Якименко І.З.

Конспект лекцій з дисципліни

Цифрова криміналістика

Тернопіль - 2019

Лекція 1.
Концептуальні засади забезпечення інформаційної безпеки України

Рівень розвитку та безпека інформаційного середовища, які є одними з найвагоміших факторів у всіх сферах національної безпеки, активно впливають на стан політичної, економічної та інших складових національної безпеки України. У зв'язку з цим доцільно розглядати інформаційну безпеку як складову інших сфер національної безпеки. Разом з цим, інформаційна безпека є самостійною складовою національної безпеки і в цьому проявляється її подвійний характер.

Інформаційні простір, ресурси, інфраструктура та технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного й культурного розвитку. Необхідний рівень інформаційної безпеки держави забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть завдати збитків чи зашкодити реалізації інформаційних прав, потреб та інтересів країни і її громадян.

Діяльність із забезпечення інформаційної безпеки має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства та людини за трьома головними напрямами:

- • інформаційно-психологічному, зокрема щодо забезпечення конституційних прав і свобод людини й громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі для утвердження загальнолюдських та національних моральних цінностей;
- • технологічного розвитку, зокрема стосовно розбудови та інноваційного оновлення національних інформаційних ресурсів, упровадження новітніх технологій створення, оброблення та поширення інформації;
- • захисту інформації, зокрема щодо забезпечення її конфіденційності, цілісності й доступності, в тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак.

Таким чином, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

Для ефективного забезпечення інформаційної безпеки необхідна підготовка відповідних висококваліфікованих фахівців. Тому видання підручника "Забезпечення інформаційної безпеки держави" є вкрай актуальним.

КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Для визначення "*інформаційної безпеки"* необхідно розглянути поняття "*безпека*" та пов'язані з ним поняття "*небезпека", "загроза", "ризик", "виклик".*

Слід зазначити, шо природні явища "безпека" і "небезпека" існують в діалектичній взаємозалежності, тобто у природі не існує окремо "стану безпеки" та "стану небезпеки". Відповідно до філософського закону "боротьби протилежностей" ми спостерігаємо, відчуваємо і усвідомлюємо певні тенденції

розвитку станів "більш безпечних" чи "більш небезпечних". Це відбувається у залежності від того, які чинники (позитивні чи негативні) домінують у природі чи суспільстві на певний визначений момент розвитку людини, національного суспільства, держави та світового співтовариства. Саме з цієї причини знайти сприятливий "стан захищеності" на тривалий проміжок часу, сховатися від небезпеки, ризику, виклику чи загрози не можливо. Система безпеки, зорієнтована лише на захисні заходи, спрямовані на створення відносного стану безпеки, тобто на створення умов відсутності чинників "небезпек – загроз" є недосяжною ідеєю.

Визначення класифікаційних критеріїв ієрархії різних рівнів небезпеки потребує особливого підходу. Варто зазначити, що є різні рівні реальності виникнення і об'єму реалізації несприятливих наслідків для безпеки об'єкту захисту або завдання йому відповідного збитку чи шкоди. Звідси встановлено чотири рівні виміру *(класифікація)*показників відхилення від нормативних вимог до стану безпеки, а саме: *виклик, ризик, загроза* та *небезпека.*

Виклик – безпосередня мінімальна протидія носієм небезпеки та/або актуалізація функціонування в обмежених масштабах інших чинників протидії (тобто завершення заходів підготовчої стадії, початок матеріалізації ризику) реалізації національних (чи корпоративних) цінностей, потреб, інтересів і цілей, вирішенню завдань забезпечення національної (чи корпоративної) безпеки, котрі виявляються у формі офіційних і неофіційних політико-дипломатичних дій джерела небезпеки, торгівельно-економічної, інформаційно-психологічної експансії тощо. Створення обмежених за масштабами несприятливих умов або завдання несуттєвого збитку чи шкоди об'єкту захисту, або погроза та демонстрація погрози завдання шкоди чи збитку.

Ризик – реальне існування можливості виникнення ситуації, за якою формуються передумови протидії реалізації національних (чи корпоративних) цінностей, потреб, інтересів і цілей забезпечення національної (чи корпоративної) безпеки в обмежених масштабах. Наявність носія та інших чинників посилення передумов матеріалізації небезпеки, природна можливість використання носієм небезпеки існуючих природних або створення штучних чинників виникнення несприятливих передумов чи безпосереднього завдання збитку або шкоди важливим національним (чи корпоративним) інтересам і національній (або корпоративній) безпеці.

Загроза – реальність виникнення суттєвого збитку, шкоди або інших негативних наслідків для життєво важливих національних (чи корпоративних) цінностей, потреб, інтересів і національній (чи корпоративній) безпеці, яка виходить за локальні межі та стосується основних національних (чи корпоративних) цінностей (суверенітету, державності, територіальної цілісності тощо).

Небезпека – віртуальне чи природне існування або потенційна можливість виникнення несприятливих передумов чи безпосереднього завдання шкоди важливим національним (чи корпоративним) інтересам і національній (чи корпоративній) безпеці.

Зазначені критерії класифікації рівнів системи "безпеки – небезпеки" можна застосовувати й до теорії інформаційної безпеки. При цьому поняття "загроза" щодо поняття "небезпека" має залежне значення. "Загроза" – це

кінцева стадія розвитку несприятливих умов, після яких спричиняється шкода, тобто висхідна тенденція небезпечного розвитку знаменується закінченням процесу розвитку якостей і потенціалу небезпеки, вона добігає свого апогею. Після цього – або настає шкода чи збиток, або за певних умов послаблення впливу несприятливих чинників – знову загрозлива ситуація переходить до рівня виклику чи ризику.

Відповідно до Закону України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" *інформаційна безпека* – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання, порушення цілісності, конфіденційності та доступності інформації.

Варто зазначити, що це визначення сформульовано не за суттєвими ознаками й тому воно громіздке. У ньому присутня лише пасивна складова – "ступінь захищеності", але відсутня активна складова – "інформаційний розвиток" (технічний, інтелектуальний, соціально-політичний, морально-етичний).

Багатоаспектність проявів інформаційної складової у різних сферах життєдіяльності зумовлює доцільність класифікації видів інформаційної безпеки за різними системоутворювальними ознаками.

Так, поклавши в основу класифікації об'єкти національної безпеки (людина і громадянин, суспільство, держава) варто розрізняти визначення *"інформаційна безпека", "інформаційна безпека особи", "інформаційна безпека суспільства", "інформаційна безпека держави"*.

Інформаційна безпека (ІБ) – стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди.

Інформаційна безпека особи – це стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, що призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану.

Інформаційна безпека суспільства – можливість безперешкодної реалізації суспільством й окремими його членами своїх конституційних прав, пов'язаних із вільним одержанням, обробленням, створенням і поширенням інформації, а також ступінь їх захисту від деструктивного інформаційного впливу.

Варто відмітити, що ІБ особи та суспільства тісно пов'язані між собою. Інформаційна безпека суспільства та окремих осіб *залежить від рівня:*

- • інтелектуальності, спеціальної теоретичної й практичної підготовки;
- • критичного мислення, морального та духовного вдосконалення;
- • гармонійного розвитку особистості в суспільстві;
- • технічних засобів захисту.

Інформаційна безпека держави – це стан її захищеності та інформаційного розвитку, при якому акції інформаційного впливу, спеціальні

інформаційні операції, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів та комп'ютерна злочинність не завдають суттєвої шкоди національним інтересам.

Акція інформаційного впливу (АІВ) – одноразова дія інформаційно-психологічного та/або інформаційно-технічного впливу, яка передбачає спланований вплив на свідомість і поведінку людей шляхом поширення упередженої, неповної чи недостовірної інформації та/або на інформаційно-технічну інфраструктуру об'єкта (об'єктів) шляхом втручання в процес функціонування його інформаційних, телекомунікаційних або інформаційно-телекомунікаційних систем.

Спеціальна інформаційна операція (СІО) – це сукупність спланованих, узгоджених та взаємопов'язаних за метою, завданнями, об'єктами і часом заходів, спрямованих на ворожу, дружню або нейтральну аудиторію з метою схилення до прийняття управлінських рішень та/або вчинення АІВ, вигідних для суб'єкта інформаційного впливу. СІО можуть передбачати також вплив на інформаційно-технічну інфраструктуру, але для більш ефективного впливу направлені на свідомість і поведінку людей Слід зауважити, що СІО складається з поєднаних між собою АІВ за часом, метою, завданнями, силами й засобами проведення.

Інформаційний тероризм – небезпечні діяння з інформаційного впливу на соціальні групи й окремих осіб, державні органи влади та управління, пов'язані з поширенням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникнення кризових ситуацій у державі, нагнітання страху й напруження в суспільстві.

Комп'ютерна злочинність – це відносно масове соціальне явище, яке полягає в суспільно небезпечних діяннях, коли електронно-обчислювальні машини, мережі, системи та представлена в них інформація є знаряддям або предметом злочинних діянь.

Роль та місце інформаційної безпеки в системі національної безпеки нашої держави визначаються відповідно до Закону України "Про основи національної безпеки України" (Рис. 1).

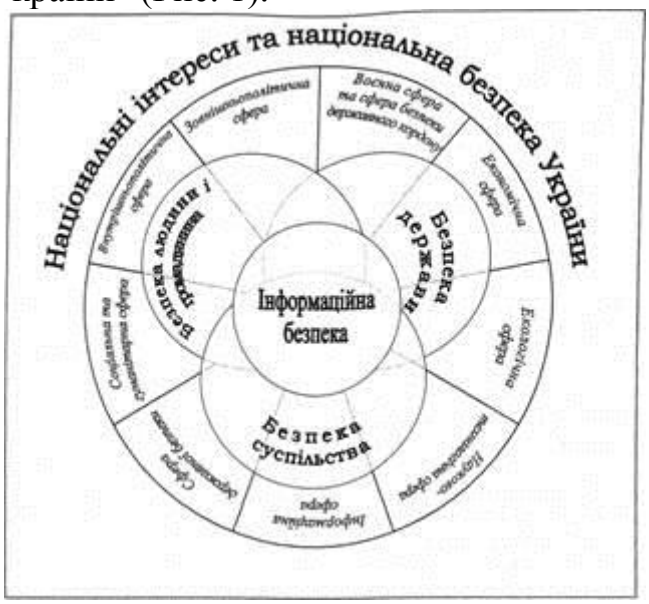


Рис. 1. Місце інформаційної безпеки в системі національної безпеки України

Інформаційна безпека є невід'ємною складовою національної безпеки у всіх без виключення сферах життєдіяльності особи, суспільства та держави, оскільки безпосередньо впливає на стан їх захищеності та розвитку:

- *– у зовнішньополітичній сфері* – інформаційний супровід державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном визначає статус України у міждержавних відносинах; захищеність від зовнішніх інформаційних впливів забезпечує інформаційний суверенітет суспільства і держави, сприяє виваженому прийняттю рішень на основі достовірної та повної інформації; організаційно-технічна, інформаційна та ресурсна підтримка державою вітчизняних засобів масової інформації, сприяє формуванню позитивного іміджу України;
- *– у сфері державної безпеки* – своєчасне та достовірне інформування органів державної влади про поточну ситуацію в державі дозволяє приймати ефективні рішення; недопущення розголошення інформації, що містить державну таємницю, забезпечує переваги у міждержавних відносинах, в тому числі у матеріальному вимірі; протидія використанню сучасних інформаційних технологій на шкоду безпеці України дозволяє запобігати деструктивним інформаційним впливам, сприяє антитерористичній діяльності; захист конституційних прав і свобод людини на доступ до інформації шляхом залучення засобів масової інформації до забезпечення неухильного додержання захисту конституційного устрою сприяє збереженню територіальної цілісності держави;
- *– у воєнній сфері* – застосування засобів, форм та способів інформаційної боротьби є ефективним засобом стратегічного протистояння в регіональних збройних конфліктах; своєчасна поінформованість військовослужбовця, військових підрозділів про оперативну обстановку, застосування сучасних інформаційно-телекомунікаційних технологій в управлінні військами і зброєю надає переваги перед супротивником; удосконалення форм і способів протидії інформаційно-психологічним операціям дозволяє посилити обороноздатність держави;
- *– у внутрішньополітичній сфері* – від фактичного стану реалізації прав доступу громадян до інформації залежать результати проведення виборчих кампаній, а відтак і ефективність взаємодії держави та суспільства; громадський контроль за діяльністю органів державної влади через засоби масової інформації забезпечує підвищення ефективності їх функціонування; протидія поширенню інформації, спрямованої на розпалення міжетнічних і міжконфесійних конфліктів, сприяє стабільності у суспільстві;
- *– в економічній сфері* – забезпечення захисту інформаційних ресурсів та комунікативних каналів від конкурентної розвідки є на сьогодні передумовою успішності будь-якого бізнесу; підтримка вітчизняних виробників високотехнологічної продукції, формування вітчизняної індустрії інформаційних послуг, комплексна інформатизація виробничих процесів сприяє розвитку промисловості; додержання вимог інформаційної безпеки в

системах збирання, обробки, зберігання і передачі статистичної, фінансової, біржової, податкової та митної інформації забезпечує конкурентні переваги;

- *– у соціальній та гуманітарній сферах* – якість інформаційних продуктів, зокрема освітніх, впливає на формування національної самосвідомості, розвиток і примноження духовних цінностей суспільства; запобігання монополізації вітчизняного інформаційного простору унеможливлює маніпулювання суспільною свідомістю;
- *– у науково-технологічній сфері* – захищеність прав інтелектуальної власності сприяє збереженню науково-технологічного потенціалу держави; застосування сучасних інформаційних технологій впливає на розвиток внутрішнього ринку високотехнологічної продукції; розвиненість високотехнологічного виробництва забезпечує технологічну конкурентоспроможність України у сфері інформатизації та зв'язку; доступ громадян до світового інформаційного простору, зокрема до наукової та науково-технічної інформації, створює умови для розвитку науки, наукоємних галузей;
- *– в екологічній сфері* – стабільність роботи та цілісність інформаційно-телекомунікаційних систем на об'єктах життєзабезпечення є запорукою уникнення надзвичайних ситуацій техногенного характеру; застосування сучасних аерокосмічних, комп'ютерно-телекомунікаційних та геоінформаційних засобів і технологій для комплексного моніторингу дозволяє своєчасно реагувати на надзвичайні ситуації;
- *– в інформаційній сфері* – розвиток системи незалежних вітчизняних засобів масової комунікації сприяє забезпеченню свободи слова, гармонійному розвитку особистості, досягненню індивідуального інформаційного суверенітету, унеможливлює маніпулювання суспільною свідомістю; популяризація української мови забезпечує формування національної самосвідомості; розвиток вітчизняної телекомунікаційної галузі забезпечує вільне спілкування, доступ громадян до інформації; використання провідних технологій зберігання та захисту інформації дозволяє запобігти комп'ютерним злочинам тощо.

В процесі забезпечення інформаційної безпеки ***об'єктами захисту*** є:

- • *інформація* (особиста, конфіденційна, власність держави, з обмеженим доступом);
- • *інформаційно-телекомунікаційна інфраструктура* (суб'єкти та засоби створення, поширення інформації та передавання даних);
- • *свідомість* (особи, групи осіб, суспільства).

Для організації протидії загрозам ІБ необхідно знати чинники, які сприяють виникненню ризиків, загроз і небезпек в ідеологічно-інформаційній сфері держави, з'ясувати їх сутність, уміти оцінювати та визначати ймовірність і рівень негативного впливу на суспільство й державу.

Основними реальними та потенційними ***загрозами інформаційній безпеці України*** є:

- 1) *у зовнішньополітичній сфері*:
  - • поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;

- • прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують стабільному та безпечному функціонуванню національних інформаційно-телекомунікаційних систем;
- • зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також інтернет;

- 2) *у сфері державної безпеки*:
  - • негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканності кордонів України;
  - • використання засобів масової інформації, інтернету для пропаганди сепаратизму за етнічною, мовною, релігійною й іншими ознаками;
  - • несанкціонований доступ до інформаційних ресурсів органів державної влади;
  - • розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;
- 3*) у воєнній сфері*:
  - • порушення встановленого регламенту збирання, оброблення, зберігання й передання інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;
  - • несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;
  - • реалізація програмно-математичних заходів із метою порушення функціонування інформаційних систем у сфері оборони України;
  - • перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління;
  - • інформаційно-психологічний вплив;
  - • на населення України, у тому числі особовий склад військових формувань, із метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;
- 4) *у внутрішньополітичній сфері*:
  - • недостатня розвиненість інститутів громадянського суспільства, недосконаліть партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;
  - • негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість;
  - • поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;
- 5) *в економічній сфері*:
  - • відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій;
  - • недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель;

- • несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах;
- • використання неліцензованого й несертифікованого програмного забезпечення, засобів і комплексів оброблення інформації;
- • недостатній рівень розвитку національної інформаційної інфраструктури;

- 6) *у соціальній та гуманітарній сферах*:
  - • відставання України від розвинутих держав за рівнем інформатизації

соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури;

- • недодержання прав людини і громадянина на отримання інформації, необхідної для захисту їх соціально-економічних прав;
- • поширення в засобах масової інформації не властивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської й національної гідності;
- • тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля;
- • послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства;
- • відставання розвитку українського кінематографу, книговидання, книгорозповсюдження й бібліотечної справи від рівня розвинутих держав;
- 7*) у науково-технологічній сфері*:
  - • зниження наукового потенціалу в галузі інформатизації та зв'язку;
  - • низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку;
  - • відтік за кордон наукових кадрів та суб'єктів права інтелектуальної власності;
  - • недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій і техніки;
  - • неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залежності України;
- 8) *в екологічній сфері*:
  - • приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру;
  - • недостатня надійність інформаційно-телекомунікаційних систем збирання, оброблення й передання інформації в умовах надзвичайних ситуацій;
  - • низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування й реагування на надзвичайні ситуації.

Життєво важливі інтереси в інформаційній сфері:

- 1) *особи*:
  - – забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

- – недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних;
- – захищеність від негативного інформаційно-психологічного впливу;

• 2) *суспільства*:

- – збереження і примноження духовних, культурних і моральних цінностей українського народу;
- – забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; формування і розвиток демократичних інститутів громадянського суспільства;

• 3) *держави*:

- – недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур;
- – ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері;
- – побудова та розвиток інформаційного суспільства;
- – забезпечення економічного та науково-технологічного розвитку України;
- – формування позитивного іміджу України;
- – інтеграція України у світовий інформаційний простір.

Для визначення "забезпечення інформаційної безпеки" необхідно дати визначення "забезпечення" і понять, які з ним пов'язані, а саме "потреби" та "інтереси".

Забезпечення *– у загальному значенні* – може тлумачитися як задоволення певних потреб та інтересів суб'єкта діяльності, тобто надання необхідних для його існування і розвитку ресурсів, створення відповідних умов надійного функціонування механізмів, відповідальних за підтримання його життєздатності; *– у професійному значенні* – це усіляка допоміжна діяльність, котра сприяє найбільш ефективному вирішенню покладених на політичні, правоохоронні, оборонні органи та спецслужби завдань, зокрема у сфері управління: кадрові, інформаційні, матеріально-технічні, фінансові тощо задоволення потреб керівних і виконавчих структур.

Потреби – це відповідна енергія, живильна сировина, що спричиняє внутрішні процеси, взаємодію останніх із зовнішнім середовищем, взаємне проникнення: внутрішньої енергії до зовнішнього середовища, зовнішньої енергії до внутрішнього середовища суб'єкта, а також взаємний позитивний чи негативний вплив, і таким чином стимулює живильну силу і підтримує життєздатність суб'єкта. Зазначені потреби (ресурси) можуть бути природного походження або штучного походження. Часто у неживому або тваринному світі зазначені потреби мало усвідомлюються і забезпечуються суб'єктом на рівні природних інстинктів самозбереження.

Інтереси – це усвідомлені суб'єктом потреби, характерні лише людині як живій істоті, яка має свідомість і здатна навіть без наявності відповідних біологічних сигналів усвідомлювати відповідні потреби заздалегідь. Людина

намагається створити необхідні умови для того, щоб, коли надійде відповідний біологічний імпульс потреби, задовольнити її.

Потреби та інтереси можуть бути у вигляді певних ресурсів: продовольчих, фінансових, технологічних, інформаційних, матеріально-технічних, сировинних, фахово-трудових, психологічних тощо.

Забезпечення інформаційної безпеки можна визначити як комплекс заходів необхідний для досягнення такого стану інформаційного розвитку (духовного, соціально-політичного, технічного) та захищеності особи, суспільства, держави, за якого сторонні інформаційні впливи не завдають суттєвої шкоди національним інтересам.

У свою чергу, під досягненням означеного стану ІБ розуміється певна діяльність, яку здійснюють суб'єкти ЗІБ щодо об'єктів ЗІБ. Ключовим об'єктом забезпечення ІБ є інформація (інформаційні ресурси). Саме інформація є предметом тих відносин, які виникають у зв'язку з необхідністю її збереження та обміну, що зумовлює доцільність захисту інформаційно-телекомунікаційної структури (телекомунікаційних мереж, програмно-апаратних засобів) та інформаційного простору (суб'єктів інформаційних відносин) в процесі ЗІБ.

Варто звернути увагу, що об'єкти ЗІБ можуть бути як об'єктами захисту, так і засобами проведення заходів, що впливають на стан ІБ. Наприклад, інформація з обмеженим доступом підлягає захисту, в той же час спеціально підібрана інформація, що розповсюджується системно на деяку цільову аудиторію є засобом впливу на свідомість. Таким чином, інформація виступає об'єктом захисту в одних випадках і засобом при здійсненні правопорушення в інших. Веб-сервер Верховної Ради України має бути захищеним, адже від цілісності, конфіденційності і доступності інформації на ньому залежить функціонування правової системи в державі, з іншої сторони – існують веб-сервери, які використовуються з метою розповсюдження інформації з обмеженим доступом. Таким чином, веб-сервер є об'єктом захисту у першому випадку та засобом для здійснення злочину в другому.

Особливістю об'єктів ЗІБ є також можливість набуття ними різних форм – у фізичному середовищі (мережі, системи обробки інформації, матеріальні носії інформації) та інформаційному (змістовне наповнення). Цей особливий симбіоз форм вияву об'єктів інформаційної сфери можна продемонструвати на прикладі глобальної мережі Інтернет: фізичне середовище передачі даних (об'єднання телекомунікаційних мереж різної архітектури) є безмежним інформаційним сховищем, призначеним для зберігання та обміну інформацією. Відповідно можна говорити про безпеку функціонування фізичної складової інформаційної сфери та безпеку (цілісність, конфіденційність, доступність) інформаційної складової.

Основу системи ЗІБ України складають відповідні органи та сили, які вживають адміністративно-правових, інформаційно-аналітичних, організаційно- управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління в інформаційній сфері.

Відповідно *систему суб'єктів ЗІБ* можна визначити як організовану державою сукупність суб'єктів державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо

захисту національних інтересів в інформаційній сфері, що здійснюють узгоджену діяльність у межах законодавства України.

Забезпечення інформаційної безпеки України має здійснюватися за такими принципами:

- • свобода збирання, зберігання, використання та поширення інформації;
- • достовірність, повнота та неупередженість інформації;
- • обмеження доступу до інформації виключно на підставі закону;
- • гармонізація особистих, суспільних і державних інтересів;
- • запобігання правопорушенням в інформаційній сфері;
- • економічна доцільність;
- • гармонізація українського законодавства в інформаційній сфері з міжнародним;
- • пріоритетність національної інформаційної продукції.

У зв'язку з тим, що стан захищеності об'єкта від інформаційних впливів тісно пов'язаний зі станом його інформаційного розвитку, то поняття "Забезпечення 1Б" можна також визначити як забезпечення інформаційного розвитку (технічного, інтелектуального, соціально-політичного, морально-етичного), за якого сторонні інформаційні впливи не завдають суттєвої шкоди національним інтересам. Зазначені визначення дають підстави виділити два аспекти забезпечення ІБ – активний і пасивний (табл. 1).

Таблиця 1– Система функцій ЗІБ

	активна складова (розвиток)	Пасивна складова (захист)
Фізичний рівень	розвиток потужної інформаційно-телекомунікаційної інфраструктури; підтримка діяльності вітчизняних засобів масової інформації; розвитку видавничої справи, кінематографу; побудова мережі корпунктів за кордоном.	захист інформаційно-телекомунікаційної інфраструктури від монополізації, використання з розвідувальною чи іншою метою, що становить загрозу національній безпеці; ○ – захист інформації (на матеріальних носіях, в мережах) від несанкціонованого доступу, модифікації, блокування; ○ – захист інформації з обмеженим доступом
Інформаційний рівень	інформаційна підтримка геополітичних позицій держави, що відповідають	захист свідомості особи, групи осіб, суспільства; захист інтелектуальної власності.

	національним інтересам; формування позитивного міжнародного іміджу держави; ○ – створення власного конкурентного інформаційного продукту; ○ – забезпечення свободи слова та доступу громадян до інформації; реалізація права на повноту і достовірність інформації; патріотичне виховання громадян.	

Відтак "забезпечення інформаційної безпеки" як **активна функція** загальнодержавної системи ЗІБ включає:

- • *на фізичному рівні* – розвиток потужної інформаційно-телекомунікаційної інфраструктури, підтримка діяльності вітчизняних ЗМІ, розвитку видавничої справи, кінематографу, побудова мережі корпунктів за кордоном;
- • *на інформаційному рівні* – інформаційна підтримка геополітичних позицій держави, що відповідають національним інтересам, формування позитивного міжнародного іміджу держави, створення власного конкурентного інформаційного продукту, забезпечення свободи слова та доступу громадян до інформації, реалізація права на повноту і достовірність інформації, патріотичне виховання громадян.

Пасивна функція (захист) передбачає:

- • *на фізичному рівні* – захист інформаційно-телекомунікаційної інфраструктури від монополізації, використання з розвідувальною чи іншою метою, що становить загрозу національній безпеці, захист інформації (на матеріальних носіях, в мережах) від несанкціонованого доступу, модифікації, блокування, захист інформації з обмеженим доступом;
- • *на інформаційному рівні* – захист свідомості особи, групи осіб, суспільства, захист інтелектуальної власності.

Система ЗІБ передбачає формування відповідної системи протидії зазначеним вище загрозам. У загальному випадку можна виділити чотири основні складові цієї системи: нормативно-правову, організаційну, технологічну та кадрову.

Нормативно-правова складова повинна забезпечувати формування й удосконалення системи правових норм протидії загрозам ІБ та механізмів їх реалізації. Вона утворюється сукупністю нормативних правових актів, інших

нормативних документів, які регулюють відносини у сфері виявлення загроз безпеці індивідуальної, групової та масової свідомості громадян і протидії цим загрозам, що забезпечує реалізацію конституційних прав та свобод, їх законних обмежень, охорону психічного здоров'я громадян, збереження соціального спокою в суспільстві.

Організаційна складова системи ЗІБ має установлювати функціональну структуру громадських організацій і державних органів, що займаються реалізацією правових норм у цій сфері, й відносини між ними, а також між цими організаціями й органами, з одного боку, та громадянами – з іншого. При цьому найважливішою частиною організаційної складової системи мають бути відповідні структури громадянського суспільства.

Організаційна складова є важливою частиною загальної системи ЗІБ, конфігурація якої має бути позначена в Доктрині інформаційної безпеки країни. Система ЗІБ повинна будуватися на основі тісної взаємодії глави держави, органів законодавчої, виконавчої й судової влади, а також громадських організацій, що займаються установленою законом діяльністю в цій сфері.

Технологічна складова цієї системи повинна забезпечувати можливість вільного та безпечного інформаційного обміну між громадянами, членами груп, групових асоціацій і запобігання протиправному інформаційному впливу на них; своєчасне виявлення загроз інформаційній безпеці особи, суспільства та держави, оцінку можливого й завданого збитку цій безпеці та організацію ефективної протидії таким загрозам.

Кадрова складова має забезпечити формування й підтримання кадрового потенціалу суспільства та держави, необхідного для ефективного функціонування системи ЗІБ.

Варто виділити також найважливіші питання інформаційно-психологічної безпеки держави, які потребують нагального вирішення:

По-перше, розроблення основ державної політики в цій сфері, що зумовлено специфічністю об'єкта й предмета забезпечення безпеки. Суспільні стосунки, які виникають при створенні умов для формування й розвитку духовної сфери суспільства та забезпечення безпеки цих процесів, значною мірою повинні регулюватися суспільством самостійно шляхом установлення та підтримання критеріїв моральності, допустимих стереотипів поведінки громадян і механізмів суспільного впливу на порушників установлених правил. Держава за допомогою цивільного права повинна забезпечити запобігання найбільш суспільно небезпечним діянням у цій царині. Помилки в розмежуванні цих груп стосунків призводять як до недостатньої ефективності правового захисту особистості, суспільства і держави, дискредитації влади, так і до відсутності належної уваги до створення суспільних інститутів, необхідних для вирішення проблеми.

По-друге, вдосконалення системи ЗМІ, що здійснює найсуттєвіший вплив на індивідуальну, групову та масову свідомість. З одного боку, відсутні досить ефективні механізми впливу суспільства на ЗМІ в інтересах захисту суспільної моральності, психічного здоров'я громадян, їхнього спокою, а з іншого – органи державної влади повільно проводять роботу з формування відкритих інформаційних ресурсів, що забезпечують громадянам можливість самостійного отримання достовірної та повної інформації про найбільш

важливі події суспільного життя, діяльність органів влади щодо протидії наявним загрозам.

По-третє, виникають значні труднощі при оцінюванні втрати психічного здоров'я громадян. Вони пов'язані з відсутністю достатнього технологічного інструментарію для вирішення цього завдання; необхідного методичного апарату визначення та фіксації характеристик психіки конкретної людини, динаміки їх зміни, виявлення причин виникнення негативних тенденцій. Це особливо важливо для проведення судових експертиз за фактами неправомірної дії на психічну сферу людини та створення комплексних методик і засобів підвищення стійкості психіки до негативних інформаційних впливів, у тому числі через канали масової інформації.

Окремим аспектом ІБ держави є створення системи підготовки кадрів для здійснення профілактичних робіт у цій сфері та проведенні експертиз і заходів щодо формування нормативного правового та технологічного забезпечення.

Держава з метою ЗІБ України має вживати таких заходів:

- 1) у зовнішньополітичній сфері:
  - • вдосконалення інформаційного супроводу державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном;
  - • організаційно-технічне, інформаційне й ресурсне сприяння держави вітчизняним засобам масової інформації, що формують у світовому інформаційному просторі позитивний імідж України;
  - • інтеграція до міжнародних інформаційно-телекомунікаційних систем та організацій на засадах рівноправності, економічної доцільності й збереження інформаційного суверенітету;
  - • гарантування своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та їх нейтралізації;
- 2) у сфері державної безпеки:
  - • залучення засобів масової інформації до забезпечення неухильного додержання конституційних прав і свобод людини й громадянина, захисту конституційного устрою, вдосконалення системи політичної влади з метою зміцнення демократії, духовних та моральних засад суспільства;
  - • підвищення ефективності функціонування органів державної влади;
  - • підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг;
  - • розвиток національної інформаційної інфраструктури на засадах стимулювання вітчизняних виробників і користувачів новітніми інформаційно-телекомунікаційними засобами й технологіями, комп'ютерними системами і мережами;
- 3) у воєнній сфері:
  - • проведення систематичного аналізу застосування засобів, форм та способів інформаційної боротьби у воєнній сфері, визначення напрямів ЗІБ держави;
  - • удосконалення законодавства з питань ІБ, координації діяльності органів державної влади та органів військового управління під час вирішення завдань ЗІБ;

- • удосконалення видів і засобів захисту інформації в інформаційно-телекомунікаційних мережах, що задіяні в управлінні військами та зброєю, від несанкціонованого доступу;
- • удосконалення форм і способів протидії акціям інформаційного впливу, спрямованим на послаблення обороноздатності держави;
- • підготовка спеціалістів з питань ІБ у воєнній галузі;
- 4) у внутрішньополітичній сфері:
- • створення дієвої та прозорої системи громадського контролю за діяльністю органів державної влади й місцевого самоврядування, громадсько-політичних структур, зокрема через створення системи Суспільного телебачення і радіомовлення України;
- • поліпшення взаємодії органів державної влади з громадськими організаціями у сфері боротьби з проявами обмеження конституційних прав і свобод людини й громадянина та маніпулювання масовою свідомістю;
- 5) в економічній сфері:
- • підтримання вітчизняних виробників високотехнологічної продукції, насамперед комп'ютерно-телекомунікаційних засобів і технологій;
- • формування вітчизняної індустрії інформаційних послуг, підвищення ефективності використання державних, корпоративних і приватних інформаційних ресурсів;
- • гармонізація законодавства України з питань ІБ в економічній сфері з міжнародними нормами й стандартами;
- • розроблення та вдосконалення методів і засобів захисту інформації;
- • забезпечення стабільного розвитку національного медіа-ринку під час впровадження в Україні цифрового телерадіомовлення;
- • посилення державного контролю за додержанням вимог ІБ в системах збирання, оброблення, зберігання й передання статистичної, фінансової, біржової, податкової та митної інформації;
- • комплексна інформатизація процесів формування, розподілення і контролю за використанням бюджетних коштів;
- • удосконалення системи статистичної звітності з метою підвищення оперативності, достовірності й релевантності звітної інформації;
- 6) у соціальній та гуманітарній сферах:
- • формування й реалізація державної політики національного духовного та культурного відродження, яка відповідає інтересам українського народу і визначає чіткі критерії та пріоритети формування інформаційної політики в соціальній сфері;
- • запобігання монополізації національного інформаційного простору;
- • вдосконалення законодавчого регулювання діяльності засобів масової інформації, зокрема з метою підтримання діяльності, спрямованої на формування оптимістичної морально-психологічної атмосфери в суспільстві, популяризації національних культурних цінностей, сприяння соціальній стабільності й злагоді;
- • державна підтримка вітчизняного виробника інформаційної продукції;

- 7) у науково-технологічній сфері:
  - • забезпечення технологічної конкурентоспроможності України у галузі інформатизації та зв'язку;
  - • розвиток міжнародного науково-технічного співробітництва в забезпеченні захисту інформації в міжнародних телекомунікаційних системах;
  - • удосконалення системи охорони та захисту права інтелектуальної власності;
  - • науково-технологічне супроводження формування й розвитку в Україні інформаційного суспільства з урахуванням вимог ЗІБ України;
  - • розширення можливостей доступу громадян до світового інформаційного простору, зокрема до наукової та науково-технічної інформації;
- 8) в екологічній сфері:
  - • проведення комплексного аналізу екологічного стану територій і їхнього виробничого потенціалу з метою вироблення інформаційної політики щодо упровадження концепції стабільного розвитку;
  - • застосування сучасних аерокосмічних, комп'ютерно-телекомунікаційних та геоінформаційних засобів і технологій для комплексного моніторингу, профілактики й своєчасного реагування на надзвичайні ситуації;
  - • створення бази даних екологічно безпечних технологій і продукції, їх розробників, виробників та постачальників, результатів маркетингових досліджень екологічного ринку;
  - • підвищення рівня інформатизації галузі страхування для акумулювання коштів на відшкодування збитків від надзвичайних ситуацій, а також на довгострокове інвестування заходів із мінімізації ризиків життєдіяльності й господарювання.

Діяльність із ЗІБ здійснюється за допомогою різних способів, засобів і прийомів, які у своїй органічній сукупності складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від тину діяльності, в якій вони використовуються, а також сфери застосування.

Важливими методами аналізу стану ЗІБ є методи опису та класифікації Для здійснення ефективного захисту системи державного управління слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу стану ЗІБ використовуються методи дослідження причинних зв'язків. За допомогою цих методів виявляються причинні зв'язки між загрозами, ризиками, викликами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод відмінності, метод сполучення схожості і відмінності, метод змін, що супроводжують, метод залишків.

Вибір методів аналізу стану ЗІБ залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо

диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери ІБ, то у ній, зазвичай, виділяють: фізичний, програмно- технічний, управлінський, технологічний, рівень користувача, мережевий та процедурний. Розглянемо детальніше кожний з цих рівнів.

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій. На програмно-технічному рівні здійснюється

ідентифікації і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи ЗІБ органів державного управління.

На технологічному рівні здійснюється реалізації політики ЗІБ за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на суб'єктів державного управління, унеможливлення інформаційного впливу з боку соціального середовища.

На мережевому рівні дана політика реалізується у форматі координації дій органів державного управління, які пов'язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання роботоздатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Варто згрупувати окремі методи ЗІБ у декілька *класів*:

- • *однорівневі методи* будуються на підставі одного принципу управління ІБ;
- • *багаторівневі методи* будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішення власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;
- • *комплексні методи* – багаторівневі технології, які об'єднані до єдиної системи координуючими функціями на організаційному рівні з метою ЗІБ виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;
- • *інтегровані високоінтелектуальні методи* – багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів із організаційним управлінням.

Загальні методи ЗІБ активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать: прийняття рішення з визначення області та контексту інформаційної загрози і складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній і соціальній сферах життєдіяльності; забезпечення адекватного сприйняття загрози та небезпеки у більш низьких організаційних ланках системи державного управління; виділення необхідних політичних,

економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи державного управління: трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

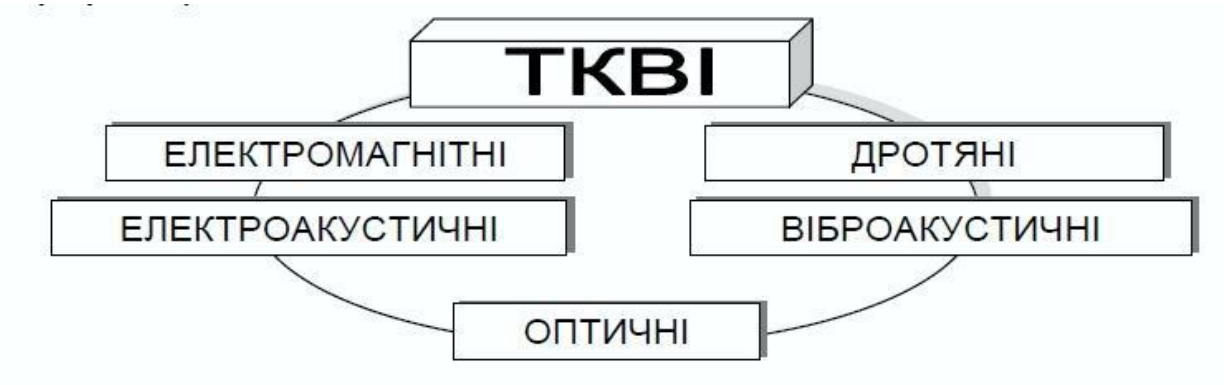
У цілому обрання цілей і методів протидії конкретним загрозам та небезпекам ІБ становить собою важливу проблему і складову частину діяльності з реалізації основних напрямів державної політики ЗІБ. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної впади, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності.

Лекція 2.
Технічні канали витоку інформації. Способи несанкціонованого зняття інформації

Для перехоплення, обробки та аналізу інформації за допомогою КВІ можуть використовуватися різноманітні технічні засоби (ТЗс), а також люди (порушники). Тоді існуючі КВІ залежно від джерел і одержувачів інформації утворюють чотири основних типи каналів: "людина – людина", "людина – ТЗс ", " ТЗс – ТЗс " і " ТЗс – людина".

Якщо інформаційний потік поширюється в напрямку від носія до одержувача, то утворюється *узагальнений канал витоку*, якщо ж інформаційний потік у вигляді явної або прихованої дії направлений за вищезгаданими чотирма типами каналів від порушника до носія інформації, то виникає так званий *узагальнений канал інформаційного впливу на носій інформації (канал спеціального впливу)*. Залежно від того, на який параметр носія інформації задумано здійснити вплив, порушником можуть бути застосовані психічні, фізичні, програмно-математичні, радіоелектронні та інші способи і засоби. Параметрами, на які задумано здійснити вплив, можуть бути різні характеристики матеріальних носіїв, у тому числі й власні характеристики головного прямого носія інформації – людини.

Найбільший потенціал інформативності мають КВІ, у яких для отримання 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.



Структура ТКВІ

При цьому процес передачі повідомлень розбивається на три основні етапи. На початку кожне повідомлення a(t) перетворюється передавачем у небезпечний (інформаційний) сигнал b(t). Небезпечний сигнал переміщується трактом 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 за 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 відповідно до наступного рисунку.

КласифікаціяТКВІ

Схема можливих каналів витоку і несанкціонованого доступу до ін

формації в типовому одноповерховому приміщенні показана на рисунку нижче

Можливі КВІ та НСД

На рисунку використанні наступні умовні позначеня:
1 – витік за рахунок структурного звуку в стінах і перекриттях;
2 – зняття інформації із стрічки принтера, погано стертих дискет і т. п.;
3 – зняття інформації з використанням відеозакладок;
4 – програмно-апаратні закладки в ПЕВМ;
5 – радіозакладки у стінах і меблях;
6 – зняття інформації із системи вентиляції;
7 – лазерне зняття акустичної інформації з вікон;
8 – виробничі й технологічні відходи;
9 – комп'ютерні віруси, логічні бомби і т. п.;
10 – зняття інформації шляхом наведень і "нав'язування";
11 – дистанційне зняття відеоінформації (оптика);
12 – зняття акустичної інформації з використанням диктофонів;
13 – крадіжка носіїв інформації;

14 – високочастотний канал витоку в побутовій техніці;

15 – зняття інформації направленим мікрофоном;

16 – внутрішні канали витоку інформації (через обслуговуючий персонал);

17 – несанкціоноване копіювання;

18 – витік за рахунок побічного випромінювання терміналу;

19 – зняття інформації за рахунок використання "телефонного вуха";

20 – зняття з клавіатури і принтера за акустичним каналом;

21 – зняття з монітора з електромагнітного канала;

22 – візуальне зняття з монітора і принтера;

23 – наведення на лінії комунікацій і сторонні провідники;

24 – витік через лінії зв'язку;

25 – витік ланцюгами заземлення;

26 – витік мережею електрогодинника;

27 – витік трансляційною мережею та гучномовним зв'язком;

28 – витік охоронно-пожежною сигналізацією;

29 – витік мережею електроживлення;

30 – витік мережею опалювання, газо- і водопостачання.

Компрометація інформації (один з видів інформаційних інфекцій). Реалізується, як правило, за допомогою несанкціонованих змін у базі даних, у результаті чого її споживач змушений або відмовитися від неї, або докладати додаткових зусиль для виявлення змін і відновлення правдивих відомостей. При використанні скомпрометованої інформації споживач піддається небезпеці прийняття правильних рішень.

Несанкціоноване використання інформаційних ресурсів, з одного боку, є наслідком її витоку й засобом її компрометації. З іншого боку, воно має самостійне значення, тому що може завдати великої шкоди керованій системі (аж до повного виходу ІТ з ладу) або її абонентам.

Помилкове використання інформаційних ресурсів, які є санкціонованими, може призвести до руйнування, витоку або компрометації зазначених ресурсів. Дана загроза найчастіше є наслідком помилок, наявних у ПЗ ІТ.

Несанкціонований обмін інформацією між абонентами може привести до одержання одним із них відомостей, доступ до яких йому заборонений. Наслідки ті ж, що й при несанкціонованому доступі.

Відмова від інформації полягає в невизнанні одержувачем або відправником цієї інформації фактів її одержання або відправлення. Це дозволяє одній із сторін розривати укладені фінансові угоди "технічним" шляхом, формально не відмовляючись від них, наносячи тим самим другій стороні значний збиток.

Порушення інформаційного обслуговування – загроза, джерелом якої є сама ІТ. Затримка з наданням інформаційних ресурсів абонентові може призвести до тяжких для нього наслідків. Відсутність у користувача своєчасних даних, необхідних для ухвалення рішення, може викликати його нераціональні дії.

Незаконне використання привілеїв. Будь-яка захищена система містить засоби, використовувані в надзвичайних ситуаціях, або засоби, які здатні функціонувати з порушенням існуючої політики безпеки. Наприклад, на

випадок раптової перевірки користувач повинен мати можливість доступу до всіх наборів системи. Зазвичай, ці засоби використовуються адміністраторами, операторами, системними програмістами й іншими користувачами, що виконують спеціальні функції. Більшість систем захисту в таких випадках використовують набори привілеїв, тобто для виконання певної функції потрібний певний привілей. Звичайно, користувачі мають мінімальний набір привілеїв, а адміністратори – максимальний.

Набори привілеїв охороняються системою захисту. Несанкціоноване (незаконне) захоплення привілеїв можливе за наявності помилок у системі захисту, але найчастіше відбувається в процесі керування системою захисту, зокрема при недбалому користуванні привілеями. Суворе дотримання правил керування системою захисту, а також принципу мінімуму привілеїв дозволяє уникнути таких порушень. Під час опису в різній літературі різноманітних загроз для ІС і способів їх реалізації широко використовується поняття атаки на ІС.

Атака – зловмисні дії зломщика (спроби реалізації ним будь-якого виду загрози). Наприклад, атакою є застосування кожної зі шкідливих програм. Серед атак на ІС часто виділяють "маскарад" і "злом системи", які можуть бути результатом реалізації різноманітних загроз (або комплексу загроз).

Під "**маскарадом**" розуміється виконання яких-небудь дій одним користувачем ІС від імені іншого користувача. Такі дії іншому користувачеві можуть бути дозволені. Порушення полягає в присвоєнні прав і привілеїв, що називається симуляцією або моделюванням. Цілі "маскараду" – приховування яких-небудь дій за ім'ям іншого користувача або присвоєння прав і привілеїв іншого користувача для доступу до його наборів даних або для використання його привілеїв. Можуть бути й інші способи реалізації "маскараду", наприклад створення й використання програм, які в певнім місці можуть змінити певні дані, у результаті чого користувач одержує інше ім'я. "Маскарадом" називають також передачу повідомлень у мережі від імені іншого користувача. Найнебезпечніший "маскарад" у банківських системах електронних платежів, де неправильна іден-тифікація клієнта може призвести до величезних збитків. Особливо це стосується платежів з використанням електронних карт. Використовуваний у них метод ідентифікації за допомогою персонального ідентифікатора досить надійний. Але порушення можуть відбуватися внаслідок помилок його використання, наприклад втрати кредитної картки або використанні очевидного ідентифікатора (свого ім'я й т. д.). Для запобігання "маскараду" необхідно використовувати надійні методи ідентифікації, блокування спроб злому системи, контроль входів у неї. Необхідно фіксувати всі події, які можуть свідчити про "маскарад", у системному журналі для його наступного аналізу. Також бажано не використовувати програмні продукти, що містять помилки, які можуть привести до "маскараду".

Під **зломом системи** розуміють навмисне проникнення в систему, коли зломщик не має санкціонованих параметрів для входу. Способи злому можуть бути різними, і при деяких з них відбувається збіг з раніше описаними загрозами. Так, об'єктом полювання часто стає пароль іншого користувача.

Пароль може бути розкритий, наприклад, шляхом перебору можливих паролів. Злом системи можна здійснити також, використовуючи помилки програми входу.

Основне навантаження захисту системи від злому несе програма входу. Алгоритм уведення ім'я й пароля, їхнє шифрування, правила зберігання й зміни паролів не повинні містити помилок. Протистояти злому системи допоможе, наприклад, обмеження спроб неправильного уведення пароля (тобто виключити досить великий перебір) з наступним блокуванням термінала й повідомленням адміністратора у випадку порушення. Крім того, адміністратор безпеки повинен постійно контролювати активних користувачів системи: їхні імена, характер роботи, час входу й виходу й т. д. Такі дії допоможуть вчасно встановити факт злому й почати необхідні дії.

Умовою, що сприяє реалізації багатьох видів загроз ІС, є наявність "люків". Люк-схованка, не документована точка входу в програмний модуль, що входить до складу ПЗ ІС і ІТ. Люк вставляється в програму, звичайно, на етапі налагодження для полегшення роботи: даний модуль можна викликати в різних місцях, що дозволяє налагоджувати окремі частини програми незалежно. Наявність люка дозволяє викликати програму нестандартним чином, що може відбитися на стані системи захисту. Люки можуть залишитися в програмі з різних причин:

- їх могли забути забрати;
- для подальшого налагодження;
- для забезпечення підтримки готової програми;
- для реалізації таємного доступу до програми після її установки.

Більша небезпека люків компенсується високою складністю їх виявлення (якщо, звичайно, не знати заздалегідь про їх наявність), тому що виявлення люків – результат випадкового й трудомісткого пошуку. Захист від люків один – не допускати їхньої появи в програмі, а при прийманні програмних продуктів, розроблених іншими виробниками, варто проводити аналіз вихідних текстів програм з метою виявлення люків.

Реалізація загроз ІС приводить до різних видів прямих або непрямих втрат. Втрати можуть бути пов'язані з матеріальним збитком: вартість компенсації, відшкодування іншого побічно втраченого майна; вартість ремонтно-відбудовних робіт; витрати на аналіз, дослідження причин і величини збитку; додаткові витрати на відновлення інформації, пов'язані з відновленням роботи й контролем даних і т. д.

Втрати можуть виражатися в обмеженні банківських інтересів, фінансових витратах або у втраті клієнтури.

Статистика показує, що у всіх країнах збитки від зловмисних дій безупинно зростають. Причому основні причини збитків пов'язані не стільки з недостатністю засобів безпеки як таких, скільки з відсутністю взаємозв'язку між ними, тобто з нереалізованістю системного підходу.

Тому необхідно випереджальними темпами вдосконалювати комплексні засоби захисту.

Лекція 3.
Методи та засоби блокування технічних каналів витоку інформації

1. Захист інформації від витоку акустичним, віброакустичним та оптоелектронним каналами

Усі заходи захисту інформації від витоку акустичним, віброакустичним та оптоелектронним каналами зводяться до зниження рівня акустичних/віброакустичних сигналів (озвучення інформації) до певного співвідношення сигнал/завада. Ступень захисту інформації визначається відповідними нормами.

Необхідного співвідношення сигнал/завада можна досягнути пасивними або активними заходами.

Пасивні заходи захисту інформації спрямовані на підвищення звукоізоляції огороджувальних конструкції (далі – ОК) ОІД (встановлення металопластикових вікон, ущільнювачів дверей, створення «плаваючої підлоги», встановлення акустичних фільтрів у повітроводи тощо).

Активні заходи захисту інформації спрямовані зниження співвідношення сигнал/завада до норми шляхом створення акустичної\віброакустичної завади на межі огороджувальних конструкцій ОІД.

Для орієнтовної оцінки вартості обладнання для захисту мовної інформації від витоку акустичним, віброакустичним та оптоелектронним каналами доцільно скористатися відповідним типовим набором засобів захисту від витоку акустичним, віброакустичним та оптоелектронним каналами.

Таблиця 1

Найменування обладнання	Примітка
Типовий набір засобів захисту на основі генератору шуму „МАРС ТЗО 4-2”	
Генератор шуму „МАРС ТЗО 4-2”	Генератор 2-х канальний. На кожний канал можна підключити 12-16 випромінювачів
Вібровипромінювач ВИ-3	Встановлюється по одному (якщо скло великих розмірів – по два) на кожне віконне скло
Вібровипромінювач ВИ-4	Встановлюється, як правило, на радіатори опалення по одному на вхідну/вихідну трубу (або один, якщо труби з’єднані), а також на стіни, колони та інші масивні конструкції.
Акустичний випромінювач „МАРС АК”	Встановлюється, як правило, в тамбурі дверей, під підвісною стелею та інших

	закритих порожнинах.
Акустичний випромінювач „МАРС АКЗ”	За призначенням аналогічний АКЗ, але у захищеному варіанті (захищений від витоку інформації каналом акустоелектричних перетворень)
Типовий набір засобів захисту на основі генератору шуму „Базальт-4ГА”	
Генератор шуму „Базальт-4ГА”	Призначення то же, що і „МАРС ТЗО 4-2”
Вібровипромінювач “Базальт-4ДВМ”	Призначення то же, що і ВИ-3
Акустичний випромінювач „Базальт-4ДА”	Призначення то же, що і „МАРС АК”

Захист інформації від витоку акустоелектричним та параметричним каналами

Типовий набір засобів захисту від витоку акустоелектричним та параметричним каналами.

Таблиця 2

Найменування обладнання	Примітка
Фільтр протизавадний ФЗП-103-2 з РКП (ЕМСБІ)	Номінальна робоча напруга - 220 В (50 Гц), номінальний струм споживання - 3 А, струм витоку не більше 3,5 мА, діапазон частот - 10 кГц ... 1000 МГ
Фільтр протизавадний ФЗП-110-2	Номінальна робоча напруга - 220 В (50 Гц), номінальний струм споживання - 10 А, струм витоку не більше 15 мА, діапазон частот - 10 кГц ... 18000 МГ
Фільтр ФЗП-125-1	Номінальна робоча напруга - 220 В (50 Гц), номінальний струм споживання - 25 А, струм витоку не більше 15 мА, діапазон частот - 10 кГц ... 18000 МГ
Фільтр мережевий протизавадний М-17	Номінальна робоча напруга - 220 В (50 Гц), номінальний струм споживання - 25 А

Фільтр протизавадний М17-3	Номінальна робоча напруга - 220 В (50 Гц), 3-х фазний, номінальний струм споживання - 25 А на фазу
Збірка фільтрів М17-3 на 50 А	То же на 50 А
Генератор шуму „Базальт-2ГС”	Робоча напруга - 198 -240 В (50 Гц), діапазон частот завади - 0,15-150 кГц
Генератор шуму „Базальт-3”	Пристрій призначений для захисту об'єктів від витоку мовної інформації по двопровідним лініям телефонного зв’язку. Забезпечує захист при покладеній телефонній слухавці шляхом фільтрації акустоелектричних перетворень, а також зашумлення лінії
Генератор шуму „Базальт-1”	Пристрій призначений для захисту об'єктів від витоку мовної інформації по каналах побічних електромагнітних випромінювань персональних комп'ютерів, робочих станцій комп'ютерних мереж і комплексів

Захист інформації від витоку через закладні пристрої

Автономні пристрої, які конструктивно об'єднують мікрофони і передавачі, називають **закладними пристроями** (ЗП) перехоплення мовної інформації.

Перехоплена ЗП мовна інформація може передаватися по радіоканалу, мережі електроживлення, оптичному каналу, з'єднувальним лініям ДТЗС, стороннім провідникам, інженерним комунікаціям в ультразвуковом діапазоні частот, телефонної лінії з викликом від зовнішнього телефонного абонента.

Прийом інформації, що передається ЗП, здійснюється, як правило, на спеціальні приймальні пристрої, які працюють у відповідному діапазоні довжин хвиль. Однак існують винятки з цього правила. Так, у випадку передачі інформації по телефонній лінії з викликом від зовнішнього абонента прийом можна здійснювати зі звичайного телефонного апарату.

Використання портативних диктофонів і ЗП, як правило, вимагає проникнення в контрольоване приміщення. Але, у деяких випадках проникати до приміщення не обов’язково, наприклад при застосування стетоскопів.

Використання ЗП вимагає проникнення до контрольованого приміщення (контрольовану зону). Коли це не вдається, для перехоплення мовної інформації використовуються спрямовані мікрофони.

Виявлення ЗП являє собою специфічний вид робіт тому він виділяється в окрему категорію робіт з технічного захисту інформації.

І.Насамперед, необхідно вжити заходів для підвищення звукоізоляції приміщення ОІД. До них можна віднести таки вимоги:

1. Приміщення, де планується створення ОІД (далі - об’єкту), повинне мати подвійні вхідні двері, що мають щільну підгонку до дверної коробки, між якими утворюється тамбур, якій має по периметру дверей ущільнюватися гумовими прокладками.

Поверхні тамбура облаштовуються звукопоглинаючими матеріалами, на підлозі встановлюються пороги. Чим більше глибина тамбура, тим вище звукоізоляція. При наявності додаткового (запасного) виходу з об’єкта, якщо він не проходить через повністю контрольовані приміщення, куди не можуть потрапити сторонні особи (наприклад, вихід здійснюється через кімнату відпочинку, підсобні приміщення тобто «зону неможливого прослуховування»), конструкція дверей повинна бути такою самою як і основних дверей.

2. Стіни та перегородки об’єкту повинні бути бетонними (залізобетонними) завтовшки не менше ніж 80 мм або цегляними завтовшки не менше ніж 120 мм, оздоблені звукопоглинаючими декоративними матеріалами.

Високу звукоізоляцію дають стіни, які мають багатошарову конструкцію з використанням звукопоглинаючих матеріалів (наприклад, гіпсокартон -мінеральна вата - цегла). При цьому, така конструкція не повинна містити металевих елементів (профілів для кріплення гіпсокартону, сітки-рабиці тощо).

Стіни повинні надійно з’єднуватися з верхнім та нижнім міжповерховим перекриттям. Об’єкт не може мати спільній простір під підвісною стелею або підлогою з іншими приміщеннями.

3. Міжповерхові перекриття не повинні містити будь-яких отворів (штучних або природних) з боку об'єкта. Якщо вони вже є, їх слід заповнити на всю глибину будівельною сумішшю (наприклад, цементно-піщаною).

4. Стеля крім декоративної функції повинна підвищувати звукоізоляцію об’єкта. Як варіант – підвісна, на еластичних підвісах, яка складається з окремих звукопоглинаючих плит. При цьому, вона не повинна мати закритих порожнин, доступ до яких ускладнений. Увесь простір під і над підвісною стелею повинен легко оглядатися.

5. Підлогу бажано зробити багатошарову (наприклад, на основі паркету, паркетної дошки, ламінованого покриття тощо) із звукопоглинаючим матеріалом усередині, яка побудована за принципом „плаваючої підлоги”.

Плінтус по периметру приміщення бажано застосовувати з еластичними краями та спеціальними каналами для кабельних комунікацій.

6. Вікна у приміщенні об’єкта бажано використовувати з підвищеною звукоізоляцією. Наприклад, металопластикові або дерев’яні з склопакетами, які мають не менше ніж дві камери (три скла).

Фурнітура повинна забезпечувати щільне прилягання до рами рухомих елементів вікна на протязі не менше двох років.

Після завершення будівництва (реконструкції, ремонту) на вікнах об’єкту необхідно встановити пристрої, які не дозволяють оглядати приміщення ззовні (штори, жалюзі тощо) незалежно від поверху і наявності будівель, розташованих навпроти.

II. Вимоги, спрямовані запобіганню несанкціонованого доступу до об’єкту або до окремих його елементів:

1. Вхідні двері зали для проведення секретних нарад з коридору обладнуються надійним замком, а також пристроєм, що сигналізує про доступ до об'єкту (чашка для опечатування, лічильник відкривання дверей, петлі для опломбування або використання плашок для опечатування тощо).

2. Кришки оглядових люків, інші елементи доступу до ніш, шахт тощо, в яких прокладені комунікації, обладнуються засобами замикання та пристроями для опломбовування.

3. Об’єкт оснащується охоронною сигналізацією, яка повинна бути виведена на пульт централізованого спостереження підрозділу охорони. Для живлення охоронної сигналізації в аварійних випадках має передбачатися автономне джерело живлення. Переключення на автономне джерело живлення має бути автоматичним.

Типи та види охоронної сигналізації повинні відповідати встановленим вимогам і мати відповідний сертифікат.

III. Вимоги, спрямовані запобіганню витоку ІзОД каналом паразитних електромагнітних випромінювань і наведень:

1. Телекомунікаційні мережі та мережі електроживлення прокладати в металевих рукавах з обов’язковим заземленням.

2. Транзитні трубопроводи, повітроводи та інші металеві елементи інженерних комунікацій не повинні проходити через ОІД, але якщо цього не уникнути, то вони обладнуються вставками з ізоляційного матеріалу.

3. Виключити транзитне проходження будь-яких кабелів (комп’ютерної мережі, сигналізації, голосового оповіщення, силових мереж тощо) через ОІД, а також спільний пробіг в одному каналі кабельних ліній різного призначення (силові та сигнальні). Відстань між ними повинна складати не менше 0,8 м.

IV. Вимоги, спрямовані на забезпечення протипожежної безпеки на ОІД:

1. Опорядження стін, матеріали підвісних стель, розсіювачі світильників повинні бути із негорючих матеріалів.

2. Як засоби шумопоглинання повинні застосовуватися негорючі (НГ) або низької горючості (Г1) спеціальні перфоровані плити, панелі, мінеральна вата з максимальним коефіцієнтом звукопоглинання у межах частот 31,5 - 8000 Гц або інші матеріали аналогічного призначення, дозволені для оздоблення приміщень органами державного санітарно-епідеміологічного нагляду.

3. Об’єкт оснащується автоматичною пожежною сигналізацією. Тип та вид пожежної сигналізації має відповідати встановленим вимогам і мати відповідний сертифікат.

V. Підготовчі роботи для обладнання ОІД технічними системами захисту інформації для подальшого створення комплексів ТЗІ (такі роботи виконуються ліцензіатами у галузі технічного захисту інформації, які у подальшому зможуть обладнати об’єкт засобами захисту та атестувати його), а саме:

1. Монтаж системи (окремих складових системи) активного захисту мовної інформації від витоку акустичним та віброакустичним каналами.

1.1 На етапі встановлення вікон, дверей, повітроводів, підвісних стель тощо прокладається акустичний кабель від місць майбутньої установки

генераторів шуму до акустичних і віброакустичних випромінювачів або прокладаються для цього приховані канали.

1.2 Здійснюється установка випромінювачів на елементи будівельних конструкцій та інженерних комунікацій, доступ до яких у подальшому буде ускладнений.

1.3 Прокладається кабель електроживлення до місць майбутньої установки генераторів акустичного шуму.

2. Монтаж системи (окремих складових системи) захисту мовної інформації від витоку каналами акустоелектричних перетворень.

2.1 У місцях вводу в приміщення кабельних комунікацій встановлюються відповідні фільтри.

2.2 У межах об'єкта або у місцях, що знаходяться під постійним контролем, на кабельні комунікації встановлюються засоби активного приховування інформації (генератори шуму).

3. Монтаж системи (окремих складових системи) моніторингу радіодіапазону для виявлення каналів витоку інформації через закладні пристрої (антижучки).

У будівельні конструкції ОІД впроваджуються виносні антени, комутатори (перемикачі), блоки живлення, попередні підсилювачі, виносні приймачі і конвертори комплексів радіомоніторингу радіоефіру і прокладаються кабелі електроживлення, управління, сигнальні, відбору сигналів тощо.

4. Монтаж системи (окремих складових системи) блокування каналів витоку мовної інформації через пристрої бездротового зв'язку та передачі даних, радіозакладних пристроїв (рекомендується).

У будівельні конструкції ОІД впроваджуються засоби активного приховування інформації (генератори прицільних завад, виносні антени генераторів) та засоби їх керуванням для бездротових мереж (GSM, CDMA, WiFi, Bluetooth тощо) та сигналів закладних пристроїв, які передають інформацію в радіочастотному діапазоні.

Лекція 4.

Поняття та кримінологічна характеристика кіберзлочинності

Кінець XX століття ознаменувався стрімким розвитком інформаційних технологій, що почали впроваджуватися в усі сфери життєдіяльності людей. Використання сучасних персональних комп'ютерів, інформаційно-обчислюваних мереж і комп'ютерізованих комунікаційних мереж забезпечило кожній особі можливості доступу до інформації, що зберігається у відповідних банках даних незалежно від доби і місцезнаходження абонента. Поряд з перевагами, комп'ютерізація має ряд негативних наслідків, серед яких є поява якісно нового виду злочинності – кіберзлочинності. Наслідки цієї злочинності зачіпають не тільки інтереси окремих осіб, що стали жертвами, але й компанії, організації, уряди і суспільство в цілому. Кіберзлочини найчастіше ставлять під загрозу життєво важливу інфраструктуру, яка в багатьох країнах не контролюється публічним сектором, і такі злочини можуть вчиняти дестабілізуючий вплив на всі верстви суспільства.

Під *кіберзлочинністю* слід розуміти сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Поняття «кіберзлочинність» часто вживається поряд з поняттями «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність». Кримінальний кодекс України оперує терміном «злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Серед вищезазначених, поняття «кіберзлочинність» є найширшим поняттям та охоплює найбільше коло злочинних посягань у віртуальному середовищі, а також його використання передбачає міжнародне законодавство. Так, Рада Європи в листопаді 2001 року прийняла Конвенцію про кіберзлочинність. Тому вважаємо обґрунтованим вживання саме цього терміну для кримінологічного дослідження цього різновиду злочинності.

Можемо виділити наступні *ознаки кіберзлочинності*:

1. Ці злочини вчиняються у віртуальному просторі або в межах комп'ютерних мереж. *Віртуальний простір* – це модульований за допомогою комп'ютера інформаційний простір, в якому містяться дані про осіб, факти, явища, процеси, представлені в математичному, символьному чи іншому вигляді. Ці відомості знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, спеціально призначених для їх зберігання, переробки та передачі (В.А.Голубєв).
2. Кіберзлочини вчиняються за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Таким чином, електронно-обчислювана техніка може виступати як засобом вчинення злочину, так і предметом злочину.

На сьогодні найбільш розповсюдженою є *класифікація кіберзлочинів* на 1) агресивні та 2) неагресивні. До першою групи належать: кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кіберсталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них). Друга група включає: кіберкрадіжка, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм.

Переходячи до *кримінологічної характеристики кіберзлочинності* слід зазначити, що більшість виявлених злочинів, що вчиняються з використанням комп'ютерних технологій, розпорошені у звітності різних підрозділів правоохоронних органів серед показників економічної та інших видів злочинності. Через таку недосконалість статистичної звітності, неможливо провести комплексну характеристику кіберзлочинності. У зв'язку з цим, проаналізуємо лише передбачені Розділом XIV Особливої частини КК України

злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Отже, *рівень цієї злочинності* за 2010 рік становив: 190 злочинів зареєстрованих злочинів, за 2011 рік – 131, за 2012 рік – 255, за 2013 рік –595 злочинів. Можна побачити, значний приріст в *динаміці* досліджуваного виду злочинності в Україні за останні 4 роки. Порівняно з 2010 роком кількість виявлених злочинів збільшилась майже втричі. *Питома вага* злочинності у сфері електронно-обчислюваних машин у структурі злочинності в Україні приблизно 0,05%. *Рівень судимості* за 2010 рік складав 68 осіб, за 2011 рік – 56 осіб, за 2012 рік – 93 особи.

Відносно *структури досліджуваної злочинності*, то найбільшу питому вагу (40-60% від усіх зареєстрованих злочинів у цій сфері) складають діяння пов'язані з несанкціоноване втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації (ст. 361 КК України), та діяння передбачені ст. 362 КК України, а саме несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп´ютерах), автоматизованих системах, комп´ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (25-45%). Певним чином це пояснюється найширшими диспозиціями зазначених вище статей Кримінального кодексу, що охоплюють більшість форм кримінальної діяльності у сфері функціонування електронно-обчислюваних машин.

Однак, зазначені вище статистичні показники, на жаль, не відбивають реальний стан кіберзлочинності, оскільки цей різновид злочинів має *високий рівень латентності*. За експертними оцінками, рівень латентності кіберзлочинів становить 90-95%. Причинами латентності найчастіше виступають складнощі виявлення та розслідування кіберзлочинів, неповідомлення потерпілих осіб про факти вчинення таких злочинів. Так, більшість великих компаній хвилюються про свою ділову репутацію та намагаються усунути наслідки кіберзлочинів власними зусиллями. Кіберзлочинність характеризується високим рівнем природної латентності.

Що стосується *кримінологічної характеристики особи кіберзлочинця,* то має важливе значення, оскільки ефективна, успішна боротьба з кіберзлочинам не можлива без всебічного аналізу образу мислення і особи порушника.

За *статтю* кіберзлочини в Україні переважно вчиняють чоловіки, але за останні 4 роки питома вага жінок значно зросла (до 30%). Це пояснюється підвищенням інтересу жінок до сучасних інформаційних технологій.

Залежно від *віку,* виділяють дві групи кіберзлочинців: від 14 до 20 років, від 21 року і старші. До особливостей вчинення кіберзлочинів першою групою осіб належить: відсутність цілеспрямованої, продуманої підготовки до злочину; оригінальність способу; неприйняття заходів для приховування злочину; факти невмотивованого бешкетництва. Діяння осіб понад 21 рік, як правило, мають усвідомлений корисливий характер. Дослідження показують, що злочинці цієї групи, як правило, є членами добре організованих, мобільних і технічно оснащених висококласним обладнанням і спеціальною технікою (нерідко

оперативно-технічного характеру) злочинних груп і співтовариств. Осіб, які входять в їх склад, загалом можна характеризувати як висококваліфікованих спеціалістів з вищою юридичною, економічною (фінансовою) і технічною освітою. Злочини носять багатоепізодний характер, обов'язково супроводжуються діями, спрямованими на приховання злочинів. Саме ця група злочинців і являє собою основну загрозу для людей, суспільства і держави, є реальним кадровим ядром комп'ютерної злочинності як в якісному, так і в кількісному плані. Правоохоронна практика показує, що на долю цих злочинів припадає найбільша кількість посягань, які мають особливо небезпечний характер (В.Б.Вехов).

Специфіка використання комп'ютерної техніки передбачає доволі високий рівень *освітнього рівня.* Тому серед осіб, що вчиняють кіберзлочини, найчастіше зустрічається вища або середня спеціальна освіта. Багато часу затраченого на отримання досвіду роботи з високими технологіями заважає особистому життю. Таким чином, *сімейний стан* більшості кіберзлочинців – переважно неодружені.

За *станом здоров'я* ці особи частіше слабо розвинуті, мають певні особливості в фізичній конструкції (худорлявість або зайва вага). Нерухомий спосіб життя часто призводить до серйозних проблем зі здоров'ям. За *ознакою зайнятості* найбільше в Україні вчиняють злочини працездатні особи, які ніде не працюють і не навчаються (45-50%). Кіберзлочинцям не властивий спеціально-кримінальний *рецидив.* Його рівень не більше 5%.

Дослідники виділяють найбільш притаманні для типового кіберзлочинця *індивідуально-психологічні риси*: виражені порушення емоційно-вольової сфери; відхилення у психосексуальному розвитку; виражені аутичні прояви у сполученні із соціальним аутсайдерством; користолюбство; мстивість; антигуманна спрямованість; озлобленість; відчуття нерівності чи другорядності; боязкість і лякливість у соціальних та між особистих стосунках; заглибленість у своїх думках, мріях, фантазіях; філософське сприйняття світу; відсутність буттєвих ціннісних орієнтацій; викривлена (збочена) система життєвих цінностей; тотальна недовірливість та виражений цинізм; прагнення уникнути перешкод у подоланні життєвих труднощів.

Зарубіжні вчені виділяють також п'ять найпоширеніших *мотивів* скоєння комп'ютерних злочинів: корисливий мотив – 66%, політичні мотиви (шпигунство, злочини, спрямовані на підрив фінансової, кредитної політики уряду, дезорганізацію валютної системи країни) – 17%, дослідницький інтерес – 7%; хуліганські мотиви – 5%, помста – 3%.

Лекція 5.
Розслідування кіберзлочинів.

Представляється необхідним коротко охарактеризувати найбільш важливі документи міжнародних організацій в області боротьби з кіберзлочинністю.

З 1985 по 1989 р. Спеціальний Комітет експертів Ради Європи з питань злочинності, пов'язаної з комп'ютерами, виробив Рекомендацію № 89, затверджену комітетом Міністрів ЄС 13.09.1989 року. Вона містить список

правопорушень, рекомендований країнам - учасницям ЄС для розробки єдиної карної стратегії, пов'язаної з комп'ютерними злочинами. Також в документі відмічена необхідність досягнення міжнародного консенсусу з питань криміналізації деяких злочинів, пов'язаних з комп'ютерами. Рекомендація містить два списки злочинів - «мінімальний» і «факультативний (додатковий)». «Мінімальний» список включає діяння, які обов'язково мають бути заборонені міжнародним законодавством і підлягають переслідуванню в судовому порядку. «Додатковий» список містить ті правопорушення, по яких досягнення міжнародної згоди представляється скрутним [12].

Значення Рекомендації № 89 важко переоцінити. На відміну від прийнятої більш ніж через 10 років після неї Конвенції Ради Європи про кіберзлочинність, яка досі не ратифікована рядом країн, що підписали її, цей документ зробив великий вплив на розвиток і зміну законодавства країн Європи.

У 1990 році VIII Конгрес ООН з попередження злочинності і поводження з правопорушниками ухвалив резолюцію, що закликає держави - члени ООН збільшити зусилля із боротьби з комп'ютерною злочинністю, модернізуючи національне карне законодавство, сприяти розвитку в майбутньому структури міжнародних принципів і стандартів запобігання, судового переслідування і покарання в області комп'ютерної злочинності [9]. 14 грудня 1990 року Генеральна Асамблеєю ООН ухвалила резолюцію, що закликає уряди держав - членів керуватися рішеннями, прийнятими на VIII Конгресі ООН.

У 1995 році в Ліоні (Франція) була проведена міжнародна конференція Інтерполу з комп'ютерної злочинності. Учасники конференції підкреслили, що викликає тривогу відсутність міжнародного механізму для раціонального і ефективного протистояння цьому виду злочинності. За підсумками конференції був зроблений висновок, що у більшості країн світу спостерігається усе зростаюче використання інформаційних технології в кримінальній діяльності. Це викликає необхідність постійного вивчення цього кримінального прояву, оскільки розвиток комп'ютерних технології призводить до використання цих інновацій при скоєні комп'ютерних злочинів [13].

Підхід Інтерполу до боротьби з кіберзлочинністю полягає в тому, щоб використовувати досвід його членів у боротьбі із злочинами у сфері інформаційних технологій шляхом функціонування робочих груп або експертних груп. Робочі групи створюються для вивчення регіонального досвіду і існують в Європі, Азії, Африці і Північній і Південній Америці.

У 1997 році міністри внутрішніх справ і міністри юстиції Великої Вісімки на зустрічі у Вашингтоні прийняли «Десять принципів боротьби з високотехнологічними злочинами», що включають, у тому числі, положення про те, що «для тих, хто зловживає інформаційними технологіями, не повинно бути ніяких» зон безпеки. Правова система повинна забезпечити захист конфіденційності, цілісності і придатності даних і систем від протиправного ушкодження і гарантувати покарання за серйозні правопорушення [6].

Продуктом багаторічних зусиль Ради Європи стала прийнята 23 листопада 2001 року у Будапешті Конвенція Ради Європи про кіберзлочинність. Це один з найважливіших документів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі і доки єдиний документ такого рівня.

Прийняття його - це своєрідна віха в історії боротьби з кіберзлочинністю [3]. Наша країна ратифікувала цю конвенцію 7 вересня 2005 року [7].

Підготовка Конвенції була тривалим процесом - за чотири роки було складено 27 проектів. Завершальна версія, що містить преамбулу і чотири глави, датована 25 травня 2001 року, була представлена Європейській комісії з боротьби з кіберзлочинністю на 50-м пленарному засіданні 18-22 червня 2001 року.

Про Конвенцію Ради Європи в цій роботі вже було сказано немало, зокрема, про види злочинів, передбачених нею. Ще раз відмітимо, що Конвенція підрозділяє злочини в кіберпросторі на 4 групи. У першу групу злочинів, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних даних і систем входять: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5). Також до цієї групи злочинів входить протизаконне використання спеціальних технічних пристроїв (ст. 6). Об'єктом злочину виступають не лише комп'ютерні програми, розроблені або адаптовані для скоєння злочинів, передбачених в статтях 2-5 Конвенцій, але і комп'ютерні паролі, коди доступу і їх аналоги, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому або будь-якій її частині (з урахуванням злочинного наміру). Норми ст. 6 Конвенцій застосовні тільки у тому випадку, якщо використання (поширення) спеціальних технічних пристроїв спрямоване на здійснення протиправних діянь.

До другої групи входять злочини, пов'язані з використанням комп'ютерних засобів : підлог і шахрайство з використанням комп'ютерних технологій (статті 7, 8 Конвенцій).

Третю групу складають злочини, пов'язані з контентом (змістом) даних. До четвертої групи увійшли порушення авторського права і суміжних прав.

Крім того, на початку 2002 р. до Конвенції ухвалив протокол, що додає в перелік злочинів поширення інформації расистського і іншого характеру, що підбурює до насильницьких дій, ненависті або дискримінації окремої особи або групи осіб, що ґрунтуються на расовій, національній, релігійній або етнічній приналежності.

Таким чином, перший розділ Конвенції присвячений видам діянь, що підлягають криміналізації. Її другий розділ освітлює процесуальні аспекти боротьби з кіберзлочинністю.

У Конвенції піднімається одна із основних проблем правового регулювання Інтернету - визначення юрисдикції (ст. 22). Конвенція пропонує традиційне рішення проблеми юрисдикції : карна юрисдикція визначається відповідно до територіальної ознаки (територія держави; борт судна або літака держави). Проте у разі, якщо злочин скоєний поза територіальною юрисдикцією держави, то застосовується карне законодавство тієї держави, громадянином (підданим) якої є злочинець. Тут виникає неясність: незрозумілий статус кіберпростору - чи поширюється на нього національне законодавство або ні? Відповіді на поставлені питання, судячи з усього, з'являться найближчими роками - у міру появи практики рішення конкретних правових суперечок в всесвітній мережі. Таким чином, проблема визначення підвідомчості і осудності злочинів в кіберпросторі як і раніше залишається

відкритою. Щоб уникнути можливих подальших суперечок в Конвенції передбачається, що внутрішні закони держав можуть містити інші норми про юрисдикцію.

Зважаючи на відсутність кордонів в глобальних мережах, Конвенція уточнює ситуацію колізії юрисдикції декількох держав: у такому разі, згідно п. 5 ст. 22, держави повинні проводити консультації для визначення відповідної юрисдикції для судового переслідування.

Глава III Конвенції – «Міжнародна співпраця» - присвячена питанням екстрадиції, спільній діяльності держав-учасників у сфері боротьби з комп'ютерними злочинами і досягнення узгодженості для збору доказів в електронній формі.

Конвенція про кіберзлочинність на сьогодні є одним з базових міжнародно-правових актів у сфері права телекомунікацій, але і цей документ не позбавлений недоліків. Ще до підписання Конвенції деякі групи по захисту громадянських прав і провайдери інтернет-послуг приводили серйозні аргументи проти укладення цього договору, який на їх погляд має неясні формулювання і пред'являє провайдерам непосильні вимоги.

У число організацій, що підписали протест проти прийняття Конвенції, увійшли «Фонд Електронних Меж» (Electronic Frontier Foundation, США), міжнародна організація «Суспільство Інтернет» (Internet Society), «Організація кіберправа і кіберсвободи» (Cyber - Rights & CyberLiberties, Великобританія), «Кріптополіс» (Kriptopolis, Іспанія) і інші. У протесті відзначається, що Конвенція несе в собі загрозу для норм захисту особи, що встановилися, невиправдано розширює поліцейські функції уряду, а також знижує відповідальність держави в правоохоронній діяльності.

Звичайно, єдиним критерієм ефективності Конвенції, так само як і справедливості заперечень критично налагоджених опонентів, являється практика її застосування положень. Окремі положення Конвенції (наприклад, що стосуються процесуальних питань, визначення юрисдикції і класифікації кіберзлочинів) надалі будуть переглянуті. Але сьогодні можна констатувати, що прийняття Конвенції послужить фундаментом для міжнародного законодавства, що формується. Навіть ті країни, які з яких-небудь причин не підписали Конвенцію можуть використовувати досвід, що накопичується, по правовому регулюванню нової предметної області – кіберпростір.

Зусилля, що робляться на міжнародному рівні, пов'язані з діями з реформування карного законодавства на національному рівні. Національні і міжнародні зусилля доповнюють один одного, забезпечуючи глобальну увагу до проблем кіберзлочинності і обумовлюючи координацію кроків по боротьбі з кіберзлочинністю і уніфікацію національних законодавств.. Міжнародні і наднаціональні організації, безумовно, внесли величезний вклад в реформування національних законодавств і координацію процесуальних, технічних і інших дій з виявлення кіберзлочинів, їх розслідування і судового переслідування.

Але навіть якщо враховувати прогрес в реформуванні національних законодавств і координації міжнародних зусиль експертами постійно підкреслюється необхідність розвитку усебічних, послідовних національних стратегій, які наслідуватимуть глобальну стратегію боротьби з

кіберзлочинністю. Зусилля, що робляться на міжнародному рівні, обов'язково повинні підкріплюватися діями на рівні окремо взятої держави.

10 березня 2004 року європейським парламентом створено європейське агентства по мережевій і інформаційній безпеці (ENISA). Це агентство Євросоюзу, створені з метою підвищення ефективності функціонування внутрішнього ринку. Агентство виступає в ролі консультанта і центру передових технології у сфері мережевої і інформаційної безпеки для країн-членів і інститутів Євросоюзу. Крім того, агентство сприяє розвитку зв'язків між країнами-членами Євросоюзу, інститутами Євросоюзу, господарюючими суб'єктами і приватним бізнесом [1].

У січні 2013 року в Гаазі відкрився Європейський центр боротьби з кіберзлочинністю (EC3). Завдання EC3 - присікати дії організованих злочинних мереж. На даний момент об'єкти уваги EC3 обмежені трьома онлайн-шахрайство, що заподіює великий збиток фінансовим організаціям і їх клієнтам; поширення дитячої порнографії, кібератаки на ключові інфраструктури і інформаційні системи [4].

У 2007 році в Україні створено CERT-UA (Computer Emergency Response Team of Ukraine – команда реагування на комп’ютерні надзвичайні події України) – спеціалізований структурний підрозділ Державного центру захисту інформаційно-телекомунікаційних систем Державної служби спеціального зв’язку та захисту інформації України (Держспецзв’язку). CERT-UA з 2009 року була акредитована у FIRST (Forum for Incident Response and Security Teams – Форум команд реагування на інциденти інформаційної безпеки) та вже протягом 5 років є його повноправним членом. Слід зазначити, що членство у FIRST, в рамках протидії кібернетичним загрозам на міжнародному рівні, надає можливість оперативно взаємодіяти з 284 командами реагування на комп’ютерні інциденти (CERT) з 61 країни світу [11].

В нашій державі нормативно-правову базу правового регулювання в даній сфері складають Конституція України, Кримінальний кодекс України, Конвенція Ради Європи «Про кіберзлочинність», Закони України «Про основи національної безпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо, Укази Президента України від 08 липня 2009 року № 514/2009, від 08 червня 2012 року № 389/2012, № 390/2012, інші нормативно-правові акти.

У ряді міждержавних нормативно-правових актів визнано, що кіберзлочинність сьогодні представляє загрозу не лише національної безпеки окремих держав, а погрожує людству і міжнародному порядку.

З початку 90-х років XX століття вказаній проблемі приділяється значна увага у багатьох країнах світу. Позначені питання знаходяться і у полі зору урядових структур нашої держави. Стимулом для цього також виступають узяті Україною зобов'язання по інтеграції у міжнародну та світову спільноту, у тому числі відповідно до Програми інтеграції України в Європейський Союз (розділ 13 - "Інформаційне суспільство") [8].

Дуже високий рівень латентності кіберзлочинності обумовлено рядом причин таких як: низький рівень спеціального технічного оснащення правоохоронних структур сучасними засобами комп'ютерної техніки і комп'ютерними технологіями; відсутність знань і навичок виявлення, розкриття

і розслідування кіберзлочинів із-за обмеження доступу до сучасних методик, тактики і техніки; низький рівень інформаційної культури, підготовленості широкого круга кадрів правоохоронних органів і суддів про залучення винних до карної відповідальності; недовіра потерпілих в правоохоронні органи (пов'язано з вищезгаданими чинниками) і т.д.

Порівняльний аналіз досліджень передового зарубіжного досвіду боротьби з кіберзлочинністю свідчить, що вона має тенденцію до росту. Однією з умов її росту є ускладнення сучасних телекомунікаційних та технічних систем глобального зв'язку і спрощення доступу до використання комп'ютерних технологій широкого круга користувачів через персональні комп'ютери.

У ведучих, економічно розвинених країнах рівень втрат від кіберзлочинності вимірюється кількісно тисячами, а економічні збитки складають мільярди доларів США. За оцінками Інтерполу тільки в Європі збиток від дій кіберзлочинців щорічно складає 750 мільярдів євро [2]. Втрати США від кіберзлочинності складають від 20 до $ 140 млрд. доларів, або близько 1% від ВВП країни, а в Латинській Америці фінансові втрати від діяльності кіберзлочинців в 2013 склали 1,1 млрд. доларів. Такі дані опублікувала неурядова організація LACNIC, що займається аналізом Інтернет - активності в регіоні [10].

Дослідження питань боротьби з кіберзлочинністю показало, що орієнтація тільки на технічні засоби забезпечення інформаційної безпеки в умовах інформатизації суспільства, у тому числі профілактики боротьби з кіберзлочинами, не досягла значних успіхів. Це в значній мірі зобов’язано з підвищенням рівня знань користувачів комп'ютерної та телекомунікаційної техніки.

Парадокс полягає в тому, що чим складніше стає програмне забезпечення (software), тим більш вразливими виявляються традиційні організаційні заходи і засоби інженерного та технічного захисту інформації в комп'ютерних та інформаційних системах, зокрема стосовно несанкціонованого доступу до комп’ютерів та мереж.

Ще однією проблемою порядку є і те, що з розвитком електронних засобів інформації розвиваються технічні засоби перехоплення і несанкціонованого доступу до інформації, яка передається по електронним системах зв'язку.

Найбільшу небезпеку для держави та суспільства складає міжнародна організована кіберзлочинність особливо у сфері економічних відносин в фінансових та банківських системах.

Правовою основою по протидії комп'ютерної злочинності на національному рівні є Кримінальний кодекс України (КК). В цьому КК окремі види комп'ютерних злочинів (кіберзлочинів) виділено в розділ VI Особливої частини - Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. 361, 361, 363). Окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочини, розміщені в інших розділах Особливої частини : В Розділу V Особливої частини зазначені окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину (ст. 163, 176, 177) та Злочини у сфері господарської діяльності (ст. 200) в Розділу VII - [5].

Серед інших організаційних заходів в Україні потрібно зазначити, що на урядовому рівні створено декілька робочих груп, які розробляють проекти законодавчих актів у сфері громадських стосунків стосовно використання інформаційних технологій, які відображають питання боротьби з кіберзлочинністю і взаємодію з різними міжнародними державними та правоохоронними структурами.

Аналіз різних ініціатив по створенню проектів нормативно-правових актів свідчить, що між державними структурами не має взаємодії, координації їхньої діяльності. На законодавчому рівні ініціюються суперечливі ідеї, що не є потрібним правотворчій діяльності. На сьогоднішній день у сфері інформаційного законодавства створені умови, які дозволяють злочинцям уникати відповідальності за скоєння злочинів використовуючи недосконалу правову базу в різних країнах Вказаний чинник можна розглядати як ознаку латентності кіберзлочинності.

Лекція 7.

Засоби копіювання даних

Як убезпечити свій комп’ютер при роботі в Інтернеті? Як запобігти втраті даних, що зберігають у комп’ютері? Про це йтиме мова сьогодні на уроці. В першу чергу з'ясуємо, що слід розуміти під словами *інформаційна безпека.*

Інформаційна безпека — *це захищеність інформації та інфраструктури (сукупності засобів), що її підтримує, від випадкових або навмисних дій природного чи штучного характеру,* які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації та інфраструктури, що її підтримує.

Основними складовими інформаційної безпеки є *доступність, цілісність і конфіденційність* інформації та ресурсів, що використовують для введення, зберігання, опрацювання й передавання даних.

Доступність — *це можливість за прийнятний час одержати необхідну інформаційну послугу*

Інформаційні системи створюють для надання певних інформаційних послуг. Якщо надати ці послуги користувачам стає неможливо, то це завдає збитку всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, її виділяють як *найважливіший елемент* інформаційної безпеки.

Особливо яскраво основна роль доступності виявляється в різного роду системах управління — виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки — і матеріальні, і моральні — може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги тощо).

Цілісність — *це актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни.*

Цілісність виявляється найважливішим аспектом інформаційної безпеки у тих випадках, коли інформація є «керівництвом до дії». Рецептура ліків, призначення медичних процедур, набір і характеристики комплектуючих виробів, хід технологічного процесу — все це приклади інформації, порушення цілісності якої може бути, в буквальному розумінні, смертельно небезпечним. Неприємним є і спотворення офіційної інформації, будь-то текст закону, або сторінки Web-сервера якої-небудь урядової організації.

Конфіденційність — *це захист від несанкціонованого доступу до інформації.*

У вищих навчальних закладах прагнуть не розголошувати дані про екзаменаційні білети до іспиту. Системні адміністратори не поширюють інформацію про окремих користувачів (облікові записи, паролі тощо). Банківські службовці не знають коди електронних карток свох клієнтів.

Системи інформаційної безпеки мають протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, атакам автоматизованим і скоординованим. Іноді напад триває долі секунди, іноді виявлення вразливих місць ведеться поволі і розтягується на години, так, тому підозріла активність практично непомітна. Метою зловмисників може бути порушення всіх складових інформаційної безпеки — доступності, цілісності або конфіденційності.

Інформаційна безпека є одним з найважливіших аспектів інтегральної безпеки на будь-якому рівні — *національному, галузевому, корпоративному або персональному*.

Правила безпечного зберігання даних

1. **Встановити паролі**. Серед усього переліку заходів безпеки, яких повинен дотримуватися користувач, перше місце займає його особиста організованість і відповідальне ставлення до важливої інформації, яку він зберігає у ПК. Найпростіший захід збереження конфіденційності даних — встановлення пароля для входу в систему комп'ютера. Звичайно, це не гарантує абсолютної безпеки, але, як мінімум, непідготовлений або випадковий «недоброзичливець» не зможе просто так проникнути у Ваш ПК, навіть якщо він матиме на це багато часу. Аналогічне блокування можна створити і для тек і файлів, якщо їх попередньо архівувати.

2. За допомогою спеціальних алгоритмів *архіватори* видаляють з файлу усю *надмірну* інформацію при стисненні. При зворотній операції видобування (розпаковування) вони відновлюють інформацію у первісному вигляді. І стиснення, і відновлення інформації відбувається без втрат. При цьому можна задати пароль на видобування з архіву. Деякі архіватири надають можливість шифрувати не лише дані файлів, але й інші важливі області архіву: назви файлів, їхні розміри, атрибути, коментарі й інші блоки. Таке *архівування з паролем* часто використовують для захисту конфіденційної інформації в електронному листуванні: заархівований файл з паролем прикріплюють як вкладення до майже порожнього листа.

3. Щоб створити надійний пароль, використовують *генератор паролів*. Він породжує випадковим чином паролі високого рівня надійності. Їх складно підібрати через використання у них великих і малих літер, чисел,

знаків пунктуації та інших знаків. Створені таким чином паролі ніде не буде збереженя, якщо ви не зробите це навмисно.

4. Потрібно пам'ятати, що який би складний пароль на архівовані файли Ви не встановлювали, ці файли можна просто видалити і, таким чином, втратити важливі дані.

5. **Розділити жорсткий диск на кілька розділів** (логічних дисків): в одному з них зберігати програмне забезпечення й системні дані, в інших — решту інформації.

6. **Створити кілька облікових записів користувачів:**

- лише один з них повинен мати права *адміністратора*, тобто права встановнювати і видаляти програмне забезпечення;
- теки, що містять програмне забезпечення, мають бути доступними лише на читання для усіх користувачів, крім адміністратора, з можливим виключенням для тек з налаштуваннями програми;
- кожний обліковий запис повинен мати теку з повним доступом лише для цього облікового запису й адміністратора. Таку теку *Домівка* операційна системи Linux створює для кожного облікового запису автоматично. Аналог для Windows — тека *Мої Документи*. Але її буде створено як усталено у тому самому розділі, у якому буде встановлено операційну систему.

7. **При використанні ОС Windows встановити Linux.** Windows «не бачить» файлової системи ext4, яку використовує Linux. Тому при ураженні вірусом програмного забезпечення на платформі Windows, завантаживши Linux, можна «витягнути» з ПК усі напрацювання до перевстановлення Windows. Лікування деяких вірусів, що уражають флеш-карти при роботі на ПК під керуванням Windows, зводиться ло простого вилучення файлів з плешки при роботі Linux.

8. **Використовувати антивірус**. Однією з головних причин втрати даних (друге місце після фактів ненавмисного видалення) є наслідки дій шкідливого програмного забезпечення. Обов'язково встановіть антивірус. Спеціалізоване сучасне ПЗ, в тому числі безкоштовне, дозволить мінімізувати загрозу, вчасно її виявити, а в разі проникнення — блокувати, вилікувати або видалити. Основні напрямки захисту від комп'ютерних вірусів є такі:

- запобігання надходженню вірусів;
- запобігання вірусній атаці, якщо вірус потрапив у комп'ютер;
- запобігання руйнівним наслідкам, якщо атака відбулася.

Інформацію про антивірусні програми, призначені для захисту комп'ютера від вірусних атак, виявлення і знищення знайдених вірусів, лікування заражених файлів, можна знайти за такими посиланнями:

- Антивірус Касперського (Windows);
- NOD32 (Windows);
- AVG Antivirus (Windows, Mac OS);
- DrWeb(Windows);
- Avira Free Antivirus (Windows, Mac OS, iOS, Android);
- Avast! (Windows, Mac OS, Android);
- McAfee (багатоплатформна);
- Norton AntiVirus (Windows);

- CLAMAV (Linux, Windows);
- F-PROT Antivirus (Linux, Unix);
- AVG Anti-Virus Free Edition (Linux).

9. **Регулярно створювати резервні копії**. На жаль, інформацію неможливо абсолютно надійно зберігати в комп'ютері. Відмова апаратної частини (жорсткий диск), вірусна атака чи неакуратність самого користувача (випадкове видалення інформації) можуть призвести до втрати важливих даних. Щоб убезпечити важливу інформацію, необхідно робити *резервне копіювання*даних.

10. **Резервне копіювання даних** — *це створення копій важливої інформації, що є на ПК, для збереження її в інших сховищах даних* (флеш-накопичувач, жорсткий диск, DVD-диск, хмарний сервіс тощо).

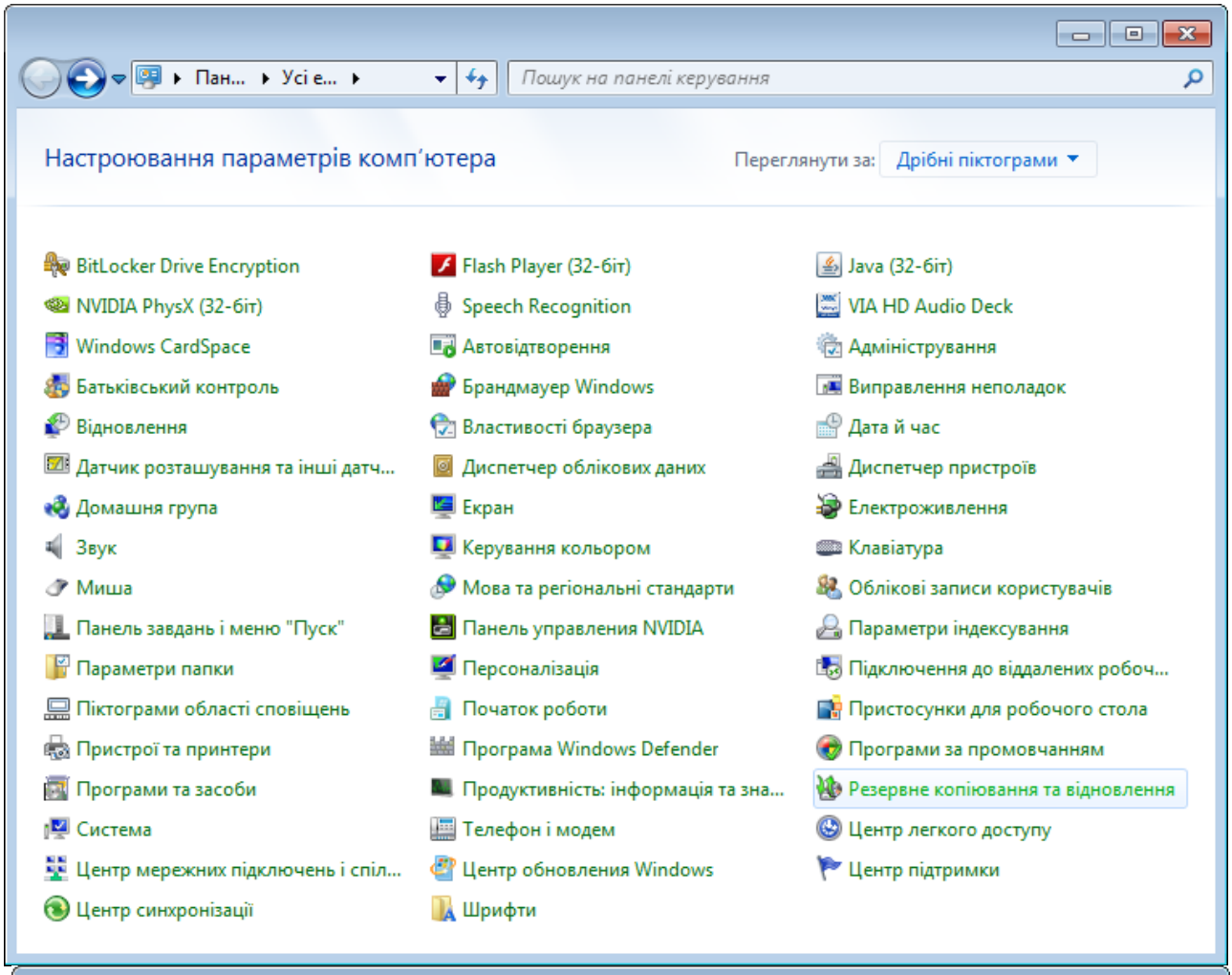
Створення резервних копій є наріжним каменем будь-якої серйозної системи безпеки даних. При можливості, таких копій повинно бути декілька. Резервне копіювання файлів дозволить захистити дані у випадку, якщо станеться вихід з ладу основного носія інформації (наприклад, жорсткого диску комп'ютера), або вірусної атаки. Розрізняють такі *типи резервних копій:*

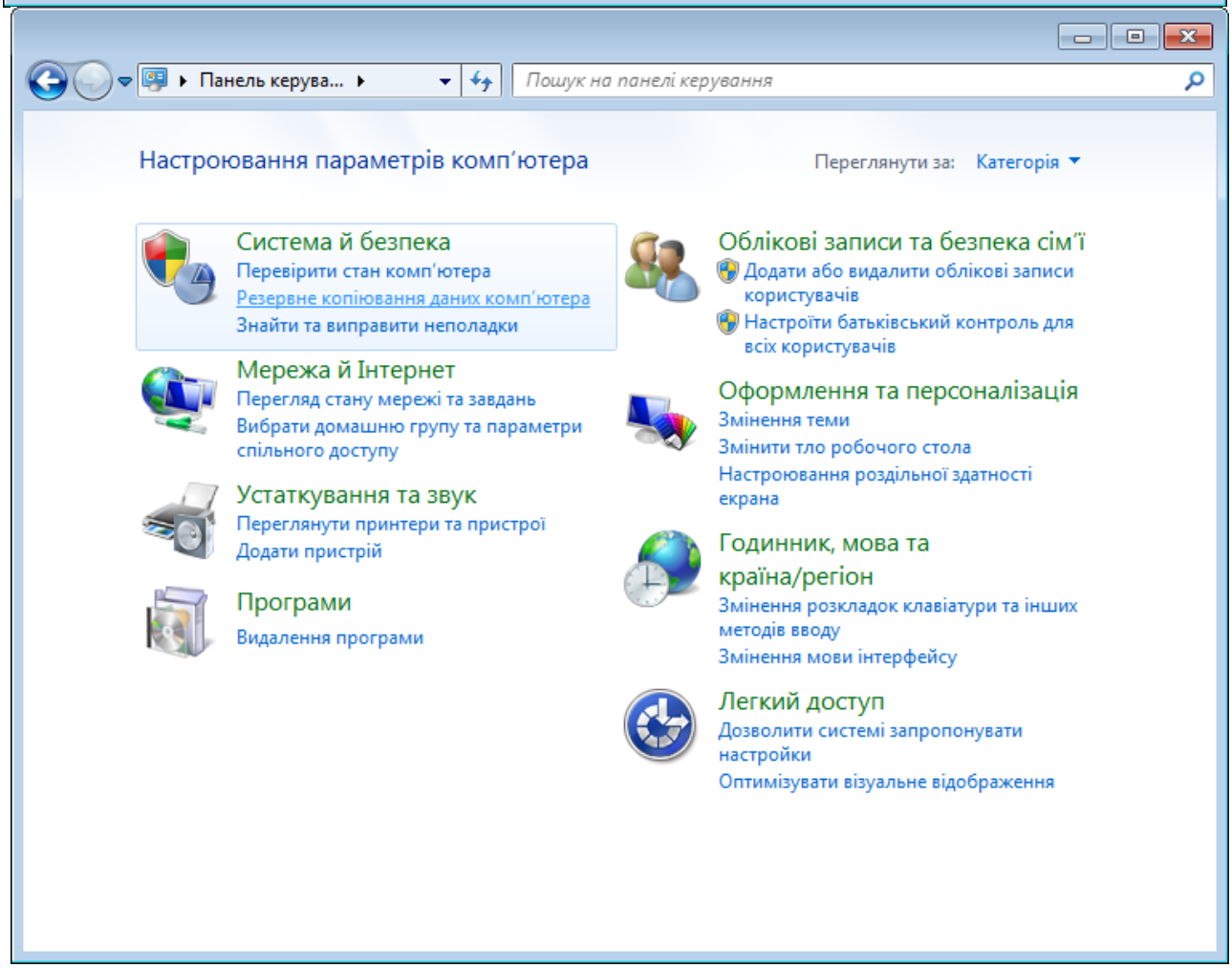
- *Резервна копія операційної системи.* Дуже корисна річ, якою часто нехтують навіть досвідчені користувачі. Потрібно встановити операційну систему, драйвери і необхідні програми. Потім зробити резервну копію налагодженої операційної системи і, у разі потреби (вірусна атака, або просто захаращення системи), відновити резервну копію. Це займає набагато менше часу, ніж нова установка і налаштування операційної системи. Як правило, для резервного копіювання операційної системи використовують спеціальні програми або засоби.
- *Резервна копія логічного диску (розділу)*.
- *Резервна копія окремих файлів і тек* — найпоширеніший спосіб резервного копіювання.

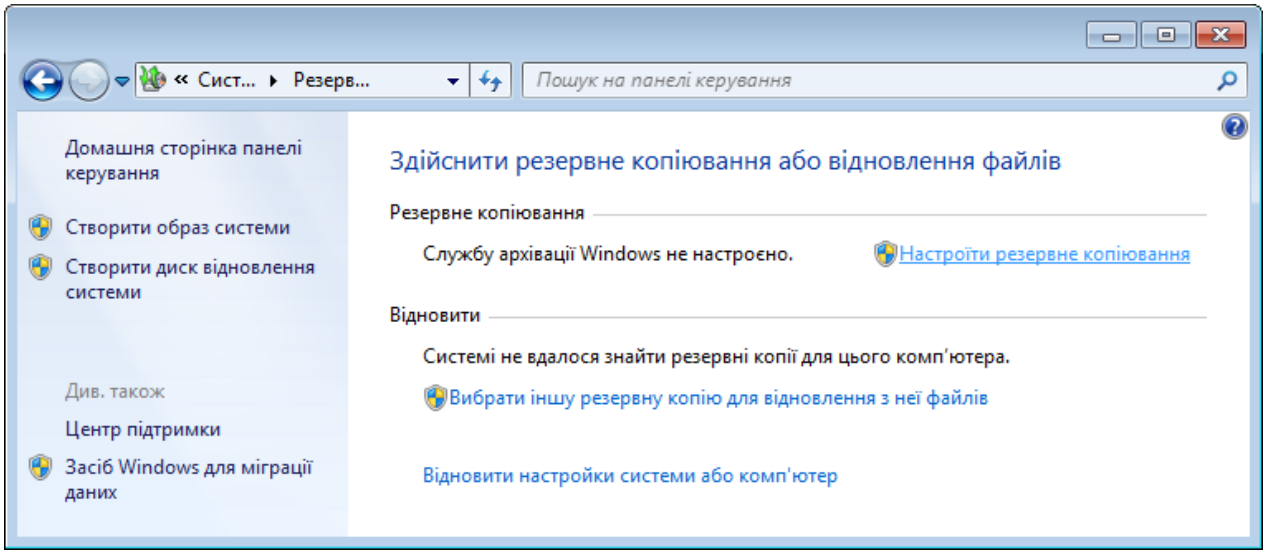
Резервне копіювання та відновлення даних є *різновидом* операцій збереження даних зі своїми *особливостями*:

- При збереженні даних ми найчастіше маємо справу з одним або декількаами файлами. При резервному копіюванні зазвичай об'єктом копіювання є набір великої кількості файлів, теки або диски. Інакше кажучи, це *комплексна дія.*
- Резервне копіювання завжди проводять на *інші* носії — на DVD–диск, флеш–накопичувач, мережні ресурси інформації, відмінні від тих, з яких копіюють.
- При резервному копіюванні значення збережених даних для користувача комп'ютера більше, ніж у випадку окремого файлу чи файлів. Тому, для таких випадків використовують спеціальні засоби — *програми для резервного копіювання даних.*

Резервне копіювання можна виконувати за допомогою спеціальних утиліт, що забезпечують створення компактних архівів. Наприклад, одна з таких утиліт, Microsoft Backup, що входить до комплекту Windows. Для використання у *Панелі керування*(див. наступні дві ілюстрації різного подання панелей) потрібно вибрати відповідне посилання (виділено на ілюстраціях).


Пан... ▸ Усі е... ▸
Пошук на панелі керування
Настроювання параметрів комп'ютера
Переглянути за: Дрібні піктограми
BitLocker Drive Encryption
Flash Player (32-біт)
Java (32-біт)
NVIDIA PhysX (32-біт)
Speech Recognition
VIA HD Audio Deck
Windows CardSpace
Автовідтворення
Адміністрування
Батьківський контроль
Брандмауер Windows
Виправлення неполадок
Відновлення
Властивості браузера
Дата й час
Датчик розташування та інші датч...
Диспетчер облікових даних
Диспетчер пристроїв
Домашня група
Екран
Електроживлення
Звук
Керування кольором
Клавіатура
Миша
Мова та регіональні стандарти
Облікові записи користувачів
Панель завдань і меню "Пуск"
Панель управления NVIDIA
Параметри індексування
Параметри папки
Персоналізація
Підключення до віддалених робоч...
Піктограми області сповіщень
Початок роботи
Пристосунки для робочого стола
Пристрої та принтери
Програма Windows Defender
Програми за промовчанням
Програми та засоби
Продуктивність: інформація та зна...
Резервне копіювання та відновлення
Система
Телефон і модем
Центр легкого доступу
Центр мережних підключень і спіл...
Центр обновления Windows
Центр підтримки
Центр синхронізації
Шрифти


Панель керува... ▸
Пошук на панелі керування
Настроювання параметрів комп'ютера
Переглянути за: Категорія
Система й безпека
Перевірити стан комп'ютера
Резервне копіювання даних комп'ютера
Знайти та виправити неполадки
Облікові записи та безпека сім'ї
Додати або видалити облікові записи користувачів
Настроїти батьківський контроль для всіх користувачів
Мережа й Інтернет
Перегляд стану мережі та завдань
Вибрати домашню групу та параметри спільного доступу
Оформлення та персоналізація
Змінення теми
Змінити тло робочого стола
Настроювання роздільної здатності екрана
Устаткування та звук
Переглянути принтери та пристрої
Додати пристрій
Годинник, мова та країна/регіон
Змінення розкладок клавіатури та інших методів вводу
Змінення мови інтерфейсу
Програми
Видалення програми
Легкий доступ
Дозволити системі запропонувати настройки
Оптимізувати візуальне відображення



Різні види архівації інколи програмно реалізовано. Розглянемо, наприклад, ті п'ять, які передбачено у *Майстрі архівації та відновлення* Windows XP Professional:

- *звичайна (normal) архівація* — архівують *всі обрані* файли й теки з позначенням усіх файлів як копійованих. У цьому випадку процес відновлення швидкий, бо архів містить поточні версії всіх файлів і немає потреби виконувати кілька завдань відновлення;
- *копіювальна (copy) архівація* — архівують *всі обрані* файли й теки але без позначення файлів як зкопійованих;
- *додаткова (incremental) архівація* — створює резервну копію файлів, створених або змінених з часу останньої архівації, і мітить їх як зкопійовані. Якщо новостворений файл не змінювати між двома послідовними додатковими архівaціями, то у другому архіві його не буде.
- *різницева (differential) архівація* — архівують лише ті з обраних файлів і тек, які було створено з часу останнньої архівації. Але на відміну від додаткової архівації, не помічає їх як зкопійовані. Якщо новостворений файл не знищувати між двома послідовними різницевими архівaціями, то його міститимуть обидва архіви;
- *щоденна архівація* — архівують тільки ті з обраних файлів і тек, які було створено або змінено у день архівації, незалежно від стану маркера.

Є ряд програм, поширюваних незалежно від операційних систем, які допомагають швидко й легко налаштувати резервне копіювання усіх необхідних даних.

Acronis True Image — наразі лідер серед програм для резервного копіювання, бо має усі необхідні функції і можливості для резервного копіювання та простий і зрозумілий інтерфейс. З допомогою цієї програми можна зберігати визначені дані (файли і теки), розділи диска цілком, або робити образ розділу з операційною системою, усіма програмами і конфігурацією. Усі ці дії можна налаштувати на автоматичне і періодичне виконання. Якщо операційну систему пошкоджено, можна завантажити *Acronis True Image* з флеш–накопичувача або іншого носія і відновити резервну копію. На жаль, Acronis True Image Home не має україномовного інтерфейсу і є

платною програмою. Серед безкоштовних аналогів цієї програми можна вказати такі:

 Clonezilla;

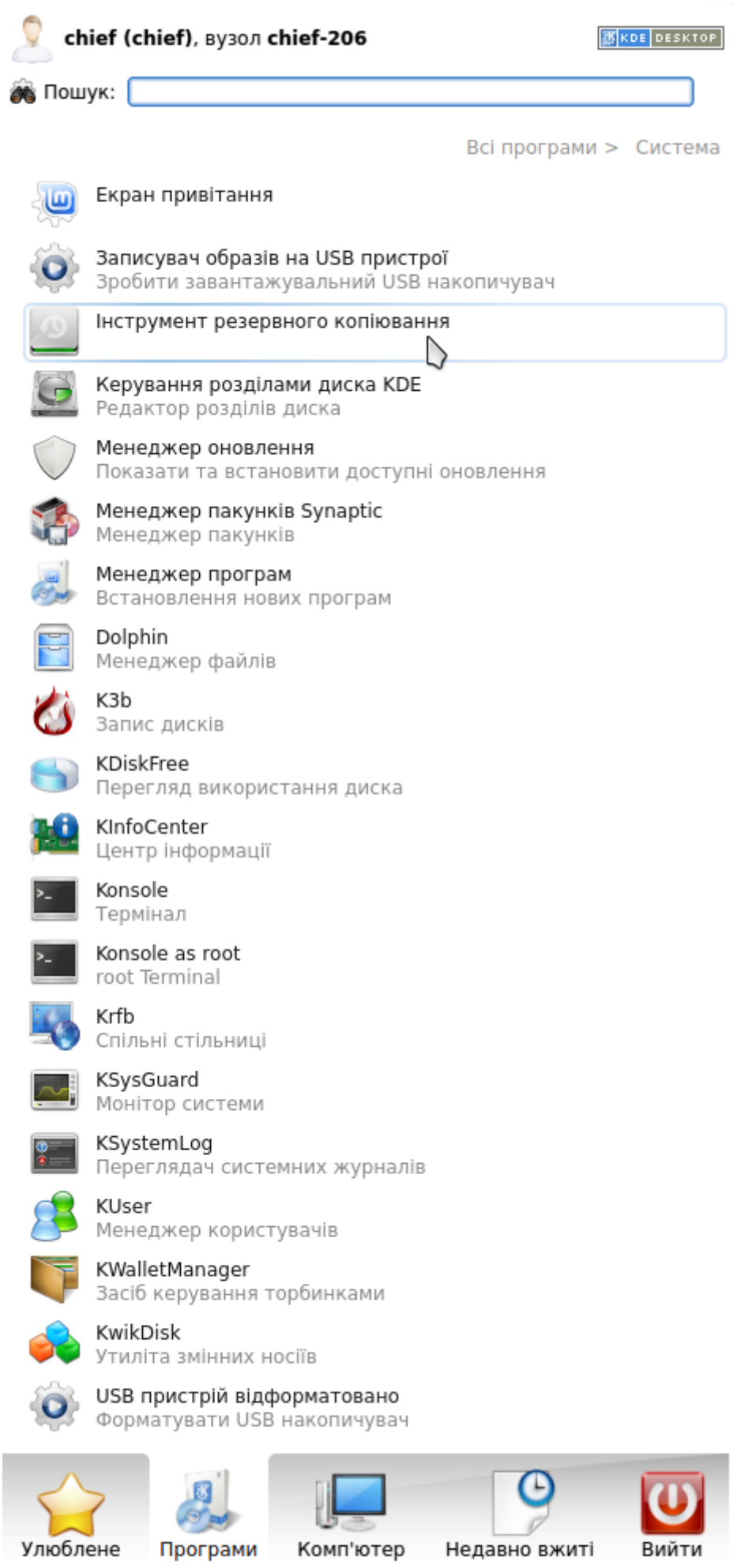
 Cobian Backup;

 Comodo Backup;

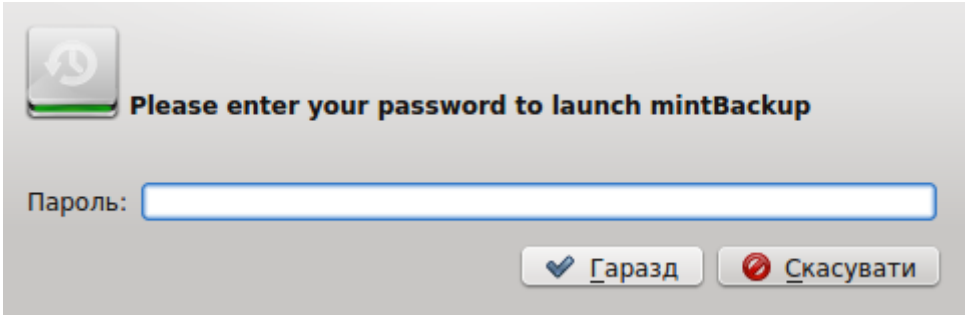
 Macrium Reflect Free.

При роботі з опеційною системою Linux Mint використовують *Інструмент резервного копіювання*.

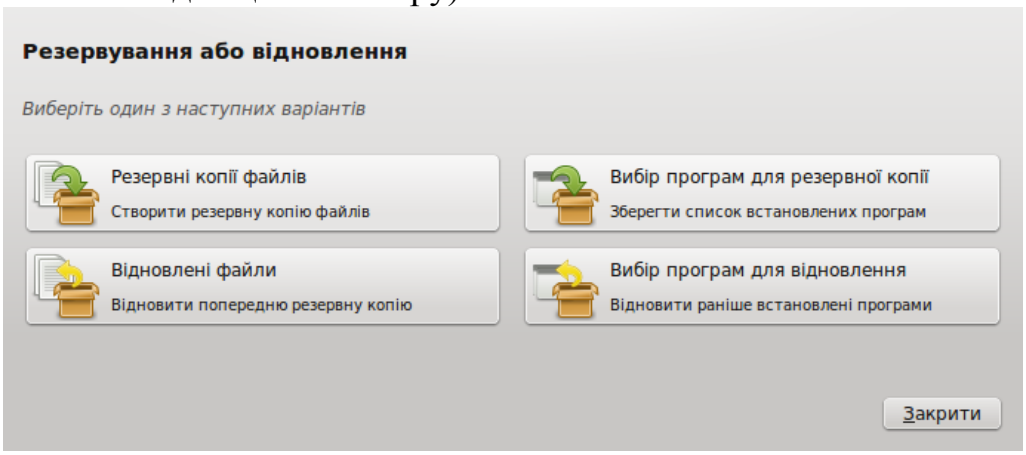
12. У режимі адміністратора викликати кнопкою запуску програм *Всі програми / Система / ...*


chief (chief), вузол chief-206
KDE DESKTOP
Пошук:
Всі програми > Система
Екран привітання
Записувач образів на USB пристрої
Зробити завантажувальний USB накопичувач
Інструмент резервного копіювання
Керування розділами диска KDE
Редактор розділів диска
Менеджер оновлення
Показати та встановити доступні оновлення
Менеджер пакунків Synaptic
Менеджер пакунків
Менеджер програм
Встановлення нових програм
Dolphin
Менеджер файлів
K3b
Запис дисків
KDiskFree
Перегляд використання диска
KInfoCenter
Центр інформації
Konsole
Термінал
Konsole as root
root Terminal
Krfb
Спільні стільниці
KSysGuard
Монітор системи
KSystemLog
Переглядач системних журналів
KUser
Менеджер користувачів
KWalletManager
Засіб керування торбинками
KwikDisk
Утиліта змінних носіїв
USB пристрій відформатовано
Форматувати USB накопичувач
Улюблене
Програми
Комп'ютер
Недавно вжиті
Вийти

13. Для запуску інструмента ввести пароль адміністратора і натиснути кнопку *Гаразд*.

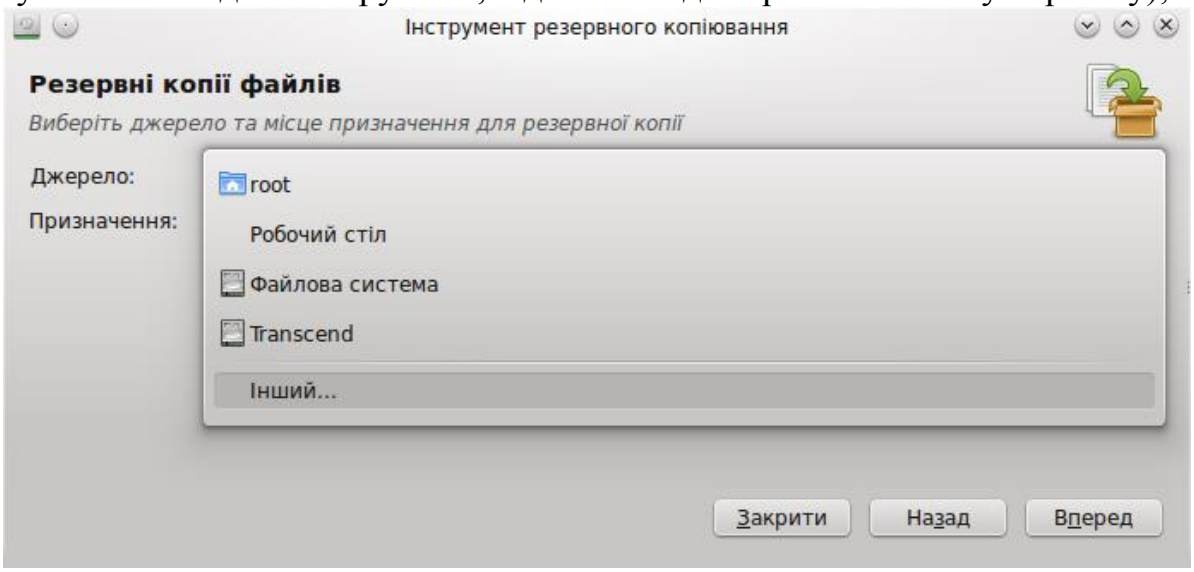


14. У вікні діалогу *Резервування або відновлення* вибрати варіант роботи. Наприклад, *Резервні копії файлів* (подальші дії описано й проілюстровано саме для цього вибору).

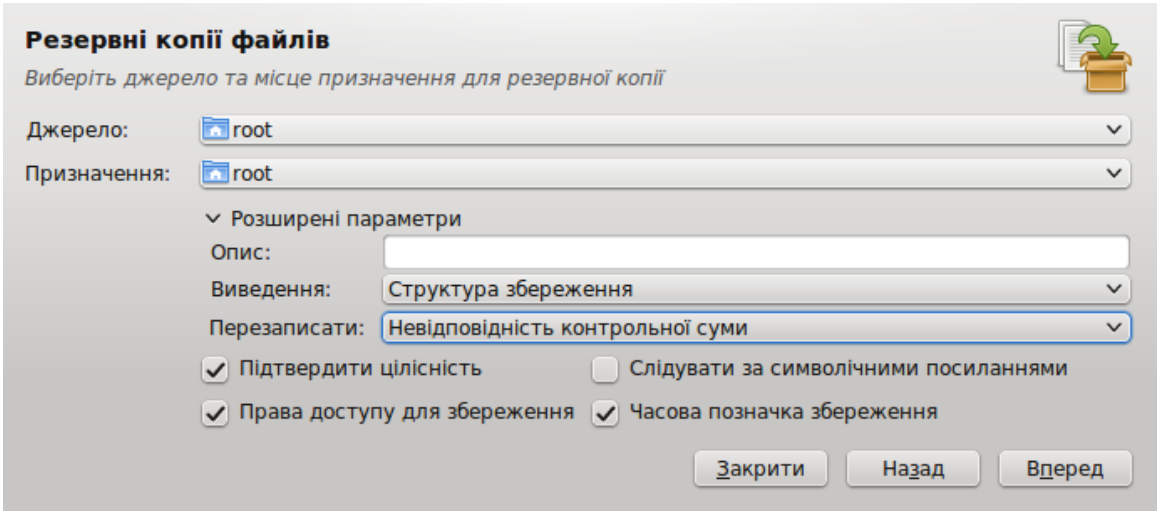


15. У вікні діалогу *Інструмент резервного копіювання*

- вказати *Джерело* і *Призначення* (що і куди копіювати, натиснути *Інший…* для вибору теки, відмінної від запропоновоних у переліку);



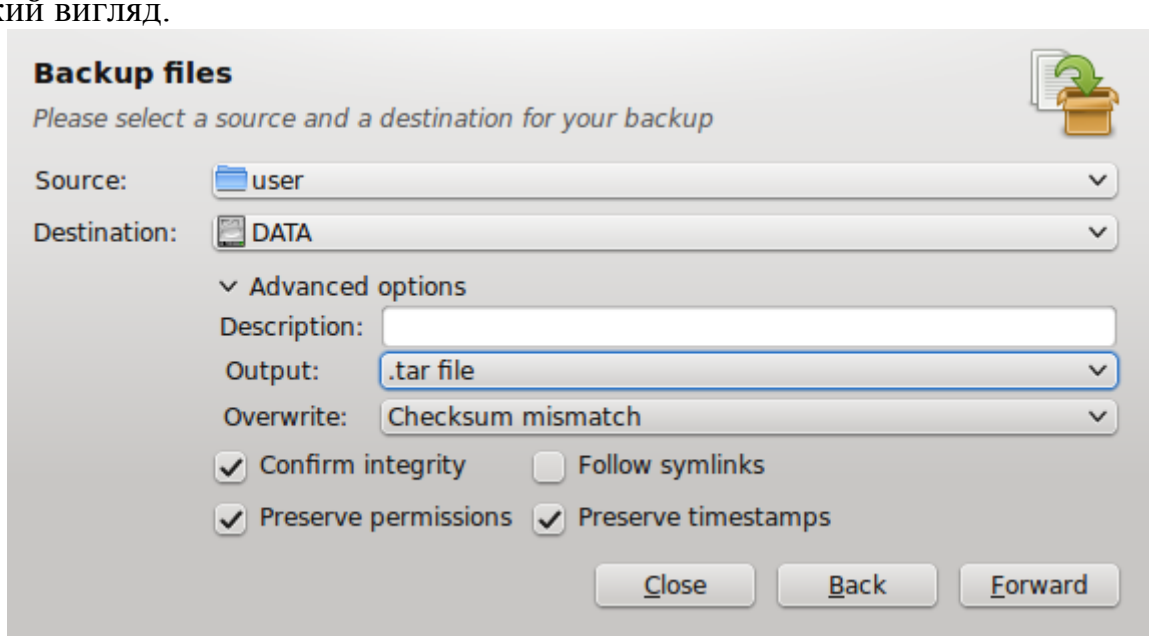
- у разі потреби налаштувати *Розширені параметри*,



у тому числі й *Виведення*;

- натиснути кнопку *Вперед*.

Англомовний інтерфейс (при створенні архівного файлу tar у теці DATA) має такий вигляд.



Рекомендації щодо резервного копіювання даних

- *Робити резервні копії періодично*. Залежно від типу даних кожного дня, тижня, місяця тощо або хоча б після істотного оновлення інформації. Інакше в разі втрати даних зможете відновити лише застарілу версію резервної копії, в якій не вистачатиме нещодавно змінених даних.
- *Тиражувати копії*. Зробивши резервну копію важливої інформації, розмножити цю копію на фізично різних носіях інформації — флеш–накопичувачах, зовнішній жорсткий диск, CD/DVD–диск, хмарне сховище тощо. Чим більше копій, тим більша ймовірність не втратити потрібну інформацію.

- *Захистити резервну копію* від сторонніх. Навіть якщо це лише копія приватних фотографій. Краще за все поєднати кілька способів захисту. Наприклад, захист даних паролем і шифрування.
- *Зберігати резервні копії у різних місцях*, навіть якщо їх зроблено на різних носіях. Інакше у разі крадіжки, пожежі чи стихійного лиха усі копії можна втратити.

Висновок. Створення резервної копії даних — дуже важлива процедура. Її повинен робити кожний користувач. Створити резервну копію не складно. Можна навіть налаштувати автоматичне створення резервних копій. Як саме робити резервну копію даних, — вирішувати Вам, але головне, не забувайте робити це систематично.

11. **Створювати контрольні точки системи**. Однією з альтернатив резервного копіювання, наприклад, при роботі з великими проектами (науковими роботами, масштабними кресленнями тощо) може служити створення *контрольних точок відновлення системи.* У разі якогось форс–мажору, або дій шкідливого програмного забезпечення, що пошкодив дані, Ви зможете «відкотитися» до стану системи з усіма параметрами і файлами на період збереження. Для цього не обов'язково встановлювати додаткове ПЗ. Сучасні операційні системи вже мають дану функцію, як вбудовану. Подібний метод дозволить не втратити всю інформацію цілком. Однак все, що було змінено, навіть за умови збереження після створення контрольної точки, швидше за все, буде втрачено. Це найголовніший недолік такого способу страхування. Але таке неповне відтворення краще, ніж повна втрата інформації.

Утиліта *Відновлення системи* ОС Windows веде постійне спостереження за всіма змінами операційної системи та створює так звані *точки відновлення,* що дає змогу в разі потреби повернути комп’ютер до стану нормального функціонування, не втративши при цьому документи користувача. Для кожної точки відновлення система створює архів файлів, потрібних для її відновлення. Для створення цього архіву потрібно до 200 МБ дискового простору. За його відсутності утиліта *Відновлення системи* не може працювати.

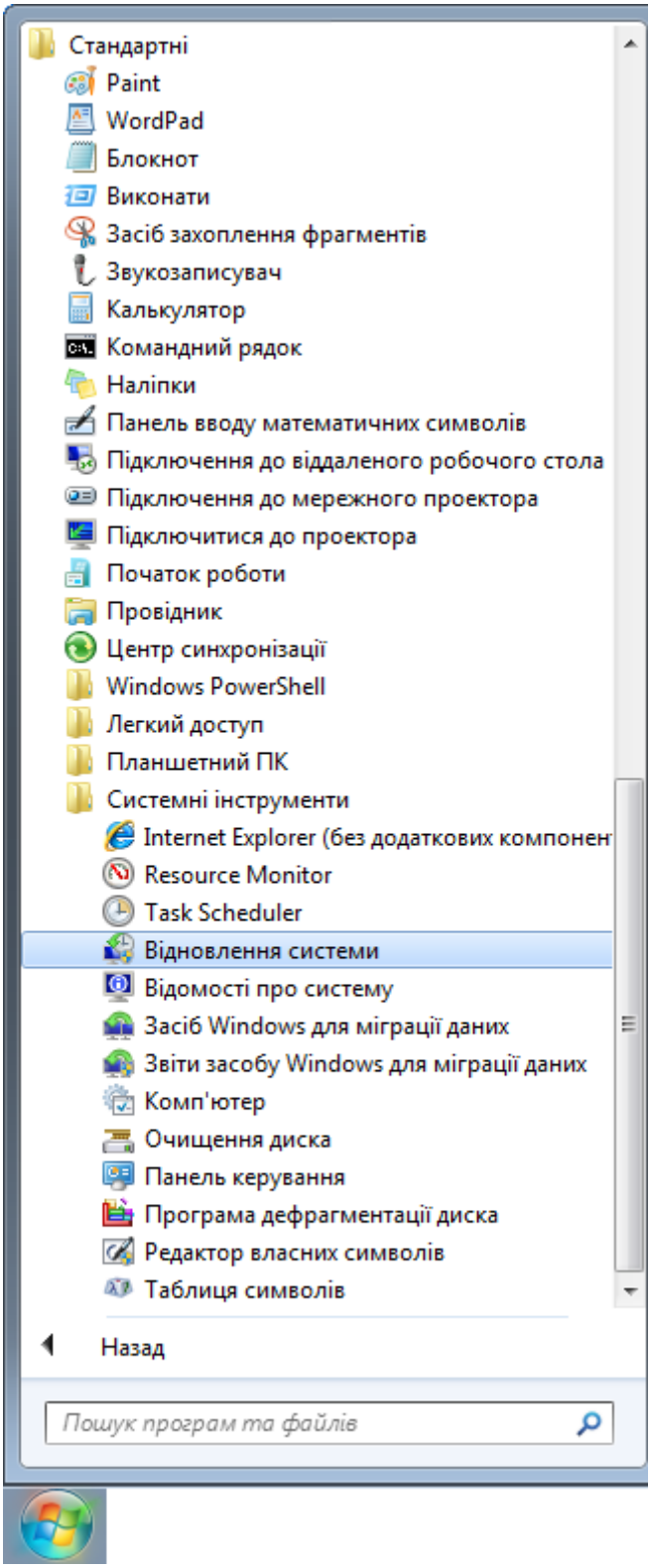
Класифікація точок відновлення

- *Точка початкової системи* — її створюють під час першого запуску на комп’ютері операційної системи для можливості повернути операційну систему та всі програми, що працюють під її керуванням, до початкового стану.
- *Точка системи* — це точка відновлення, що її автоматично створює утиліта щодоби навіть за відсутності будь-яких змін у системі. Якщо комп’ютер у час, призначений для створення точки відновлення, вимкнено, то цю точку буде створено одразу після його увімкнення.
- *Точка встановлення програми* — це точка відновлення, яку створює утиліта у процесі встановлення нового програмного забезпечення. Їх використовують для повернення системи до стану, у якому вона була до початку інсталяції програми.
- *Точка автоматичного оновлення ОС Windows* — це точка відновлення, яку створює утиліта в разі автоматичного оновлення операційної системи.

- *Точка користувача* — це точкf відновлення, які користувач створює, щоб зафіксувати вдалу конфігурацію системи аби повернутися до її стану в разі невдалого змінення.
- *Точка програми Відновлення системи* — це точка, що їх автоматично створює утиліта відновлення для повернення системи до попереднього стану, якщо відновлення в результаті її роботи виявиться невдалим.
- *Точка драйвера пристрою* — це точки відновлення, яку створюють у разі встановлення драйверів, не сертифікованих для роботи в цій операційній системі.
- *Точка програми резервного копіювання* — цю точку створюють на початку архівування під час роботи з програмою резервного копіювання.

Для роботи з утилітою *Відновлення системи* потрібно зробити таке:

8. Зберегти відкриті файли та закрити всі програми.
9. Натиснувши кнопку *Пуск*, у Головному меню вибрати *Програми / Стандартні / Системні інструменти (Службові) / Відновлення системи*



або вибрати відповідну дію у *Панелі керування.*

10. Обрати одну з можливих дій.

При налагодженні роботи системи вручну потрібно видалити програми і драйвери, після встановлення яких виникла проблема.

При роботі з ОС Windows драйвери видаляють у вікні *Диспетчер пристроїв*, відкрити яке можна з допомогою *Панелі керування*:

11. У переліку пристроїв вибрати той драйвер, який було встановлено перед виникненням проблем.

12. Викликати контексне меню пристрою, клацнувши правою кнопкою миші.

13. Виберати *Властивості*.

14. У вікні діалогу на вкладенні *Драйвер* натиснути кнопку *Видалити*.

15. Перезавантажити комп'ютер і встановити інший драйвер або працювати з тим, який система встановить самостійно при завантаженні.

Програми, що стали причиною збоїв, видаляють за допомогою утиліти *Програми та засоби*, яка запускають з *Панелі керування*.

Серйозні збої операційної системи можуть привести до її відмови завантажуватися. У цьому випадку на самому початку завантаження потрібно натиснути клавішу *F8*, виберати *Безпечний режим* і виконати послідовно попередні поради. Після цього перезавантажити комп'ютер у звичайному режимі.

12. **Використовувати хмарні сервіси.** *Системою зберігання даних у хмарі* називають мережу розподілених центрів опрацювання даних, які надають користувачу і сприймаються ним як один єдиний віртуальний сервер. Користування системою зберігання даних надається у вигляді Інтернет–сервісу.

Зростання попиту користувачів на такі сервіси обумовлено зручністю користування інформацією, зокрема доступу до неї будь–де та будь–коли. Важлива інформація буде завжди в швидкому доступі. Але користувачу доведеться запам'ятати пароль доступу, без якого дані, назавжди залишаться у небесному сховищі під замком. Найпростішим хмарним сховищем можна вважати скриньку електронної пошти, на яку можна відправляти дані самому собі.

Можна виділити такі популярні в Україні та світі хмарні сервіси зберігання даних: AmazonCloudDrive, AmazonCloudPlayer,Bitcasa, Box.net, Carbonite, Crash Plan, DollyDrive, Dropbox, Flickr, GoogleDrive, JungleDisk, iCloud, MediaFire, Mozy, Office365,OneDrive, Photobucket, RapidShare, Sendspace, SmugMug, SpiderOak, Strongspace, SugarSync, Wuala, Yandex.Disk.

Серед них є сервіси, що позиціонують себе як найбільш захищене хмарне сховище даних.

13. У більшості випадків питання безпеки залишається відкритим. Але рішення є — шифрування файлів перед завантаженням у хмару. Інакше кажучи, використовувати файли на своєму ПК у звичайному форматі, а на сервері зберігати їх у зашифрованому вигляді.

Найпопулярнішими серед спеціалізованих хмарних сервісів на сьогоднішній день є Dropbox і Google Drive. Наразі безкоштовний обсяг на хмарних сховищах такий.

	Dropbox	Google Drive	Mega	Яндекс.Диск	Облако@mail.ru
Назва					
Безкоштовний обсяг	2 GB + 36 GB - за виконання завдань	15 GB	50 GB	10 GB	100 GB

	Bitcasa	Yunpan 360	4shared	OneDrive	Copy.com
Назва					
Безкоштовний обсяг	20 GB	36 TB Детальніше на yunpan.ru	15 GB	7 GB	15 GB + 7 GB за додаткові завдання

14. **Шифрувати власні дані**. Якщо важливо не лише зберегти інформацію, але й звести до нуля можливість скористатися нею, варто звернути увагу на можливість шифрування важливої інформації. Сьогодні існує достатня кількість платних і безкоштовних програм, які шифруванням перетворюю Ваші дані у беззмістовний для стороннього набір символів. Ці програми працюють за принципом створення контейнерів — інформаційних об'єктів, які зберігають у зашифрованому вигляді. Програми випадковим чином генерують «ключ», за допомогою якого відбувається шифрування інформації. При відкритті зашифровані дані набувають початкового вигляду, а після закриття дані знову зашифровують.

Останні десять років найпопулярнішим шифрувальником була програма TrueCript. Сьогодні їй можна знайти альтернативи, наприклад DiskCryptor — вільне програмне забезпечення з відкритим кодом, призначене для шифрування логічних дисків (у тому числі системних), зовнішніх USB–накопичувачів та образів CD/DVD.

При пересиланні важливих і конфіденційних даних електронною поштою їх потрібно зашифруввати і тим самим надійно захистити.

15. **Безпечно видаляти дані.** Багато хто думає, що коли кинути файл у *Смітник* (*Кошик*), то інформація буде знищено. Це не так. Тут все як у реальному житті — якщо сміттєвий кошик не виніс з будинку, то все сміття залишиться на тому місці, де його було покладено. *Смітник* (*Кошик*) потрібно чистити.

Але очищення *Кошика* означає лише видалення даних про розташування початку файлу. Біти даних як і раніше записано на диску доти, поки їх не буде перезаписано. Інколи навіть після форматування диска, при бажанні і наявності відповідних навичок та інструментів, дані можна відновити.

При роботі з ОС Windows використовують такі програми:

- Recuva — навіть користувачі–початківці відновлюють файли, видалені з різних носіїв;
- CCleaner — один з кращих наборів інструментів для оптимізації операційної системи та очищення її від усякого сміття;
- Eraser — інтегрується у *Провідник* Windows. Після її встановлення досить клацнути правою кнопкою миші на файлі або теці й вибрати з контекстного меню пункт *Eraser*. Підтримується режим стирання файлів після перезавантаження комп'ютера, що може виявитися дуже зручним у тому разі, якщо Windows не дозволяє виконати відповідну операцію відразу;
- **xShredder** — забезпечать безпечне видалення даних з неможливістю їх подальшого відновлення. Вільно поширювана програма. Має набір інструментів для роботи з жорсткими дисками. Власник комп'ютера зможе вивчати вміст носія і отримувати додаткову інформацію про диск та інші компоненти системи, здійснювати форматування або дефрагментацію диска, блокувати доступ до окремих розділів тощо. Працює під керуавнням 32-бітних і 64-бітових версій операційної системи Windows XP, Vista, а також Windows 7 і 8. Завантажити *xShredder 7.7.4.9* можна за посиланнямhttp://rsload.net/soft/cleaner-disk/11741-xshredder.html

Різні програми пропонують різні технології стирання, що дозволяють виконувати неодноразовий перезапис дискового простору. Але, цілком природно, що коли Ви перезапишете файл 35 разів, то ймовірність його відновлення буде набагато нижче, ніж після одноразового перезапису.

16. **Використовувати перезаписуваний профіль для збереження налаштувань користувача** за умови великої кількості недисциплінованих користувачів, що використовують один і той самий обліковий запис. Наприклад, у навчальних закладах і бібліотеках (див., наприклад, опис для Linux Mint).

4. Закріплення вивченого матеріалу

1. Дати стисле тлумачення таких понять:
   - інформаційна безпека;
   - складові інформаційної безпеки
   - вірус;
   - антивірус;
   - пароль;
   - пароль для входу в систему ПК;
   - пароль для тек і файлів;
   - шифрування;
   - дешифрування;
   - резервне копіювання даних;
   - типи резервних копій;
   - відмінності резервного копіювання від операцій збереження даних;
   - правила резервного копіювання даних;
   - програми для резервного копіювання даних;
   - відновлення даних;
   - точки відновлення системи;

- хмарні сервіси зберігання даних;
- переваги та недоліки зберігання даних у хмарі;
- безпечне видалення даних;

Лекція 8.
Засоби блокування запису.

Є апаратні блокатори запису більш надійними в порівнянні з програмними?

Проведення криміналістичних досліджень при розслідуванні інцидентів інформаційної безпеки, провадження судових експертиз і багато інші напрями діяльності, пов'язані з комп'ютерною криміналістикою, вимагають максимально можливого збереження цілісності досліджуваних даних. Для цього використовуються блокатори запису програми або пристрою, що не дозволяють записати що-небудь на досліджуваний накопичувач. Необхідність застосування таких засобів відбувається як з вимог процесуального законодавства (наприклад, КПК РФ), так і з різних рекомендацій методичного та іншого характеру, а також із стандартів (наприклад, СТО БР ІББС-1.3-2016). Деякі аспекти функціонування блокіраторів запису і будуть розглянуті в цій статті.

Один з ранніх апаратних блокіраторів запису (2002 рік)

Багато фахівців з комп'ютерної криміналістики та юристи поділяють думку, що апаратні блокатори запису є більш надійними, ніж програмні блокатори запису; це судження ще можна знайти, прямо або побічно, у різних публікаціях [1] [2] [3]. У цій статті я постараюся розкрити внутрішній устрій апаратних і програмних блокіраторів запису, показавши різні проблеми, існуючі в даних продуктах.

Принципи функціонування

Апаратні блокатори запису

Всі апаратні блокатори записи можуть бути розділені на дві групи в залежності від того, як вони обробляють команди, отримані від хоста:

працюють на базі білого списку;

працюють на базі чорного списку.

Апаратний блок запису працює на базі білого списку, коли він блокує будь-яку команду накопичувачу, якщо вона не включена у список відомих безпечних команд (не вносять зміни у збережені на диску дані). У цьому режимі роботи блокіратор запису буде блокувати всі невідомі команди, включаючи специфічні для виробника (наприклад, для проведення низькорівневої діагностики накопичувача) і нові (ще не реалізовані у вбудованій програмі блокіратора запису). Такий блокіратор запису може блокувати нові стандартизовані безпечні команди, інтерпретуючи їх як невідомі.

Апаратний блок запису працює на базі чорного списку, коли він блокує команди, включені в список небезпечних команд (вносить зміни до даних, збережених на диску дані або здійснюють інші небезпечні дії), і дозволяє проходження до накопичувача будь-яких інших команд. У такому режимі роботи блокіратор запису буде дозволяти невідомі (специфічні для виробника або нові стандартизовані) небезпечні команди накопичувача.

Крім того, всі апаратні блокатори записи можуть бути розділені на дві групи в залежності від деталей їх реалізації:

- працюють як транслятора команд;
- працюють в якості модулів, що надають доступ до блокового пристрою.

Апаратний блок запису працює як транслятора команд, коли він просто транслює дозволені команди, отримані від інтерфейсу-джерела, шляхом їх повторення в інтерфейс-одержувач. Наприклад, простий блокіратор запису типу SATA-to-USB може отримувати SCSI-команди від USB-інтерфейсу (використовує набір команд «SCSI transparent command set» для класу «mass storage»), а потім для кожної дозволеної SCSI-команди виробляти запит SATA-контролера через AHCI, перенаправляючи будь-які відповіді назад хосту по протоколу SCSI.

Апаратний блок запису працює в якості модуля, який надає доступ до блокового пристрою, коли він містить повноцінну операційну систему загального призначення, підключений накопичувач визначається як блочний пристрій в цій операційній системі, а доступ до читання з цього блокового пристрою розділяється з хостом через спеціальний драйвер. Такий блокіратор запису з USB-підключенням до хосту визначить підключений накопичувач як блочний пристрій, а потім буде використовувати USB-гаджет для емуляції

USB-накопичувача із застосуванням зазначеного блочного пристрою в якості джерела даних для емульованого накопичувача. У такій конфігурації апаратний блок запису не здійснює безпосередню трансляцію команд, отриманих від хоста в адресу накопичувача, він транслює отримані від хоста команди у внутрішні запити, використовувані для читання даних з блочного пристрою-джерела. Таким чином, множинні команди читання, отримані від хоста, можуть бути з'єднані в один запит на читання, що приводить до відправлення підключеного накопичувача однієї команди читання. Крім того, вбудована програма блокіратора запису може здійснювати завчасне читання (read-ahead) в кеш, це призводить до того, що одна команда читання, отримана від хоста, може і не призвести до негайної відправки відповідної команди читання підключеного накопичувача, оскільки потрібні дані вже були прочитані і додані в кеш вбудованої програмою.

Крім того, апаратні блокатори записи можуть надавати особливі функції для деяких типових і нетипових застосувань:

- робота в режимі «читання-запис»;
- дозвіл команд запису, збереження модифікованих даних на іншому диску;
- подання накопичувача хосту з позначкою захисту від запису (це додає ще один рівень захисту, оскільки очікується, що операційна система не буде писати на накопичувач з позначкою захисту від запису);
- приховування помилок запису;
- надання доступу до прихованим з допомогою HPA або DCO областях даних;
- дозвіл деяких небезпечних команд, використовуваних для відкриття доступу до прихованим областях даних (видалення DCO або перманентне видалення HPA);
- прозоре вичитування даних з поганих (пошкоджених) секторів накопичувача, прозора робота з несправними накопичувачами.

Програмні блокатори запису

Деталі реалізації програмних блокіраторів записи залежать від операційної системи. В операційних системах, які працюють в реальному режимі, на зразок DOS, програмні блокатори запису перехоплюють переривання BIOS 0x13, що використовується для читання та запису даних диска, відфільтровуючи запити на запис і викликаючи вихідний обробник переривання для запитів на читання. Сучасні операційні системи як Windows і GNU/Linux використовують драйвери прямого доступу для взаємодії з накопичувачами, переривання BIOS 0x13 використовуються завантажувачем для читання ядра та інших даних (зразок драйверів прямого доступу) тільки на ранньому етапі завантаження. Таким чином, існує безліч шляхів для реалізації функціональності блокування запису, наприклад:

- драйвер, що працює в режимі «тільки читання», для певного класу накопичувачів (PATA, SATA, SCSI, USB і ін);
- програма (драйвер), отфильтровывающая запити на запис на їх шляху до драйвера певного класу накопичувачів більш низького рівня;
- драйвер, що надає блочний пристрій в режимі «тільки читання» для вибраного накопичувача або розділу, з паралельним існуванням в операційній системі блочного пристрою в режимі «читання-запис» для того ж накопичувача або розділу передбачається, що використання різних програм буде відбуватися стосовно до блокового пристрою в режимі «тільки читання»).

В залежності від реалізації, програмні блокатори записи можуть аналізувати або блокувати такі види запитів:

- читання, запис, скидання кешу і інші запити в уніфікованому форматі, специфічному для операційної системи (який не заснований на протоколі взаємодії з накопичувачем на низькому рівні);
- запити у форматі, заснованому на протоколі, що використовується для взаємодії з накопичувачем (наприклад, SCSI), або який безпосередньо реалізує цей протокол.

Крім того, програмний блокіратор запису може представляти накопичувач операційній системі з позначкою «тільки читання».

В сучасних операційних системах були зустрінуті з реалізації блокування запису:

Windows:

- установка фільтруючого драйвера для пакетів з I/O-запитами, які використовуються для передачі SCSI-команд низкорівневому порт-драйверу накопичувача (операційна система використовується протокол SCSI для взаємодії з порт-драйверами накопичувачів, пакети запитів транслюються, якщо це необхідно, у протокол, який використовується конкретним обладнанням).

Linux:

- установка пристрою-«петлі» в режимі «тільки читання» для блочного пристрою накопичувача (або розділу), в цій ситуації драйвер пристрою-«петлі» відфільтровує запити на запис, що йдуть до основного блокового пристрою (ядро використовує власну структуру для опису запитів до накопичувача на читання, запис, скидання кешу тощо), передбачається використання саме пристрої-«петлі» для доступу до даних;
- патчінг ядра з метою фільтрування запитів на запис, що йдуть на адресу блочного пристрою в режимі «тільки читання».

При роботі з запитами, сформованими на базі рідного протоколу (зразок SCSI Windows), програмний блокіратор запису може працювати з чорними і білими списками, як було показано раніше.

В цілому, програмні блокатори записи повинні перехоплювати запити або в одній точці (наприклад, перед передачею запиту одному з багатьох драйверів накопичувачів), або у всіх місцях відразу (наприклад, у всіх драйверах накопичувачів).

Слід зазначити, що програмний блокіратор запису не може перекрити всі можливі шляхи передачі небезпечною команди накопичувача. Наприклад, ядро може надавати інтерфейс для відправки «сирих» запитів накопичувача (зразок інтерфейсу SG_IO в Linux), або архітектура драйверів накопичувачів може дозволяти будь-якого драйвера відправити запит в обхід фільтруючого драйвера (як у Windows), або низькорівневий драйвер може самостійно відправляти небезпечні команди, або яка-небудь програма може просто відключити блокіратор запису. І хоча можна зробити деякі заходи проти таких недоліків, ідея проста — завжди існує шлях, який обходить програмний блокіратор запису.

Програмні квазиблокираторы запису

Існує можливість створити таку операційну систему, яка не буде відправляти небезпечні команди підключених накопичувачів під час і після завантаження, крім ситуацій, коли користувач явно запускає програму, що відправляє небезпечні запити. У такому випадку немає компонента, що блокує запис, але немає і команд, що підлягають блокуванню (і такі операційні системи часто відносять до містить механізм блокування запису, тому в даному розділі і використовується позначення «квазі»)

На жаль, деякі продукти описуються, як містять програмний блокіратор запису, але в дійсності в них немає такого блокіратора, а в залежності від різних обставин подібний продукт може відправляти підключеного накопичувача небезпечні команди.

Порівняння апаратних блокіраторів запису з програмними
Можуть бути відзначені наступні важливі відмінності між апаратними і програмними блокаторами запису:

- Апаратні блокатори записи роблять розрив між хостом і накопичувачем, в результаті небезпечні команди від хоста підлягають блокуванню незалежно від їх походження. Програмні блокатори записи можуть бути обійдені шкідливою програмою, як було показано раніше.
- Програмні блокатори запису для драйверів прямого доступу неактивні під час раннього етапу завантаження: блокування запису відсутня, коли завантажувач використовує переривання BIOS 0x13 або сервіси EFI для завантаження ядра та інших компонентів сучасної операційної системи. У той же час апаратні блокатори запису до завершення їх ініціалізації не обробляють які-небудь команди.

Є думка, що програмні блокатори записи не можуть бути надійними, тому що залежать від тендітної програмної середовища: наприклад, оновлення операційної системи, або оновлення драйвера, або помилка (в апаратному або програмному забезпеченні) може перешкоджати механізму блокування запису; апаратні блокатори запису, з іншого боку, вважаються надійними, тому що містять стабільний, добре протестований апаратне забезпечення і вбудоване програмне забезпечення[4].

Перевірка криміналістичної правильності

Програмні квазиблокираторы запису

SUMURI PALADIN 4.01

PALADIN — це не вимагає установки дистрибутив (заснований на Linux), розроблений для завантаження досліджуваного комп'ютера з метою попереднього перегляду даних або їх збору. Крім того, цей дистрибутив може використовуватися на криміналістичної робочої станції як вже готової операційної системи.

Згідно документації, доступною у **PALADIN 4.01**, *PALADIN був модифікований для захисту від запису всіх підключених накопичувачів після початку завантаження* (*«PALADIN has been modified to write-protect all attached media upon boot»*). Тим не менш, дана версія не містить будь-якого компонента, що блокує запис; також були виявлені наступні факти запису на підключені накопичувачі під час завантаження дистрибутива (цей і наступні розділи не містять вичерпного переліку виявлених проблем (недоліків), зазначаються лише деякі характерні проблеми; з тієї ж причини аналогічні проблеми в інших криміналістичних продуктах на основі Debian, Ubuntu і інших дистрибутивів не вказані):

- якщо підключений накопичувач містить «брудну» (не отмонтированную належним чином) файлову систему Ext3/4, то ця файлова система відновлюється з допомогою її журналу;
- якщо підключений накопичувач містить «брудну» файлову систему NTFS, журнал ($LogFile) цієї файлової системи очищається.

Ці проблеми належать до раннього етапу завантаження не потребують встановлення дистрибутивів на базі Ubuntu або Debian, коли програми стартової (початкової) файловій системі (initial RAM file system) запускаються з метою знайти завантажувальний накопичувач шляхом монтування файлових систем на кожному накопичувачі (включаючи об'єкти дослідження) і пошуку певних сигнатур у цих файлових системах (зразок файлу, що містить певний UUID). Ці дії необхідні для завершення переходу з переривання BIOS 0x13 або сервісів EFI, використовуваних завантажувачем, на драйвери прямого доступу, що використовуються ядром для читання з завантажувального накопичувача.

Хоча такі проблеми присутні в цій та інших версіях PALADIN, даний дистрибутив пройшов валідацію NIST без будь-яких зауважень про дані проблеми[5].

Програмні блокатори запису

SUMURI PALADIN 6.01

PALADIN 6.01 включає компонент ядра (Linux) для блокування запису, який був негласно включений без будь-яких згадок документації або в журналі змін. Цей компонент був негласно виключений з більш пізніх версій даного дистрибутива (наприклад, PALADIN 6.07).

Під час валідації була виявлена наступна помилка в реалізації блокування запису: на ранньому етапі завантаження, коли запускаються програми з стартової файлової системи, компонент блокування запису блокує запити на запис і вивільнення (discard), адресовані всім блочних пристроїв зі старшим номером 8 (і тільки). У такій реалізації тільки накопичувачі PATA/SATA/SCSI/USB захищені від запису на зазначеному етапі завантаження, в той же час, наприклад, носії у считывателях карт (MMC) не захищені від запису, а тому схильні до дії проблемних моментів, зазначених раніше.

Апаратні блокатори запису

Криміналістичний дуплікатор Tableau TD3

Криміналістичний дуплікатор **Tableau TD3** (версія програмного забезпечення: 2.0.0) може бути використаний в якості мережевого блокіратора запису, що відкриває доступ до підключеного досліджуваного накопичувача по протоколу iSCSI. Драйвер iSCSI блокує запити на запис, адресовані досліджуваного накопичувача, при цьому компонент блокування запису в ядрі (Linux) або в апаратному забезпеченні відсутня. Було виявлено, що підключення накопичувача з файлової системи Ext4, в журналі якій зафіксована помилка I/O, призводить до відправлення дупликатором декількох команд запису (модифікуючих файлову систему) через «заблокований від запису» порт, тому що використовувана дупликатором операційна система (на основі Linux) автоматично монтує файлові системи на диску, підключеному через «заблокований від запису» порт.

Криміналістичний міст Tableau T356789iu

Криміналістичний міст **Tableau T356789iu** (версія програмного забезпечення: 1.3.0) блокує спроби читання хостом секторів, прилеглих до поганого. Було виявлено, що один поганий сектор на підключеному накопичувачі призводить до того, що 128 поганих секторів не можуть бути прочитані хостом нібито з-за помилки читання. Встановлено, що криміналістичний міст використовує функціональність попереджувального читання і кешування ядра (Linux) при читанні даних з підключеного накопичувача (ядро може прочитати і відправити в кеш вміст секторів до того, як воно буде запитано програмою, запити на читання обробляються через кеш), а ядро має погане «роздрібнення» помилок (воно не перечитує окремі сектори всередині великого кешируемого блоку після помилки читання цього блоку).

Криміналістичний міст Tableau T35es

Згідно інформації від компанії Guidance Software[6], криміналістичні мости **Tableau T35es** зі старою версією програмного забезпечення дозволяли передачу SCSI-команд WRITE(16), отриманих від хоста через USB-з'єднання, на адресу підключеного накопичувача. Ця проблема є прикладом нестачі роботи на базі чорного списку.

Криміналістичний міст Tableau T8-R2

Згідно інформації від компанії Guidance Software[7], криміналістичні мости **Tableau T8-R2** зі старою версією програмного забезпечення відправляли на підключений накопичувач команди запису, будучи підключеними до хосту через USB-з'єднання, при невказаних обставин. Подробиці повідомлені не були, за винятком того, що записувані дані є випадковими.

Висновки

Можна цілком впевнено сказати, що апаратні блокатори запису не надійніше програмних, в кожному з них можливе існування критичних проблем (особливо в ситуаціях, коли апаратний блок запису містить повноцінну операційну систему загального призначення). Але ця відповідь не можна визнати задовільним для криміналістичного спільноти, оскільки він не дає нам способи вирішення проблеми.

Лекція 9.

Аналіз зібраної інформації.

Сніфер – це програма або програмно-апаратний пристрій, який застосовується для захоплення і докладного аналізу перехопленого трафіку або окремого сегменту мережі. В процесі захоплення всіх потоків, аналізатор захоплює і записує всі пакети, отримані з інтернет-трафіку. У разі докладного і інформативного аналізу відбувається декодування пакетів з зашифрованої форми подання в ту, яку можна прочитати. Існує два основних види роботи сніферів в комп'ютерних мережах: за місцем розташування (в певній мережі сніфер захоплює трафік і відправляє в іншу мережу або в зворотну сторону; якщо ж він встановлений на маршрутизаторі конкретного провайдера вашого інтернету, то є можливість відстеження трафіку користувачів цієї мережі) та на крайовому вузлі.

Аналізатор трафіку, або сніфер - мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів. Аналіз трафіку, який пройшов через сніфер дозволяє:

- виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережевого обладнання та каналів зв'язку (сніфери тут малоефективні; як правило, для цих цілей використовують збір різноманітної стати- 12 стики серверами і активним мережевим обладнанням і її подальший аналіз);

- перехопити будь-який незашифрований (а часом і зашифрований) призначений для користувача трафік з метою отримання паролів і іншої інформації;

- локалізувати несправність мережі або помилку конфігурації мережевих агентів (для цієї мети сніфери часто застосовуються системними адміністраторами). Наразі існує значна кількість програмних продуктів, які призначені для аналізу мережевого трафіку.

Розглянемо найбільш поширені з них, та визначимо програмний продукт з найбільшим функціоналом. Wireshark - програма-аналізатор трафіку для комп'ютерних мереж Ethernet і деяких інших. Має графічний користувальницький інтерфейс. Wireshark - це програма, яка «знає» структуру самих різних мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня [3, 4].

Оскільки для захоплення пакетів використовується pcap, існує можливість захоплення даних тільки з тих мереж, які підтримуються цією бібліотекою. Проте, Wireshark уміє працювати з безліччю форматів вхідних даних, відповідно, можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення. Iris Network Traffic Analyzer крім стандартних функцій збору, фільтрації та пошуку пакетів, а також побудови звітів, пропонує унікальні можливості для реконструювання даних. Iris The Network Traffic Analyzer допомагає детально відтворити сеанси роботи користувачів з різними web-ресурсами і навіть дозволяє імітувати відправку паролів для доступу до захищених web-серверів за допомогою cookies. Унікальна технологія реконструювання даних, реалізована в модулі дешифрування (decode module), перетворює сотні зібраних двійкових мережевих пакетів у звичні для ока електронні листи, web-сторінки і ін. EEye Iris дозволяє проглядати незашифровані повідомлення web-пошти та програм миттєвого обміну повідомленнями, розширюючи можливості наявних засобів моніторингу та аудита.

Аналізатор пакетів eEye Iris дозволяє зафіксувати різні деталі атаки, такі як дата і час, IP-адреси і DNS-імена комп'ютерів хакера і «жертви», а також використані порти. Ethernet Internet traffic Statistic відображає кількість отриманих та прийнятих даних (в байтах - всього і за останню сесію), а також швидкість підключення. Для наочності зібрані дані відображаються в режимі реального часу на графіку. Працює без інсталяції, інтерфейс - російська та англійська мови. Утиліта для контролю за ступенем мережевої активності - показує кількість отриманих та відправлених даних, ведучи статистику за сесію, день, тиждень і місяць. CommTraffic – мережева утиліта для збору, обробки і відображення статистики інтернет-трафіку через модемне (dial-up) або виділене з'єднання. При моніторингу сегмента локальної мережі, CommTraffic показує інтернет-трафік для кожного комп'ютера в сегменті.

CommTraffic включає в себе зрозумілий користувачеві інтерфейс, який легко настроїти та показує статистику роботи мережі у вигляді графіків і цифр. З числа розглянутих програманалізаторів мережевого трафіку хотілося б виділити Wireshark, яка має більшу кількість функціональних можливостей. Дана програма надає можливість аналізу мережевих пакетів і розбір мережевих протоколів будь-якого рівня, а також інформативний розбір всього трафіку, що проходить в мережі, використовуючи мережеву карту в режимі promiscuous mode. Здатний аналізувати структуру всіх доступних мережевих протоколів і здійснювати їх фільтрацію за конкретними параметрами.

Для здійснення повноцінного аналіз мережевого трафіку локальної мережі з використанням wireshark, необхідно виконати наступні дії: запуск і настроювання програми аналізатора Wireshark; захоплення трафіку; перегляд захопленого трафіку; аналіз Проблеми інформатизації та управління,3(59)’2017 13 захоплених пакетів; аналіз присутніх протоколів; знаходження пакетів з помилками; геопозіція ір джерел; перехоплення файлів, що скачали з захопленого трафіку; відновлення введених логінів і паролів. Після запуску та налаштування програми аналізатора Wireshark активуємо захоплення мережевого трафіку локальної мережі. Програма аналізатор Wireshark безперервно відображає одержувані пакети з мережевого інтерфейсу. Для здійснення ефективного аналізу, необхідно працювати з захопленим трафіком в пасивному режимі. Необхідна інформація для виконання наступних кроків аналізу представлена в головній панелі інтерфейсу програми Wireshark, в якій знаходяться основні дані про захоплених пакетах. Основні дані мережевих пакетів в головній панелі (рис. 1): No - порядковий номер захопленого пакета; Time - час захоплення пакета в секундах; Source - мережеву адресу відправника; Destination - мережеву адресу одержувача; Protocol - протокол, що використовується; Length - довжина пакетаInfo - інформація про захопленому пакеті.

Рис. 1. Інформація про захоплені пакети

Для аналізу необхідно відобразити статистичні дані по захопленому мережевому трафіку в табл. 1, щоб оперувати цими значеннями в наступних етапах виконання аналізу.

Таблиця 1. Статистичні дані захопленого трафіку

Характеристика	Значення
First packet/Початок захоплення	2017-09-13 23:23:24
Last packet/ Останній захоплений пакет	2017-09-13 23:59:51
Elapsed/Час захоплення, хв.	00:36:28
Packets/Захопленні пакети	75133
Packets size/Розмір всіх пакетів, Мбайт	68 Mb
Average kbytes/s / Середня швидкість пакетів	67 kbytes/s
Average kbits/s / Середня швидкість	538 kbit/s

Використання Wireshark дає можливість отримання інформації про розподіл трафіку, необхідного для інтерпретації протоколів. Для цього

необхідно впорядкувати весь захоплений трафік за наявністю різних протоколів та представити це у табл.2.

Таблиця 2. Протоколи, які використані в захоплених пакетах

Protocol /Прото-кол	Packets/ Пакети, kbit	Packets Size byte/ Розмір всіх пакетів	Avera-ge kbits/s/ Сере-дня швид-кість
Ipv6	796	72940	591
Ipv4	60635,7	6600731	534
UDP	678	107824	873
DNS	504	99700	808
TCP	16426,3	63665319	534
HTP	820	548548	444
ARP	5273	315822	456
Всього	75133 пакетів	71303168 Byte	

Для візуального представлення захоплених пакетів необхідно використовувати такий інструмент як Wireshark IO Graphs, в якому можна відобразити появу захоплених пакетів в залежності від усього часу захоплення (рис. 2). На даному графіку представлена поява пакетів, які відносяться до чотирьох основних протоколів мережі. На графіку видно, що більшість 14 пакетів належать протоколу IP [7]. Не важко побачити, що захоплення пакетів на конкретному проміжку часу нерівномірне, а стрибкоподібне, пояснюється це тим, що швидкість з'єднання з мережею інтернет не постійна. У процесі аналізу мережевого трафіку локальної мережі за допомогою системного інструменту можна визначити наявність пакетів з помилками або попередженнями [5-6]. Для цього існує спеціальний інструмент, передбачений Wireshark. Expert Information - журнал в якому відображені помилки, попередження, примітки, викликані мережевими «аномаліями». (рис. 3).

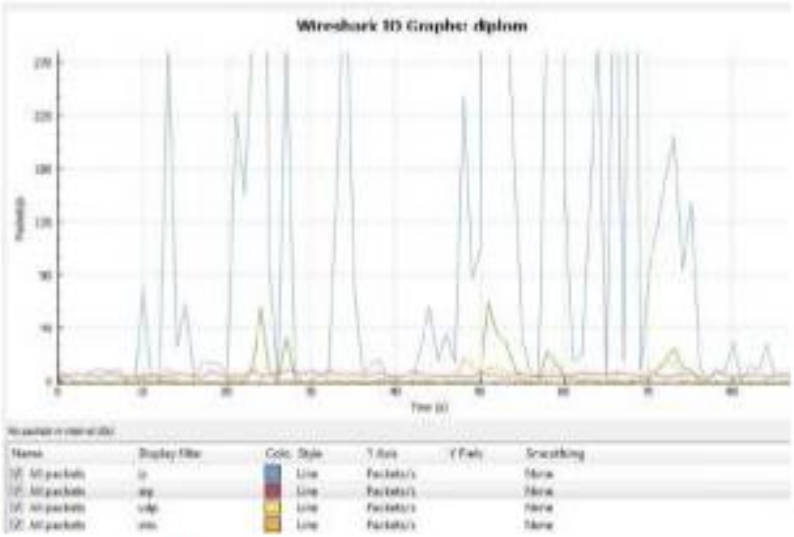


Рис. 2. Графічне представлення захоплення пакетів

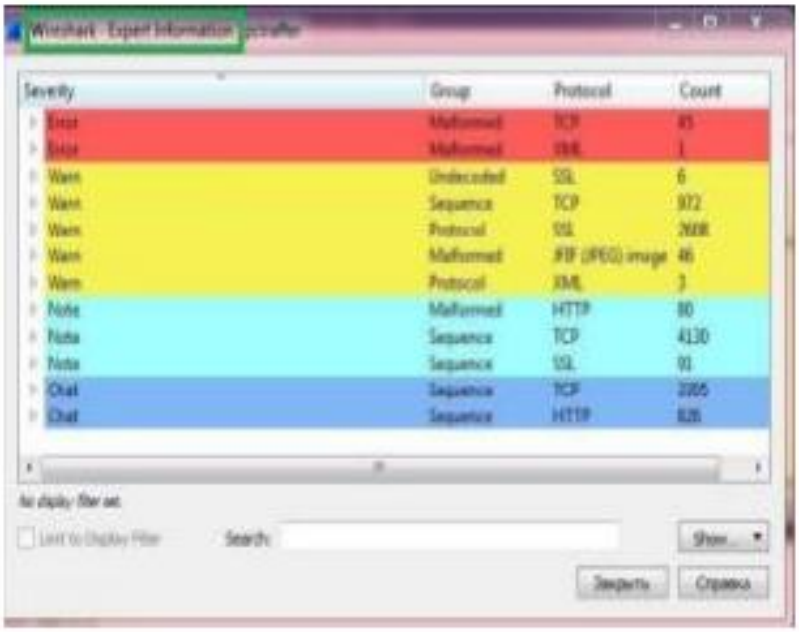


Рис. 3. Expert information

Одним з корисних інструментів в Wireshark є GeoIp Database. Даний інструмент дозволяє додати додаткову інформацію по захопленим пакетам. Додатковою інформацією буде прикріплення до кожного захопленого пакету інформації про ір адресу, а саме його місце розташування на карті. Це дає можливість дізнатися звідки був отриманий пакет, з якої країни, адреса, власник ір адреси і його місце розташування на карті.

Лекція 10
Відновлення даних

Іноді виникають ситуації, коли вже видалений файл виявляється дуже потрібним. Сучасні носії інформації дають змогу відновлювати такі файли.

Видалення – поняття відносне. Справа в тому, що насправді дані при видаленні залишаються на носію, просто Windows їх не відображає і в подальшому не буде «турбуватися» про їх збереження. Тобто, якщо користувач після видалення файлу на той самий носій буде зберігати інші дані, операційна система може записувати їх поверх видалених файлів, що знижує ймовірність успішного їх відновлення за необхідності.

Практично нереально відновити видалений файл, якщо на носій після його видалення був збережений файл такого ж формату з такою ж назвою. Це стосується у першу чергу носіїв для фото-, відеокамер та інших пристроїв, які автоматично, за певним алгоритмом, створюють назви для файлів, які ними записуються.

Як відбувається втрата даних

Є кілька причин «зникнення» інформації з жорстких дисків, карт пам'яті чи Flash.

1. Файли було видалено через недогляд чи то з незнання. Поки вони знаходяться в кошику Windows, їх порятунок можливо без спеціальних коштів. Інакше доведеться використовувати програму відновлення даних.

2.Користувач відформатував чи випадково видалив на жорсткому диску одне із розділів. У цьому всі дані, записані ньому, губляться.

3.Додаток працював з помилками і неправильно зберіг файл.

4.Шкідлива програма змінила чи видалила файли з жорсткого диска.

5.Апаратна несправність чи механічні ушкодження призвели до того, що окремі файли і навіть весь диск стають недоступними для Windows.

Операційна система намагається запобігти випадковим втратам і запрошує підтвердження на видалення інформації, але ефективність цього

украй низка. Для будь-якого більш-менш просунутого користувача це вже ритуал - натисни Delete, потім Enter. Попередження ніхто не читає, а кнопка «Так» виділена за умовчанням.

Дієвим методом є двоетапне видалення. При цьому файл, що видаляється, спочатку поміщається в спеціальну системну теку - Корзину. З Корзини помилково видалений файл легко повернути на колишнє місце. Але і це не дає стовідсоткової гарантії. По-перше, багато хто видаляє файли мимо Корзини - для цього треба утримувати Shift при натисненні клавіші або виборі пункту меню Delete. По-друге, Корзина може бути відключена або переповнена. Ніяких спеціальних попереджень при цьому не виникає. По-третє, файли, видалені з командного рядка, програми DOS або будь-якої 16-розрядної програми, в Корзину не потрапляють. Нарешті, корзину можна просто очистити.

Але і це ще не все видаливши з дискети інформацію слід пам′ятати, що для дискети «Корзина» не працює. Точно також йде справа і з накопичувачами - на знімних дисках, Корзина за умовчанням не передбачена.

На щастя програмісти Microsoft були вельми ледачі або просто економили ресурси системи. Файлова система влаштована так, що навіть остаточно видалений файл насправді нікуди не віддаляється і не стирається. Він просто позначається як видалений, але залишається на своєму місці, живий і здоровий. І лише коли при черговому записі на диск операційна система перезапише нову інформацію на це ж місце - ось тоді з файлом можна попрощатися. Втім, говорять, що спецслужби за допомогою особливих прийомів можуть відновлювати інформацію навіть після двох-трьох перезаписів, але простому смертному такі методи недоступні.

Види втрати даних. Порятунок даних

Шанси на успіх за відновлення даних залежать, передусім, причини, що спричинила їх втрату.

- Кошик. Якщо є ще зберігаються у кошику Windows, їх можна безборонно відновити засобами самої ОС, оскільки файли не віддалені, а й

просто переміщені в папку Recycler. Подвійний щиголь по значку кошика покаже все які у ній файли. Правою кнопкою миші клацніть по значку файла й у розпочатому меню виберіть «Відновити» – файл повернеться на початкове місце.

Важливо! Кошик має обмежену ємність, за умовчанням 5–10% від розміру диска. Якщо місце закінчується, Windows автоматично видаляє найстаріші файли, й у разі функція «Відновити» не допоможе.

- Файли відсутні в кошику. Якщо файли вже стерті у зв'язку з старістю, чи було видалено безпосередньо, без проміжного приміщення у кошик, ситуація значно гірше. У Windows немає необхідних коштів, для доступу до таких файлам.

Бо тепер вони відсутні як і файлової системі ОС, і у головною файлової таблиці (>MFT –MasterFileTable) жорсткого диска, Windows звільняє займане ними місце для записи інших файлів. Проте файли усе ще перебувають на жорсткому диску. Часто є підстави відновлено в цілому або хоча б частково з допомогою спеціальних програм. Але це має зроблено якомога швидше, поки Windows не затерла їх.

Важливо! Чим раніше запустять програму відновлення, тим більша імовірність спасіння даних. Якщо шукані файли були затерті на диску, програма здебільшого відновлює їх повністю.

Хороша програма вміє рятувати, поки що тільки неперезаписані області віддалених файлів.

- Видалений чи відформатований розділ жорсткого диска. При форматуванні будь-якого диска його зміст повністю очищається. Попри це, хороші програми-реаніматори здебільшого у змозі відновити багато файлів.

Програмне забезпечення зможе допомогти у тому разі, коли було видалено весь розділ. Якщо після цього ніякі нові розділи не створювалися, файли ще збереглися і з них може бути врятовані програмою відновлення.

- Багаторазово перезаписані файли. Файли, стерті з допомогою програм безпечного видалення, (наприклад Paragon Disk Wiper), а як і багаторазово

перезаписані іншою інформацією. У такому разі не допоможуть навіть кращі програми відновлення даних, і фахівці з лабораторій, «інформація справді загублена незворотньо».

- Механічний дефект. Як і кожен механічний пристрій, жорсткий диск може просто зламатися. На старих, порівняно гучних жорстких дисках знайти несправність дозволяв гучний стукіт включення чи раптове припинення «дзижчання» диска.

У накопичувачів про загрозу появи дефекту кажуть лише малопомітні ознаки

Програми для відновлення даних

Відновити видалений файл в FAT дуже легко. Настільки легко, що це використовується як завдання для лабораторної роботи по програмуванню на першому курсі інституту. Більш того, файли часто можна відновити навіть після "швидкого" форматування диска. У NTFS це лише небагато чим складніше. Тому в Інтернеті видимо-невидимо утиліт для відновлення даних на будь-який смак. Деякі програми є комерційними і коштують від декількох десятків до сотень доларів. Сюди можна віднести, наприклад, відому утиліту Unerase з пакету Norton Utilities, File Rescue Software компанії Shelf International, File Scavenger компанії Quetek Consulting і RECOVERNT від LC Technology International.

Багато програм розповсюджуються за принципом Shareware, надаючи користувачеві демо-версію з деякими обмеженнями, наприклад по терміну використання або розміру відновлюваних файлів. Деякі shareware-програми повністю функціональні, за одним-єдиним виключенням - не дозволяють до оплати зберегти відновлювані файли. Вельми непоганий прийом для залучення покупців. До shareware відноситься дуже могутня і багатофункціональна програма Easy Recovery.

Але звичайним користувачам, не схильним до склерозу або нападів люті, утиліти для відновлення потрібні раз на рік, і купувати програму для відновлення видаленої фотографії «Я і мій собака» морочливо і невигідно. Горюватимемо і

забудемо? Ні, вихід є! Можна знайти freeware-програму, тобто абсолютно безкоштовну. Звичайно, функціональність таких програм трохи менше, чим у комерційних, але адже ми і не збираємося відновлювати RAID-масиви?

Отже, Undelete Plus від Touchstone Software. Безкоштовна, але добротно зроблена програма. Розмір дистрибутива - 850 кілобайт. Для порівняння, Easy Recovery 6 не уміщалася в 28 мегабайт. Про якість розробки можна судити вже по тому, що інтерфейс програми доступний на 27 мовах, перемиканих «на льоту». У числі підтримуваних - російський, японський, турецький і навіть африканський. Робота з програмою інтуїтивно зрозуміла і не викликає особливих затруднень.

Після запуску ми потрапляємо в основне вікно програми. У лівій частині вікна необхідно вибрати диск, файли на якому ми хочемо відновити, а потім натиснути кнопку «Сканувати». При скануванні диска програма шукає всі видалені файли і відображає їх в списку в правій частині вікна. Undelete Plus автоматично аналізує стан файлу і, залежно від шансів на відновлення, класифікує по чотирьох групах - «відмінний», «хороший», «так собі» і «перезаписаний».

Список файлів, особливо для жорстких дисків, виходить вельми значний. Список можна фільтрувати по початковому місцеположенню, типам файлів, частині імені, розміру файлів, датам створення і модифікування, так що знайти необхідний файл простіше простого. Відзначивши потрібні файли і вибравши місце для їх відновлення, натискаємо кнопку «Відновити». І ось диво відбулося! Звичайно, може опинитися, що усередині файлу замість осмисленого тексту записано сміття, але відсоток відновлення достатньо великий.

Для збільшення шансів на благополучне завершення процесу необхідно дотримувати декілька правив. Це торкається не тільки Undelete Plus, але і будь-якої іншої програми відновлення. Перш за все, як тільки ви виявили пропажу інформації, негайно вимикайте комп'ютер. Звичайно, не варто видирати вилку з розетки, може опинитися, що разом з однією фотографією ви втратите весь диск цілком.

Але чим менше працював комп'ютер з моменту видалення, тим більше шансів на відновлення. Ідеальний варіант - витягнути диск і всі експерименти проводити, підключивши його до іншого комп'ютера. Ще одна хитрість - у жодному випадку не слід вибирати для запису відновлених файлів той же диск, на якому вони були розташовані. До моменту відновлення всі ці файли для операційної системи - примари. Отже, записуючи один файл, вона легко погубить інший. І ще невідомо, який з них був цінніший.

У всього цього є і оборотна сторона. Тепер ви знаєте, що видалити файли і очистити Корзину абсолютно недостатньо для захована ваших секретів. Тому для видалення дійсно важливої інформації слід використовувати спеціальні програми для знищення файлів. Принцип їх дії простий - на місце файлу, що видаляється, вони записують випадкове сміття, причому роблять це декілька десятків разів, і лише потім позначають файл як видалений. Такі програми також можна легко знайти в Інтернеті, причому багато - абсолютно безкоштовно.

Проте не варто думати, що все виправно. Як говорив Остап Бендер, «повний спокій може дати людині тільки страховий поліс». За інформацією фахівців компанії Ontrack, одна година простою через втрату інформації для крупної брокерської компанії може обійтися в сотні мільйонів доларів. У наше століття загальної інформатизації всього лише десятиденну бездіяльність комп'ютера наносить необоротний фінансовий збиток будь-якій фірмі. Майже половина компаній, постраждавших від втрати інформації, протягом подальших п'яти років перестали існувати.

Практичне використання

Як показала практика не кожен спосіб відновлення даних про які розповідається на сайтах і блогах всесвітньої мережі є настільки дієвим наскільки потрібно, і як про нього розказують. Виявилось, що програма Undelete про яку в Інтернеті я знайшла хороші відгуки не виконала того що від неї очікувалось. З відновленням видалених файлів найкраще впоралась програма Recuva, вона допомогла нам вішукати ті файли які були видалені. Ще одним завданням було відновлення видаленого диску. Тож для цього завдання

ми використовували програму Acronis Disk Director 11.0.234. Рекомендацій як таких і відгуків у всесвітній мережі небагато, але для тих хто знає нічого дивного немає. Отож, для відновлення різних видів файлі і різного виду причин їх знищення ми знайшли декілька програм, але використали ті, які виявились найкращими.

Висновки

Отже, навіть якщо ви необережно видалили необхідні вам файли, чи через збій в системі вони зникли, не варто зневірюватись. Все можна повернути, головне правильно це зробити. Як показала практика найдієвішим способом відновлювати втрачені дані є використання спеціальних програм таких як Recuva та Undelete, якщо ж необхідно відновити цілий диск то найкраще використовувати програму Acronis Disk Director 11.0.234.

Лекція 11.
Продукти аналізу і обробки ризиків інформаційної безпеки

Рівень інформаційного суспільства провідної держави світу характеризується показниками сучасних наукоємних технологій у яких відіграють основну роль інформаційно-телекомунікаційні системи (ІТС). Захист інформації є важливою складовою частиною підтримання національної безпеки України. Організація захисту інформації здійснюється за допомогою системи правових, організаційних та інженерно-технічних заходів. Розвиток національної безпеки і оборони держави залежить від взаємодії та спільного використання інформаційних технологій об’єднаних у єдиний інформаційно-телекомунікаційний простір.

Сучасний етап розвитку нашої держави визначається соціально-політичною та економічною нестабільністю різних суспільних факторів, які приводять до ведення інформаційних війн. У протидії інформаційним війнам слід приділяти велику увагу захисту державним інформаційним ресурсам. Адже загрози інформаційної безпеки держави відіграють головну роль в системі захисту ІТС [1, с. 16]. Визначення терміну «інформаційна безпека» (ІБ) у більш вузькому значенні має характер процесу забезпечення конфіденційності, цілісності та доступності.

Існує досить великий клас систем обробки інформації, під час розробці яких фактор безпеки відіграє першорядну роль (наприклад, банківські, інформаційні, медичні, економічні та лінгвістичні системи). Одним з важливих організаційних заходів захисту інформації в комп’ютеризованих системах є визначення переліку загроз інформації, які порушують її властивості –

конфіденційність, цілісність та доступність. Одна або декілька загроз можуть використовувати ряд уразливостей інформації. Будь-яка зміна загроз та уразливостей може мати значний вплив на ІБ. Раннє виявлення або знання про ці зміни збільшує можливості щодо прийняття необхідних заходів для обробки ризику та забезпечення безпеки ІТС у цілому. Це досягається за рахунок інструментальних методів визначення ризиків інформаційної безпеки в ІТС. Таким чином метою статті є проведення аналізу існуючих інструментальних методів визначення ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах, що і зумовлює актуальність тематики статті.

Питання аналізу ризиків інформаційної безпеки висвітлені у наукових працях та інформаційно-довідкових матеріалах. Проблемами дослідження інформаційної безпеки в ІТС займаються як вітчизняні вчені (Горбенко І. Д., Домарєв В. В., Корченко О. Г., Юдін О. К.), так і зарубіжні (Астахов А. М., Daniel Wentre, Thomas R., Whitman M.). У праці [1, с. 2] проведено аналіз сучасного забезпечення захисту державних інформаційних ресурсів (ДІР) в ІТС. Проведено аналіз та систематизовано підходи до класифікації загроз інформаційним ресурсам у цілому. В монографії проведено нормативно-правовий аналіз напрямів, пов’язаних із впровадженням реєстру державних Наукоємні технології № 3 (35), 2017 216 © Бучик С. С., Шалаєв В. О., 2017 електронних інформаційних ресурсів, досліджено шляхи подальшої реалізації проблематики, в тому числі шляхом подальшого розроблення інструментального засобу аналізу ризиків ІБ ДІР. У праці [2, с. 138] розглянуто підходи і програмні рішення оцінки і контролю інформаційних ризиків як фундаментального організаційного етапу при побудові системи захисту інформації комп’ютеризованих систем. У праці [3, с. 128] проведено аналіз процесу управління ризиками інформаційної безпеки в контексті забезпечення неперервності функціонування система захисту інформації. Надана оцінка процесу управління ризиками, проаналізовані сучасні методики управління ризиками інформаційної безпеки. Запропоновано удосконалений алгоритм адаптованої методики управління ризиками при забезпеченні живучості та неперервності функціонування системи захисту інформації в інформаційно-телекомунікаційній системи. У праці [4, с. 33] запропоновано та проаналізовано удосконалену методику оцінювання інформаційного ризику в автоматизованій системі. Висвітлено необхідні нормативно-правові документи інформаційної безпеки. Розглянуто роботу прототипу експертної системи, яка дозволяє оцінити рівень інформаційного ризику для певної автоматизованої системи та визначити необхідність застосування додаткових заходів інформаційної безпеки. У праці [5, с. 75] проведено аналіз процесу роботи найбільш поширених моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах. Розкрито основні підходи до оцінювання ризиків інформаційної безпеки. У праці [6, с. 60] розглянуто

програмні продукти аналізу та управлінням інформаційними ризиками. Одержано чітку структуру функціонування програм: розкрито алгоритмічні принципи побудови, формати шаблонів, графічні інтерфейси, методики управління та визначення рівня загрози ризику. Проаналізовано програмні продукти управлінням інформаційними ризиками на відповідність вимогам основних міжнародних стандартів інформаційної безпеки. У праці [7, с. 2] розглянуто підходи і програмні рішення оцінки і контролю інформаційних ризиків як фундаментального організаційного етапу при побудові системи захисту інформації комп'ютеризованих систем. Постановка завдання Виходячи з поставленої мети, необхідно здійснити аналіз існуючих інструментальних методів оцінювання та управління ризиками в інформаційно-телекомунікаційних системах з використанням вимог сучасних стандартів у галузі управління інформаційною безпекою та провести аналіз їх основних характеристик. Виклад основного матеріалу З розвитком інформаційних технологій на сьогодні постає проблема забезпечення інформаційної безпеки та технічного захисту інформаційних ресурсів в комп'ютеризованих системах [2, с. 138]. Як показує огляд інформаційних джерел, у галузі оцінки та управління інформаційними ризиками в ІТС на даний момент переважають інструментальні засоби їх оцінки такі, як CRAMM, Risk Watch, ГРИФ 2006, NIST, COBRA, OCTAVE. Оцінка ризиків є зараз одним з актуальних напрямків у сфері регулювання банківської діяльності. У загальному випадку можна виділити такі складові управління ризиками [4, с. 36–37]: 1. Моніторинг та оцінювання організаційних ризиків функціонування системи. 2. Моніторинг та оцінювання ризиків технічних засобів. 3. Прийняття рішення з управління ризиками на основі наявних оцінок. 4. Проведення безпосередньої роботи з управління ризиками. Умовно проблематику аналізу ризиків можна поділити на дві групи. До першої належить розроблення наукових методів аналізу ризиків на основі відомих теорій та вимог стандартів щодо створення системи управління інформаційної безпеки (СУІБ). Друга група містить спеціалізовані програмні продукти, які, зазвичай базуються на методах першої групи, але мають більшу практичну спрямованість і краще враховують специфіку об'єкта захисту. Серед існуючих загроз, що сформувалися з розвитком інформаційних технологій, важливу роль необхідно приділити засобам впливу на інформаційну інфраструктуру ІТС та захищеність ДІР (комп'ютерні віруси, мережеві «трояни», які спотворюють, знищують інформацію та здійснюють інші види комп'ютерної злочинності). Відповідно до стандартів ISO/IEC 27005 та ISO/IEC TR 13335-2 оцінювання ризиків включає такі етапи:

1. Оцінку ймовірності можливих загроз і уразливостей.

2. Розрахунок ступеню впливу, який може мати загрозу на кожен актив.

3. Визначення кількісної (виміряної) або якісної (описуваної) вартості ризику. Наукоємні технології № 3 (35), 2017 217 © Бучик С. С., Шалаєв В. О.,

2017 Оцінювання ризиків полягає у визначенні кількісних та якісних показників, формуванні реєстру ризиків та ранжируванні ризиків [11].

Метод, який використовується для роботи вибраного продукту оцінювання ризиків ІБ ІТС повинен з високою ефективністю відображати формування звітів про результати оцінки ризиків. Ефективність використання продукту залежить від того, на скільки добре користувач його розуміє, а також від правильності встановлення та налаштування даного продукту [11]. З аналізу інструментальних методів визначення ризиків інформаційної безпеки, які є найбільш поширеними для вирішення задачі протиборства інформаційним загрозам в ІТС, схема інструментальних методів визначення ризиків інформаційної безпеки може бути приведена до вигляду рис. 1.

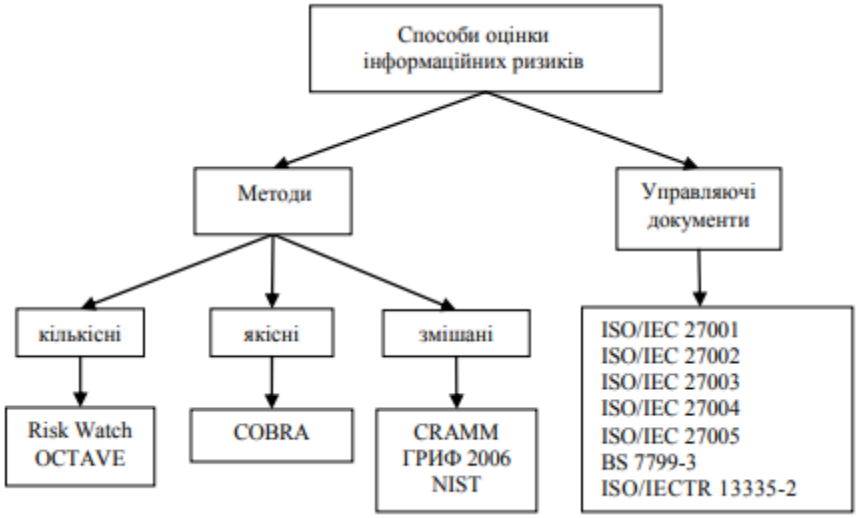


Рис. 1. Схема інструментальних методів визначення ризиків інформаційної безпеки в ІТС

Автор праці [12, с. 424] вважає, що при розробці методу визначення оцінки ризиків ІБ обов'язково повинне проводитися оцінювання граничнодопустимого та існуючого ризику виникнення загрози протягом деякого часу. А для цього має бути отримані значення вірогідності виникнення загрози на протязі певного часу.

Практика показує, що для більшості існуючих загроз неможливо отримати достовірні дані про вірогідність реалізації загрози, тому для вирішення цієї проблеми існують методи кількісної оцінки визначення ризиків ІБ. При розробці методу визначення ризиків можуть бути використані методи системного аналізу. Проаналізуємо методи визначення ризиків ІБ, які найбільш поширені в ІТС та банківських структурах для забезпечення захисту інформації та визначення ризиків, які переростають в потенційну загрозу. Британський CRAMM (the UK Government Risk Analysis and Management Method). Інтерфейс інструментального засобу оцінювання ризиків ІБ CRAMM наведено на рис. 2. Метод CRAMM був розроблений службою безпеки Великої Британії та взятий на озброєння як державний стандарт. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, який поєднує кількісні та якісні методи

аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій для отримання відповідних результатів економічного обґрунтування витрат організації на забезпечення інформаційної безпеки [9, с. 80].

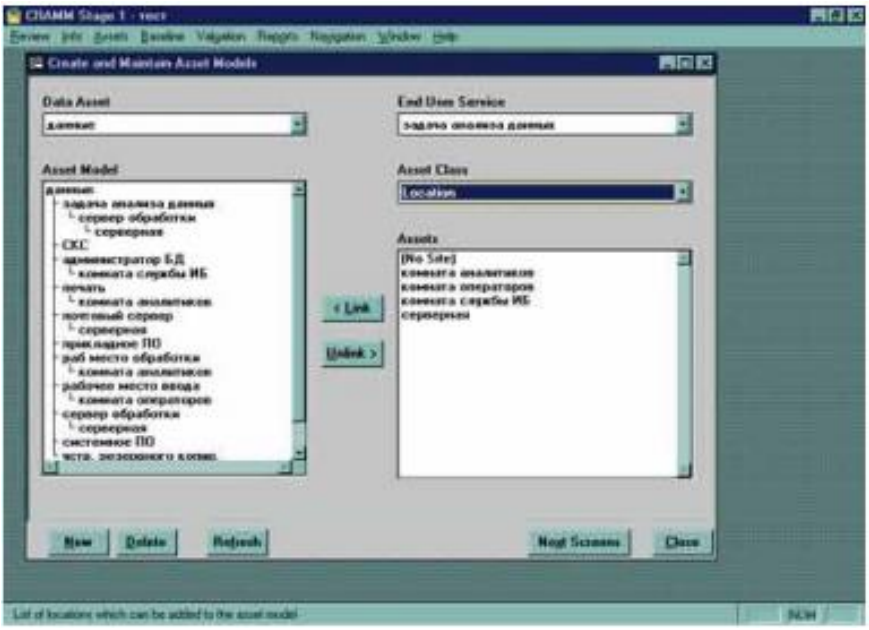


Рис. 2. Інтерфейс методу CRAMM

Метод CRAMM має базу знань по ризикам і видам їх мінімізації, засоби збору інформації, формування звітів, а також реалізує алгоритм для визначення величини ризику [11].

Метод CRAMM пропонує всі процедури методу поділити на три послідовних етапи, які розглянуто на рис. 3. У метод CRAMM закладено широкий набір типових рекомендацій щодо проведення контрзаходів для зменшення ризиків ІБ ІТС, але її ефективне використання можливе тільки фахівцями вищої кваліфікації. Перевагами методу CRAMM:

− даний метод є універсальним і підходить, як для державного, так і комерційного використання;

− має властивість кількісної та якісної оцінки ризиків;

− оптимальні затрати на засоби контролю та захисту інформації;

− оперативність в прийнятті рішення з питань управління безпекою [9, с. 89].

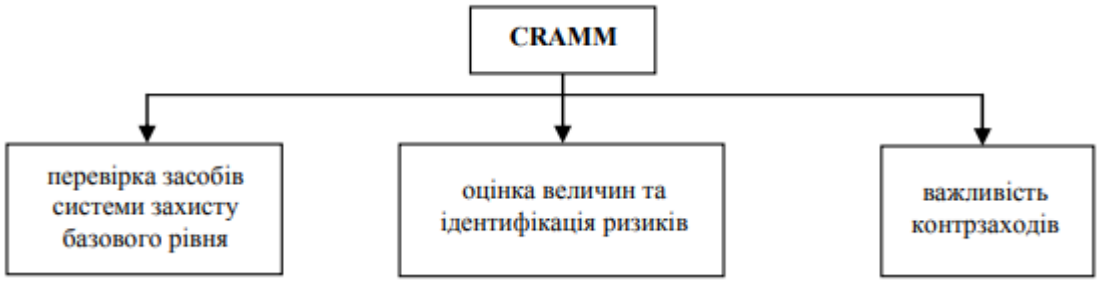


Рис. 3. Етапи проведення аналізу ризиків ІБ методом CRAMM

До недоліків CRAMM можна віднести:

− використання даного методу вимагає спеціальної підготовки користувача;

− потребує велику кількість годин безперервної роботи з аналізу інформації; − відсутня можливість внесення додатків у базу даних та знань;

− припускає використання лише методів зниження рівня ризиків ІБ, такі способи управління ризиками, як «уникнення» або «прийняття», не розглядаються;

− програмне забезпечення CRAMM існує тільки на англійській мові [3, с. 131];

− дане програмне забезпечення є платним — вартість від $ 2000 до $ 5000.

Наступним програмним забезпеченням є експертна система Risk Watch (розроблений компанією Risk Watch), яка презентує себе як потужний засіб аналізу та управління ризиками. Інтерфейс експертної системи аналізу та управління ризиками ІБ Risk Watch представлено на рис. 4. RiskWatch являє собою сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів [11, 5, с. 76].

Рис. 4. Інтерфейс методу RiskWatch

Система Risk Watch допомагає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту ІБ в ІТС. Даний метод забезпечує проведення аналізу ризиків ІБ та включає чотири етапи роботи, які представлено на рис. 5 [5, с. 76].

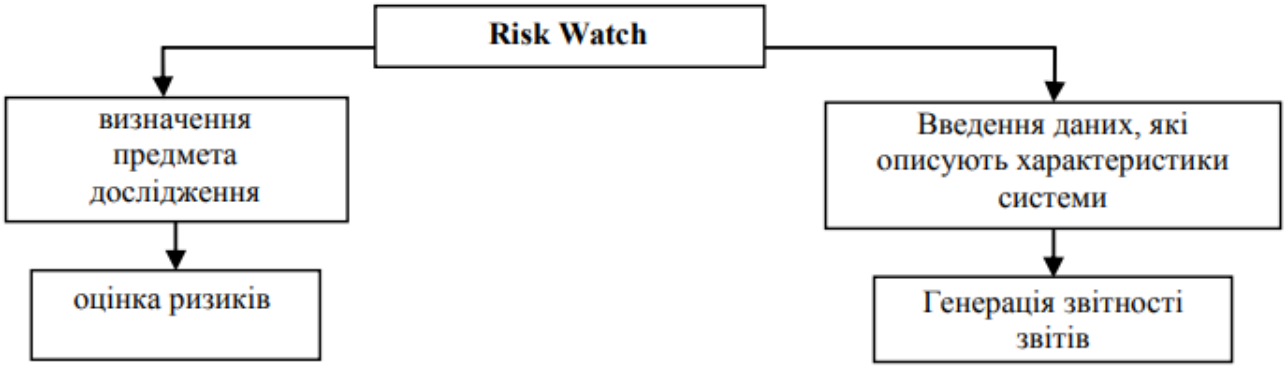


Рис. 5. Етапи проведення аналізу ризиків ІБ методом Risk Watch

У результаті аналізу експертної системи Risk Watch можна дійти висновку, що трудомісткість робіт з аналізу ризиків цим методом порівняно невелика.

З точки зору вітчизняного споживача порівняльною характеристикою Risk Watch є його простота, мала трудомісткість перекладу інтерфейсу і велика гнучкість, що забезпечує можливість створення своїх нових профілів захищеності та є основною перевагою даного методу.

До недоліків Risk Watch можна віднести:

− метод ефективний лише при проведенні аналізу ризиків на програмно-технічному рівні захисту без урахування організаційних і адміністративних чинників;

− дане програмне забезпечення англомовне;

− висока вартість ліцензії — $ 15000.

На основі цього методу вітчизняні розробники можуть створювати свої профілі, що відбивають вітчизняні вимоги у сфері безпеки, розробляти відомчі методики аналізу і управління ризиками [2, с. 141]. На рис. 6 представлено інтерфейс методу ГРИФ 2006.

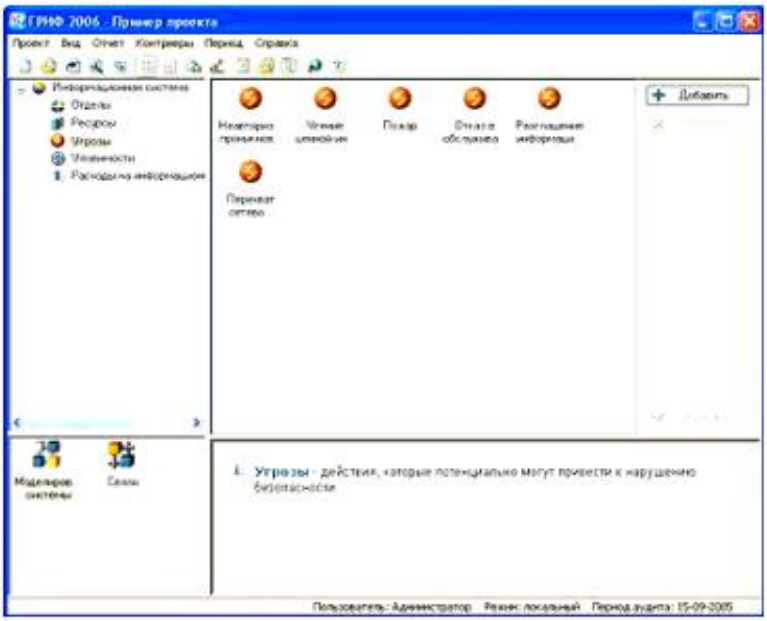


Рис. 6. Інтерфейс методу ГРИФ 2006

Для побудови повної моделі автоматизованої системи з погляду ІБ є програмний комплекс ГРИФ 2006 з достатньо простим та зрозумілим для користувача інтерфейсом. Основним завданням даного методу — надати можливість користувачу самостійно (без залучення сторонніх експертів) оцінити рівень ризиків в інформаційній системі, оцінити ефективність існуючої практики щодо забезпечення безпеки системи. Для визначення рівня ризиків в інформаційній системі метод ГРИФ 2006 передбачає такі етапи роботи, які розглянуто на рис. 7. Метод ГРИФ 2006 має модуль управління ризиками, який надає змогу проаналізувати всі причини того значення ризику, який отримується після обробки алгоритмів занесених даних. Отже знаючи причини інформаційного ризику користувач буде володіти всіма даними необхідними для реалізації контрмір [8, с. 55].

У результаті роботи методу ГРИФ формується звіт рівня ризику за систему, причини виникнення ризику та аналіз уразливостей з оцінкою економічної ефективності всіх можливих контрмір.

Перевагами методу ГРИФ 2006 є:

− просте в використанні програмне рішення оцінки рівня ризиків в ІТС;

− можливість здійснення оцінки ризиків по різним інформаційним ресурсам;

− ефективність управління ризиками за допомогою вибору контрзаходів;

− не потребує спеціальних знань у сфері інформаційної безпеки.

До недоліків ГРИФ 2006 можна віднести:

− відсутність прив’язки до бізнес-процесів;

− відсутня можливість зрівнювання звітності на різних етапах втілення комплексу мір із забезпечення захищеності інформації.

Метод NIST (National Institute of Standards and Technology) є методом оцінки ризиків Національного інституту стандартів і технологій США. Запропонований процес управління ризиками ІБ представлено на рис. 8.

Рис. 7. Етапи методу ГРИФ 2006 для оцінки рівня ризиків в інформаційній системі

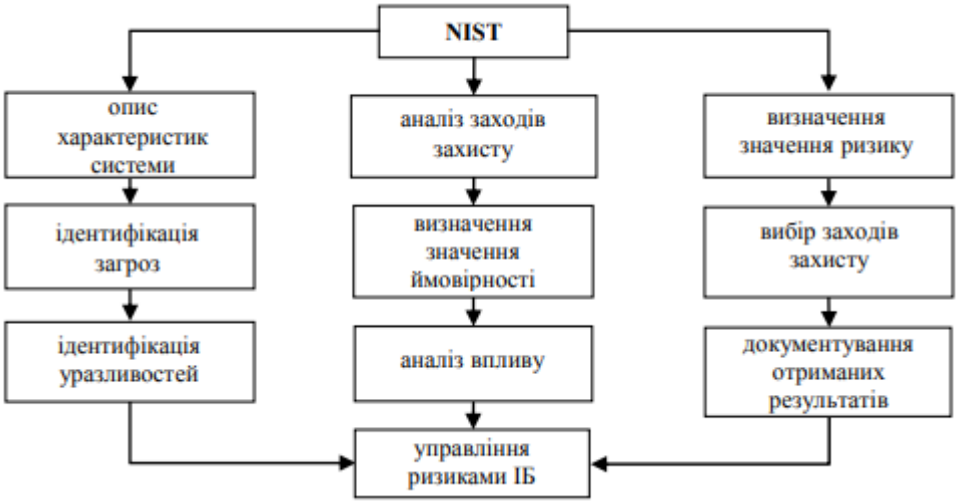


Рис. 8. Поетапний порядок роботи методу NIST

Цей метод передбачає попереднє оцінювання двох параметрів: потенційного збитку і ймовірності можливого інциденту. Такий механізм отримання оцінки ризику значно обмежує точність результатів, забезпечуючи при цьому оперативність та відтворюваність. Реалізація загрози ІБ в даному методі охоплює широке коло завдань, головним з яких є розроблення власної системи управління ризиками [3, с. 129]. Аналізуючи працю автора [2] можна дійти висновку, що дана методика охоплює широке коло завдань, які пов'язані з управлінням інформаційних ризиків і є основою для побудови власної системи управління ризиками. Інтерфейс методу NIST представлено на рис. 9.

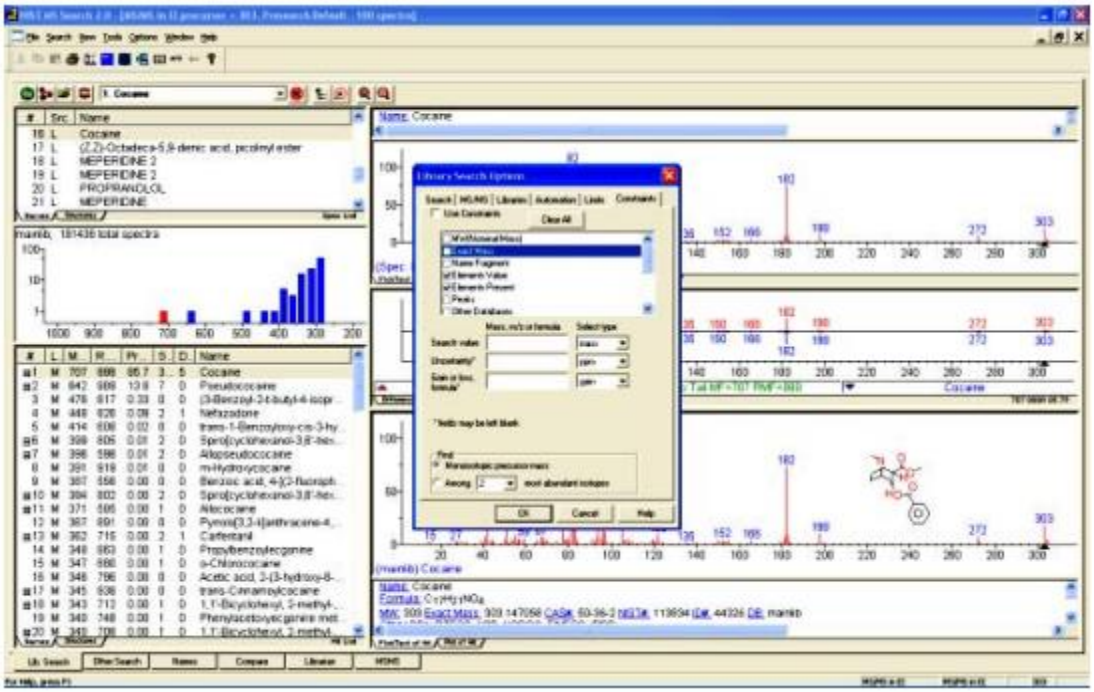


Рис. 9. Інтерфейс методу NIST

Перевагами методу NIST є:

− порівняно простий в реалізації; − детально описує всі можливі ризики для інформаційних активів;

− припускає використання способів зниження ризиків усіх можливих варіантів (прийняття, зниження, перенесення, уникнення ризику);

− програмному забезпеченню властива відносна легкість та зручність у використанні;

− не велика вартість ліцензії порівняно з іншими подібними експертними системами $ 149– $ 254.

До недоліків NIST можна віднести:

− довготривалий процес аналізу;

− програмне забезпечення розроблено на англійській мові;

− потребує спеціальних знань в області ІБ; − аналіз ризику проводиться за трирівневою шкалою.

Метод COBRA (Consultative Objective and BiFunctional Risk Analysis, developer — C & A Systems Security Ltd, Велика Британія) орієнтований на підтримку вимог стандарту ISO 17799. У комплект програмного забезпечення (ПЗ) входять модулі COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant, а також менеджер модуля COBRA, який призначений для налаштування та зміни наявної бази знань [10]. Цей метод дозволяє виконати в автоматизованому режимі найпростіший варіант оцінювання інформаційних ризиків будь-якого підприємства. Він оцінює відносну важливість усіх загроз і уразливостей, генерує відповідні рішення та рекомендації. Для цього пропонується використати спеціальні електронні бази знань та процедури логічного виводу, які відповідають вимогам відповідних стандартів [8]. Аналіз ооцінювання ризиків на основі тематичних запитів проводиться за наступними категориям, які розглянуто на рис. 10 [10].

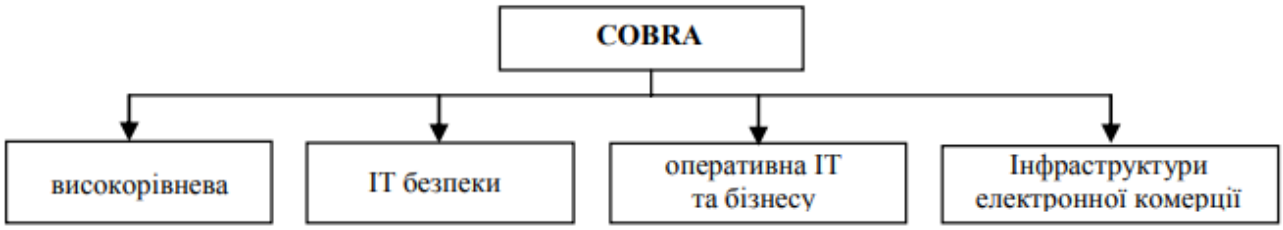


Рис. 10. Етапи оцінювання ризиків на основі тематичних запитів

Після описання всіх категорій та встановлення рівнів ризику, проводять певні міри щодо їх зниження. У результаті аналізу експертної системи COBRA можна дійти висновку, що аналіз ризиків, який буде здійснено даним методом, відповідає базовому рівню безпеки, тобто рівень ризиків не визначається, що і є основним недоліком для даного методу. Інтерфейс методу COBRA представлено на рис. 11.

Рис. 11. Інтерфейс методу COBRA

Переваги методу COBRA: • простота у використанні і, відносно, прийнятна вартість (усе залежить від бюджету, виділеного на ІБ) — $ 895 і $ 1995 за систему з модулем аналізу ризиків базового рівня. До недоліків COBRA можна віднести: • знання спеціальних електронних баз знань та процедур логічного виводу; • застарілий, не дуже зручний для користувача інтерфейс; • не визначається рівень ризиків, а лише базовий рівень безпеки; • відсутність підтримки української та російської мов; • виникають проблеми з генерацією звіту та можлива нестабільна робота під Win2000. OCTAVE. Зміст методу OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх робіт. Метод OCTAVE передбачає три фази аналізу ризиків: 1. Розробка профілю загроз, пов’язаних з активом. 2. Ідентифікація інфраструктурних уразливостей. 3. Розробка стратегії та планів безпеки. Цей метод пропонує скласти профіль загроз та дерево варіантів. Профіль загрози включає в себе вказівки на актив (asset), тип доступу до активу (access), джерело загрози (actor), тип порушення або мотив (motive), результат (outcome) і посилання на описи загрози в загальнодоступних каталогах [3, с. 133]. Методика OCTAVE пропонує при описі профілю використовувати «дерево варіантів», приклад подібного дерева представлено на рис. 12.

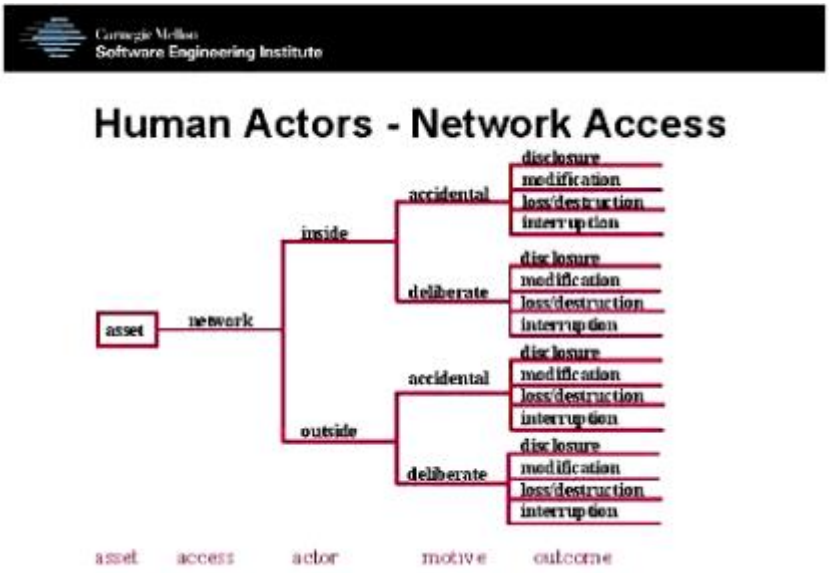


Рис. 12. Дерево варіантів, що використовується при описі профілю

Профіль загроз містить інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки [3, с. 131]. Відповідно до аналізу методики OCTAVE можна дійти до висновку, що дану експертну систему широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками ІБ в ІТС. Етапи аналізу ризику за методикою OCTAVE представлено на рис. 13 [6, с. 63].

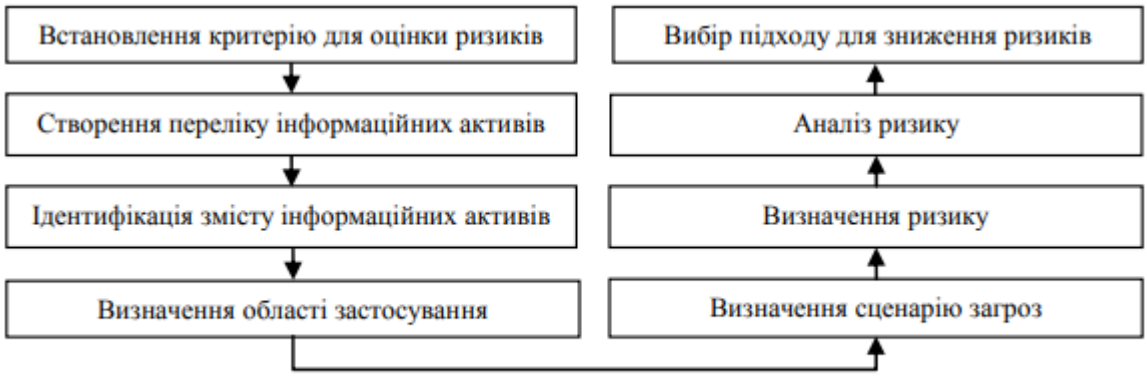


Рис. 13. Етапи аналізу ризику за методом OCTAVE [3, с. 131]

Переваги методу OCTAVE: • швидко впроваджується; • можливе застосування для організацій різного розміру та галузей застосування; • високий рівень гнучкості. До недоліків OCTAVE можна віднести: • відсутність надання кількісної оцінки ризиків; • припускає використання способів зниження ризиків і прийняття рішення; • не спрямований на специфіку банківської сфери. Існують різні OCTAVE методи, засновані на OCTAVE критеріях: OCTAVE, OCTAVE-S і OCTAVE Allegro. Інтерфейс методу OCTAVE представлено на рис. 13.

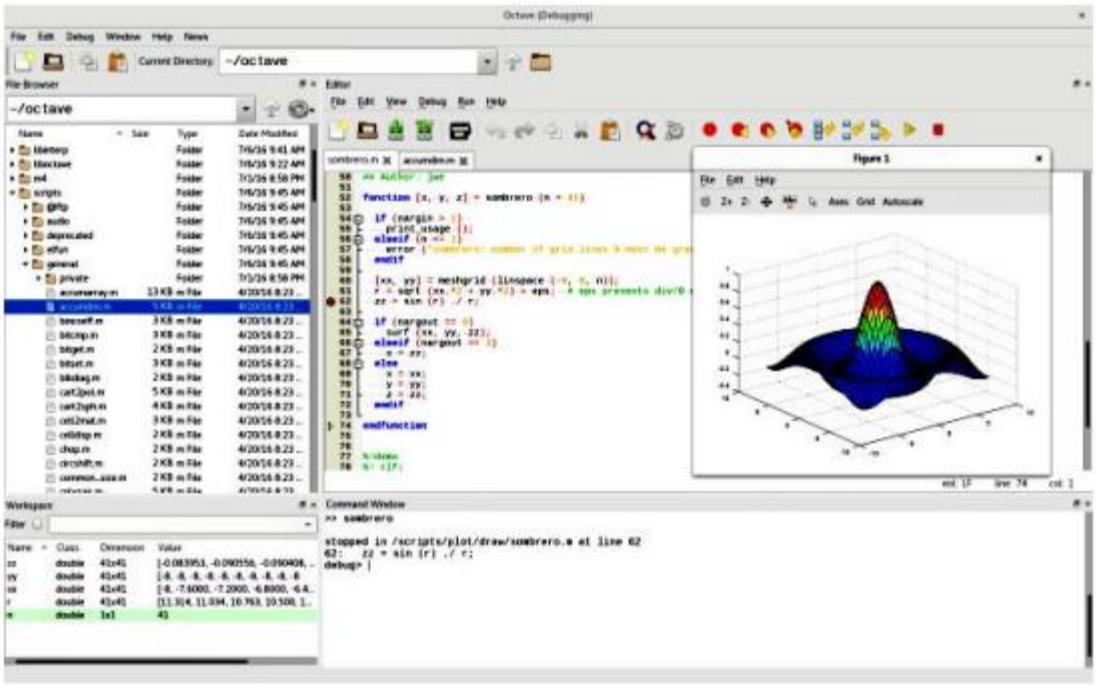


Рис. 13. Інтерфейс методу OCTAVE

Відмінністю методу OCTAVE від вище переглянутих є те, що при оцінці ризику дана експертна система дає тільки оцінку очікуваного збитку, без оцінки вірогідності. А також загальнодоступною та безкоштовною є вся документація по OCTAVE. Сьогодні існують окремі нормативно-правові документи, які регламентують питання ІБ, як основу для створення методів оцінювання інформаційних ризиків в ІТС [3]. Більшість програмних експертних систем відповідають міжнародному стандарту ISO/IEC 27001:2005. Відповідні Міжнародні стандарти визначають вимоги до СУІБ, управління ризиками, метрики і вимірювання, а також керівництво з впровадження [13, 8, с. 54]. Ключовою моделлю, що використовується у сфері управління ризиками інформаційної безпеки (УРІБ) модель, що знайшла відображення в усіх стандартних підходах до УРІБ і являє собою основу ISO/IEC 27005 і BS 7799-3 [13, 8, с. 55].

Дана модель дає перелік і послідовність таких необхідних для управління ризиками ІБ процесів, як планування, реалізація, перевірка, дія. Відповідно з даним стандартом документація, яка визначає управління інформаційними ризиками організації, повинна включати: документовану заяву про політику та цілі СУІБ; область програми СУІБ; процедури і засоби управління на підтримку СУІБ; опис методології оцінки ризиків; звіт про оцінки ризиків; план обробки ризиків [7, с. 199]. Цей стандарт підготовлений в якості моделі для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та покращення системи забезпечення інформаційної безпеки. Окрім вищезазначеного міжнародного стандарту існує ряд інших у галузі забезпечення ІБ в ІТС, розглянуті в табл. 1.

Таблиця 1 Міжнародні стандарти з керування методів для визначення інформаційних ризиків та їх коротка характеристика

Стандарт	Назва стандарту	Коротка характеристика
ISO/IEC 27002-2012	Інструкція з менеджменту інформаційної безпеки для телекомунікаційних організацій	Цей стандарт надає додаткові рекомендації з реалізації та менеджменту ІБ в телекомунікаційних організаціях. Визначає цілі, вимоги оцінки ризику до системи ІБ та забезпечує контроль управління. Діючий Міжнародний стандарт пропонує рекомендації та основні принципи введення, реалізацію, підтримку й поліпшення менеджменту ІБ
ISO/IEC 27003-2012	Інструкція з реалізації системи менеджменту ІБ	У цьому Міжнародному стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження в СМІБ відповідно зі стандартом ISO/IEC 27001:2005, який розглядає процес визначення та розробку СМІБ від початку до стану впровадження
ISO/IEC 27004-2011	Менеджмент інформаційної безпеки вимірювання	Цей стандарт містить рекомендації з розробки та використання вимірювань і заходів вимірювання для проведення оцінки ефективності реалізованої СМІБ. Процес вимірювання реалізується у вигляді програми, пов'язаний з ІБ. Програма вимірювань надає допомогу користувачу у виявленні і оцінюванні вимог, яким не відповідає процес ефективності контролю і управління СМІБ, а також визначення пріоритетів дій, спрямованих на удосконалення або зміну цих процесів
ISO/IEC 27005-2010	Менеджмент ризику інформаційної безпеки який конкретизує поняття інформаційного ризику	Цей стандарт поданий у вигляді додатку прикладу типових загроз, уразливостей та потреб інформаційної безпеки. Проблема оцінювання та дослідження інформаційних ризиків насамперед асоціюється з британським стандартом BS 7799, а саме з його двома частинами: першою — BS 7799-1 «Звіт правил з менеджменту безпеки інформації» та другою — BS 7799-2 «Системи менеджменту безпекою інформації», у яких вперше питання аналізу стану безпеки інформації та формування її захисту були напряму пов'язані з інформаційними ризиками. Однак, безпосередньо, аспекти оцінювання та управління ризиками були докладніше розглянуті у третій частині стандарту BS 7799-3 «Настанови з менеджменту ризиками безпеки інформації»
ISO/IEC TR 13335-2:1997	Настанови з керування безпекою інформаційних технологій (IT)	Надати рекомендації, а не конкретні рішення з керування безпекою інформаційних технологій (IT). Кваліфікація осіб, відповідальних за безпеку IT у межах організацій повинна бути достатньою для адаптування матеріалів, поданих у цьому стандарті, до конкретних потреб організацій

Аналізуючи основні міжнародні стандарти BS 7799-3 та ISO/IEC 27005, стає очевидним, що вони визначають усі найважливіші аспекти, пов'язані з інформаційними ризиками. Це стосується процесної моделі, елементів управління ризиками, підходів до аналізу ризиків, способам їх обробки тощо. Стандарт BS 7799-3 допускає використання, як якісних, так і кількісних методів оцінки ризику. Характерною рисою цього стандарту є принцип усвідомленості процесів оцінювання, оброблення, контролю та оптимізації ризиків в організації [11, 8, с. 55].

Лекція 12

Оцінка захищеності інформаційних систем від несанкціонованого доступу та інших загроз інформаційній безпеці.

Оцінкою інформаційної безпеки займаються з початку появи інформаційних технологій. З цієї тематики є багато праць, але найбільш актуальними та фундаментальними працями є нормативні документи, що зробили вагомий теоретичний та практичний внесок у розв'язання задач забезпечення інформаційної безпеки, а саме:

"Помаранчева книга" [2], у якій викладені та систематизовані критерії оцінки захисту комп'ютерних систем;

Європейські критерії оцінки безпеки інформаційних технологій [3], що врахували усі недоліки та обмеження, викладені у "Помаранчевій книзі";

Канадські критерії оцінки безпеки надійності комп'ютерних систем [4];

Федеральні критерії США [5], розроблені на замовлення уряду США і спрямовані на усунення обмежень, незручностей практичного застосування і недоліків "Помаранчевої книги";

Міжнародний стандарт ISO/IEC 15408 – "Критерії оцінки безпеки інформаційних технологій" [6–8]; Стандарт CEM-97/017 – "Загальна методологія оцінки безпеки інформаційних технологій" [9].

Окремо необхідно відзначити публікацію [10], в якій розглянуто використання коефіцієнта емерджентності для визначення рівня захисту інформаційних потоків для певного класу архітектури комп'ютерної мережі. Розглянуті нормативні документи є основою єдиної міжнародної науково-методологічної бази вирішення проблем забезпечення інформаційної безпеки в інформаційних ресурсах, системах та технологіях. Для вирішення завдань досягнення інформаційної безпеки, поряд з формальними методами моделювання процесів та оцінки ефективності функціонування систем, необхідно використовувати методи декомпозиції та структуризації компонентів систем і процесів, неформальні методи оцінки ефективності функціонування та прийняття рішень.

Використання сучасних систем інформаційної безпеки вимагає, з одного боку, відстеження швидких змін в інформаційних технологіях і загрозах, що з'являються, а з іншого боку – врахування реальних характеристик апаратного й програмного забезпечення корпоративних мереж і систем. Процедура придбання пристроїв інформаційної безпеки нескладна. Істотно складнішим є вирішення проблеми – як захищати і які засоби безпеки застосовувати з урахуванням мінімізації витрат. Упроваджуючи різні засоби захисту, необхідно визначити баланс між можливим збитком від несанкціонованого витоку інформації та розміром вкладень, які витрачені для забезпечення захищеності інформаційних ресурсів. Щоб підвищити ефективність захисту інформаційних ресурсів, необхідно дослідити підходи щодо оцінки рівня їх захисту та систем

захисту. Така оцінка для кожного окремого випадку є індивідуальною та залежить від багатьох факторів (вартість інформації, статусу організації, важливості інформації, рівня апаратного та програмного забезпечення тощо). Особливості захисту інформаційних ресурсів у корпоративних мережах Захист інформаційних ресурсів корпорації залежить від рівня програмних та апаратних засобів, що використовуються. Упроваджуючи інформаційні системи, кожна організація очікує максимально корисної функціональності для підтримки її бізнес-процесів. Захист даних в інформаційних системах будується заради захисту важливої інформації, втрата чи пошкодження якої призведе до значних грошових втрат.

Забезпечення захисту вимагає використання сучасних апаратних та програмних засобів для захисту інформаційних ресурсів компанії, що повинно забезпечувати цілісність, доступність та певний режим доступу до кожного з ресурсів. Цілісність передбачає незмінність інформації у будь-який час від моменту її створення, тобто вона повинна бути достовірною та містити сенс, що заклав її власник. Інформаційний ресурс зберігає цілісність за умов дотримання прав доступу до нього. Існування інформаційного ресурсу неможливе в автономному режимі без віддаленого доступу до нього, тому доступність інформації зумовлена нормальною взаємодією між її носієм та користувачем. Інформація зберігає доступність, якщо не втрачається взаємодія між носієм та користувачем інформації. Встановлення розподіленого режиму доступу забезпечує конфіденційність інформації на певному ресурсу.

Конфіденційність розуміють як недоступність інформації для користувачів, яким не надана можливість її використання. Конфіденційність інформації зберігається, якщо дотримується режимна адекватність під час ознайомлення з нею. Говорячи про інформаційні ресурси, необхідно зазначити, що їх функціонування неможливе без корпоративних мереж, тому доцільно висвітлити деякі їхні особливості. Корпоративна мережа, як правило, є територіально розподіленою, тобто об’єднує офіси, підрозділи та інші структури, значно віддалені один від одного. Часто вузли корпоративної мережі виявляються розташованими в різних містах, а іноді й країнах.

Принципи, за якими будується така мережа, доволі сильно відрізняються від тих, що використовуються під час створення локальної мережі, навіть якщо вона охоплює декілька будівель. Відповідно зростає складність системи захисту. Одним з принципів, покладених в основу створення мережі, є максимальне використання типових рішень, стандартних уніфікованих компонентів. Конкретизуючи цей принцип стосовно до прикладного програмного забезпечення, можна виділити універсальні сервіси, які доцільно зробити базовими компонентами захисту. Діяльність будь-якої сучасної організації багато в чому залежить від мережі Internet і тих сервісів, які вона надає, тому питання про доцільність використання Internet виникає дуже рідко.

Водночас дуже гостро ставиться питання про можливість використання всіх привілеїв та переваг, що надає мережа Internet, з мінімальним ризиком для діяльності організації. Тому сьогодні на перший план виходить проблема забезпечення безпеки в комп'ютерних інформаційних систем з боку мережевого впливу [1]. Цей сегмент удосконалюється і постійно розвивається, причому дуже динамічно.

Основними засобами захисту комп'ютерних інформаційних систем були, є і залишаються мережеві екрани (брандмауер, firewall, фільтрувальні маршрутизатори тощо). Мережеві екрани є лише інструментом системи безпеки. Вони надають певний рівень захисту і є засобом реалізації політики безпеки на мережевому рівні. Рівень безпеки, що надає мережевий екран, може варіюватися залежно від вимог безпеки. Існує традиційний компроміс між безпекою, простотою використання, вартістю, складністю тощо.

Мережевий екран є одним з декількох механізмів, що використовують для управління і спостереження за доступом до мережі з метою її захисту [11]. Сьогодні ніхто не заперечуватиме важливості системи антивірусної безпеки в інформаційній інфраструктурі будь-якої організації – це здебільшого найактуальніша система зі всього ряду розгорнутих систем забезпечення інформаційної безпеки. Звичайно, така ситуація виникла не сама по собі, а зумовлена передусім обвальним зростанням кількості нових комп'ютерних вірусів. Поширення глобальних мереж передавання даних надає можливість об'єднувати територіально віддалені локальні мережі організацій для створення так званих приватних віртуальних мереж (VPN). Глобальні мережі в цьому випадку виступають як транспортний компонент, що об'єднує локальні мережі в єдину інформаційно-обчислювальну систему.

Створення віртуальних мереж зумовило стрімке зростання глобальних мереж, однак для їх об'єднання використовуються виділені канали передавання даних, що призвело до: високої вартості оренди виділених каналів зв'язку; жорсткої прив'язки до розташування. Наприклад, у разі переїзду офісу одного з відділів організації з розгорнутим сегментом локальної мережі, що пов'язаний виділеним каналом із загальною мережею організації, виникають додаткові проблеми з подальшим під'єднанням локальної та загальної мережі.

Для вирішення проблеми передавання інформації через відкриті канали Інтернету використовують VPN рішення. VPN – це об'єднання декількох локальних мереж, підключених до мережі загального призначення, в єдину віртуальну (логічно виділену) мережу. VPN кошти організовують захищений тунель між двома точками засобами криптографії, надаючи широкі можливості з виборів алгоритмів аутентифікації, шифрування та перевірки цілісності потоку даних [12]. Оцінки рівня захисту інформаційних ресурсів Як правило, для оцінки рівня захисту необхідно спочатку визначити поточний стан інформаційної безпеки. Сьогодні існують два підходи щодо оцінки поточного

стану інформаційної безпеки, а саме “дослідження знизу догори “ та “дослідження згори донизу”.

Використання першого підходу полягає у тому, що адміністратори починають перевіряти систему захисту на усі відомі їм види атак. Отже, адміністратори виступають в ролі зловмисників, які роблять спроби порушити захист інформаційного ресурсу. Але відразу стає зрозуміло, що найталановитіші адміністратори не можуть знати усі можливі методи злому, а також усі програмноапаратні засоби зловмисників. Підхід “згори донизу” ґрунтується на детальному аналізі усіх відомих схем зберігання та обробки даних.

Спочатку визначають інформаційні об’єкти та потоки захисту, а потім досліджують сучасний стан систем інформаційного захисту з метою визначення реалізованих методик захисту інформаційних ресурсів, а також їх стан та рівень.

Далі проводиться класифікація всіх інформаційних об’єктів за класами відповідно до їх конфіденційності, вимог до доступності та цілісності.

Останнім кроком є “оцінка ризику” що полягає у визначенні розміру збитків фірми через порушення захисту кожного конкретного інформаційного ресурсу.

Наближеним ризиком називається добуток “можливого збитку від атаки” на “ймовірність цієї атаки”. Як правило, оцінка ризику складається з аналізу ризиків та оцінювання збитку. Під час аналізу ризиків проводиться інвентаризація та впорядкування інформаційних ресурсів, з’ясовуються нормативні, технічні, договірні вимоги до ресурсів у сфері інформаційної безпеки, після чого з урахуванням цих вимог визначають вартість ресурсів. У вартість входять усі потенційні витрати, пов’язані з можливим несанкціонованим доступом до інформаційних ресурсів, що захищаються.

Наступним етапом аналізу ризиків є складання переліку переважних загроз та перелік вразливостей до них кожного інформаційного ресурсу, а потім обчислюється ймовірність реалізації можливих загроз чи атак. За стандартом [13] загрози інформаційної безпеки мають подвійне тлумачення, а саме: умова реалізації вразливості ресурсу (в цьому випадку вразливості та погрози ідентифікуються окремо); загальна потенційна подія, здатна призвести до несанкціонованого доступу до інформаційного ресурсу (коли наявність можливості реалізації вразливості і є загрозою). Оцінюють ризик, обчислюючи його й зіставляючи із заданою шкалою. Величину ризику обчислюють множенням ймовірності виникнення несанкціонованого доступу до інформації чи ресурсу на значення збитку компанії від цього. Встановлене значення ризику дає змогу визначити важливість для компанії кожного інформаційного ресурсу.

Усі сучасні стандарти в сфері безпеки відображають сформований у міжнародній практиці загальний підхід до організації управління ризиками.

Управління ризиками розглядається як базова частина системи менеджменту якості організації. Стандарти мають відверто концептуальний характер, що дозволяє експертам з інформаційної безпеки реалізувати будь-які методи, засоби і технології оцінки, відпрацювання та управління ризиками. В різних стандартах допускається використання кількісних та якісних методів оцінки ризику інформаційної безпеки, але немає обґрунтування та рекомендацій щодо вибору математичного та методологічного апарату.

У додатку до стандарту [13] наводиться приклад якісного методу оцінювання, а саме використання три- та п’ятибальної оцінних шкал. За п'ятибальною шкалою рівні вартості ідентифікованого ресурсу оцінюють як: “незначний”, “низький”, “середній”, “високий”, “дуже високий”. За трибальною шкалою – як “низький”, “середній”, “високий”. Загальні критерії оцінки безпеки повинні застосовуватись на єдиній загальній методологічній основі, що ґрунтується на синтезі заходів, засобів та сервісів безпеки для мінімізації інформаційних ризиків. Використовують загальну методологію оцінки інформаційної безпеки експерти, розробники та замовники для оцінки й контролю інформаційної безпеки ресурсів [9].

З погляду розробника профілю захисту застосування загальної методології дає змогу виконати його незалежну і послідовну оцінку та обґрунтування. Розробникові застосування загальної методології дасть змогу:

• незалежно обґрунтувати та перевірити задокументовані у профілі та проекті показники захисту безпеки кожного інформаційного ресурсу;

• переконати споживача у тому, що об’єкт оцінки відповідає необхідним показникам безпеки;

• ефективно використати отримані під час оцінки інших продуктів і систем результати для побудови систем безпеки;

• зменшити витрати часових та матеріальних ресурсів у процесі оцінки безпеки системи.

За загальною методологією оцінки інформаційної безпеки вона повинна здійснюватися за три етапи: підготовчий, основний, заключний. На підготовчому етапі основними дійовими особами є замовник оцінки та експерт. Замовник інформує всі сторони щодо необхідності оцінки профілю захисту або об’єкта оцінки, забезпечує експерта необхідною документацією, матеріалами за профілем захисту й об'єкта оцінки. Завдання експерта – визначити можливість успішного здійснення оцінки на основі отриманих матеріалів, а за необхідності вимагати додаткових матеріалів у замовника або розробника. Підсумком підготовчого етапу є укладання між замовником і експертом угоди на виконання робіт з оцінки об’єкта або профілю захисту. Результатом основного етапу є розроблення та надання експертом технічного звіту оцінки, що містить обґрунтування прийнятого рішення. На основному етапі експерт досліджує подані йому матеріали, профіль захисту або об’єкт оцінки. Експерт складає цілу

низку звітів з вимогами надання пояснень за вимогами органу контролю, виявленими недоліками та іншою інформацією про хід оцінки. Контролюючий орган здійснює безперервний моніторинг процесу оцінки відповідно до схеми оцінки.

На заключному етапі здійснюється всебічний аналіз технічного звіту оцінки органом контролю на предмет його відповідності загальним критеріям загальної методології та вимогам схем оцінки безпеки.

На основі технічного звіту формується підсумковий звіт з оцінювання з рішенням про відповідність необхідним вимогам. Усі залучені в процес оцінювання сторони вивчають підсумковий звіт та мають право вимагати відповідних пояснень. Більшість організацій з різних причин не мають можливості здійснити повну оцінку захисту інформаційних ресурсів, тому пропонується використовувати кількісну оцінку рівня захищеності. Її використання можливе на стадії впровадження.

У результаті застосування кількісної оцінки є можливість точніше порівняти декілька варіантів захисту, що дає змогу вибрати найефективніший. Для її застосування визначають ймовірність виникнення загроз та вразливості інформаційних ресурсів, вартість ресурсів, що захищаються (оцінка втрати в разі виходу з ладу інформаційного ресурсу) та частоту загроз кожного виду в загальному потоці загроз. Обов’язковим є визначення обмежень на вартість системи захисту інформації та зниження рівня продуктивності системи.

Для здійснення оцінки захищеності пропонується виконати наведені нижче кроки:

• на першому кроці складають список загроз з позиції забезпечення інформаційної безпеки, визначають ймовірності виникнення загроз та ймовірності їх відображення системою захисту, вартість інформаційних ресурсів;

• на другому кроці вводять обмеження на вартість системи захисту інформації та на зниження рівня продуктивності комп’ютерної інформаційної системи;

• на третьому кроці проводиться оцінка за математичними формулами загального рівня захисту комп’ютерної інформаційної системи вибраними засобами;

• на четвертому кроці з розглянутих та оцінених варіантів вибирають той, що максимально відповідає вимогам і не виходить за задані обмеження. Фактично рівень захисту визначається як відношення ризиків у захищеній системі до ризиків у незахищеній системі.

Такий підхід дає змогу точніше описувати інформаційні ресурси через характерні для них вразливості, вартість самих ресурсів, ранжувати ризики та відповідно інформаційні ресурси за ступенем критичності для діяльності організації.

Лекція 13

ПЗ для розслідування комп'ютерних злочинів

В україні функціонує лабораторія комп'ютерної криміналістики та інформаційної безпеки ЕПОС пропонує спеціалізовані технічні й програмні засоби для проведення досліджень в сфері комп'ютерної криміналістики.

Особливістю компанії ЕПОС є наявність відділу науково-дослідних і дослідно-конструкторських робіт, у функції якого входить розробка спеціалізованих апаратних і програмних засобів для зняття, відновлення і аналізу даних на різноманітних цифрових носіях. Завдяки цьому, Лабораторія комп'ютерної криміналістики ЕПОС має у розпорядженні засоби розслідування комп'ютерних пригод власної розробки.

Вони співпрацюють з провідними світовими розробниками засобів розслідування IT-інцидентів: ACELab, ICS, Decision Group, Guidance Software, Cellebrite, Tableau, eDEC, iStorage, Barracuda Networks, X-Ways, NRTeam, Rapid7.

ACE Laboratory (ТОВ НВП «ACE», Росія) – спеціалізоване обладнання і програмне забезпечення для ремонту HDD, відновлення даних з пошкоджених HDD, копіювання інформації на HDD.

Intelligent Computer Solutions, Inc. (США) – обладнання для швидкісного криміналістичного збору даних з жорстких дисків. Продукти компанії розробляються в співпраці з правоохоронними органами США та інших країн.

Decision Group (Тайвань) – широкий спектр програмно-апаратних засобів моніторингу використання ресурсів Інтернет, запобігання витоку інформації, аналізу й відновлення втрачених даних, розслідування комп'ютерних злочинів та інцидентів.

Guidance Software Inc. (США) – розробник всесвітньо відомого ПЗ для розслідування комп'ютерних пригод «EnCase» - серії

програмних засобів для підприємств будь-якого масштабу, державних і правоохоронних організацій.

Cellebrite Mobile Synchronization Ltd. (Ізраїль) – високопродуктивні рішення в області судово-криміналістичних пристроїв для вилучення, декодування і аналізу даних з телефонів, смартфонів, планшетних та інших портативних пристроїв.

Tableau (США) – засоби розслідування комп'ютерних пригод: пристрої копіювання, апаратні блокіратори, апаратні прискорювачі та програмне забезпечення. З травня 2010 р. компанія «Tableau» входить до складу корпорації «Guidance Software, Inc.»

eDEC Digital Forensics (США) – пристрої та програми для комп'ютерної криміналістики, що відповідають новітніми віянням в галузі. Компанія відома своїми засобами зняття даних зі смартфонів китайського виробництва.

iStorage Limited (Великобританія) – захищені накопичувачі з прямим введенням пароля і апаратним шифруванням інформації. Пріоритетами компанії є використання новітніх технологій і доступні ціни.

Barracuda Networks, Inc. (США) – широкий спектр пристроїв для комп’ютерних мереж і хмарних послуг із забезпечення безпеки електронної пошти та інших мереже-орієнтованих застосувань для організацій різноманітних розмірів.

X-Ways Software Technology AG (Німеччина) – криміналістичне ПЗ. Продукти компанії призначені для розслідування комп'ютерних пригод, відновлення і глибокого аналізу даних, гарантованого видалення інформації.

NRTeam (NAND Recovery Team, Росія) – програмні та апаратні засоби відновлення даних із Flash-накопичувачів. Найвідоміший проект лабораторії - ПЗ "Dumppicker" для логічного відновлення інформації з Flash-накопичувачів.

Rapid7 (США) – продукти аналізу і обробки ризиків інформаційної безпеки, широкий набір функціональних можливостей для виявлення і зменшення ризиків, а також перевірки відповідності різноманітним стандартам інформаційної безпеки.

Secusmart GmbH (Німеччина) – апаратно-програмні засоби шифрування мобільного зв'язку: дзвінків, повідомлень SMS та електронної пошти. Свої продукти компанія розробляє в співпраці з Федеральним відомством безпеки інформаційних технологій (BSI) та виробниками мобільних телефонів.

BelkaSoft (Росія) – програмне забезпечення для комп'ютерних експертиз, що забезпечує пошук і аналіз цифрових доказів в історіях миттєвих повідомлень, інтернет-браузерів, ящиках поштових клієнтів, слідах відвідування соціальних мереж, файлах відео і зображень.

Addonics (США) – захищені модульні системи зберігання даних, засоби шифрування інформації на накопичувачах, дублікатори та перетворювачі інтерфейсів. Технології, розроблені компанією, розраховані на забезпечення максимальної сумісності з будь-яким устаткуванням і ОС.

Amped Software (Італія) – програмне забезпечення для криміналістичного дослідження цифрового фото- та відеоматеріалу. Продукти компанії застосовуються експертами-криміналістами державних і приватних організацій всього світу.

Лекція 14
Апаратно-програмні засоби шифрування мобільного зв'язку.

Апаратно-програмні засоби захисту комп’ютерної інформації

Перші операційні системи для персональних комп’ютерів не мали власних засобів захисту, що і породило проблему створення додаткових засобів захисту. Актуальність цієї проблеми практично не зменшилася з появою більш потужних ОС з розвинутими підсистемами захисту. Це обумовлено тим, що більшість систем не здатні захистити дані, які перебувають за її межами, наприклад при використанні мережного інформаційного обміну. Апаратно-програмні засоби, що забезпечують підвищений рівень захисту, можна розбити на п’ять основних груп, рис. 5.4 [Error: Reference source not found].

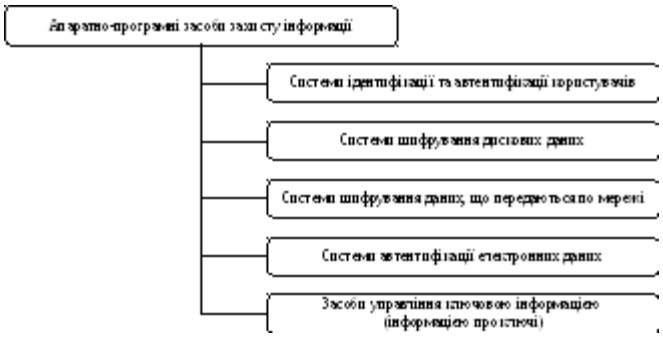


Рис. 5.4. Апаратно-програмні засоби захисту комп’ютерної інформації

Першу групу утворюють системи ідентифікації та автентифікації користувачів. Такі системи застосовуються для обмеження доступу випадкових та незаконних користувачів до ресурсів комп'ютерної системи. Загальний алгоритм роботи цих систем полягає в тому, щоб отримати від користувача інформацію, яка посвідчує його особу, перевірити її справжність і потім надати (чи не надати) цьому користувачу можливість роботи з системою. При побудові подібних систем виникає проблема вибору інформації, на основі якої здійснюються процедури ідентифікації та автентифікації користувача. Можна виділити наступні типи:

1. секретна інформація, якою володіє користувач (пароль, персональний ідентифікатор, секретний ключ тощо); цю інформацію користувач повинен запам'ятати або ж можуть бути застосовані спеціальні засоби зберігання такої інформації;
2. фізіологічні параметри людини (відбитки пальців, рисунок райдужної оболонки ока) чи особливості поведінки людини (особливості роботи на клавіатурі – „клавіатурний почерк" тощо).

Системи ідентифікації, що базуються на першому типі інформації, прийнято вважати традиційними. Системи ідентифікації, що використовують другий тип інформації, називають біометричними. Слід відзначити тенденцію все більшого використання біометричних систем ідентифікації.

Другу групу засобів, що забезпечують підвищений рівень захисту, складають системи шифрування дискових даних. Основна задача, що вирішується такими системами, полягає у захисті від несанкціонованого використання даних, розміщених на магнітних носіях інформації. Забезпечення конфіденційності даних, що розміщуються на магнітних носіях, здійснюється шляхом їх шифрування з використанням симетричних алгоритмів шифрування. Основною класифікаційною ознакою для комплексів шифрування служить їх рівень вбудованості у комп'ютерну систему.

Робота прикладних програм з дисковими накопичувачами складається з двох етапів – логічного та фізичного.

Логічний етап відповідає рівню взаємодії прикладної програми з операційною системою (наприклад, виклик сервісних функцій читання/запису даних). На цьому рівні основним об'єктом є файл.

Фізичний етап відповідає рівню взаємодії операційної системи та апаратури. У якості об'єктів цього рівня виступають структури фізичної організації даних – сектори диску.

В результаті системи шифрування даних можуть здійснювати криптографічні перетворення даних на рівні файлів (захищаються окремі файли) та на рівні дисків (захищаються цілі диски).

Іншою класифікаційною ознакою систем шифрування дискових даних є спосіб їх функціонування. За способом функціонування системи шифрування дискових даних поділяються на два класи:

1. системи прозорого шифрування;
2. системи, які спеціально викликаються для здійснення шифрування.

У системах прозорого шифрування (шифрування „на льоту“) криптографічні перетворення здійснюються в режимі реального часу непомітно для користувача. Наприклад, користувач записує підготовлений у текстовому редакторі документ на захищуваний диск, а система в процесі запису здійснює його шифрування. Системи другого класу зазвичай представляють собою утиліти, які необхідно спеціально викликати для виконання шифрування. До них відносяться, наприклад, архіватори з вбудованими засобами парольного захисту.

До третьої групи засобів, що забезпечують підвищений рівень захисту, відносяться системи шифрування даних, що передаються по комп’ютерним мережам. Розрізняють два основних способи шифрування: канальне шифрування та кінцеве(абонентське, термінальне) шифрування.

У випадку канального шифрування захищається уся інформація, що передається по каналу зв’язку, включаючи і службову. Відповідні процедури шифрування реалізуються, наприклад, за допомогою протоколу канального рівня семирівневої еталонної моделі взаємодії відкритих систем OSI [Error: Reference source not found]. Цей спосіб має суттєву перевагу – вбудовування процедур шифрування у канальний рівень дозволяє використовувати апаратні засоби, що сприяє підвищенню продуктивності системи. Однак у даного підходу є й суттєві недоліки:

- шифруванню на даному рівні підлягає уся інформація, включаючи службові дані транспортних протоколів, що ускладнює механізм маршрутизації мережних пакетів та вимагає розшифровування даних в пристроях проміжної комутації (шлюзах, ретрансляторах тощо);
- шифрування службової інформації, неминуче на даному рівні, може привести до появи статистичних закономірностей у шифруванні даних, що впливає на надійність захисту і накладає обмеження на використання криптографічних алгоритмів.

Кінцеве (абонентське) шифрування дозволяє забезпечити конфіденційність даних, що передаються між двома прикладними об’єктами (абонентами). Кінцеве шифрування реалізується за допомогою протоколу прикладного чи представницького рівня еталонної моделі OSI [Error: Reference source not found]. В цьому випадку захищається тільки зміст повідомлення, вся ж службова інформація залишається відкритою. Даний спосіб дозволяє

уникнути проблем, пов'язаних із шифруванням службової інформації, але при цьому виникають інші проблеми. Зокрема, зловмисник, який має доступ до каналів зв'язку комп'ютерної мережі, отримує можливість аналізувати інформацію про структуру обміну повідомленнями, наприклад, про відправника і отримувача, про час і умови передачі даних, а також про об'єм даних, що передаються.

Четверту групу засобів захисту складають системи автентифікації електронних даних. При обміні електронними даними по мережах зв'язку виникає проблема автентифікації автора документу та самого документу – встановлення справжності автора та перевірка відсутності змін в отриманому документі. Для автентифікації електронних даних застосовують код автентифікації повідомлення (імітовставку) чи електронний цифровий підпис. При формуванні коду автентифікації повідомлення та електронного цифрового підпису використовують різні типи систем шифрування.

Код автентифікації повідомлення формують за допомогою симетричних систем шифрування даних. Зокрема, симетричний алгоритм шифрування даних DES при роботі в режимі зчеплення блоків шифру CBC дозволяє сформувати за допомогою секретного ключа та початкового вектора IV код автентифікації повідомлення MAC (Message Authentication Code) [Error: Reference source not found]. Перевірка цілісності прийнятого повідомлення здійснюється шляхом перевірки коду MAC отримувачем повідомлення. Аналогічні можливості надає алгоритм ГОСТ 28147-89 [Error: Reference source not found], в якому передбачено режим вироблення імітовставки, яка забезпечує імітозахист – захист системи шифрування зв'язку від нав'язування неправдивих даних. Імітовставка виробляється з відкритих даних шляхом спеціального перетворення шифрування з використанням секретного ключа і передається по каналу зв'язку в кінці зашифрованих даних. Імітовставка перевіряється отримувачем повідомлення, який володіє секретним ключем, шляхом повторення процедури, виконаної раніше відправником, над отриманими відкритими даними.

Електронний цифровий підпис (ЕЦП) представляє собою відносно невеликий об'єм додаткової автентифікуючої цифрової інформації, що передається разом із „підписаними" даними. Для реалізації ЕЦП використовуються принципи асиметричного шифрування. Система ЕЦП включає процедуру формування цифрового підпису відправником з використанням секретного ключа відправника та процедуру перевірки підпису отримувачем з використанням відкритого ключа відправника.

П'яту групу засобів, що забезпечують підвищений рівень захисту, утворюють засоби управління ключовою інформацією. Під ключовою інформацією тут розуміється сукупність усіх використовуваних в комп'ютерній системі чи мережі криптографічних ключів. Безпека будь-якого криптографічного алгоритму визначається використовуваними криптографічними ключами. У випадку ненадійного управління ключами

зловмисник може заволодіти ключовою інформацією та отримати повний доступ до всієї інформації в комп'ютерній системі чи мережі. Основною класифікаційною ознакою засобів управління ключовою інформацією є вид функції управління ключами. Розрізняють такі основні види функцій управління ключами [Error: Reference source not found]: генерація ключів, зберігання ключів та розповсюдження ключів.

Способи генерації ключів розрізняються для симетричних і асиметричних криптосистем. Для генерації ключів симетричних криптосистем використовуються апаратні та програмні засоби генерації випадкових чисел, зокрема системи із застосуванням блочного симетричного алгоритму шифрування. Генерація ключів для асиметричних криптосистем є значно складнішою задачею у зв'язку з необхідністю отримання ключів з певними математичними властивостями.

Функція зберігання ключів передбачає організацію безпечного зберігання, обліку та знищення ключів. Для забезпечення безпечного зберігання та передачі ключів застосовують їх шифрування з використанням інших ключів. Такий підхід приводить до концепції ієрархії ключів. До ієрархії ключів зазвичай входять головний ключ (майстер-ключ), ключ шифрування ключів та ключ шифрування даних. Слід зазначити, що генерація та зберігання майстер-ключів є критичними питаннями криптографічного захисту.

Розповсюдження ключів є найвідповідальнішим процесом в управлінні ключами. Цей процес повинен гарантувати секретність розповсюджуваних ключів, а також оперативність і точність їх розповсюдження. Розрізняють два основних способи розповсюдження ключів між користувачами комп'ютерної мережі:

- використання одного чи кількох центрів розповсюдження ключів;
- прямий обмін сеансовими ключами між користувачами.

Лекція 15.

Захищені модульні системи зберігання даних

Системи зберігання даних

Системи зберігання даних є одним з ключових елементів сучасного Центру Обробки Даних (ЦОД) будь-якого масштабу. На них лягає завдання консолідації даних критичних корпоративних додатків, забезпечення високого рівня доступності до них і надійного зберігання.

Компанія Integrity Systems є одним з лідерів ринку України за рішеннями систем зберігання даних для компаній середнього та великого бізнесу.

У портфелі компанії успішні проекти рішень систем зберігання даних класу SAN (Storage Area Network), DAS (Direct Attach Storage), NAS (Network Attach Storage), iSCSI.

Фахівці проектної команди Integrity Systems мають вищі інженерні сертифікації HP в області серверів, Блейд, SAN-мереж і систем зберігання даних, які дозволяють проектувати і впроваджувати рішення зберігання даних практично будь-якого масштабу.

Підтвердженням успішної роботи Integrity Systems на даному ринку є лідерські позиції компанії за кількістю реалізованих проектів на базі систем зберігання даних HP в канальному комерційному і банківському сегментах ринку.

1. Організація кластерних рішень високої доступності;
2. Консолідація даних, що забезпечує простоту управління даними на підприємстві;
3. Віртуалізація, яка забезпечує необхідний рівень доступності, продуктивності та утилізації ресурсів IT інфраструктури;
4. Побудова катастрофостійких рішень, які забезпечують цілісність і доступність даних навіть при виході з ладу серверної площадки і допоможе забезпечити захист бізнесу навіть від стихійних загроз;
5. Забезпечення високої доступності даних:

1. Висока продуктивність контролерів і каналів зв'язку, у порівнянні з підсистемами всередині серверів;
2. Високий рівень відмовостійкості забезпечується дублюванням всіх критичних компонентів дискової підсистеми.

Система Збереження Даних HP MSA – сприяють розвитку бізнесу

Віртуалізація та інші зростаючі навантаження лише більш занурюють SMB замовників у море складності, аніж допомагають зростаючому бізнесу. Більшість замовників у складних умовах браку персоналу та бюджетних коштів змушені обирати між продуктивністю СЗД та ціною такого рішення на користь останнього. Але новітні системи збереження HP MSA четвертого покоління покликанні усунути цей компроміс, пропонуючи замовнику високу потужність у рамках обмеженого бюджету. На вибір пропонується більш бюджет орієнтована версія MSA 1040, та оптимізована під високі навантаження система MSA2040. Система MSA1040 має потужність на 50% більшу за попереднє покоління MSAP2000 G3, а система MSA2040 у 2-4 рази по відношенню до MSAP2000 G3. Крім того, обидва стореджі пропонують зручний та простий у використанні веб інтерфейс, що забезпечує можливість керування системою з будь-якої точки і навіть з мобільних пристроїв. Адміністрування такою системою не потребує якихось спеціальних знань, будь-яку потребу можна виконати за пару кліків у веб інтерфейсі. Тож обидві системи простоті

у використанні, пропонують надійність та потужність за оптимальні кошти — *ідеальне рішення для малого та середнього бізнесу.*

	MSA 1040 *Найбюджетніший* сторедж на ринку 	MSA 2040 *Найпотужніший* сторедж на ринку у своїй категорії 
Типи портів	1GbE, 8GbFC, 10GbE iSCSI	1/10GbE, 8Gb/16Gb FC, 6/12Gb SAS Converged SAN (SFP-defined), підтримка кількох протоколів (iSCSI/FC)
Максимальна кількість НМЖД	99	199
Початкова прайсова ціна	**6 000$**	**12 000$**
Підтримка шифрування	ні	так
Підтримка знімків томів(snapshot)	Так	
Підтримка реплікації		
Проста у використанні		
Надійність		
Краще співвідношення потужність/ціна на ринку		

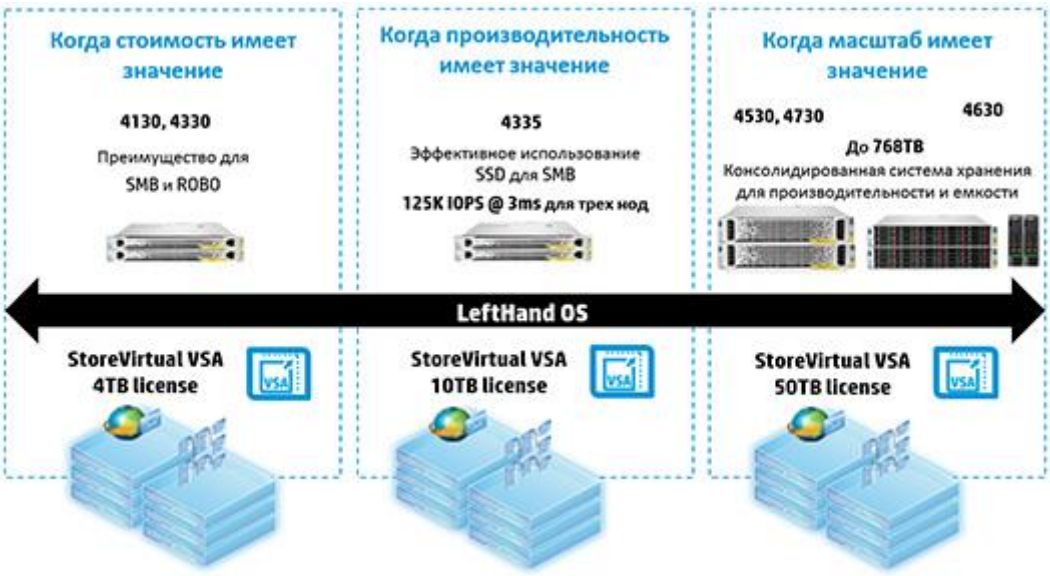
Компанія Integrity Systems допоможе провести аналіз серверної інфраструктури та мережі збереження даних для вибору рішення, яке повніст'ю відповідає потребам замовника. Компетенція підтверджена наявною спеціалізацією HP Gold Storage та партнерським сертифікатом найвищого рівня — HP Platinum Partner.

HP StoreVirtual - платформа для катастрофостійких рішень для великого та середнього бізнесу

За даними досліджень Gartner, програмно-визначувані системи зберігання (Software-Defined Storage, SDS) потрапляють в топ-тренди IT-ринку останні пару років. Найчастіше використовують програмні СЗД або повністю будують на них свою інфраструктуру малий і середній бізнес, а також сервіс-провайдери. При цьому на ринку існує багато розробок таких систем зберігання з різною функціональністю і можливостями масштабування, але особливу увагу заслуговує одна з перших SDS — HP StoreVirtual VSA (Virtual Storage Appliance), раніше відома як LeftHand. Система виконана у вигляді віртуальної машини VSA для гіпервізорів Hyper-V і ESXi. Вона цікава не тільки тим, що за багато років розробки її давно вже можна рекомендувати для корпоративного сегмента, а також і тим, що StoreVirtual доступна ще й у варіанті апаратного виконання. У продуктових середовищах замовників налічується вже більше 12 тис. Віртуальних СЗД HP StoreVirtual VSA.

Ще однією сильною стороною даної СГД є можливість забезпечити катастрофостійкість «з коробки» без додаткових витрат. Саме на цьому (катастрофостійкості) і зосереджено увагу цієї статті.

Модельний ряд HP StoreVirtual включає в себе як апаратно-програмні рішення 4000 серії, так і повністю програмні VSA-продукти (мал. 1).



Мал. 1. Модельний ряд StoreVirtual

Технологія HP StoreVirtual

HP StoreVirtual 4000 - це конвергентная система зберігання даних, яка за рахунок унікальної технології кластеризації може вирішувати задачі невеликого бізнесу з малими обсягами даних і масштабуватися до системи корпоративного рівня з підвищеними вимогами до продуктивності й схоронності даних. Основне застосування цих систем - це віртуалізовані середовища і територіально рознесені інфраструктури, де необхідно забезпечити реплікацію даних між декількома майданчиками одночасно на малих і великих територіях по Ethernet-каналах зв'язку і інтерфейсу iSCSI.

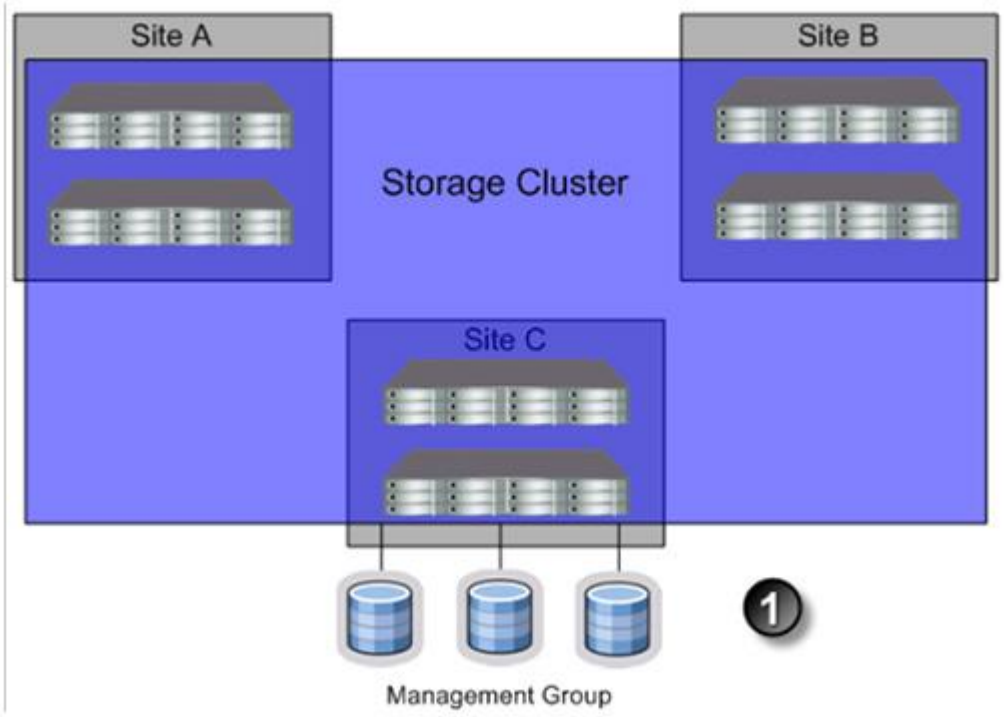
Якщо розглядати системи, подібні StoreVirtual, то ми побачимо, що кожен вузол - це власна СЗД та взаємодія із собі подібними системами відбувається за допомогою технологій синхронної реплікації, для настроювання якої потрібно розглядати кожен вузол як незалежну систему зберігання. А StoreVirtual - це спочатку кластерна система зберігання даних, і кожен вузол - це пул ресурсів, який розширює ємність і продуктивність кластера і відмовостійкість системи в цілому.

Взаємодія вузлів StoreVirtual в кластері відбувається за технологією Network RAID - мережевий RAID. Якщо ми об'єднуємо, наприклад, кілька вузлів у кластер і в ньому створюємо віртуальний диск (LUN) з мережевим RAID 10, то кожен блок даних на цьому диску буде віддзеркалюватись між двома вузлами. Якщо в кластері два вузли і всі віртуальні диски об'єднані в RAID 10, то це, можна сказати, синхронна реплікація між двома вузлами. Відзначимо, що цей приклад є всього лише окремим випадком технології кластеризації StoreVirtual, так як її можливості набагато ширші.

Для серверів кластер зберігання - це єдиний пул ресурсів. Кожен LUN вони бачать по одному Virtual IP і звертаються до нього, як до єдиної системи зберігання, одночасно взаємодіючи з усіма вузлами кластера. При цьому розміщення вузлів StoreVirtual на різних майданчиках ніяк не позначається на роботі серверів.

Один кластер рекомендується розносити не більше ніж між трьома майданчиками (мал. 2). Система StoreVirtual дозволяє рознести вузли кластера і

між чотирма майданчиками із збереженням однієї копії даних на кожному майданчику (Network RAID10 + 2), але для цього потрібно забезпечити підвищені вимоги до каналів зв'язку між майданчиками. Оскільки таке рішення потрібно дуже рідко, то в рекомендаціях «Best Practice» воно не вказано, але при цьому можливо і реалізовується.



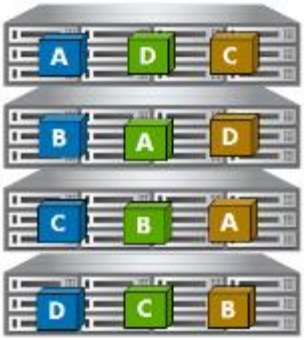
Мал. 2. Розподілений між двома майданчиками кластер системи зберігання StoreVirtual з шести вузлів, де логічні диски є загальними і розподіленими між усіма майданчиками

В одному кластері можна організовувати різні рівні мережевого RAID для кожного віртуального диска (LUN):

• Network RAID 10 (2-Way Mirror) будується як мінімум на двох StoreVirtual в кластері, кожен блок даних зберігатися на двох вузлах (мал. 3);

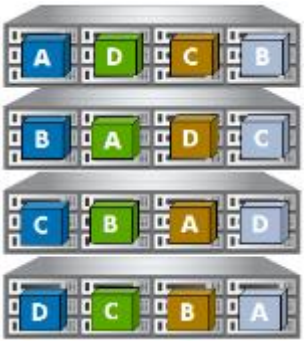
Мал. 3. Розміщення блоків даних у середині кластера StoreVirtual з чотирьох вузлів, якщо для логічного диска обраний Network RAID 10

• Network RAID 10 + 1 (3-Way Mirror) - будується як мінімум на трьох StoreVirtual в кластері, кожен блок даних зберігається на трьох вузлах (мал. 4);



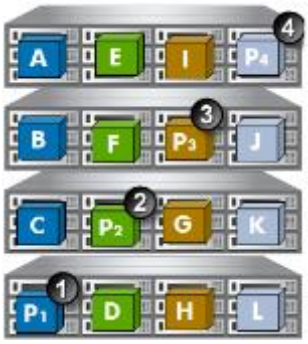
Мал. 4. Розміщення блоків даних усередині кластера StoreVirtual з чотирьох вузлів, якщо для логічного диска обраний Network RAID 10 + 1

• Network RAID 10 + 2 (4-Way Mirror) - будується як мінімум на чотирьох StoreVirtual в кластері, кожен блок даних зберігається на чотирьох вузлах (мал. 5);



Мал. 5. Розміщення блоків даних усередині кластера StoreVirtual з чотирьох вузлів, якщо для логічного диска обраний Network RAID 10 + 2

• Network RAID 5 (Single Parity) - будується як мінімум на трьох StoreVirtual в кластері, якщо, наприклад, у нас три вузли, то один блок даних пишеться на один вузол, другий блок даних - на другий вузол і парність цих даних - на третій вузол і так далі зі зміщенням на один вузол (мал. 6);



Мал. 6. Розміщення блоків даних усередині кластера StoreVirtual з чотирьох вузлів, якщо для логічного диска обраний Network RAID 5

• Network RAID 6 (Dual Parity) - будується як мінімум на п'яти StoreVirtual в кластері, працює, як Network RAID 5, але при цьому записується два парності для підвищеної відмовостійкості (мал. 7);

Мал. 7. Розміщення блоків даних усередині кластера StoreVirtual з шести вузлів, якщо для логічного диска обраний Network RAID 6

• Network RAID 0 - будується як мінімум на одному StoreVirtual в кластері, кожен блок даних зберігається на одному вузлі, відмовостійкість між вузлами не забезпечується.

У разі виходу з ладу одного майданчика серверам не потрібно час, щоб переключиться між СЗД - сервер просто втрачає один з альтернативних шляхів до виділеного логічного диску, і MPIO-драйвер перестає через нього посилати дані, поки шлях не відновиться. Для додатків це прозоро і не вимагає пауз і зупинок.

Щоб уникнути втрати синхронізації майданчиків у разі порушення зв'язку між майданчиками, так званого «split-brain», існує StoreVirtual Failover Manager. Це віртуальна машина, яка розміщується на окремій або логічно відокремленому майданчику і стежить за тим, яка площадка повинна працювати, а яка повинна зупиниться автоматично при втраті каналу.

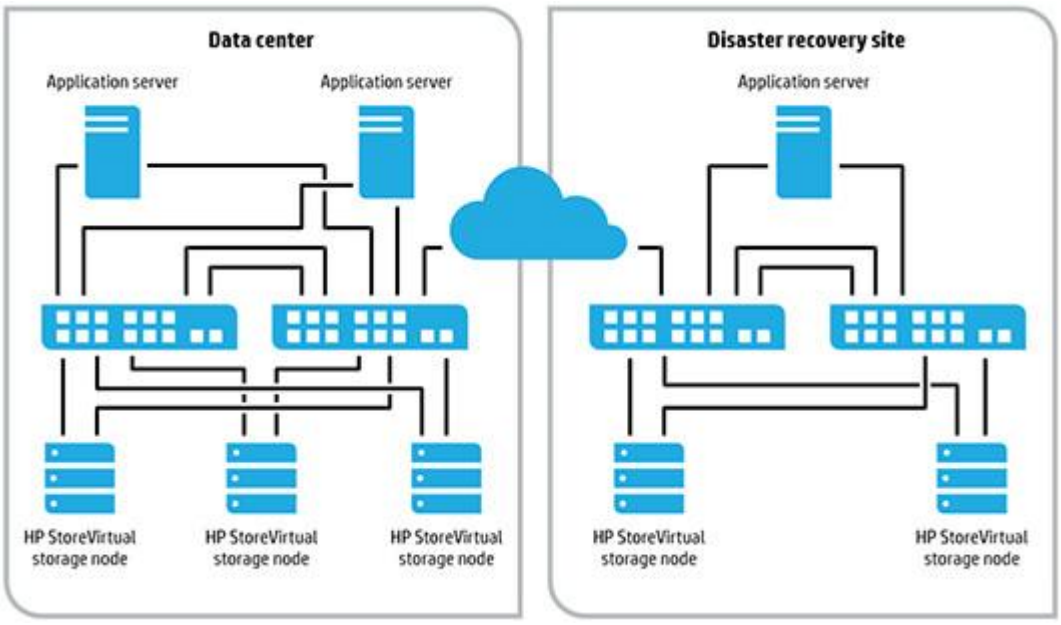
Вимоги до мережі для побудови одного кластера, разнесенного між майданчиками, наступні:

• рекомендована пропускна здатність для одного вузла - 50 МБ/с, але також потрібно враховувати, що вузли з 25-ма дисками і більше або з дисками SSD вимагають більшу пропускну здатність в залежності від навантаження і додатків;

• латентність - до 2 мс; система може працювати і з більшою латентністю, якщо додатки не вимогливі, але при великих затримках в каналі рекомендується будувати два кластери або більше і переходити на асинхронну реплікацію між кластерами;

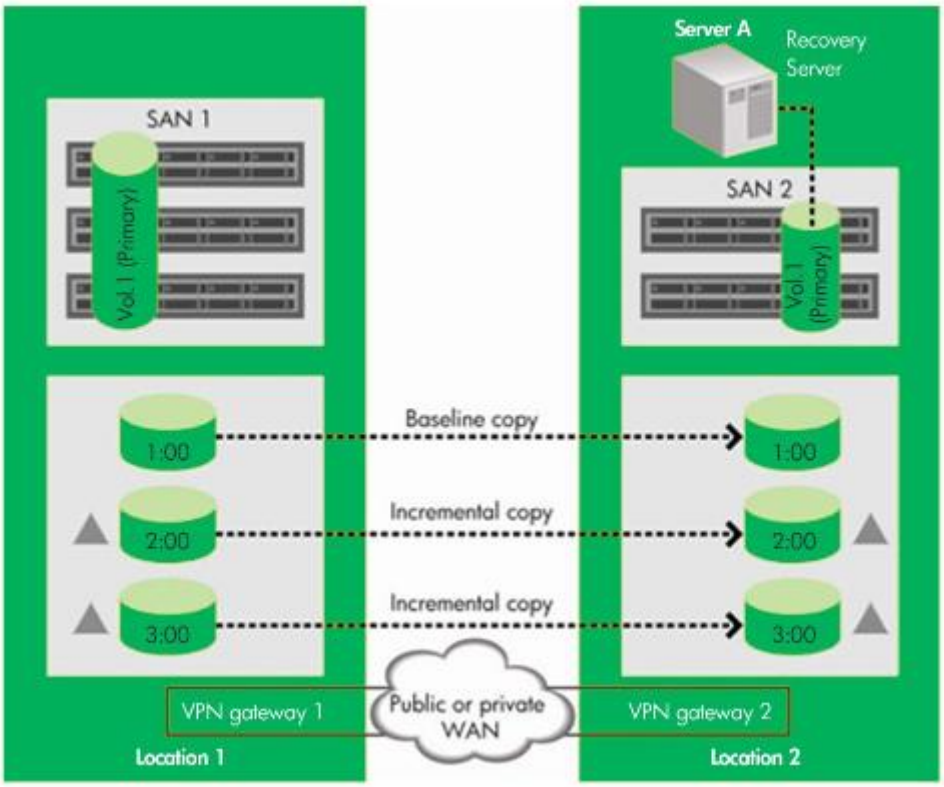
• рекомендується використовувати одну підмережу. Якщо ж це нездійсненно, тоді можна використовувати різні підмережі на різних майданчиках. Але на одному майданчику потрібно використовувати одну підмережу.

Якщо відстань між майданчиками велика чи канал зв'язку не задовольняє вимогам, то на основному і резервному майданчиках будується окремий кластер StoreVirtual (мал. 8).



Мал. 8. Схема підключення вузлів StoreVirtual на основному і резервному майданчиках, які рознесені на велику відстань

Між кластерами, а точніше, між віртуальними дисками в кожному кластері, настроюється асинхронна реплікація за принципом Remote Snap. При цьому потрібно враховувати, що RPO і RTO збільшуються залежно від частоти снапшотов (мал. 9).



Мал. 9. Схема асинхронної реплікації з розподіленим на велику відстань логічним диском за допомогою Remote Snap між кластерами StoreVirtual на різних майданчиках для забезпечення катастрофостійкості

Рішення StoreVirtual володіє достатньо простою і зрозумілою консоллю управління, яка дозволяє управляти одночасно всіма сайтами і виділяти ресурси всього за кілька натискань миші.

StoreVirtual найчастіше застосовується для віртуалізованних середовищ з територіально рознесеною інфраструктурою. Наприклад, у випадку кількох корпусів навчального закладу або на території заводу з декількома будівлями СЗД може бути ідеальним вибором як для забезпечення відмовостійкості, так і мінімізації інвестицій, так як при використанні протоколу iSCSI не потрібно додаткового ліцензування.