та з іншими екранувальними конструкціями. Для одержання надійного електричного контакту поверхня фланців повинна мати антикорозійне струмопровідне покриття.

Остаточний висновок про ефективність заходів технічного захисту інформації робиться за результатами інструментального контролю.

9. Захист програмного забезпечення в інформаційних системах

9.1. Безпека програмного забезпечення

Захист програмного забезпечення (ПЗ) визначають як комплекс заходів, спрямованих на захист ПЗ від несанкціонованого придбання, використання, поширення, модифікування, вивчення й відтворення аналогів. Інформація є експлуатованим ресурсом для ПЗ ІС, безпека ПЗ ІС є важливою складовою безпеки інформації загалом.

При вирішенні завдання забезпечення безпеки інформаційних ресурсів ІС виходять із припущення, що найімовірнішим інформаційним об'єктом деструктивних дій в ІС буде ПЗ, особливо ПЗ критичних ІС, блокування або порушення функціонування яких може призвести, наприклад, до екологічних і техногенних катастроф.

Під безпекою ПЗ розуміють властивість певного ПЗ функціонувати без прояву негативних наслідків для конкретної ІС. При цьому *рівень безпеки ПЗ* у процесі його експлуатації визначають як імовірність забезпечення *функціональної придатності* ІС.

Функціональну придатність визначено стандартом ISO 9126:2001 як здатність розв'язувати потрібний рівень задач.

До загальних причин, що призводять до зниження рівня безпеки ПЗ, зараховують:

збої ІС;

помилки програмістів і операторів;

дефекти ПЗ.

Дефекти ПЗ умовно поділяють на навмисні та ненавмисні.

Ненавмисні дефекти ПЗ є, як правило, результатом помилкових дій людини, навмисні дефекти ПЗ – результатом зловмисних дій.

У загальному випадку, дослідження проблем безпеки ПЗ, пов'язаних із потенційною можливістю наявності в ньому навмисних дефектів, передбачає вирішення таких завдань:

визначення кола способів виявлення і ідентифікації дефектів ПЗ;

визначення найімовірніших наслідків активації дефектів ПЗ.

9.2. Життєвий цикл програмного забезпечення

У загальному випадку *життєвий цикл ПЗ* представляють такими базовими етапами:

системний аналіз і обґрунтування вимог до ПЗ;

попереднє (ескізне) і детальне (технічне) проєктування ПЗ;

розроблення програмних компонентів, їх об'єднання та від лагодження ПЗ у цілому;

випробування, дослідна експлуатація та тиражування ПЗ;

регулярна експлуатація ПЗ, підтримування експлуатації та аналіз її результатів;

супровід ПЗ, його модифікація й удосконалення, створення нових версій.

Теорія проектування ПЗ включає такі основні моделі життєвого циклу:

каскадна;

ітераційна;

спіральна.

Каскадна модель життєвого циклу має такі особливості:

послідовним виконанням етапів;

завершення кожного попереднього етапу до початку наступного;

відсутністю (або певним обмеженням) повернення до попередніх етапів;

наявністю результату в кінці розроблення.

Ітераційна модель життєвого циклу ПЗ – це поетапна модель із проміжним контролем, наявністю проміжних зв'язків між етапами, що дає можливість здійснення перевірок і корегувань проектованого ПЗ на кожній стадії розроблення.

Спіральна модель життєвого циклу ПЗ підтримує ітераційний підхід ,властивий ітераційній моделі, проте увага приділяється початковим етапам проєктуванння: аналізу вимог, проектування специфікацій, попереднього проектування та детального проектування. Кожний віток спіралі відповідає ітераційній моделі створення фрагмента або версії ПЗ, при цьому уточнюють цілі та вимоги до ПЗ, оцінюють якість розробленого фрагмента або версії й планують роботи для наступної стадії розроблення.

На практиці застосовують комбіновану модель життєвого циклу. За основу беруть «спіральну» модель, в якій із секторами спіралі, що є етапами процесу, зіставляють відповідні етапи каскадної моделі, якщо такі є.

Сукупність етапів життєвого циклу ПЗ умовно поділяють на дві частини.

У першій частині «технологічній» здійснюють системний аналіз, обґрунтування вимог, проектування, розроблення, тестування, випробування, дослідну експлуатацію та тиражування ПЗ.

Друга частина – «експлуатаційна» стосується підтримання експлуатації й супроводу ПЗ.

Відповідно вирізняють:

технологічну безпеку ПЗ – властивість ПЗ не бути навмисно зміненим і (або) обладнаним шкідливими компонентами на технологічній частині життєвого циклу;

експлуатаційну безпеку ПЗ – властивість ПЗ не бути навмисно зміненим і (або) обладнаним шкідливими компонентами на експлуатаційній частині життєвого ціклу.

9.3. Загрози безпеці програмного забезпечення

До *загроз безпеці ПЗ* належать:

незаконне розповсюдження та збут ПЗ (піратство);

незаконне використання алгоритмів (порушення авторського права на інтелектуальну власність);

несанкціонована модифікація ПЗ (упровадження навмисних дефектів);

несанкціоноване використання ПЗ (копіювання).

Основну загрозу безпеці ПЗ ІС несуть такі програмні засоби деструктивної дії на ІС, які за своєю природою мають руйнівний характер – *руйнівні програмні засоби (РПЗ)*:

комп'ютерні віруси;

закладки;

способи й засоби, що дають змогу впроваджувати комп'ютерні віруси й закладки в ІС і керувати ними на відстані за допомогою атак на ІС.

Необхідною умовою віднесення програмного засобу деструктивної дії до класу РПЗ є наявність у ньому процедури нападу, яку можна визначити як процедуру *порушення цілісності обчислювального середовища,* оскільки об'єктом нападу РПЗ завжди є елементом цього середовища.

Під *обчислювальним середовищем розуміють* сукупність установлених для такої ІС алгоритмів використання системних ресурсів, програмного та інформаційного забезпечення, яка потенційно може бути надана користувачеві для розв'язання прикладних задач.

Частину обчислювального середовища, надану користувачеві для вирішення конкретної задачі, називають *операційним середовищем.*

Для опису основних класів РПЗ застосовують концептуальну модель, яка передбачає наявність у їх складі такого набору функцій:

захоплення управління;

самовідтворення;

самомодифікація;

маскування.

9.4. Комп'ютерні віруси

Під *комп'ютерним вірусом* розуміють РПЗ, що функціоную автономно та має здатність до самостійного впровадження в тіла інших програм із подальшим самовідтворенням і само розповсюдженням в ІС та окремих комп'ютерах.

Достатньою умовою для віднесення РПЗ до класу вірусів є наявність у його складі процедури відтворення.

Троянські програми не здатні до самовідтворення, маскуються під широко відомі програми масового застосування й містять приховані фрагменти, що виконують шкідливі дії.

Стадії життєвого циклу комп'ютерного вірусу:

латентна стадія, на якій вірус жодних дій не здійснює;

інкубаційна стадія, на якій основна задача вірусу – це створення якомога більше своїх копій;

активна стадія, на якій вірус, продовжуючи розмноження, проявляється й виконує свої деструктивні дії.

Початок активної стадії зумовлений:

настанням певної дати;

запуском програми;

відкриванням документа тощо.

Структурно вірус складається з голови й хвоста.

Головою вірусу називають його частину, що отримує управління, *хвостом* – частину, розташовану в тексті інфікованої програми окремо від голови.

Віруси, що складаються з однієї голови, називаються *несегментованими,* а віруси, що містять голову і хвіст – *сегментованими.*

Інфіковану вірусом програму називають *вірусоносієм*.

За *режимом функціонування* розрізняють:

резидентні віруси – віруси, які після активізації постійно знаходяться в оперативній пам'яті до моменту вимкнення або перезавантаження комп'ютера і контролюють доступ до його ресурсів;

нерезидентні віруси – віруси ,які не інфікують пам'ять комп'ютера і є активними протягом обмеженого проміжку часу.

За *об'єктом впровадження* бувають:

файлові віруси – віруси, що інфікують файли із програми;

завантажувальні віруси – віруси, що інфікують програми, які зберігаються в системних областях дисків, наприклад, у завантажувальному секторі системного диска;

файлово-завантажувальні віруси інфікують як файли, так і завантажувальні сектори дисків;

мережеві віруси – поширюються в інформаційних мережах, використовуючи для свого розповсюдження команди, протоколи й програмне забезпечення таких мереж (електронної пошти).

Файлові віруси поділяються на віруси, що інфікують:

виконувані файли;

командні файли й файли конфігурації;

файли, створені макромовами програмування, або файли, що можуть містити макрокоманди;

файли із драйверами пристроїв;

файли з бібліотеками вихідних, об1єктних, завантажувальних і оверлейних модулів, бібліотеками динамічного компонування;

Завантажувальні віруси поділяються на віруси, що інфікують:

системний завантажувач, розташований у завантажувальному секторі дискет і логічних дисків;

позасистемний завантажувач, розташований у завантажувальному секторі жорстких дисків.

Серед мережевих вірусів виділяють клас вірусів-самореплікаторів – мережевих хробаків (мережевих черв'яків), які не інфікують ПЗ безпосередньо ,а поширюють свої копії інформаційними системами із метою проникнення на комп'ютер-жертву, запуску своєї копії на комп'ютері й подальшого розповсюдження, завдаючи шкоди завдяки споживанню пропускної здатності або, видаленню файлів чи надсиланню документів електронною поштою.

Мережеві хробаки використовуються для транспортування інших шкідливих РПЗ до вузлів мережі. До таких РПЗ належать *логічні бомби* – програми, які запускаються за певних часових чи інформаційних умов для

здійснення шкідливих дій, спрямованих на порушення цілісності, конфіденційності та доступності інформації.

За ступенем і способом маскування комп'ютерні віруси поділяються на:

віруси, що не використовують засобів маскування;

стелс-віруси (віруси-невидимки) – віруси,що намагаються бути невидимими на основі контролю доступу до інфікованих елементів, приховуючи себе за спроби виявлення;

віруси-мутанти – віруси, що містять алгоритми шифрування, які забезпечують відмінність зашифрованих копій вірусу, чим унеможливлюють пошук вірусів за сигнатурами – характерними послідовностями байтів у фрагментах коду вірусів. Структурно вірус-мутант складається із зашифрованого тіла та шифрувальної частини.

Серед вірусів мутантів вирізняють:

звичайні віруси-мутанти;

поліморфні віруси.

Здійснення вірусами цільових функцій спричиняє ефекти, які поділяють на групи:

порушення цілісності файлової системи або окремих файлів;

ініціалізація помилок у системному або прикладному ПЗ;

імітація збоїв апаратних засобів;

створення візуальних і звукових ефектів.

Основними ознаками прояву функціонування вірусів є:

непередбачувана втрата працездатності комп'ютера або його компонентів;

неможливість завантаження операційної системи;

часті зависання та збої комп'ютера;

непередбачуване сповільнення роботи комп'ютера;

суттєве зменшення обсягу доступної вільної оперативної пам'яті;

порушення цілісності даних у CMOS пам'яті комп'ютера;

непередбачуване форматування логічних та фізичних дисків;

порушення цілісності файлів, каталогів чи файлової системи загалом;

непередбачуване збільшення кількості файлів;

непередбачувана зміна атрибутів файлів, дати й часу ї модифікації;

порушення працездатності прикладних програм;

непередбачуване зниження пропускної здатності каналів зв'язку в ІС;

поява непередбачуваних повідомлень, зображень та звукових сигналів, що можуть ввести користувача в оману або утруднити його роботу.

9.5. Алгоритмічні і програмні закладки

Під *алгоритмічною закладкою* розуміють навмисну, приховану зміну частини алгоритму програми або побудови так, що в результаті програмного здійснення цього алгоритму за певних умов проходження обчислювального процесу можлива поява нових або змінювання вже передбачених специфікацією ПЗ функцій.

Під *програмною закладкою* розуміють навмисно, приховано привнесенні в програмне забезпечення функцій ні об'єкти, які при певних умовах протікання обчислювального процесу ініціюють виконання непередбачених специфікацією ПЗ функцій.

Дії алгоритмічних та програмних закладок на інформацію, що обробляється в ІС, поділяють на три класи:

зміна функціонування ІС;

несанкціоноване читання інформації;

несанкціоноване змінювання інформації (як даних, так і ПЗ), аж до її знищення.

зміна функціонування ІС супроводжують такі прояви:

зменшення швидкості роботи ІС;

імітація апаратних збої;

часткове або повне блокування роботи ІС;

обхід криптографічних програмно-апаратних засобів захисту;

переадресація повідомлень;

забезпечення доступу в систему з несанкціонованих периферійних пристроїв.

Другий клас дій полягає у:

перехопленні паролів та їх обожненні з користувачами;

підміні паролів;

отримання секретної інформації;

ідентифікація інформації користувачів;

контролі активності користувачів ІС для отримання непрямих даних про їх взаємодію й характер інформації, якою вони обмінюються.

Несанкціоноване змінювання інформації є найнебезпечнішим різновидом дії алгоритмічних і програмних закладок. У цьому класі дій виокремлюють:

внесення прихованих змін до інформаційних масивів;

руйнування даних і кодів ПЗ;

упровадження програмних закладок в інше ПЗ;

змінювання пакетів повідомлень.

Програмні закладки можуть бути впроваджені в ПЗ на різних етапах його життєвого циклу. Відповідно поділяються на дві категорії:

апріорні (природжені);

апостеріорні.

Апріорні закладки вносяться на етапі розроблення ПЗ, тому вони стосуються питань забезпечення технологічної безпеки.

Апостеріорні закладки – на етапах випробування, експлуатації або модернізації ПЗ, тому стосуються забезпечення експлуатаційної безпеки ПЗ.

Дія програмної закладки, привнесеної до ПЗ на технологічній частині його життєвого циклю, практично не відрізняється від дії програмної закладки, впровадженої до ПЗ на експлуатаційній частині.