Міністерство освіти і науки України
Центральноукраїнський національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ ДО ВИКОНАННЯ ПРАКТИЧНИХ РОБІТ

з навчальної дисципліни

“Основи управління кібербезпекою”

для студентів денної та заочної форм навчання
освітнього ступеню "Бакалавр",
за спеціальністю 125 Кібербезпека

Видання оновлене та доповнене

ЗАТВЕРДЖЕНО
Протокол засідання кафедри
кібербезпеки та програмного
забезпечення
29.08.2018 № 1

Кропивницький
2018

Методичні вказівки до виконання практичних робіт з навчальної дисципліни “Основи управління кібербезпекою” [для студ. денної та заочної форми навч. освітнього ступеню "Бакалавр", за спеціальністю 125 Кібербезпека] Видання оновлене на доповнене / Уклад. І. А. Лисенко – Кропивницький: ЦНТУ, 2018.– 64 с.

Укладач Лисенко І.А., канд. техн. наук

Рецензенти: Смірнов О. А., д-р техн. наук, професор;
Якименко Н. М., канд. фіз.-мат. наук, доцент.

Методичні вказівки висвітлюють організаційні та практичні аспекти виконання практичних робіт з навчальної дисципліни “Основи управління кібербезпекою” для студентів денної та заочної форм навчання освітнього ступеню "Бакалавр", за спеціальністю 125 Кібербезпека, а також рекомендації щодо ходу виконання робіт, підготовки та представлення отриманих результатів.

© Лисенко І.А., уклад., 2018
© Центральноукраїнський національний технічний університет, 2018

ЗМІСТ

Вступ

Система управління інформаційною безпекою, а разом з нею і кібербезпекою, як її невід'ємною складовою, є сучасним процесом забезпечення безпеки інформаційних ресурсів організації, яка побудована на кращих світових практиках. Стандарти України засновані на міжнародних стандартах ISO 27001 та ISO 27002 з додаванням вимог із захисту інформації, зумовлених конкретними потребами сфери діяльності і правовими вимогами, які вже висунуто в нормативних документах України.

Відповідність системи управління інформаційною безпекою стандартам України СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010 гарантує відповідність міжнародним стандартам ISO 27001 та ISO 27002 і надає можливість отримати відповідний сертифікат.

Необхідність впровадження в організаціях та на підприємствах України стандартів з управління інформаційною безпекою зумовлена вимогами МВФ з управління та зменшення ризиків бізнес-процесів.

Впровадження в організаціях та на підприємствах України стандартів з управління інформаційною безпекою дозволить:

- оптимізувати вартість побудови та підтримання системи інформаційної безпеки;
- постійно відслідковувати та оцінювати ризики з урахуванням цілій бізнесу;
- ефективно виявляти найбільш критичні ризики та знижувати ймовірність їх реалізації;
- розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання;
- ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу;
- забезпечити розуміння питань інформаційної безпеки керівництвом та всіма працівниками банку;
- забезпечити підвищення репутації та ринкової привабливості банків;
- знизити ризики рейдерських та інших шкідливих для банку атак;
- тощо.

Слід зазначити, що наведені вище переваги не будуть досягнуті шляхом лише "формального" підходу до розроблення, впровадження, функціонування системи управління інформаційною безпекою та незацікавленості керівництва і працівників у підвищенні рівня інформаційної безпеки загалом та, зокрема, кібербезпеки.

Практична робота № 1

Тема: Дослідження системи законодавства у сфері інформаційних відносин

Загальні відомості

В Україні інформаційне поле формується під могутнім впливом закордонних чинників. Поряд з безумовністю вимог відкритості інформаційного простору України для інформаційних потоків з-за кордону зрозуміло, що втрата важелів впливу на процеси у ньому може призвести до значних негативних наслідків для майбутнього країни. Саме тому надзвичайної актуальності набувають проблеми регулювання інформаційної сфери, створення відповідних умов для випереджаючого розвитку вітчизняного інформаційного виробництва. Провідним інструментом реалізації національних інтересів у такій чутливій галузі суспільних відносин, як інформаційна сфера, повинно стати право. Остання теза усвідомлена ще на початку 1990-х років.

Показово, що одним з перших законів незалежної держави став Закон «Про інформацію».

Аналіз відповідних статей Конституції України дозволяє дійти висновку про намагання вітчизняного законодавця побудувати інформаційну політику на основі демократичних та ліберальних норм та принципів, одночасно забезпечивши їхню адаптацію до українських умов.

Положення Конституції України розвиваються та конкретизуються у понад 200 документах, які встановлюють правові норми в інформаційній сфері. Серед них базові Закони України «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення та радіомовлення», «Про інформаційні агентства», «Про державну таємницю», «Про зв'язок», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про рекламу», «Про Концепцію національної програми інформатизації», «Про Національну програму інформатизації», «Про науково- технічну інформацію», «Про захист

інформації в автоматизованих системах», «Про електронний підпис», «Про електронний документообіг» та інші.

Експертиза українського інформаційного законодавства, котра неодноразово здійснювалася протягом останніх років, зокрема представниками ОБСЄ, свідчить про те, що законодавча та нормативно-правова база функціонування інформаційної сфери України в цілому відповідає європейським нормам. Проте, якщо формальний бік справи не викликає, значного занепокоєння, то існує нагальна проблема недотримання встановлених норм усіма суб'єктами інформаційних відносин, зокрема органами державної влади всіх рівнів. Рівень правової культури громадян України змушує розглядати ситуацію із зовсім іншого боку порівняно з країнами Європейського Союзу.

Історично в Україні склався принципово відмінний від західноєвропейського погляд на писаний договір — одну з основ сучасного права. Більшість відносин у суспільстві регулювалася звичаями, неформальними домовленостями. Події 20 сторіччя, зокрема й 90-х років, також не сприяли формуванню європейської правової культури.

Недостатньо ретельне та чітке дотримання законодавства складає найважливішу проблему правової політики держави, зокрема це стосується й інформаційної сфери. Показовим є намагання певних сил створити новітні зони недоторканості, сформувати потужні системи пільг та переваг, що діють поза законодавством. Забезпечення єдності та невідворотності дії Закону є провідним завданням держави.

Важливою проблемою залишається певна несистемність вітчизняної правової політики в інформаційній сфері. Значна кількість законодавчих актів ухвалюється з метою вирішення певних тактичних завдань, задоволення кланових інтересів, часто без урахування стратегічних орієнтирів та реальних українських умов. Показовим з цієї точки зору є спроби перегляду законодавства щодо дозволу рекламування алкоголю та тютюну.

Взагалі, нормативно-правове забезпечення інформаційної сфери потребує суттєвого удосконалення. Одним з напрямків удосконалення

системи інформаційного законодавства України може стати розроблення та ухвалення Інформаційного кодексу України, що дозволить розв'язати проблему подолання протиріч у законодавчих та нормативно-правових актах, забезпечити єдність та нефрагментованість нормативно-правового поля. Нещодавно вийшло розпорядження КМУ "Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України" № 155-р, яким передбачено 19 завдань, які мають бути виконанні протягом 2017 року за наступними напрямами:

- нормативно-правове забезпечення діяльності у сфері кібербезпеки (гармонізація законодавства із захисту державних інформаційних ресурсів, впровадження системи аудиту інформаційної безпеки об'єктів критичної інфраструктури тощо);

- створення технологічної складової національної системи кібербезпеки;

- налагодження більш тісного співробітництва з міжнародними партнерами України;

- налагодження процесу підготовки кадрів у сфері кібербезпеки.

Рішення прийняте з метою реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.2016 № 96.

Значна кількість питань функціонування інформаційної сфери донині неврегульована на законодавчому рівні. Це стосується як проблем інфраструктури, так і діяльності ЗМІ, інформаційно-аналітичних установ тощо. Як приклад проаналізуємо законодавче забезпечення такої важливої складової інформаційної політики держави, як інформаційної прозорості та відкритості функціонування органів державної влади і управління. В Україні сформовано певну законодавчу базу забезпечення відкритості функціонування органів державної влади. Насамперед йдеться про Конституцію України (ст. 3, 32, 57 тощо), Закони «Про інформацію», «Про друковані ЗМІ (пресу) в Україні», «Про телебачення та радіомовлення», «Про інформаційні агентства», «Про державну службу» тощо.

Основним недоліком чинного законодавства є його пасивний характер — декларовано лише необхідність забезпечення відкритості органів державної

влади у відповідь на звернення громадян чи засобів масової інформації. Громадянин для отримання певної інформації має підготувати та подати до відповідної установи запит і протягом місяця очікувати відповідь. Як бачимо з цього, державні органи фактично відсутні в інформаційному просторі. Непоодинокими є випадки, коли про державну політику повідомляє не сама держава, а сторонні особи, нерідко її опоненти. Тоді, як законодавство демократичних країн передбачає активну інформаційну діяльність, обов'язкову звітність влади перед населенням незалежно від наявності звернень або запитів щодо надання тієї чи іншої інформації, обов'язкове, може навіть дещо надмірно активне, інформування громадян про поточну діяльність органів державної влади.

Разом з тим, важливим є не лише обсяг наданої інформації, а й її якість. А забезпечити її можна лише вжиттям комплексу заходів, зокрема, а, можливо, й насамперед не правового характеру.

Левова частка інформаційних відносин регулюється підзаконними, а подекуди й відомчими нормативними актами. Характерним прикладом останнього є відсутність законодавчого визначення режимів обмеження доступу до інформації, окрім державної таємниці. Незважаючи на те, що в законодавстві існують поняття комерційної, лікарської, банківської службової таємниці, інформації «не для друку» тощо, їхнє чітке визначення відсутнє. Режим доступу до інформації, що належить державі, встановлюється постановами Кабінету Міністрів України.

Значну проблему становить фактична відсутність правового регулювання функціонування в Україні міжнародних інформаційних систем, найяскравішим прикладом яких є Інтернет. Зокрема, відсутність відповідних нормативно-правових актів створює певні проблеми для Інтернет-ЗМІ та сприяє їхньому використанню у деструктивних цілях. Розвиток інформаційної інфраструктури вимагає відповідної законодавчої підтримки. Досить суперечлива ситуація склалася у нормативно-правовому забезпеченні діяльності ЗМІ. Поряд з тим, що за роки незалежності створено розгалужену нормативну базу, відсутні нормативно-правові акти, які б сприяли

становленню економічно незалежних ЗМІ. Значні проблеми зберігаються і в правовому регулюванні питань інформаційної безпеки. Майже відсутнє законодавче забезпечення формування національних інформаційних ресурсів та міжнародних інформаційних обмінів, не врегульовано на законодавчому рівні статус конфіденційної інформації, а також передбачених законодавством України видів таємниці, насамперед банківської, комерційної, лікарської тощо.

Суб’єктами забезпечення кібербезпеки в Україні є:

- Рада національної безпеки і оборони України;
- Міністерство внутрішніх справ України;
- Міністерство оборони України;
- Генеральний штаб Збройних Сил України;
- Служба безпеки України;
- Державна служба спеціального зв'язку та захисту інформації України;
- Розвідувальні органи України.

6 травня 2017 року Верховна Рада відправила на повторне друге читання законопроект №2126а "Про основні засади кібербезпеки України". Поточна версія законопроекту вводить важливі базові поняття і визначає права і обов'язки державних органів щодо кібербезпеки. Проте, нажаль, враховуючи, що законопроект конче необхідний в державі, він все ще не прийнятий Верховною Радою.

Теоретичні питання:

Бути готовим відповіти на запитання по темі роботи та коротко охарактеризувати основні елементи створеної бази даних.

Практичне завдання:

1. Створити базу даних нормативно-правових актів та органів державного регулювання в сфері кібербезпеки в Україні. База даних повинна додатково містити (за можливістю) посилання на офіційні сайти державних органів в мережі Internet та нормативно-правових актів на сайті Верховної Ради України. Обов’язково до кожного розділу БД та запису – анотація.

Практична робота № 2

Тема: Структура систем управління кібербезпекою

Загальні відомості

Система управління інформаційною безпекою (Information Security Management System) є частиною загальної системи управління, що базується на аналізі ризиків і призначеної для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області інформаційної безпеки (кібербезпеки). Систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Основними **цілями інформаційної безпеки** є:

• конфіденційність інформації, тобто необхідність введення обмежень доступу до даної інформації для певного кола осіб;

• неможливість несанкціонованого доступу до інформації, тобто ознайомлення з конфіденційною інформацією сторонніх осіб;

• цілісність інформації та пов'язаних з нею процесів (створення, введення, обробка і виведення), яка полягає в її існуванні в неспотвореному вигляді (незміненому по відношенню до деякому фіксованому її станом);

• доступність інформації, тобто здатність забезпечувати своєчасний і безперешкодний доступ осіб до їх інформації;

• мінімізація ризиків інформаційної безпеки шляхом виконання компенсаційних заходів;

• облік усіх процесів, пов'язаних з ризиками.

Досягнення заданих цілей здійснюється в ході вирішення **наступних завдань**:

• введення в систему термінів інформаційної безпеки;

• класифікації інформаційних ресурсів підприємства;

• визначення власників процесів, відповідальних за інформаційну безпеку;

• розробки спектра ризиків інформаційної безпеки та проведення їх експертних оцінок;

• визначення групи доступу до інформаційних ресурсів;

• розробки системи управління ризиками інформаційної безпеки (методи та їх оцінка);

• складання переліків адміністративних і технічних заходів для мінімізації та компенсації ризиків;

• здійснення заходів інформаційної безпеки та періодичного контролю за станом ризиків;

• забезпечення фізичної безпеки та безпеки персоналу;

• розробки вимог до інформаційної системи з погляду інформаційної безпеки;

• контролінгу інформаційної безпеки на підприємстві.

Виділяються **чотири стадії реалізації** системи управління інформаційною безпекою:

1) формування політики в галузі ризиків;

2) аналіз бізнес-процесів;

3) аналіз ризиків;

4) формування цільової концепції.

Формування політики в галузі ризиків передбачає визначення принципів управління ними для всього підприємства в цілому. Ці принципи базуються на цілях підприємства, його стратегії, також на вимогах, пропонованих законом і стандартами в галузі інформаційної безпеки. Чинником ефективності системи управління інформаційною безпекою є її побудова на базі міжнародних стандартів ISO / IEC 17799: 2005 та ISO / IEC 27001: 2005.

Стандарт ISO / IEC 17799: 2005 визначає принципи та є керівництвом з розробки, впровадження, супроводу та поліпшення системи управління інформаційною безпекою, а також описує механізми визначення цілей контролю і його цінності у таких областях:

• політика безпеки (встановлення принципів управління і засобів забезпечення захисту інформації);

• управління безперервністю бізнес-процесів (запобігання втручання в ділові операції і захист процесів обробки інформації від наслідків серйозних

несправностей або катастроф);

• дотримання правових норм (виняток порушень кримінального та цивільного права, установлених законом зобов'язань, регулятивних або контрактних зобов'язань, а також вимог щодо безпеки);

• організація активів і ресурсів (управління захистом інформації всередині організації);

• фізична безпека і безпека навколишнього середовища (запобігання несанкціонованого доступу, пошкодження і проникнення в службові приміщення або втручання в ділову інформацію);

• класифікація і управління активами (виявлення та захист інформаційних активів);

• захист персоналу (зниження ризиків, пов'язаних з помилкою оператора, крадіжкою, шахрайством або зловживанням обладнанням);

• управління доступом (контроль доступу до інформації);

• управління засобами зв'язку і експлуатацією устаткування (коректне і безпечне функціонування засобів обробки інформації);

• розробка та обслуговування систем (впровадження засобів захисту в інформаційні системи).

Стандарт ISO / IEC 27001: 2005 встановлює вимоги до системи управління інформаційною безпекою підприємства, є керівництвом за визначенням, мінімізації та управління небезпеками і погрозами, яким може піддаватися інформація, і розроблений з метою забезпечення допомоги у виборі ефективних і адекватних засобів для його захисту. Застосування стандарту ISO / IEC 27001: 2005 на підприємстві дозволяє:

• встановити вимоги і цілі в області інформаційної безпеки;

• гарантувати впевненість у тому, що управління ризиками в області інформаційної безпеки є ефективним, а також те, що діяльність підприємства відповідає законодавству та іншим нормативним документам;

• реалізувати процес контролю за впровадженням системи управління інформаційною безпекою;

• ідентифікувати і відстежувати існуючі процеси управління

інформаційною безпекою;

• керівництву підприємства визначити стан процесів управління захистом інформації;

• внутрішнім і зовнішнім аудиторіям встановити рівень відповідності політики безпеки регламентам;

• забезпечити партнерів і постачальників відповідною інформацією про стандарти, процедурах та політиці підприємства.

Модель системи інформаційної безпеки підприємства - це сукупність зовнішніх і внутрішніх факторів, їх вплив на стан інформаційної безпеки підприємства і забезпечення схоронності ресурсів. Модель системи інформаційної безпеки підприємства містить в собі напрямки впливу між наступними факторами:

• загрозами інформаційній безпеці, які характеризуються ймовірністю виникнення та реалізації;

• вразливістю системи інформаційної безпеки, що впливає на ймовірність реалізації загрози;

• ризиками, що відображають передбачуваний збиток в результаті реалізації загрози інформаційній безпеці.

Інформація та матеріальні ресурси, які необхідно захищати, називаються **об'єктами захисту**.

Загрози, з якими може зіткнутися підприємство, класифікуються за природою їх виникнення, тобто загрози випадкового або навмисного характеру, і по тому, як вони ставляться до захищається, тобто зовнішні і внутрішні загрози.

Джерелами зовнішніх загроз є:

• діяльність конкурентів з перехоплення важливої інформації;

• навмисні дії з руйнування, знищення або модифікації інформації;

• ненавмисні дії співробітників сторонніх організацій, які потягли за собою відмову в роботі елементів системи;

• стихійні лиха та катастрофи, аварії, екстремальні ситуації.

До **джерел внутрішніх загроз** відносяться:

• відсутність координації діяльності підрозділів підприємства у сфері захисту інформації;

• навмисні дії персоналу по знищенню або модифікації інформації;

• ненавмисні помилки персоналу, відмови технічних засобів і збої в інформаційних системах;

• порушення встановлених регламентів збору, накопичення, зберігання, обробки, перетворення, відображення та передачі інформації.

Порушення можуть бути декількох видів.

Організаційно-правові порушення - порушення, пов'язані з відсутністю єдиної узгодженої політики підприємства у сфері захисту інформації, невиконанням вимог нормативних документів, режимом доступу, зберігання та знищення інформації.

Організаційні види порушень включають несанкціоноване отримання доступу до баз і масивам даних, несанкціонований доступ до активного мережевого обладнання, серверів, некоректне вбудовування засобів захисту і помилки в управлінні ними, порушення в адресності розсилки інформації при веденні інформаційного обміну.

Під фізичними видами порушень розуміють пошкодження апаратних засобів автоматизованих систем, ліній зв'язку і комунікаційного устаткування, крадіжки або несанкціоноване ознайомлення зі змістом носіїв інформації, їх розкрадання.

До радіоелектронних видів порушень відносяться впровадження електронних пристроїв перехоплення інформації, отримання інформації шляхом перехоплення і дешифрування інформаційних потоків, фотографування моніторів, нав'язування неправдивої інформації в локальних обчислювальних мережах, передачі даних і лініях зв'язку.

Для протидії загрозам і припинення порушень на підприємствах організовується процес управління ризиками, який є основою системи інформаційної безпеки підприємства.

Побудова ефективної системи інформаційної безпеки - це комплексний

процес, спрямований на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси і час.

З погляду процесного підходу систему інформаційної безпеки підприємства можна представити як процес управління ризиками, який включає в себе наступні складові.

1. **Опис бізнес-процесів**. Виконується коригування та аналіз бізнес-процесів. За критеріями, які визначаються в ході формування політики в галузі ризиків, здійснюється ідентифікація бізнес-процесів.

2. **Збір ризиків**. Проводиться для виявлення ступеня схильності підприємства загрозам, які можуть завдати істотної шкоди. Для цього здійснюється аналіз його бізнеспроцесів і опитування експертів предметної області. Результатом (виходом) даного процесу вважається класифікаційний перелік всіх потенційних ризиків.

До **стандартних ризиків інформаційної безпеки** відносяться:

• вилучення конфіденційної інформації з локальних місць;

• навмисне зміна інформації з метою знищення;

• копіювання важливих документів і передача конкуренту;

• незаконне проникнення в корпоративну мережу;

• знищення з технічних причин.

3. **Оцінка ризиків**. Визначаються характеристики ризиків і ресурси інформаційної системи. Основним результатом (виходом) даного процесу є перелік всіх потенційних ризиків з їх кількісними та якісними оцінками збитку і можливості реалізації, а додатковим - перелік ризиків, які не будуть відслідковуватися на підприємстві.

Процес оцінки ризиків складається з наступних кроків:

• опис об'єкта і заходів захисту;

• ідентифікація ресурсу і визначення його кількісних показників;

• аналіз загроз інформаційної безпеки;

• оцінка вразливостей;

• оцінка існуючих і передбачуваних засобів забезпечення інформаційної безпеки.

4. **Планування заходів**. Метою планування заходів щодо мінімізації ризиків є визначення термінів та переліку робіт по виключенню або мінімізації збитку у разі мінімізації ризику.

Виділяються наступні **види заходів з інформаційної безпеки**:

• організаційні;

• правові;

• організаційно-технічні;

• програмні;

• інженерно-технічні.

5. **Реалізація заходів**. Під реалізацією заходів щодо мінімізації ризиків розуміють виконання запланованих робіт, контроль якості отриманих результатів та термінів. Результатом даного процесу є виконані роботи з мінімізації ризиків і час їх проведення.

6. **Оцінка ефективності**. Оцінка ефективності системи управління інформаційною безпекою - це системний процес отримання та оцінки об'єктивних даних про поточний стан системи, дії і події, що відбуваються в ній, встановлює рівень їх відповідності певним критеріям.

Цілями процесу є:

• оцінка поточного рівня ефективності системи;

• локалізація "вузьких" місць у системі;

• оцінка відповідності системи підприємства існуючим стандартам в галузі інформаційної безпеки;

• вироблення рекомендацій і регламентів по забезпеченню безпеки об'єктів захисту.

Результати процесу можуть використовуватися в цілях аудиту для підготовки підприємства до сертифікації за стандартом ISO / IEC 27001: 2005.

Теоретичні питання:

1. Яким чином визначаються терміни інформаційної безпеки? Назвіть приклади.

2. Розкрийте поняття "заходи інформаційної безпеки".

3. Яким чином може здійснюватись забезпечення фізичної безпеки та

безпеки персоналу на підприємстві чи в організації?

4. Яким чином відбувається аналіз ризиків?

5. Розкрийте поняття "об’єкти захисту", що до них відноситься, наведіть приклади.

6.Що таке "загрози"? Їх види та джерела. Наведіть приклади.

7. Види заходів інформаційної безпеки. Докладно розкрийте кожен з них.

8. Яким чином та з якою метою відбувається оцінка ефективності системи управління кібербезпекою?

Практичне завдання:

У будь-якому графічному редакторі зобразити модель системи інформаційної безпеки підприємства.

Практична робота № 3

Тема: Ідентифікація активів підприємства

Загальні відомості

На цей час актуальним є питання забезпечення інформаційної безпеки. В свою чергу, для забезпечення інформаційної безпеки як окремих підприємств, так і держави в цілому важливим є питання оцінки ризиків, які виникають в процесі діяльності підприємств. Для оцінки ризиків інформаційної безпеки використовуються різні методики і стандарти управління інформаційними ризиками (УІР).

Аналіз ризиків інформаційної безпеки є методом виявлення вразливостей і загроз, оцінки можливого впливу, що дозволяє вибирати адекватні захисні заходи для тих систем і процесів, у яких вони необхідні. Методики аналізу інформаційних ризиків дозволяють забезпечити ефективний і актуальний захист інформаційного простору підприємств і можливість вчасно реагувати на загрози інформаційній безпеці.

В цілому аналіз ризиків інформаційної безпеки передбачає облік активів і встановлення їхньої цінності для підприємства, класифікацію загроз і вразливостей, визначення ймовірності й впливу на діяльність підприємства цих потенційних загроз, а також оптимізацію витрат між збитками від впливу загроз і вартістю захисних заходів. Активи бувають матеріальні (мережеве обладнання, комп'ютери, програмне забезпечення, устаткування, матеріали) і нематеріальні (репутація, інформація, авторське право). Кількісно оцінити вартість нематеріальних активів набагато важче, ніж матеріальних.

Оцінка активів може проводитися кількісними та якісними методами. Фактична вартість активів визначається на підставі вартості їх придбання, розробки й підтримки. Цінність активів визначається мірою їх необхідності для уповноважених і неуповноважених користувачів і власників.

Для забезпечення ефективності аналізу ризиків інформаційної безпеки на підприємстві має бути створена група управління інформаційними ризиками. До складу цієї групи входять керівники підрозділів, IT-працівники,

розроблювачі додатків. Одним з перших завдань УІР-групи є визначення вартості активів підприємства і формування звіту з цих питань. Керівництво підприємства, проаналізувавши цей звіт, визначає обсяг УІР-проекту.

При визначенні вартості активів УІР-група повинна враховувати корисність і значення активів для підприємства; цінність активів для конкурентів, користувачів і власників цих активів; витрати на купівлю, розроблення, захист, заміну або ремонт активів при їх виході з ладу або втраті; наслідки у випадку компрометації активів тощо. Саме цінність активів визначає механізми безпеки та захисні заходи для їх захисту.

Після визначення цінності активів, відбувається ідентифікація загроз інформаційній безпеці підприємства, яка дозволяє встановити найбільш вразливі місця. Під час цієї ідентифікації встановлюються джерела загроз та їх наслідки, після чого проводиться аналіз можливих вразливостей від цих загроз і окреслюються шляхи протидії загрозам. Наприклад, джерелом загроз може бути хакер, який одержує доступ до конфіденційної інформації, за рахунок вразливості у вигляді великої кількості служб, запущених на сервері підприємства.

Після виявлення вразливостей і пов'язаних з ними загроз УІР-група повинна проаналізувати ризики потенційного збитку, а саме несанкціоноване розголошення конфіденційної інформації, зниження продуктивності роботи, пошкодження інформації або інформаційних систем та інші і доповісти про це керівництву підприємства для вживання адекватних заходів протидії.

Проведемо порівняльний аналіз найбільш поширених на цей час методик оцінки ризиків інформаційної безпеки.

Методикою оцінки ризиків OCTAVE займається американський інститут Software Engineering Institute [1]. Ця методологія передбачає здійснення процесу аналізу ризиків інформаційної безпеки лише працівниками підприємства без залучення зовнішніх консультантів, через те що такі працівники краще розуміють потреби підприємства і властиві йому ризики.

За цією методикою відбувається розробка профілю загроз, встановлення

вразливостей інформаційній безпеці і розроблення стратегії забезпечення безпеки. Для кожного джерела загроз будується дерево варіантів, яке наочно показує вигляд загрози і шляхи її усунення. При оцінці ризиків інформаційній безпеці формується шкала за трьома позиціями: високий, середній та низький рівень ризику і встановлюється можливий фінансовий збиток. Основною перевагою даної методики є загальнодоступність і безкоштовність.

Для проведення якісної оцінки ризиків використовується груповий процес аналізу ризиків FRAP. Ця методика побудована таким чином [2], що будь-яка людина з навиками організації групової роботи зможе успішно провести аналіз ризиків інформаційної безпеки. Згідно з цією методикою необхідно здійснити такі етапи, як мозкова атака для встановлення всіх загроз інформаційній безпеці підприємства; визначення ймовірності та вразливостей для кожної загрози за шкалою велика/середня/низька; формування звіту за результатами можливого впливу кожної із загроз. Перевагою цієї методики є швидкість і простота прийняття рішень.

Також заслуговує на увагу метод аналізу й керування ризиками Центрального агентства по комп'ютерах і телекомунікаціях (ССТА) Великобританії CRAMM. Цей метод поєднує кількісні та якісні методики оцінки ризиків. Метод є універсальним і може використовуватися великими і малими, державними і комерційними підприємствами.

Версії програмного забезпечення CRAMM орієнтовані на різні типи підприємств і відрізняються своїми базами знань [3]. Для комерційних підприємств існує комерційний профіль, а для державних - урядовий профіль. Урядовий профіль дозволяє проводити аудит на відповідність вимогам стандарту ITSEC.

Метод CRAMM дозволяє економічно обгрунтувати витрати підприємства на забезпечення інформаційної безпеки і безперервність бізнесу. Він розділений на три сегменти: ідентифікація й оцінка активів, аналіз загроз і вразливостей, вибір контрзаходів. Цей метод, назважаючи на значну універсальність та функціональність, має такі недоліки як необхідність спеціальної підготовки користувачів і значна вартість ліцензії.

Для оцінки ризиків інформаційної безпеки існують інші методики, які подібні до представлених.

З проведеного аналізу можна навести такі рекомендації по вибору методик оцінки ризиків інформаційної безпеки: для невеликих підприємств доцільно використовувати методику OCTAVE, для середніх – FRAP, а для великих – CRAMM.

Теоретичні питання:

1. Розкрийте поняття "нематерільні активи підприємства", що відноситься до цієї категорії?

2. Що таке стратегічні активи підприємства? Наведіть приклади

3. Активи підприємства, їх джерела та класифікація.

4. Проаналізуйте метод аналізу й керування ризиками Центрального агентства по комп'ютерах і телекомунікаціях (ССТА) Великобританії CRAMM.

5. Проаналізуйте методику оцінки ризиків OCTAVE.

6. Проаналізуйте груповий процес аналізу ризиків FRAP.

7. Якими методами проводиться оцінка активів підприємства?

8. Розкрийте поняття "матерільні активи підприємства", що відноситься до цієї категорії?

Практичне завдання:

Класифікуйте інформаційні активи, що знаходяться на вашому пристрої (мобільному телефоні, ноутбуці, домашньому ПК і т.д.), сформулюйте потенційні загрози інформації, визначіть методи та засоби їх уникнення. Представити у вигляді таблиці відповідності "інформація-загрози-методи і засоби уникнення".

Практична робота № 4

Тема: Структура та вимоги стандарту ISO/IEC 27001

Загальні відомості

Основні вимоги та структура стандарту ISO/IEC 27001 буди докладно розглянуті у лекції №5. Розглянемо приклади вразливостей, які можуть бути використані для реалізації відповідних загроз для комерційної структури (на прикладі банку):

Приклади загроз	*Приклади вразливостей*
Фізичне пошкодження/втрата будівлі/обладнання/інформації від пожежі	• Відсутність пожежної сигналізації • Відсутність системи пожежогасіння • Дозвіл на паління в приміщенні • Наявність легкозаймистих матеріалів • Неякісна електропроводка • Відсутність захисту від блискавки • Неконтрольований ремонт • Наявність зловмисного підпалювача • Халатність персоналу • Необізнаність персоналу • Злочинні дії
Фізичне пошкодження/втрата будівлі/обладнання/інформації від пошкодження водою/повінню	• Невдале розташування будівлі • Невдале розміщення обладнання у підвальному приміщенні /на перших поверхах будівлі • Приміщення банку в аварійному стані • Неякісна каналізаційна система
Фізичне пошкодження/втрата будівлі/обладнання/інформації від техногенної аварії	• Наявність будівництва поряд • Старе приміщення банку (в аварійному стані) • Неякісна каналізаційна система • Відсутність контролю системи електроживлення • Відсутність резервних джерел електроживлення • Відсутність резервних каналів зв’язку • Відсутність резервного обладнання • Відсутність віддаленого резервного пункту
Фізичне пошкодження/втрата обладнання/інформації від крадіжки	• Неефективна система охорони • Недостатній контроль за переміщенням майна за межі банку • Недбалість персоналу • Неправильний підбор персоналу • Необізнаність персоналу • Відсутність резервного обладнання/ програмного забезпечення

Фізичне пошкодження/втрата будівлі/обладнання/інформації від тероризму	• Відсутність інструкції стосовно дій у надзвичайних ситуаціях • Неефективна система охорони • Неправильний підбор персоналу • Відсутність резервного обладнання/ програмного забезпечення
Фізичне пошкодження/втрата будівлі/обладнання/інформації від масових заворушень, політичної нестабільності	• Відсутність інструкції стосовно дій у надзвичайних ситуаціях • Неефективна система охорони • Неправильний підбор персоналу • Відсутність резервного обладнання/ програмного забезпечення • Відсутність віддаленого резервного пункту
Фізичне пошкодження/втрата будівлі/обладнання/інформації від кліматичних та метеорологічних явищ	• Старе приміщення банку (в аварійному стані) • Неякісна каналізаційна система • Відсутність контролю системи електроживлення • Відсутність резервних джерел електроживлення • Відсутність резервних каналів зв’язку • Відсутність резервного обладнання • Відсутність віддаленого резервного пункту
Фізичне пошкодження/втрата будівлі/обладнання/інформації від сейсмічних загроз	• Старе приміщення банку (в аварійному стані) • Неякісна каналізаційна система • Відсутність контролю системи електроживлення • Відсутність резервних джерел електроживлення • Відсутність резервних каналів зв’язку • Відсутність резервного обладнання • Відсутність віддаленого резервного пункту
Фізичне пошкодження/втрата обладнання/інформації від електромагнітної радіації	• Відсутність екранування серверного приміщення • Чутливість обладнання до електромагнітної радіації • Неефективна охорона
Фізичне пошкодження/втрата обладнання/інформації від неконтрольованого ремонту	• Відсутність належного контролю за працівниками третіх сторін • Відсутність вимог з інформаційної безпеки в угодах з третіми сторонами • Відсутність резервних джерел електроживлення • Відсутність резервних каналів зв’язку • Відсутність резервного обладнання

Часткове/повне пошкодження /втрата обладнання/даних від неефективності системи кліматконтролю або водопостачання	• Неправильний розрахунок потужності обладнання для відведення тепла • Відсутність або недостатність вимог з інформаційної безпеки в угодах з третіми сторонами • Неефективне обслуговування обладнання працівниками третіх сторін або персоналом банку • Відсутність належного контролю та моніторингу обладнання
Часткове/повне пошкодження /втрата обладнання/даних від збоїв електроживлення	• Неправильний розрахунок необхідної потужності електроживлення • Відсутність контролю та моніторингу системи електроживлення • Відсутність резервних джерел електроживлення • Відсутність резервного обладнання • Відсутність або недостатність вимог з інформаційної безпеки в угодах з третіми сторонами • Неефективне обслуговування обладнання працівниками третіх сторін або персоналом банку

Часткове/повне пошкодження /втрата обладнання/даних від недбалості персоналу	• Недосвідченість персоналу • Відсутність системи моніторингу роботи IT інфраструктури • Недосконала IT система • Неефективна охорона • Відсутність контролю за переміщенням майна банку • Відсутність або недостатність тестування обладнання/програмного забезпечення • Можливість використання обладнання/програмного забезпечення не за призначенням • Неефективне розмежування прав доступу до програмного забезпечення/даних • Недостатня захищеність вузла доступу до загальних мереж (наприклад, інтернет) від зовнішніх зловмисників • Недостатньо ефективна система розподілу прав доступу до інформації • Відсутність “logout” під залишення працівником робочої станції • Передача/втрата контролю за носіями криптографічних ключів • Передача/компрометація паролів доступу • Передача або повторне використання середовища збереження даних без відповідного знищення інформації • Невиконання процедур резервного копіювання інформації • Незахищене зберігання даних/ документів • Неконтрольоване копіювання інформації
Часткове/повне пошкодження /втрата даних від відмови телекомунікаційного обладнання	• Відсутність резервних каналів зв’язку • Відсутність резервного телекомунікаційного обладнання • Недбалість персоналу • Необізнаність персоналу • Відсутність або недостатність вимог безпеки в угодах з провайдерами зв’язку • Зловмисні дії персоналу провайдерів зв’язку • Погане з’єднання та розміщення кабелів • Наявність єдиної точки відмови

Часткове/повне пошкодження /втрата даних від порушення експлуатації обладнання/ програмного забезпечення	• Необізнаність персоналу • Відсутність системи моніторингу роботи IT інфраструктури • Недосконала IT система • Ускладнений інтерфейс користувача • Відсутність документації • Недосконале або нове програмне забезпечення • Відсутність або недостатність тестування обладнання/програмного забезпечення • Відсутність перевірки цілісності програмного забезпечення під час його запуску • Можливість використання обладнання/програмного забезпечення не за призначенням • Неефективне розмежування прав доступу до програмного забезпечення/даних • Наявність єдиної точки відмови
Часткове/повне пошкодження /втрата даних від неавторизованого використання обладнання/програмного забезпечення	• Відсутність контролю за використанням обладнання/програмного забезпечення • Відсутність контролю за внесенням змін до складу обладнання/програмного забезпечення • Наявність незахищеного з'єднання з публічними мережами • Відсутність політик використання обладнання/програмного забезпечення • Неефективне розмежування прав доступу до програмного забезпечення/обладнання • Неефективна політика управління мережею
Часткове/повне пошкодження /втрата даних від збою обладнання/програмного забезпечення	• Відсутність плану забезпечення безперервної роботи • Необізнаність персоналу • Відсутність системи моніторингу роботи IT інфраструктури • Недосконале або нове програмне забезпечення • Відсутність контролю цілісності програмного забезпечення під час його запуску • Відсутність або недостатність тестування обладнання/програмного забезпечення • Можливість використання обладнання/програмного забезпечення не за призначенням • Неефективне розмежування прав доступу до програмного забезпечення/даних • Наявність єдиної точки відмови • Відсутність або недосконаліть системи резервного копіювання інформації • Відсутність резервного обладнання • Неадекватне реагування для підтримки сервісів • Відсутність або недосконаліть угоди про рівень обслуговування третіми сторонами

Часткове/повне пошкодження /втрата даних від неправильного використання обладнання/ програмного забезпечення	• Необізнаність персоналу • Відсутність системи моніторингу роботи IT інфраструктури • Недосконала IT система • Ускладнений інтерфейс користувача • Відсутність документації • Недосконале або нове програмне забезпечення • Відсутність або недостатність тестування обладнання/програмного забезпечення • Можливість використання обладнання/програмного забезпечення не за призначенням • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність або недосконаліть системи резервного копіювання інформації • Відсутність резервного обладнання • Неадекватне реагування для підтримки сервісів
Компрометація інформації за допомогою віддаленого шпіонажу	• Небезпечна архітектура мережі • Відсутність або неефективність ідентифікації та аутентифікації користувача • Передавання паролів у відкритому вигляді • Незахищене з'єднання з публічними мережами • Недостатній контроль за функціонуванням та управлінням мережею • Недостатня обізнаність персоналу у питаннях інформаційної безпеки
Компрометація інформації за допомогою перехоплення побічних електромагнітних сигналів	• Відсутність екранування серверної кімнати • Неефективна охорона та пропускний режим для відвідувачів
Компрометація інформації за допомогою підслуховування	• Наявність незахищених комунікаційних ліній • Відсутність процедури безпечного проведення нарад • Наявність незахищеного конфіденційного трафіку • Необізнаність персоналу
Компрометація інформації за допомогою відновлення середовища, що повторно використовується або викинуто	• Відсутність процедури знищення інформації • Необізнаність персоналу • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки

Компрометація інформації за допомогою розкриття/продажу інформації працівниками банку	• Неправильний підбір персоналу • Необізнаність персоналу у питаннях інформаційної безпеки • Відсутність класифікації інформації • Відсутність затвердженої процедури поводження з інформацією з обмеженим доступом • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Незахищене з'єднання з публічними мережами • Відсутність контролю за роботою електронної пошти • Відсутність або неефективність ідентифікації та аутентифікації користувача • Недостатній контроль за функціонуванням та управлінням мережею • Неефективне розмежування прав доступу до програмного забезпечення/даних
Компрометація інформації за допомогою підробки обладнання/програмного забезпечення	• Відсутність або неефективність процедури контролю вводу нового програмного забезпечення/обладнання • Неправильний підбір персоналу • Відсутність або неефективність ідентифікації та аутентифікації користувача • Недостатній контроль за функціонуванням та управлінням мережею • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки
Компрометація інформації за допомогою шахрайського копіювання даних	• Неправильний підбір персоналу • Відсутність або неефективність ідентифікації та аутентифікації користувача • Недостатній контроль за функціонуванням та управлінням мережею • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту

Компрометація інформації за допомогою нелегального оброблення даних	• Неправильний підбір персоналу • Відсутність або неефективність ідентифікації та аутентифікації користувача • Доступність сервісів, в яких немає необхідності • Недостатній контроль за функціонуванням та управлінням мережею • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту
Компрометація інформації за рахунок помилки/недбалості персоналу під час оброблення даних	• Необізнаність персоналу • Відсутність або неефективність навчання персоналу • Ускладнений інтерфейс користувача • Доступність сервісів, в яких немає необхідності • Відсутність документації • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту Підробка програмного забезпечення
Компрометація інформації за рахунок зловживання працівником правами доступу до інформації	• Неправильний підбір персоналу • Відсутність або неефективність ідентифікації та аутентифікації користувача • Доступність сервісів, в яких немає необхідності • Відсутність формальної процедури реєстрації та відміни реєстрації прав доступу користувача • Відсутність формальної процедури перегляду прав доступу користувачів • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність або неефективність процедур контролю прав доступу • Відсутність регулярних аудитів • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту

Компрометація інформації за рахунок підробки прав доступу до інформації	• Неправильний підбір персоналу • Відсутність або неефективність ідентифікації та аутентифікації користувача • Доступність сервісів, в яких немає необхідності • Наявність незахищених таблиць паролів • Недосконале управління паролями доступу • Неправильні параметри інсталяції програмного забезпечення • Недосконале програмне забезпечення • Відсутність формальної процедури реєстрації та відміни реєстрації прав доступу користувача • Відсутність формальної процедури перегляду прав доступу користувачів • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність або неефективність процедур контролю прав доступу • Відсутність регулярних аудитів • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту
Компрометація інформації за рахунок отримання несанкціонованого доступу до інформації зовнішніми зловмисниками	• Небезпечна архітектура мережі • Відсутність або неефективність ідентифікації та аутентифікації користувача • Передавання паролів у відкритому вигляді • Незахищене з’єднання з публічними мережами • Відсутність або недостатність вимог з інформаційної безпеки з клієнтами та/або третіми сторонами • Недостатній контроль за функціонуванням та управлінням мережею/програмним забезпеченням • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту • Недостатня обізнаність персоналу у питаннях інформаційної безпеки

Компрометація інформації за рахунок неправильної роботи системи захисту інформації	• Помилки під час проектування та розроблення системи захисту інформації • Відсутність документації • Необізнаність персоналу • Відсутність або неефективність навчання персоналу • Ускладнений інтерфейс користувача • Відсутність контролю цілісності системи захисту інформації під час її запуску/ініціалізації • Відсутність записів про роботу системи захисту в журналах аудиту
Компрометація інформації за рахунок навмисного невикористання системи захисту інформації	• Помилки під час проектування та розроблення системи захисту інформації • Відсутність записів про роботу системи захисту в журналах аудиту • Неправильний підбір персоналу • Відсутність регулярних аудитів • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки
Компрометація інформації за рахунок компрометації паролів доступу	• Необізнаність персоналу • Порушення персоналом правил зберігання паролів • Доступність сервісів, в яких немає необхідності • Наявність незахищених таблиць паролів • Недосконале управління паролями доступу • Відсутність формальної процедури перегляду прав доступу користувачів • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність або неефективність процедур контролю прав доступу • Відсутність регулярних аудитів • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту

Компрометація інформації за рахунок компрометації ключів криптографічного захисту інформації	• Помилки під час проектування та розроблення системи захисту інформації • Помилки під час генерації ключів, в тому числі генерація ключів без паролю • Неефективна процедура розповсюдження ключів • Відсутність документів стосовно поводження з криптографічними ключами для користувачів • Відсутність записів про роботу системи захисту в журналах аудиту • Відсутність регулярних аудитів • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки
Викривлення/підробка інформації/даних за рахунок помилок програмного забезпечення	• Помилки під час проектування та розроблення програмного забезпечення в питаннях використання системи криптографічного захисту інформації • Невикористання електронного цифрового підпису для захисту цілісності електронних банківських документів • Відсутність перевірки електронного цифрового підпису під час роботи з електронними документами, які зберігаються в базах даних/сховищах даних/електронних архівах • Відсутність записів про роботу системи захисту в журналах аудиту • Відсутність документації • Ускладнений інтерфейс користувача
Неправильна робота системи захисту інформації	• Помилки під час проектування та розроблення системи захисту інформації • Невикористання електронного цифрового підпису для захисту цілісності електронних банківських документів • Відсутність документації • Необізнаність персоналу • Відсутність або неефективність навчання персоналу • Ускладнений інтерфейс користувача • Відсутність записів про роботу системи захисту в журналах аудиту

Компрометація/передача особистих ключів електронного цифрового підпису	• Помилки під час проектування та розроблення системи захисту інформації • Помилки під час генерації ключів, в тому числі генерація ключів без паролю • Неефективна процедура розповсюдження ключів • Відсутність документів стосовно поводження з ключами електронного цифрового підпису для користувачів • Відсутність записів про роботу системи захисту в журналах аудиту • Відсутність регулярних аудитів • Відсутність належного визначення відповідальності за інформаційну безпеку • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки

Загрози можуть бути навмисними (Н), випадковими (В), природними (П) і можуть бути результатом втрати будь-яких сервісів. У таблиці наведений перелік типових загроз із наданням джерела загроз. Цей перелік не може вважатися вичерпним і може бути доповненим або скороченим.

Загроза	*Джерело*	*Тип*
Фізичне пошкодження/втрата будівлі/обладнання/інформації	Пожежа	В, Н, П
	Пошкодження водою/повінь	В, Н, П
	Техногенна аварія	В, Н
	Крадіжка	В, Н, П
	Тероризм	В, Н
	Масові заворушення, політична нестабільність	В, Н
	Кліматичні та метеорологічні явища	П
	Сейсмічні загрози	П
	Електромагнітна радіація	В, Н
	Неконтрольований ремонт	В, Н
Часткове/повне пошкодження /втрата обладнання/даних	Неефективність системи клімат- контролю або водопостачання	В, Н
	Збої електроживлення	В, Н, П
	Недбалість персоналу	В, Н
	Відмова телекомунікаційного обладнання	В, Н
	Порушення експлуатації обладнання/програмного забезпечення	В, Н
	Неавторизоване використання обладнання/програмного забезпечення	В, Н
	Збої обладнання/програмного забезпечення	В, Н
	Неправильне використання обладнання/програмного забезпечення	В, Н
	Віддалений шпіонаж	Н
	Перехоплення побічних електромагнітних сигналів	Н
	Підслуховування	Н
	Відновлення середовища, що повторно використовується або викинуто	Н

Компрометація інформації	Розкриття/продаж інформації працівниками банку	В, Н
	Підробка обладнання/програмного забезпечення	Н
	Шахрайське копіювання даних	Н
	Нелегальне оброблення даних	Н
	Помилка/недбалість персоналу під час оброблення даних	В, Н
	Зловживання працівником правами доступу до інформації	Н
	Підробка прав доступу до інформації	Н
	Отримання несанкціонованого доступу до інформації зовнішніми зловмисниками	Н
	Неправильна робота системи захисту інформації	В, Н
	Навмисне невикористання системи захисту інформації	Н
	Компрометація паролів доступу	В, Н
	Компрометація ключів криптографічного захисту інформації	В, Н
Викривлення/підробка інформації/даних	Помилки програмного забезпечення	В, Н
	Неправильна робота системи захисту інформації	В, Н
	Компрометація/передача особистих ключів електронного цифрового підпису	В, Н

Особливу увагу слід звернути на людські джерела загроз, які можуть мати різну мотивацію від політичних причин до простого самоствердження. Найбільш вірогідними та найбільш серйозними можна вважати загрози від власних працівників банку, в тому числі ті загрози, які можуть виникати від недостатньої обізнаності персоналу в питаннях інформаційної безпеки. Приклади таких загроз наведені нижче у таблиці.

Джерело загрози	*Загроза*
Хакери, кракери	• Хакерські дії • Соціальна інженерія • Втручання до системи, злом • Неавторизований доступ до системи
Комп’ютерні злочинці	• Комп’ютерні злочини • Шахрайські дії • Продаж інформації • Спуфінг • Втручання до системи • Руйнування інформаційної системи
Тероризм	• Бомба/тероризм • Інформаційна війна • Атаки на систему (наприклад, розподілена відмова в обслуговуванні) • Підробка системи • Фінансування терористичних організацій

Дії конкурентів	• Політична перевага • Економічні дії • Крадіжка інформації • Вручання в особисте життя • Соціальна інженерія • Проникнення до системи • Неавторизований доступ до системи
Персонал	• Напад на персонал • «Чорна пошта» • Перегляд інформації з обмеженим доступом • Комп'ютерні зловживання • Шахрайство і крадіжка • Продаж інформації • Фальсифікація та підробка даних • Перехоплення • Зловмисні коди (віруси, троянські коні,тощо) • Продаж персональної інформації • Дефекти системи • Втручання до системи • Системний саботаж • Неавторизований доступ до системи

Теоретичні питання:

1. Розкрийте основні вимоги до створення та менеджменту системи інформаційної безпеки.

2. Які основні вимоги до забезпечення документацією?

3. Які саме існують, згідно стандарту, обов'язки керівництва з управління трудовими ресурсами?

4. Яким чином відбувається внутрішній аудит системи інформаційної безпеки?

5. Яким чином відбувається перевірка системи менеджменту інформаційної безпеки?

6. Етапи вдосконалення системи менеджменту інформаційної безпеки.

7. Які коректуючи міри здійснюються для вдосконалення системи менеджменту інформаційної безпеки?

8. Які попередні міри здійснюються для вдосконалення системи менеджменту інформаційної безпеки?

Практичне завдання:

Визначити основні вразливості, відповідно переліку, відділення банку «Укрсоцбанк», що знаходиться у фойє університету. Зазначити джерела цих загроз.

Практична робота № 5

Тема: Оцінка ризиків інформаційної безпеки з використанням програмного комплексу "Гриф" компанії Digital Security

Загальні відомості

Ознайомлення з класифікацією загроз DSECCT (Digital Security Classification of Threats)

За характером загрози ІБ діляться на технологічні і організаційні.

Технологічні загрози ІБ по виду впливу діляться на фізичні і програмні (логічні). Наступний щабель класифікації - джерело загрози. Джерелами фізичних загроз можуть бути дії порушника (людини), форс-мажорні обставини, відмова обладнання і внутрішніх систем життєзабезпечення. Незалежно від джерела фізичні погрози впливають на ресурс і на канал зв'язку. Джерелами програмних загроз може бути локальний або віддалений порушник. Об'єктом локального порушника може бути тільки ресурс. При цьому, на ресурсі локальний порушник може реалізувати загрози, спрямовані на операційну систему, прикладне програмне забезпечення та інформацію. Загрози, які виходять від віддаленого порушника, можуть впливати на ресурс і на канал зв'язку. При доступі до ресурсу віддалений порушник може впливати на операційну систему, мережеві служби і на інформацію. При впливі на канал зв'язку віддалений порушник може реалізувати загрози, спрямовані на мережеве обладнання та протоколи зв'язку.

Організаційні загрози по джерелу впливу поділяються на вплив на персонал і дії персоналу. Вплив на персонал може бути фізичним і психологічним. Як фізичне, так і психологічне вплив на персонал направлено на співробітників компанії з метою отримання інформації та порушення безперервності ведення бізнесу. Причинами дій персоналу, здатних викликати загрози ІБ, можуть бути умисні або ненавмисні дії. Загрози, викликані умисними діями персоналу, можуть бути спрямовані на інформацію і на безперервність ведення бізнесу. Загрози, викликані умисними діями

персоналу, можуть бути спрямовані на інформацію і на безперервність ведення бізнесу.

1. Загрози технологічного характеру
1.1) Фізичні
- Дії порушника (людини)
• На ресурс
• На канал зв'язку
- Форс-мажорні обставини
• На ресурс
• На канал зв'язку
- Відмова устаткування і внутрішніх систем життєзабезпечення
• На ресурс
• На канал зв'язку
1.2) Програмні (логічні)
- Локальний порушник
• На ресурс
- На операційну систему
- На прикладне програмне забезпечення
- На інформацію
- Віддалений порушник
• На ресурс
- На операційну систему
- На мережеві служби
- На інформацію
• На канал зв'язку
- На мережеве обладнання
- На протоколи зв'язку
2. Загрози організаційного характеру
2.1) Вплив на персонал
- Фізична
•Отримання інформації
• Порушення безперервності ведення бізнесу
- Психологічний
•Отримання інформації
• Порушення безперервності ведення бізнесу
2.Дії персоналу
- Умисні дії
• На інформацію
• На безперервність ведення бізнесу

- Ненавмисні дії
• На інформацію
• На безперервність ведення бізнесу

Таким чином, класифікація загроз ІБ поділяється за характером загрози, виду впливу, джерела і об'єкта загрози. З самими погрозами, запропонованими компанією Digital Security, можна познайомиться в процесі виконання роботи.

Ознайомлення, установка і первісна настройка програмного продукту «Гриф» компанії з Digital Security Office 2006.

Програмний продукт Digital Security Office 2006 складається з серверної і клієнтської частини. У локальній мережі досить встановити одну серверну частину.

В папці Сервер_full виберіть інсталяційний файл dsoffice2006_academic_edition_server і далі дотримуйтесь стандартних інструкцій з установки (рис.1.1).

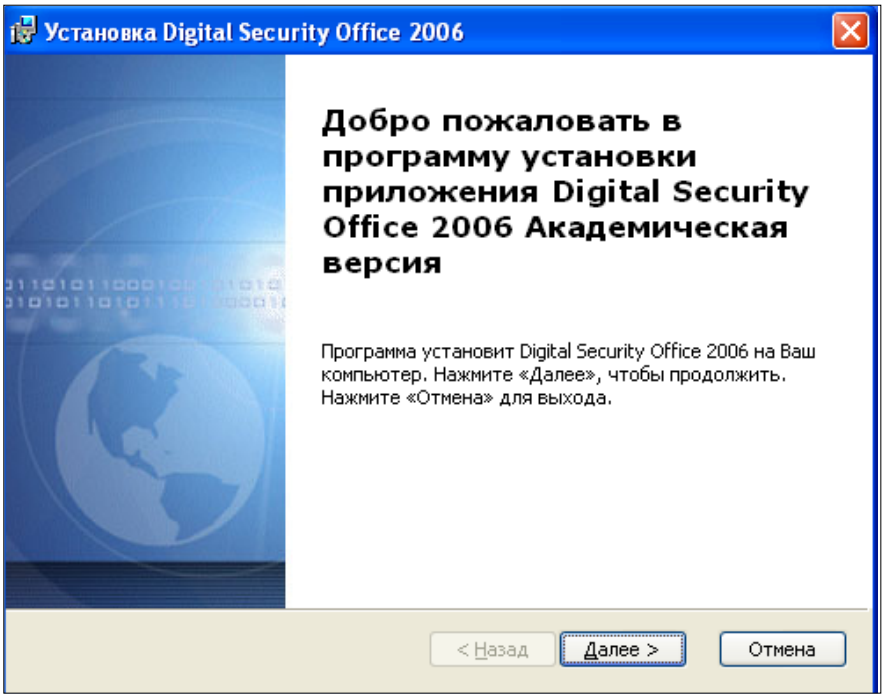

Рис.1.1. Установка Digital Security Office 2006

Після перезавантаження програма попросить ввести ключ. Для цього скопіюйте ідентифікатор на електронний носій. Ідентифікатор відправляється в центр генерації ключів. У відповідь приходить ім'я і ключ.

Увага! Ім'я необхідно вводити з клавіатури, а ключ копіювати.

Встановлення клієнта

В папці Кліент_full виберіть інсталяційний файл dsoffice2006_academic_edition_client і далі дотримуйтесь стандартні заходи установки. Після перезавантаження запустіть "Гриф" з робочого столу (якщо встановлено ярлик) або Пуск -> Програми -> Digital Security -> Digital Security Office 2006 Клієнт -> ГРИФ 2006. Програма попросить ввести ключ (рис.1.2).

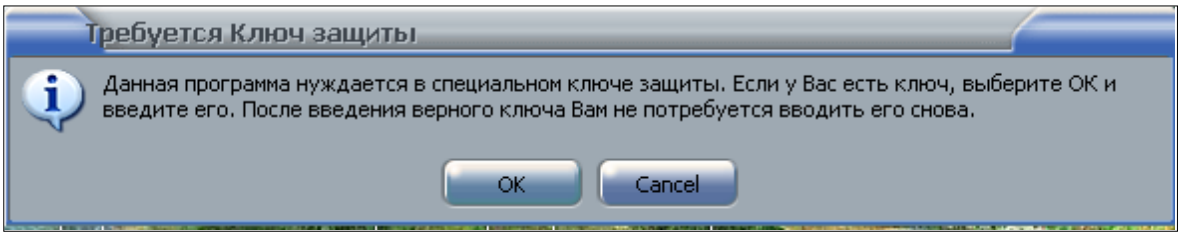

Рис.1.2. Підтвердження існування ключа захисту

Скопіюйте системний ідентифікатор на електронний носій. Ідентифікатор відправляється в центр генерації ключів. У відповідь приходить ім'я і ключ.

Увага! Ім'я необхідно вводити з клавіатури, а ключ копіювати (рис.1.3).

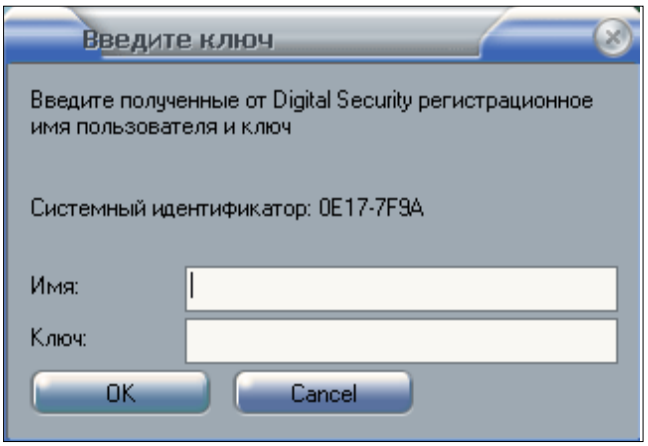

Рис.1.3. Реєстрація користувача.

Налаштування

Після введення ключа програма попросить ввести ім'я користувача. Цього користувача необхідно додати в список користувачів на серверної частини і дати йому права адміністратора, інакше користувач не зможе створити власний проект. Для цього (рис.1.4):

- Увімкніть сервер. (Нижня панель меню -> Запустити сервер)
- Адміністрування. (Там же)

• Натисніть "Додати". Задайте ім'я користувача і надайте йому права адміністратора.

• Переконайтеся, що користувач може створювати проект. Для цього Пуск -> Програми -> Digital Security -> Digital Security Office 2006 Клієнт -> ГРИФ 2006. Введіть ім'я користувача і пароль. Створіть проект.

• Перейдіть в локальний режим, зупинивши сервер. Тепер ви не залежите від сервера.

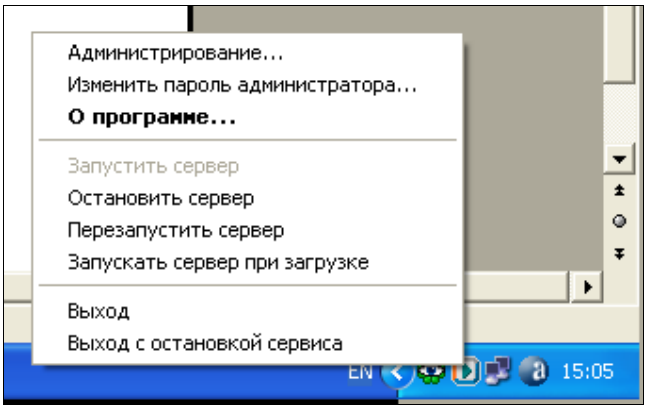

Рис.1.4. Адміністрування

Ознайомлення з алгоритмом роботи програми «Гриф»

Для оцінки ризиків ІС компанії захищеність кожного цінного ресурсу визначається за допомогою аналізу загроз ІБ, що діють на конкретний ресурс, і вразливостей, через які дані загрози можуть бути реалізовані. Оцінюючи ймовірність реалізації актуальних для цінного ресурсу загроз і ступінь впливу реалізації загрози на ресурси, аналізуються інформаційні ризики ресурсів компанії.

В результаті роботи алгоритму програма представляє наступні дані:

• Інвентаризація.

• Значення ризику для кожного цінного ресурсу компанії.

• Перелік всіх вразливостей, які стали причиною отриманого значення ризику.

• Значення ризику для ресурсів після завдання контрзаходів (залишковий ризик).

• Ефективність контрзаходів.

Перед заповненням програми «Гриф» проводиться інвентаризацію цінних ресурсів та інформації компанії, тобто визначити, всю цінну інформацію компанії і ресурси, на яких вона зберігається.

Далі власники інформації або відповідальні особи (як правило, начальники відділів, в яких ведеться обробка інформації) повинні визначити шкоду, який понесе компанія при здійсненні погроз конфіденційності, цілісності та доступності цієї інформації. Якщо власник інформації не може оцінити збиток інформації в грошах, програма дозволяє заносити збиток в рівнях (кількість і оцінку рівнів власник вибирає самостійно (в діапазоні від 2 до 100), але для всіх видів інформації в ІС компанії кількість і оцінка рівнів повинні бути однакові).

У програму «Гриф» заносяться тільки ресурси, на яких обробляється цінна інформація, тобто інформація, для якої можна оцінити збиток при реалізації загроз.

Далі фахівець служби ІТ визначає загрози, що діють на ресурси з цінною інформацією, і уразливості, через які реалізуються загрози, критичність загроз і ймовірність реалізації загроз через зазначені уразливості.

Фахівці відділу ІБ надають дані про витрати на ІБ.

Різним типам співробітників, які заповнюють програму, потрібно внести дані як це показано в табл.1.

Таблиця 1.1. Відповідальність за внесення даних.

Данные, которые заносятся в программу	**Сотрудник, отвечающий за предоставление данных**
Ресурси, на яких зберігається цінна інформація	Спеціаліст служби ІТ
Критичність ресурсу, на якому зберігається цінна інформація	Власник інформації (або начальник відділу, в якому здійснюється обробка інформації)
Відділи, до яких відносяться ресурси	Як правило, збігаються з організаційною структурою компанії
Загрози, що діють на ресурси	Спеціаліст служб ІТ та ІБ
Уразливості, через які реалізуються загрози	Спеціаліст служб ІТ та ІБ
Витрати на ІБ	Спеціаліст служб ІТ та ІБ

. З точки зору базових загроз ІБ існує два режими роботи алгоритму:

• Одна базова загроза (сумарна).

• Три базові загрози.

С точки зору одиниць виміру критичності і ризику ресурсу існують два режими роботи алгоритму:

• В грошових одиницях.

• У рівнях (відсотках).

При роботі з алгоритмом використовується шкала від 0 до 100%. Максимальне число рівнів - 100, тобто шкалу можна розбити на 100 рівнів. При розбитті шкали на менше число рівнів, кожен рівень займає певний інтервал на шкалі. Причому, можливо два варіанти поділу:

• Рівномірний.

• Логарифмічні

Змоделюати інформаційну мережу (ІМ) філії банку.

Схема системи, що моделюється«філія банку» представлена на рис.1.5.

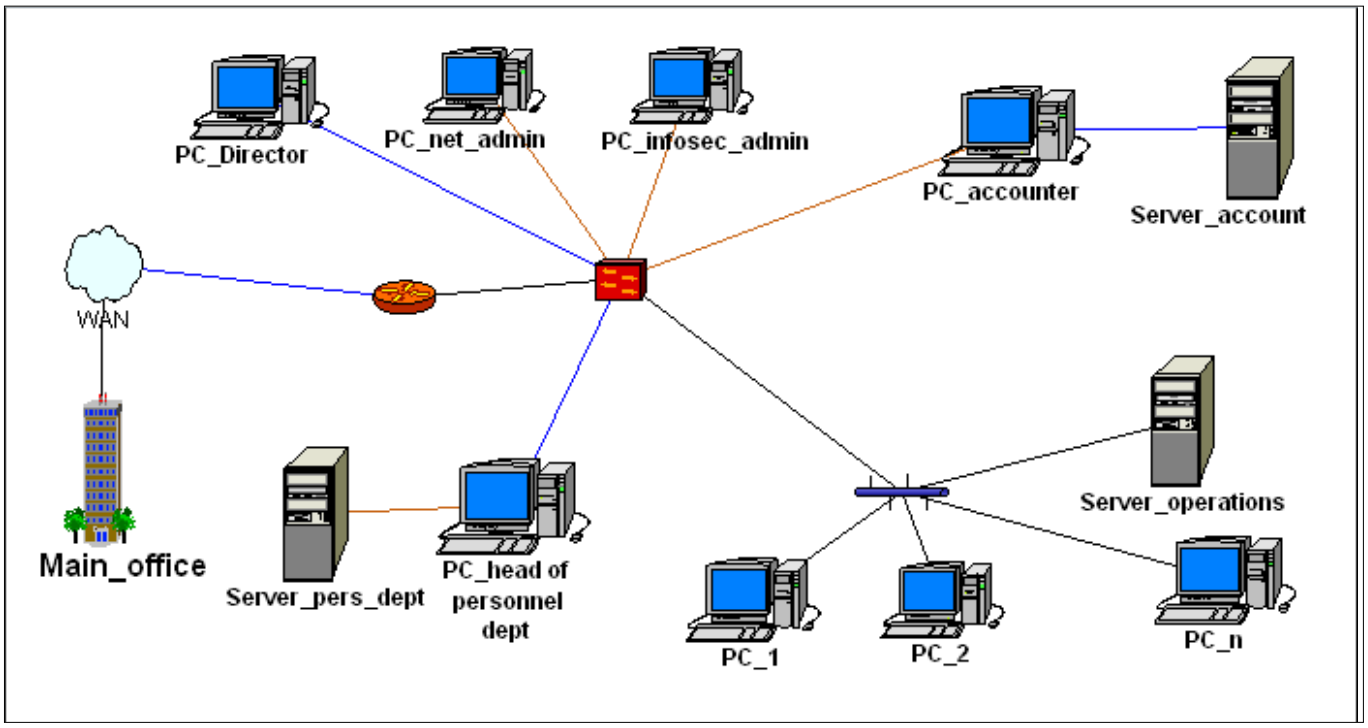

Рис.1.5. Схема системи «філія банку»

Створення проекту

1. Запустити програму «Гриф»: Пуск –> Программы –> Digital Security –> Digital Security Office 2006 Клиент -> ГРИФ 2006.

2. Введіть им'я коритувача і пароль (рис.1.6).

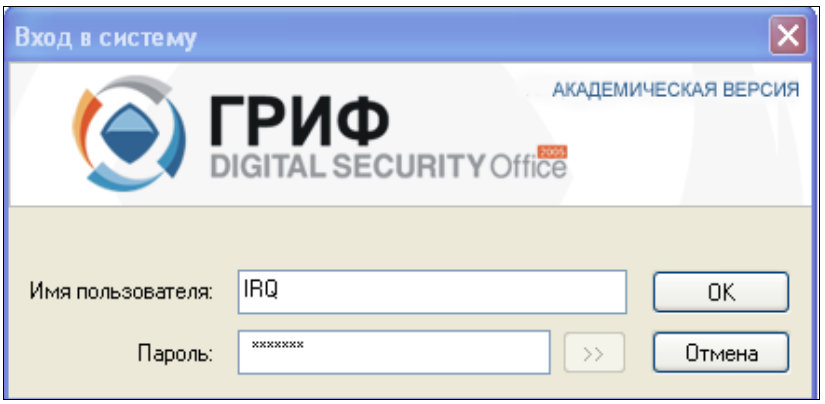

Рис.1.6. Вхід в систему

3. Выберіть Алгоритм «Анализ модели угроз и уязвимостей» и створіть проект (рис.1.7).

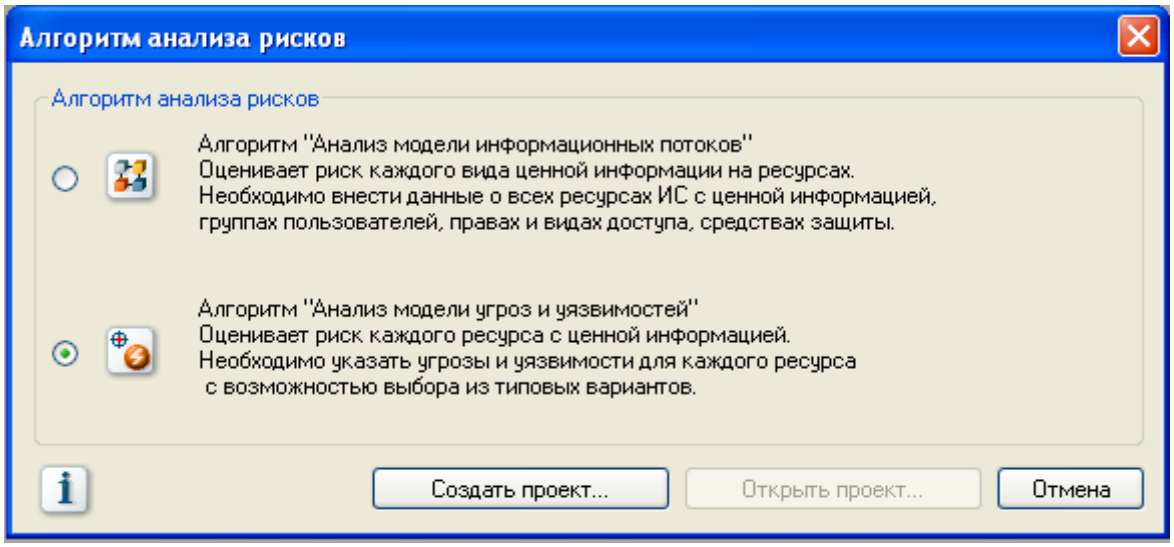

Рис.1.7. Створення проекту «анализ модели угроз и уязвимостей»

4. Задайте им'я проекту. З'явиться вікно такого вигляду (рис.1.8):

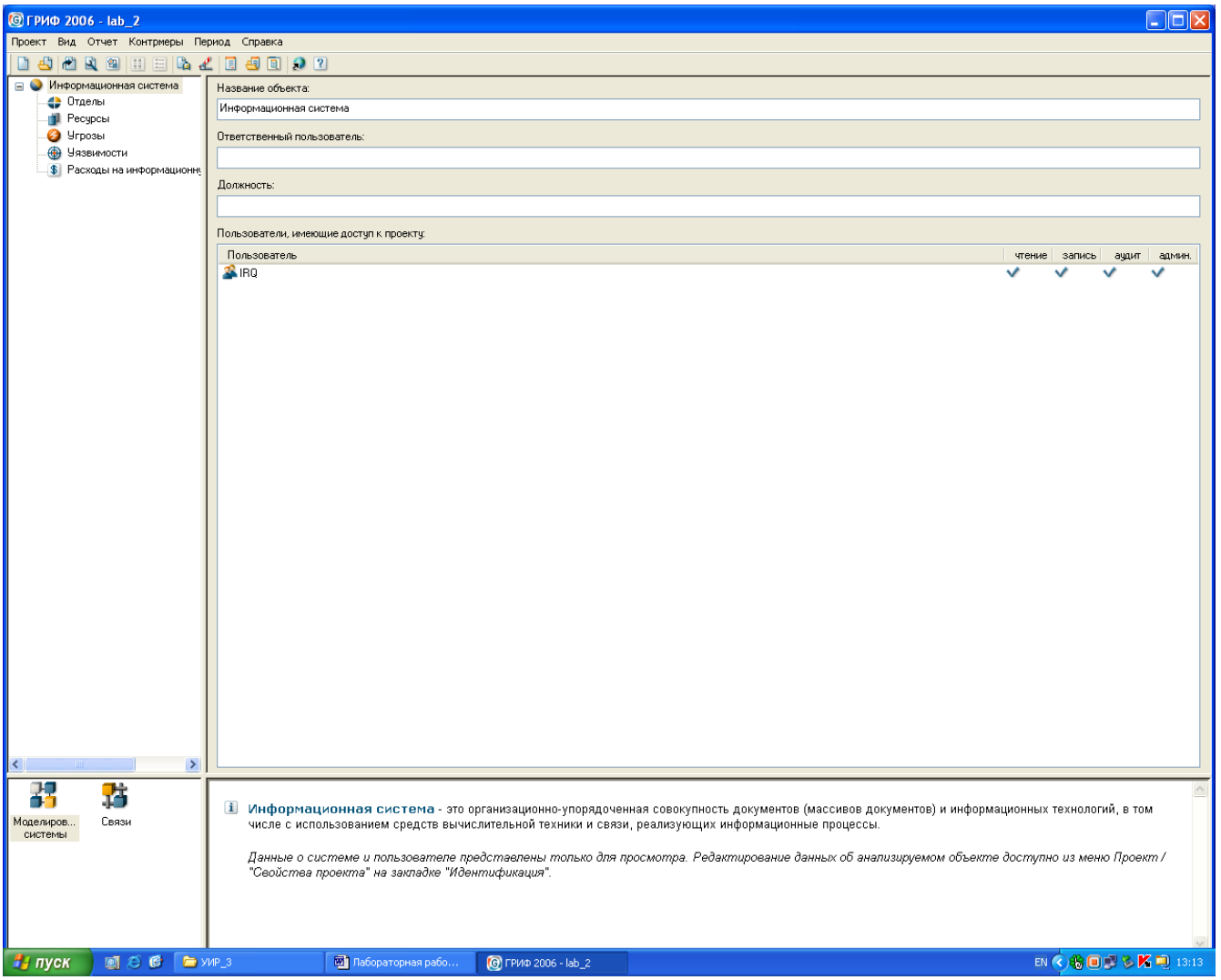

Рис.1.8. Вікно проекту

Встановлення властивостей проекту

У верхній панелі меню (рис.1.8) виберіть «Проект» - > «Свойства проекта».

У вкладках задайте/змініть властивості проекту проекта.

– **Ідентифікація**: тут можна задати назву об'єкта, відповідального користувача і його посаду.

– **Контроль доступу**: Змінить доступ до проекту для інших користувачів, наприклад, дозволити їм переглядати проект.

– **Рівні**: за замовчуванням встановлюється три рівні в шкалі (наприклад, критичності ресурсу). Можна змінити розбивку шкали (рис.1.9).

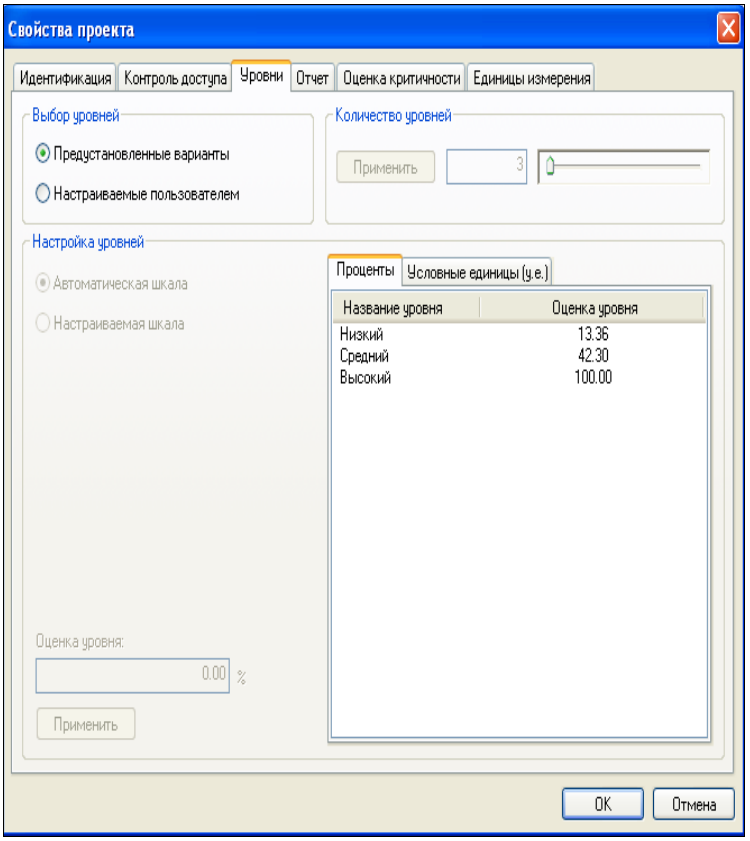

Рис.1.9. Властивості проекту

– **Звіт**: тут можна змінити склад і форму звіту. Рекомендується вибрати максимально повний звіт.

– **Оцінка критичності**: вибираємо оцінку критичності з прив'язкою до видів загроз.

– **Одиниці виміру**: тут можна вибрати одиниці виміру (відсотки або гроші).

Створення звітного періоду

На верхній панелі меню оберіть «Управление периодами» - > «Добавить» (рис.1.10).

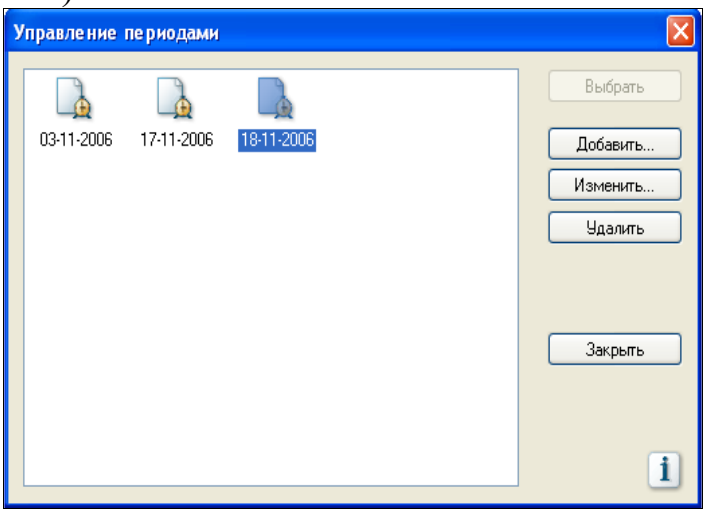

Рис.1.10. Створення звітного періоду

Моделювання системи

Змоделюйте систему філії банку за наступною схемою:

1.**Отдел**.

Для створення відділів зліва в списку виберете «Відділи» і справа натисніть «Додати».

Створіть наступні відділи (рис.1.11):

- Керівництво
- Відділ кадрів
- Бухгалтерія
- Відділ роботи з клієнтами.

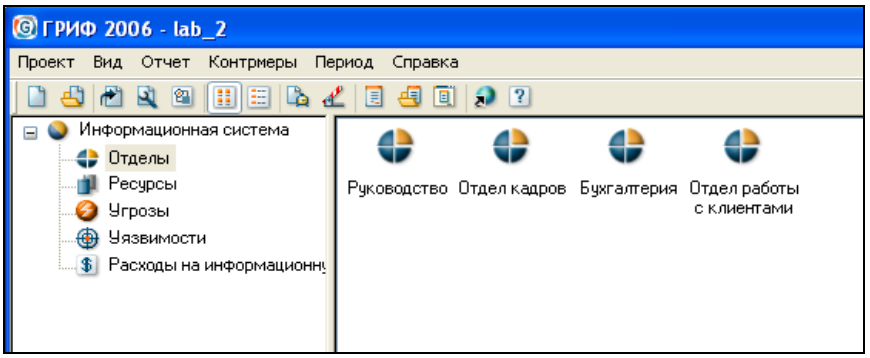

Рис.1.11. Отделы моделируемой системы

Ресурси

Для створення ресурсів перейдіть за списком нижче на «Ресурси» і справа натисніть «Додати».

Створіть наступні об'єкти із зазначенням типу ресурсів, відділу, до якого відноситься даний ресурс (табл.1.2). Критичність кожного ресурсу визначте на свій розсуд (рис.1.12).

Таблица 1.2. Ресурси системи, що моделюється.

Ресурс	Тип ресурсу	Відділ
ПК_Директор	Рабочая станция	Руководство
ПК_Админ_АБС	Рабочая станция	Руководство
ПК_Админ_ИБ	Рабочая станция	Руководство
ПК_начальник_отдела_кадров	Рабочая станция	Отдел кадров
Сервер_отдела_кадров	Сервер	Отдел кадров
ПК_бухгалтер	Рабочая станция	Бухгалтерия
Сервер_бухгалтерии	Сервер	Бухгалтерия
Сервер_клиентских_данных	Веб_сервер	Отдел работы с клиентами
ПК_1, ПК_2, ПК_3	Рабочая станция	Отдел работы с клиентами

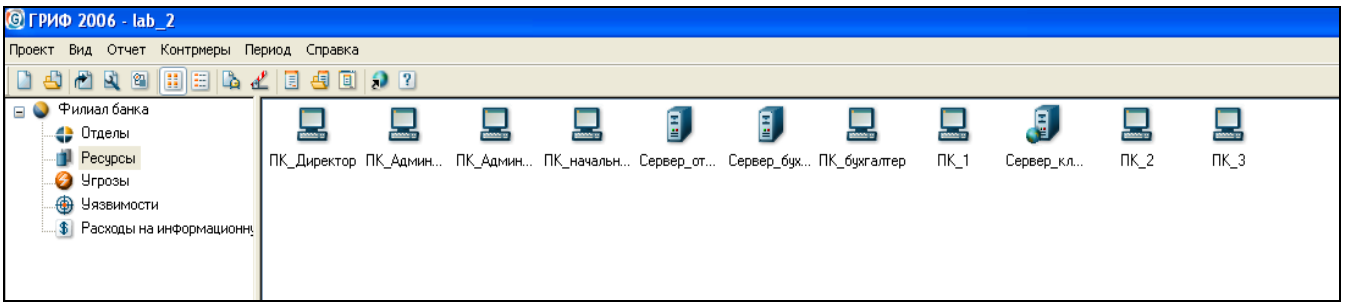

Рис.1.12. Ресурси системи, що моделюється.

Загрози

Для визначення загроз існуючих в системі виберете «Загрози» в списку ліворуч і натисніть «Додати» (рис.1.13).

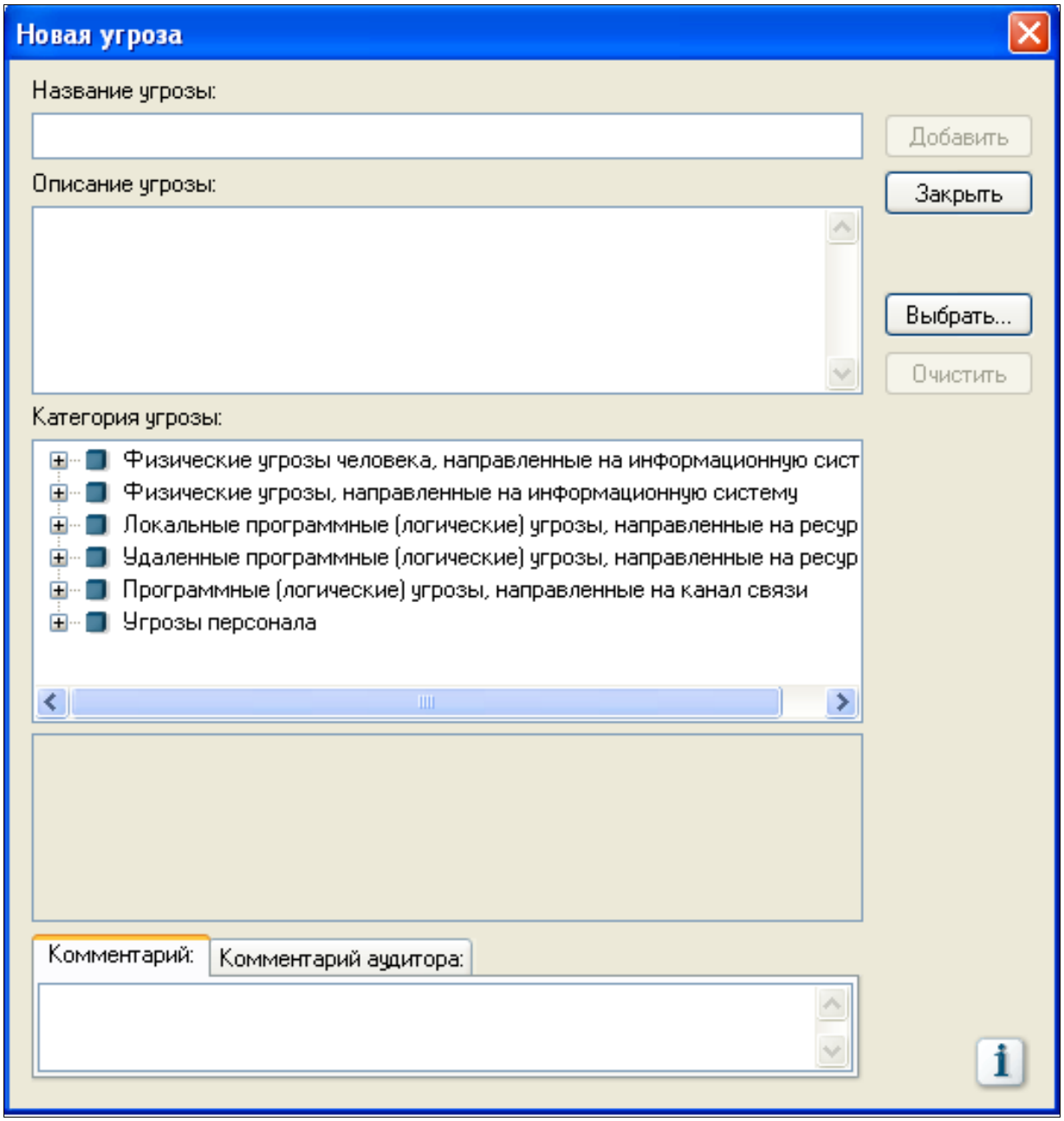

Рис.1.13. Вікно списку загроз, які визначені ПК «Гриф»

Натисніть «Вибрати». З'явиться список загрози відповідно до класифікації, прийнятої в компанії Digital Security. Виберете загрози, актуальні на вашу думку для змодельованої системи. Наприклад: виберіть «Фізичні загрози людини, спрямовані на інформаційну систему» -> «На ресурс» -> «Знищення або псування носіїв з цінною інформацією», задайте ім'я загрозу і натисніть «Додати». Визначте таким чином 10 загроз.

Також можна додати ті загрози, які є в системі, але немає в запропонованому списку загроз. Для цього вкажіть ім'я загрози і її опис. Наприклад (рис.1.14):

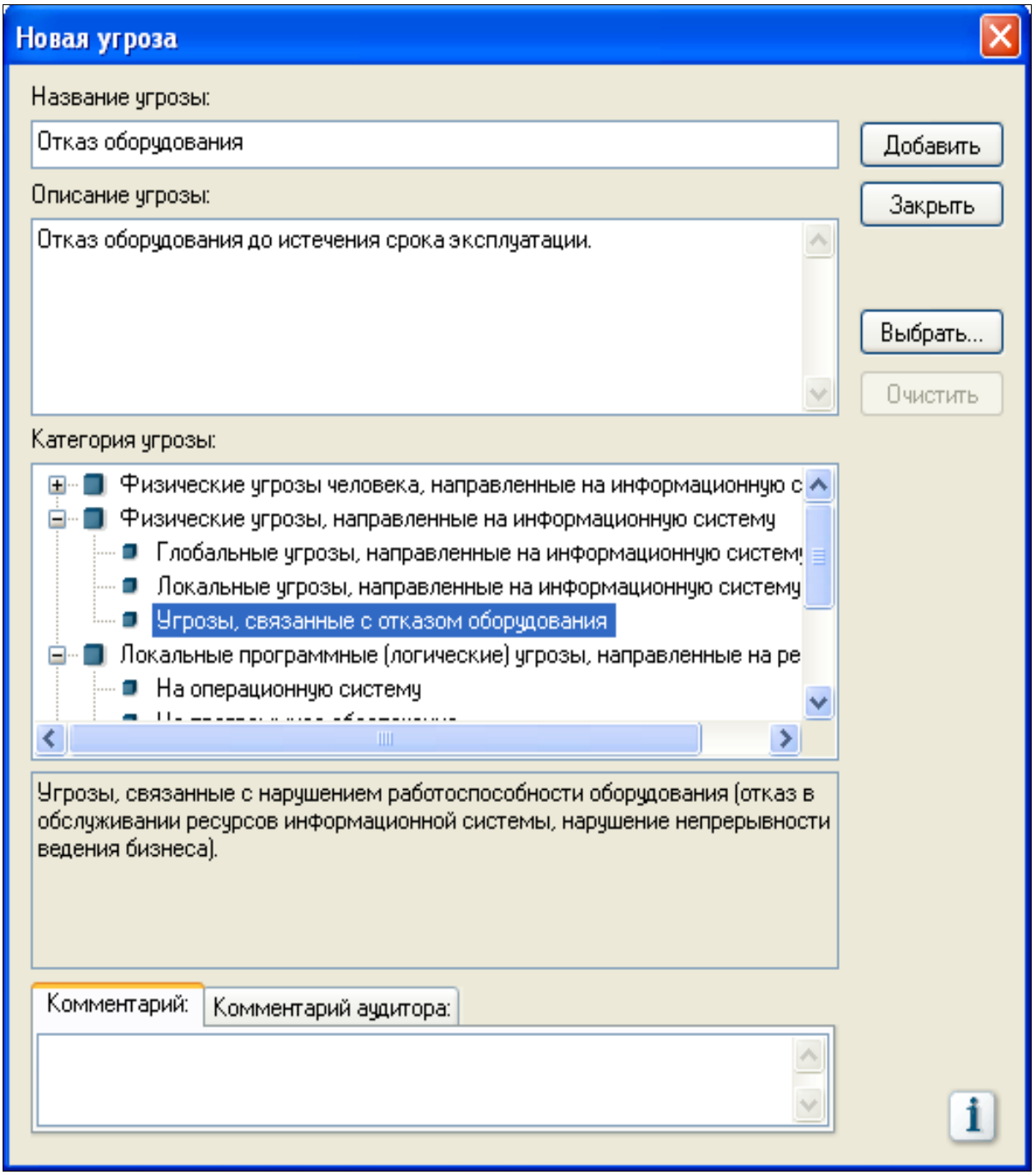

Рис.1.14. Додавання опису нової загрози

Уразливості

Для визначення вразливостей, існуючих в системі, виберете вкладку «Уразливості» і натисніть «Додати» (рiс.1.15). Відповідно до виявлених на попередньому етапі погрозами вкажіть уразливості, які можуть бути причиною реалізації цих загроз. Наприклад: «Фізичні загрози людини, спрямовані на інформаційну систему» -> «На ресурс» -> «Знищення або псування носіїв з цінною інформацією» -> «Відсутність контролю за персоналом, який обслуговує ресурси з цінною інформацією».

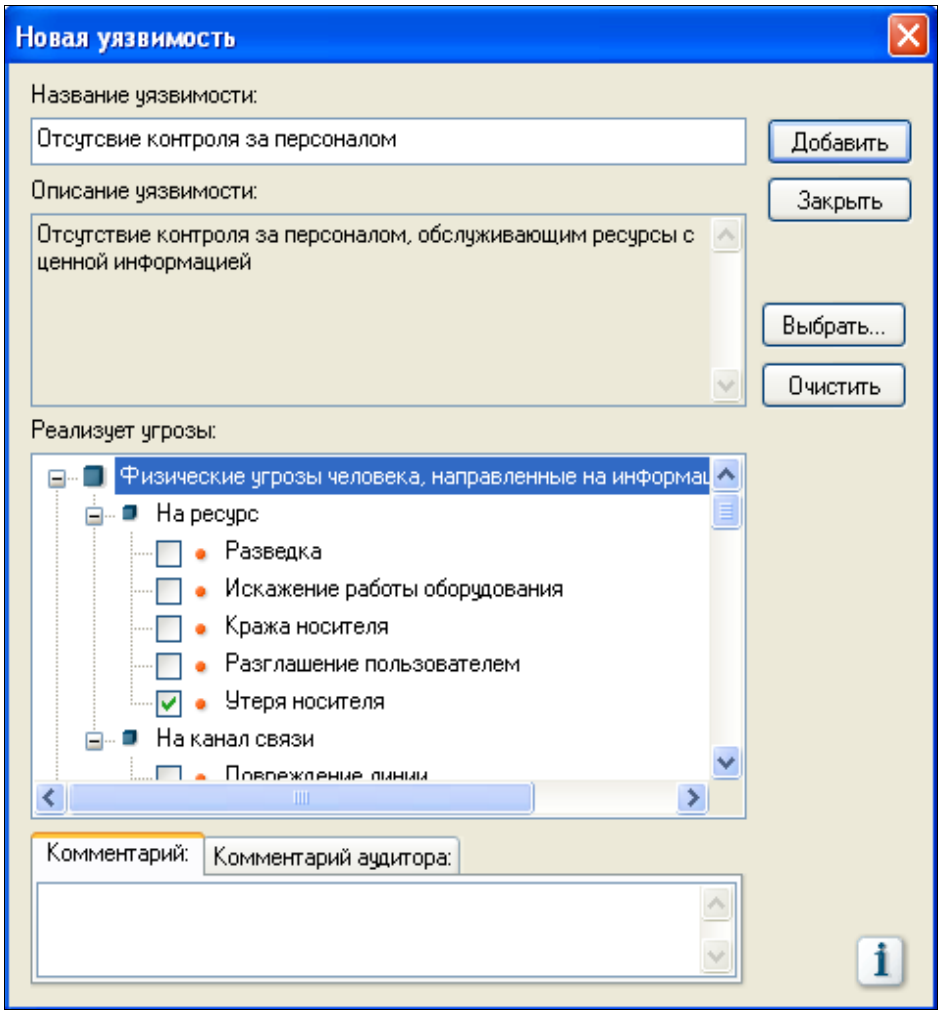

Рис.1.15. Вікно визначення вразливостей системи

Врахуйте, що одна уразливість може призводити до реалізації декількох видів загроз. Наприклад: відсутність в системі захищеного документообігу може привести до ненавмисного перекручування інформації і до ненавмисного її видалення.

Якщо необхідної уразливості немає в запропонованому списку, можна описати її самі таким же чином, як і загрозу.

Витрати на інформаційну безпеку

Заповніть самі.

Зв'язки

Для кожного ресурсу зв'яжіть загрози, виявлені для нього, з уразливими, породжують ці загрози.

У лівому нижньому кутку виберете «Зв'язки». Зліва ви побачите список відділів. Розгорніть відділ «Керівництво», виділіть лівою кнопкою миші перший об'єкт «ПК_Діректор». З'являться вкладки «Загрози» і «Уразливості» (рис.1.16):

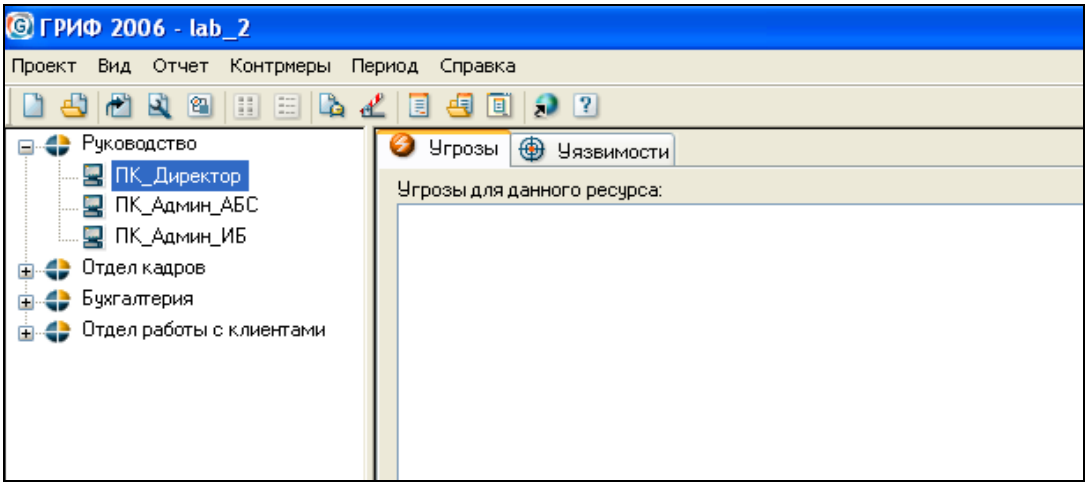

Рис.1.16. Визначення зв'язків між загрозами та уразливостями

Натисніть «Додати». З'явиться вікно зі списком загроз, які були визначені для модельованої системи. Виберіть із запропонованого списку ті загрози, які мають відношення до об'єкту «ПК_Діректор». Буде запропонований список вразливостей, що реалізують цю загрозу. Виберіть потрібну (потрібні), вкажіть ймовірність і критичність реалізації загрози (рис.1.17).

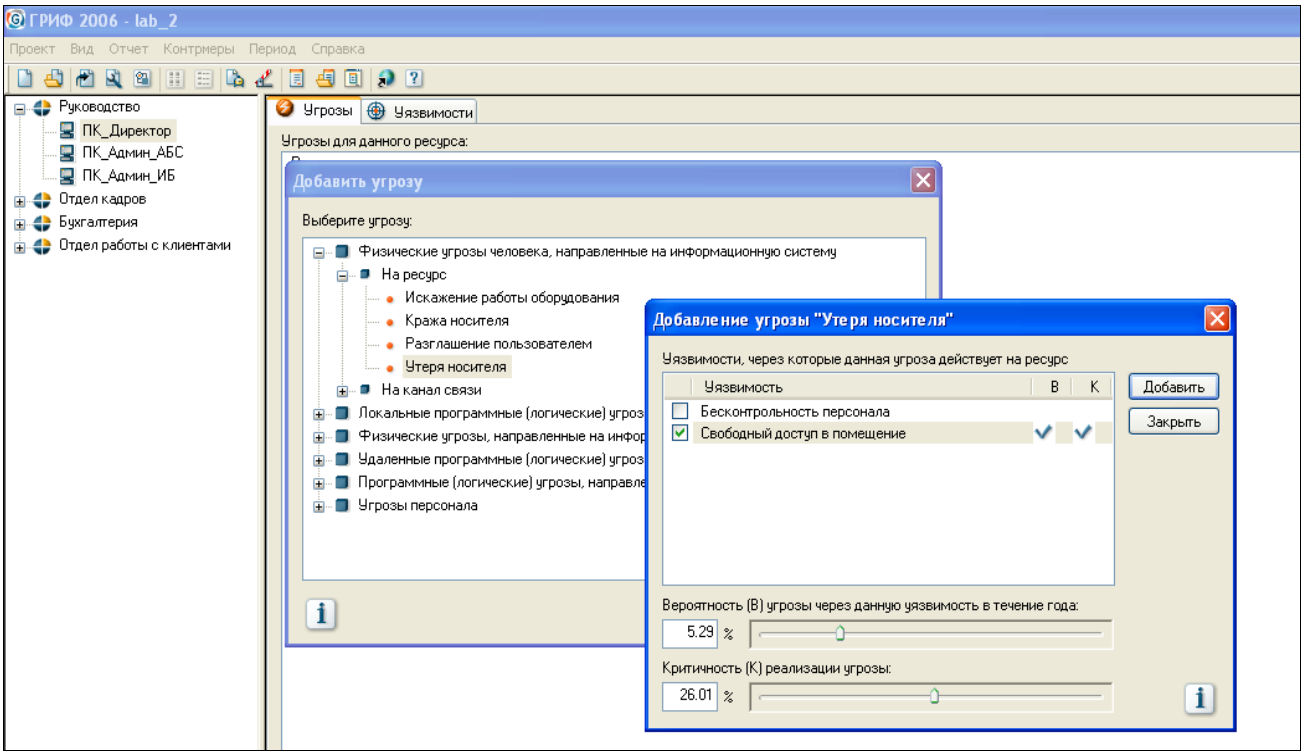

Рис.1.17. Зв'язок між загрозами і уразливістями

Таким чином зв'яжіть загрози і вразливості з ресурсами ІС. Для кожного об'єкта вийде список загроз і вразливостей.

Генерація звіту

На верхній панелі інструментів виберіть «Звіт» -> «Створити звіт» (рис.1.18). У вікні «Конфігурація звіту» виберете пункти, які ви хочете включити в звіт.

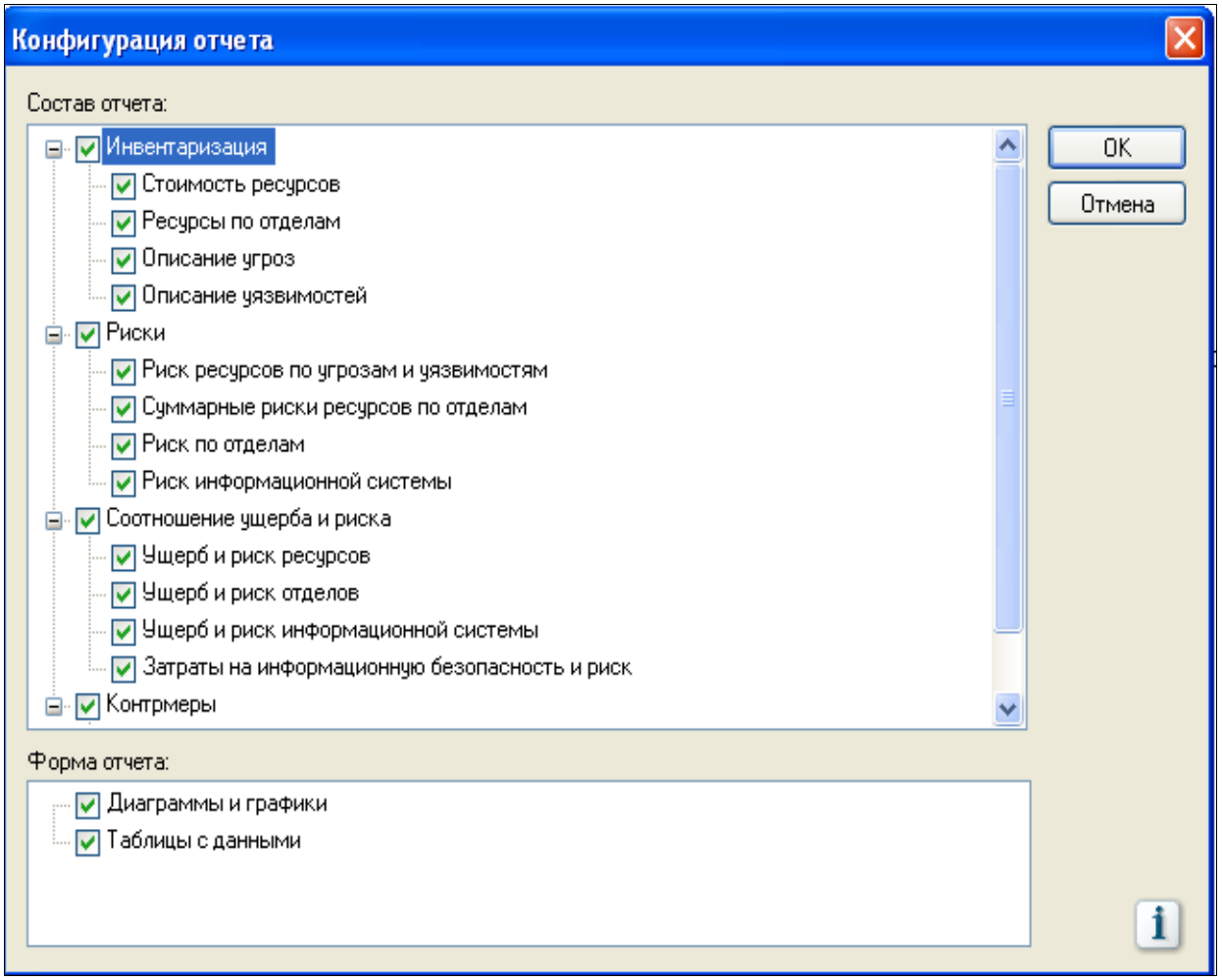

Рис.1.18. Генерація звіту

Ознайомтеся зі складом звіту:

Термінологія.

Умовні позначення.

1 **Інвентаризація**

1.1 Вартість ресурсів

1.2. Ресурси по відділах

1.3 Опис загроз (рис.1.19)

1.4 Опис вразливостей

1.3. Описания угроз

Имя	Описание
Разведка	Получение конфиденциальной информации без применения специальных средств (прослушивание, визуальное наблюдение)
Искажение работы оборудования	Порча или злонамеренное изменение режимов работы оборудования
Кража носителя	Кража носителей информации (бумажные носители, дискеты, компакт-диски, флэш-карты и т.д.)
Икажение БД	Неавторизованная модификация информации в базе данных, хранящейся на ресурсе
Отказ ПО	Отказ в обслуживании прикладного программного обеспечения
Отказ ОС	Отказ в обслуживании операционной системы
Дефект носителя	Дефектные носители данных
Пожар	Пожар
Перепады напряжения	Резкие колебания напряжения в электрической сети
Отключение эл-ва	Отказ внешних источников энергоснабжения
Повреждение линии	Повреждение кабелей
Разглашение пользователем	Разглашение, передача или утрата атрибутов разграничения доступа (идентификационных карточек, пропусков и т.д.)

Рис.1.19. Звіт: опис загроз

2 **Інформаційні ризики**

2.1 Ризик ресурсів з питань загроз і вразливостей

2.2 Сумарні ризики ресурсів по відділах

2.3 Ризик по відділах

2.4 Ризик інформаційної системи

3 **Співвідношення збитків і ризику**

3.1 Збиток та ризик ресурсів (рис.1.20)

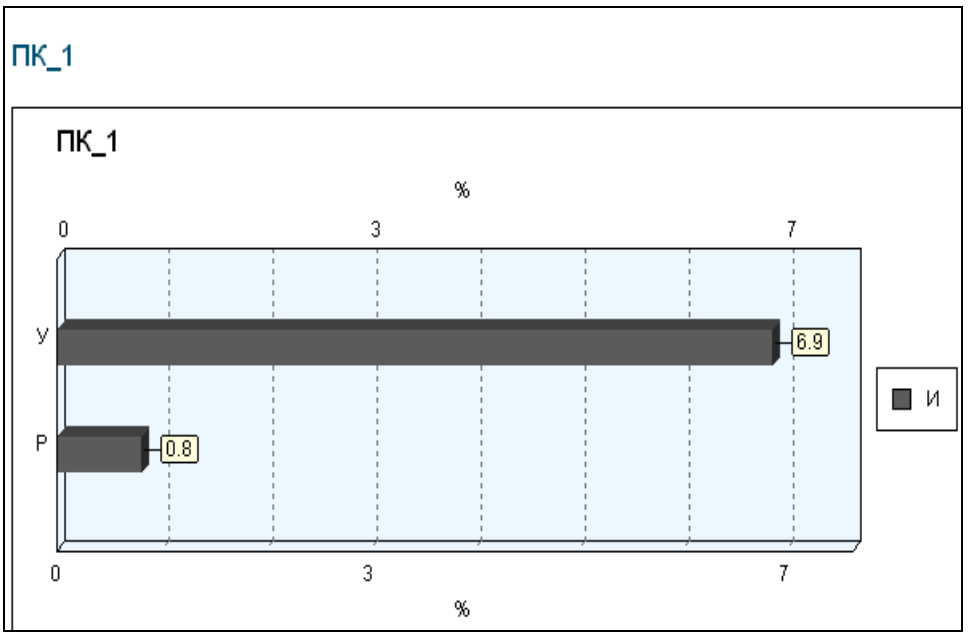

Рис.1.20. Збиток інформаційного ресурсу ПК_1

3.2 Збиток та ризик відділів

3.3 Збиток та ризик інформаційної системи

4 **Контрзаходи**

4.1 Контрзаходи по ресурсам

4.2 Ефективність комплексу контрзаходів

Керування ризиками інформаційної безпеки

Створіть новий звітний період

На верхній панелі інструментів виберете «Контрзаходи» -> «Управління ризиками» (рic1.21). Для кожного об'єкта представлений список вразливостей. Поточний рівень ризику визначає, ресурси з яким рівнем ризику вимагають контрзаходів. Наприклад, якщо виставити поточний рівень ризику 10%, то в списку об'єктів відобразяться тільки ті, ризик яких більше 10%, відповідно для них будуть запропоновані контрзаходи в правій частині вікна.

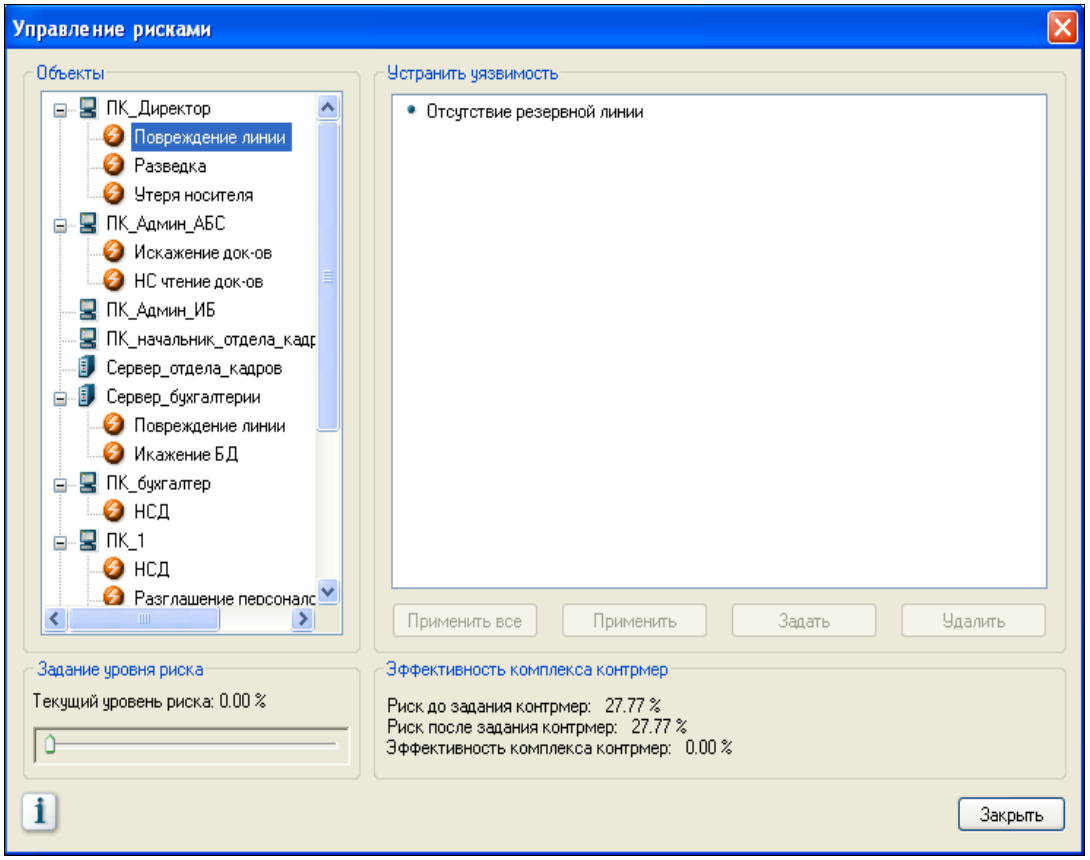

Рис.1.21. Управління ризиками

Виділіть вразливість і задайте контрзахід. Вкажіть назву контрзаходи для звіту, вартість її впровадження, можливе зниження витрат на ІБ. Наприклад (рис.1.22):

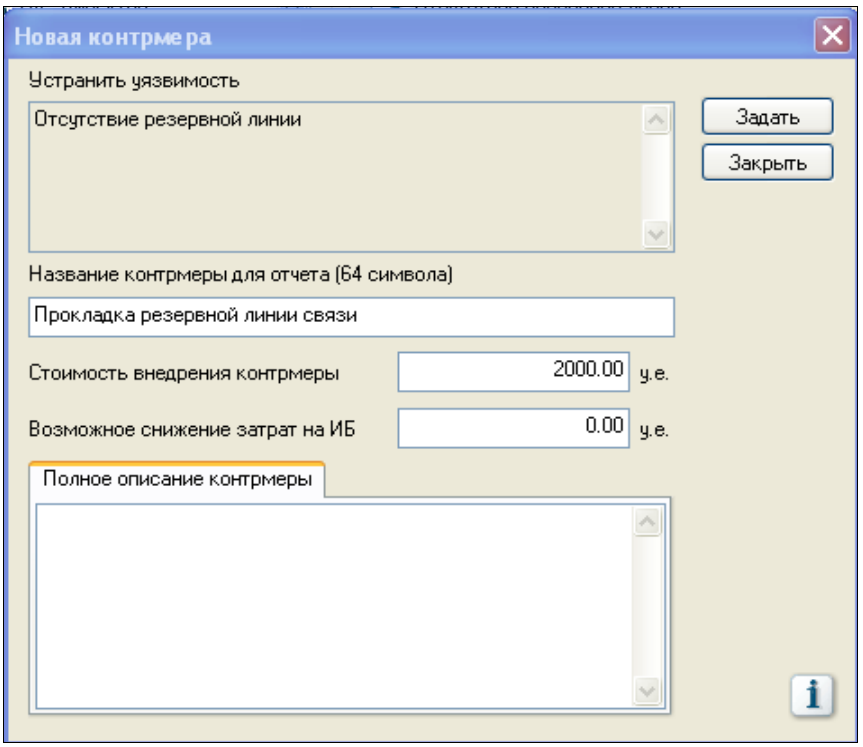

Рис.1.22. Завдання контрзаходів

Натисніть кнопку «Применить контрмеру». Ви побачите, що після застосування контрзаходів вразливість зникне зі списку. Задайте контрзаходи для декількох вразливостей.

Повторна генерація звіту та аналіз результату

Створіть звіт. Порівняйте з попереднім.

Дайте відповідь на **контрольні питання**

1. Які ресурси системи виявилися найбільш вразливими в системі? Чому?

2. Що змінилося в звіті після завдання контрзаходів?

3. Прокоментуйте рекомендації експертів в звіті. Для кількох пунктів поясніть їх доцільність.

4. Які рекомендації експертів вам здаються зайвими? Чому?

5. Як треба було спочатку побудувати систему, щоб вона відповідала вимогам по ІБ?

Підготуйте звіт за результатами роботи.

Практична робота № 6

Тема: Електронний документообіг. Створення цифрового підпису за допомогою формування пар відкритих та закритих ключів

Загальні відомості

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, які можуть бути реалізовані за допомогою обчислювальних засобів. Відомо більш десятка перевірених алгоритмів шифрування, які, при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу. Широко використовуються такі алгоритми шифрування як Twofish, IDEA, RC4, DEC, та ін.

У багатьох країнах прийняті національні стандарти шифрування. У 2001 році в США прийнятий стандарт симетричного шифрування AES на основі алгоритму Rijndael з довжиною ключа 128, 192 і 256 біт. Алгоритм AES прийшов на зміну колишньому алгоритмові DES, який тепер рекомендовано використовувати тільки в режимі Triple-DES (3DES).

Тривалий час під криптографією розумілось лише шифрування — процес перетворення звичайної інформації (відкритого тексту) в незрозумілий набір знаків (тобто, шифротекст). Дешифрування — це обернений процес відтворення інформації із шифротексту. Шифром називається пара алгоритмів шифрування/дешифрування. Дія шифру керується як алгоритмами, так і, в кожному випадку, ключем. Ключ — це секретний параметр (в ідеалі, відомий лише двом сторонам) для однозначного шифрування/дешифрування повідомлень. Ключі дуже важливі, оскільки без змінних ключів алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків.

До алгоритмів симетричного шифрування належать способи шифрування, в яких і відправник, і отримувач повідомлення мають однаковий ключ (або один ключ легко обчислюється з іншого). Ці алгоритми

шифрування були єдиними загально відомими до липня 1976.

На відміну від симетричних, асиметричні алгоритми шифрування використовують пару споріднених ключів — відкритий та секретний. При цьому, не зважаючи на пов'язаність відкритого та секретного ключа в парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим.

У сучасному світі системи електронного документообігу розвинені дуже широко. Великі корпорації, державні установи та організації, урядові системи керування діяльністю – важливою частиною цих систем є електронний обмін документами. Питання збереження таємниці, захист інформації, що міститься в документах, одне з найперших, що вирішує спеціаліст з управління інформаційною безпекою. Розглянемо одну з простих програм, яка добре ілюструє принцип роботи електронно-цифрового підпису.

PGP (англ. Pretty Good Privacy) — комп'ютерна програма, що дозволяє виконувати операції шифрування (кодування) і цифрового підпису повідомлень, файлів і іншої інформації, представленої в електронному вигляді. ЇЇ першу версію розробив Філіп Циммерман у 1991 році.

PGP має безліч реалізацій, сумісних між собою і рядом інших програм (GNUPG, Filecrypt і ін.) завдяки стандарту OPENPGP (RFC 4880), які мають різний набір функціональних можливостей. Існують реалізації PGP для всіх найпоширеніших операційних систем. Окрім вільно поширюваних, є комерційні реалізації.

Користувач PGP створює ключову пару: відкритий і закритий ключ. При генерації ключів задаються їх власник (ім'я і адреса електронної пошти), тип ключа, довжина ключа і термін його дії. PGP підтримує три типи ключів RSA v4, RSA legacy (v3) і Diffiehellman / dss (Elgamal в термінології GNUPG).

Для ключів RSA legacy довжина ключа може складати від 1024 до 2048 біт, а для Diffie-hellman/dss і RS A — від 1024 до 4096. Ключі RSA legacy містять одну ключову пару, а ключі Diffie-hellman/dss і RSA можуть містити один головний ключ і додаткові ключі для шифрування. При цьому ключ електронного підпису в ключах Diffie-hellman/dss завжди має розмір 1024.

Термін дії для кожного з типів ключів може бути визначений як необмежений або до конкретної дати. Для захисту ключового контейнера використовується секретна фраза. Ключі RSA legacy (v3) для шифрування зараз не використовуються і виведені із стандарту OPENPGP.

Електронний цифровий підпис формується шляхом підпису дайджеста (хеш-значення) повідомлення (файлу) закритим ключем відправника (автора). Для формування дайджеста можуть використовуватися алгоритми Md5, Sha-1, Ripemd-160, Sha-256, Sha-384, Sha-512. У нових версіях PGP підтримка Md5 здійснюється для збереження сумісності з ранніми версіями. Для підпису використовуються алгоритми RSA або DSA (залежно від типу ключа).

Шифрування здійснюється з використанням одного з п'яти симетричних алгоритмів (AES, Cast5, TRIPLEDES, IDEA, Twofish) на сеансовому ключі. Сеансовий ключ генерується з використанням криптографічного стійкого генератора псевдовипадкових чисел. Сеансовий ключ зашифровується відкритим ключем одержувача з використанням алгоритмів RSA або Elgamal (залежно від типу ключа одержувача).

Для отримання практичних навичок шифрування інформації використаємо саме програму PGP, головна перевага якої – простота використання.

Підготовчий етап заняття. Актуалізація знань

Віднайдіть ваш файл з особистим офіційним документом та скопіюйте його в буфер обміну.

Створіть нову папку для організації криптографічного захисту та вставте в неї скопійований файл.

Для генерації та використання ключів встановіть програму PGP 8.0 (для ОС до Windows XP) чи PDP Desktop 10 (для Windows 7).

Створення пари відкритого і закритого ключів для шифрування повідомлень

Для завантаження програми генерації ключів віднайдіть та виберіть у меню **Пуск** операційної системи в групі **PGP** посилання **PGPkeys** для Windows XP (чи **PGP Desktop** для Windows 7).

З метою створення власної пари відкритого і закритого ключів оберіть в меню **Keys** для Windows XP (рис. 1) чи в меню **File** для Windows 7 (після активації розділу **PGP Keys** (рис. 2)) пункт **New key**.

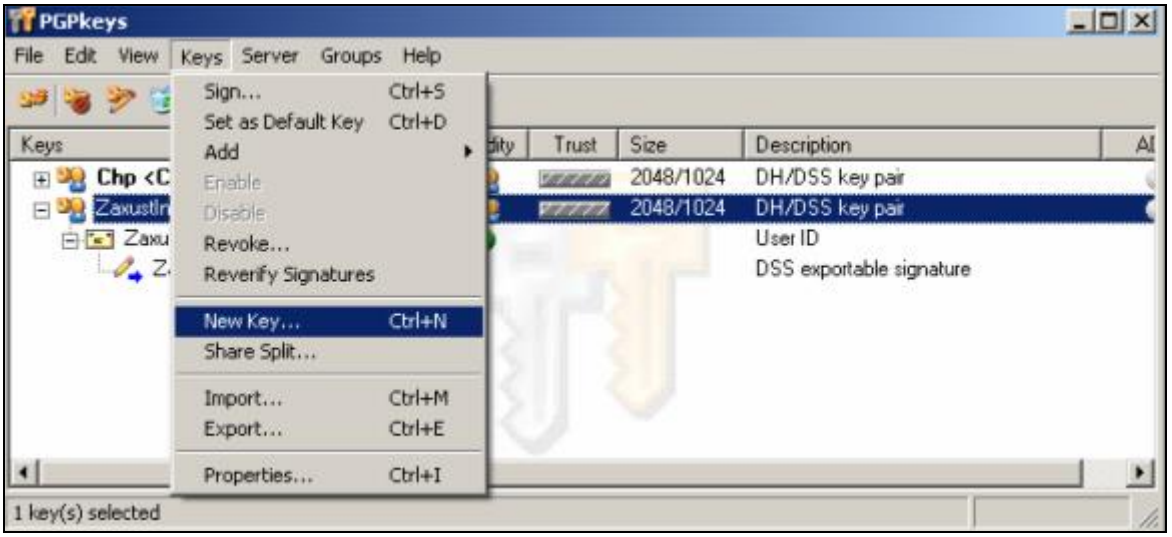

Рис. 1. Меню **Keys** програми адміністрування ключів **PGPkeys**

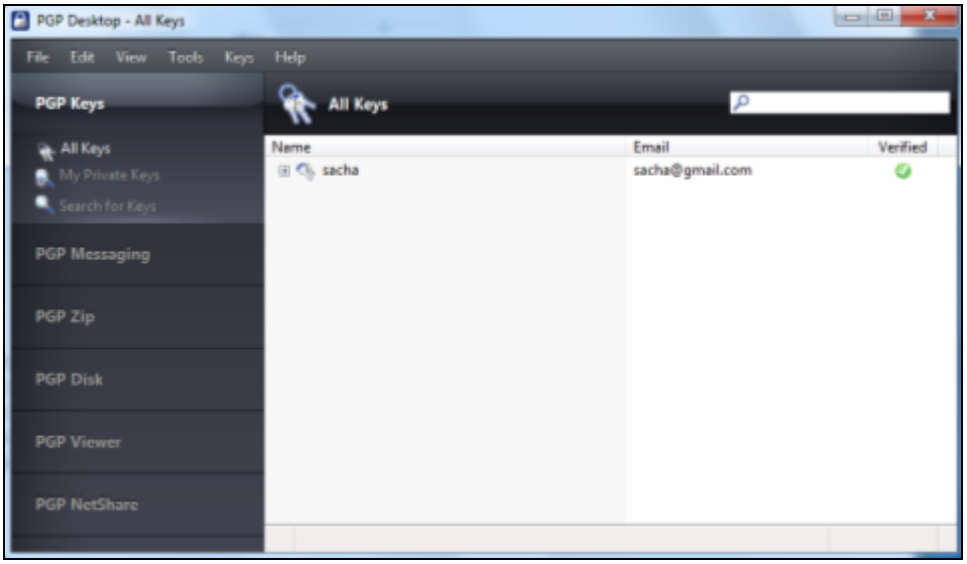

Рис. 2. Розділ **PGP Keys** програми **PGP Desktop**

На першому кроці майстра створення ключів введіть латинськими літерами своє прізвище, ім’я та адресу електронної пошти (рис. 3).

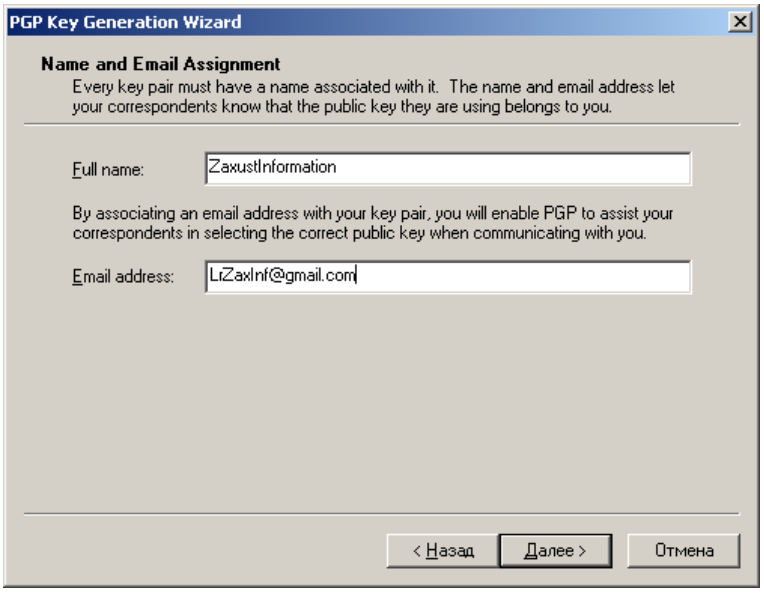

Рис. 3. Вікно першого кроку майстра створення нової пари ключів

Для забезпечення використання пари ключів лише вами на другому кроці цього майстра латинськими літерами вкажіть та підтвердіть ключову фразу, знявши попередньо прапорець **Hide Typing** (рис. 4).

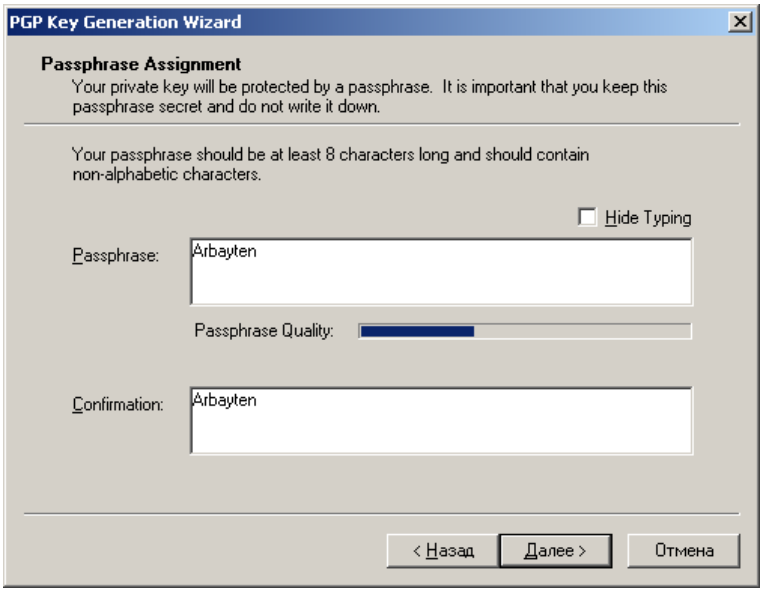

Рис. 4. Вікно другого кроку майстра створення нової пари ключів

Самостійно завершіть створення нової пари ключів.

Віднайдіть в головному меню програми чи в контекстному меню ключа можливості вибору ключа по замовчуванню та активації/деактивації ключа.

Використання пари відкритого і закритого ключів для передачі зашифрованих повідомлень

Використовуючи пункт головного меню програми **Keys** – **Export** (рис. 1) чи **File** – **Export** (рис. 2), створіть файл з вашим відкритим ключем. Перешліть його електронною поштою двом обраним вашим одногрупникам.

З метою організації передачі зашифрованих повідомлень вашим

одногрупникам перенесіть з отриманих вами листів їх відкриті ключі у вашу папку для організації криптографічного захисту.

Використовуючи пункт головного меню програми **Keys** – **Import** (рис. 1) чи **File** – **Import** (рис. 2), перенесіть відкриті ключі одногрупників в програму адміністрування ключів.

Для передачі зашифрованих повідомлень одногрупникам, **які надіслали вам свої відкриті ключі**, віднайдіть та виберіть у меню **Пуск** операційної системи посилання **PGPmail** чи активізуйте розділ **PGP Zip** у програмі **PGP Desktop** (рис. 5).

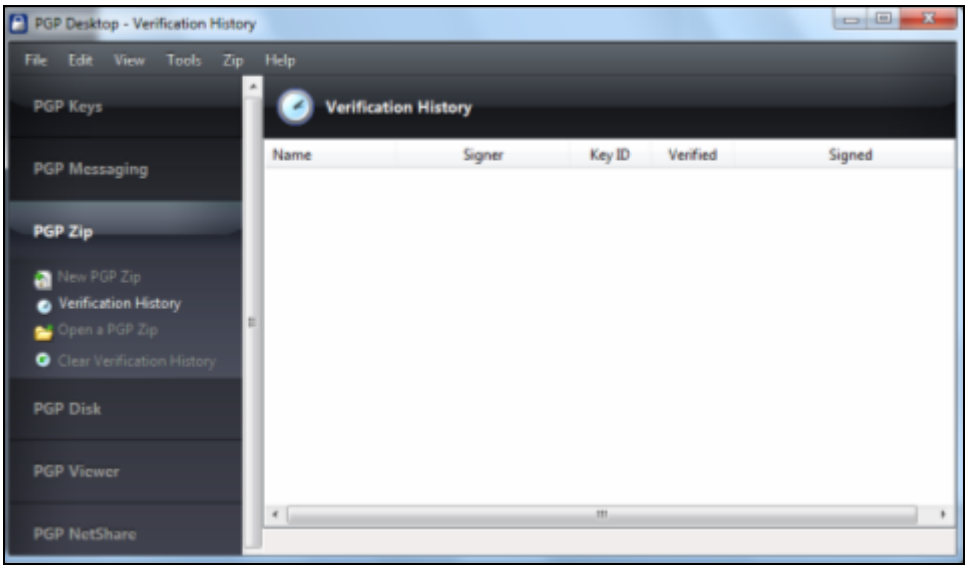

Рис. 5. Розділ **PGP Zip** програми **PGP Desktop**

Для створення зашифрованого файла з вашим особистим офіційним документом кожному з вибраних одногрупників послідовно декілька разів виконайте такі дії:

1.1. В ОС Windows XP натисніть на панелі інструментів програми **PGPmail** (рис. 6) другу кнопку зліва чи в ОС Windows 7 оберіть посилання **New PGP Zip** (рис. 5);

Рис. 6. Панель елементів програми шифрування/розшифровування **PGPmail**

1.2. На першому кроці завантаженого майстра оберіть файл для шифрування;

1.3. На другому кроці майстра у вікні вибору ключів шифрування **оберіть відкритий ключ одногрупника, якому бажаєте передати**

повідомлення (рис. 7);

1.4. На наступних кроках майстра введіть назву для зашифрованого файла та самостійно завершіть його створення.

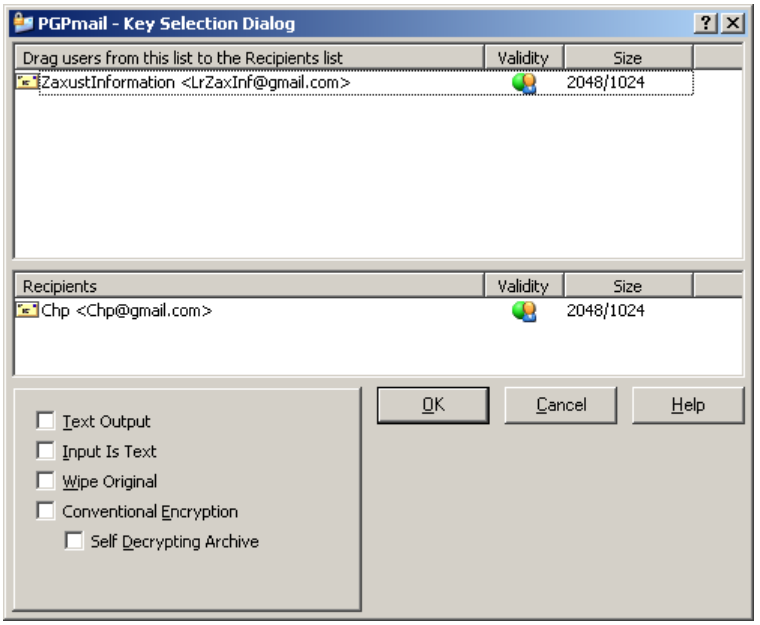

Рис. 7. Вікно вибору ключів шифрування програми **PGPmail**

Перешліть електронною поштою зашифровані файли двом обраним вашим одногрупникам, відповідними **відкритими ключами яких ви користувалися для шифрування**.

Після отримання від одногрупників файлів, **зашифрованих вашим ключем**, розшифруйте їх, натиснувши в ОС Windows XP на панелі інструментів програми **PGPmail** (рис. 5) п'яту кнопку зліва чи в ОС Windows 7 оберіть в програмі PGP Desktop (рис. 5) посилання **Open a PGP Zip** або аналогічний пункт – у контекстному меню зашифрованого файла.

Теоретичні питання:

1. Чому для шифрування даних на сьогодні крім обраних алгоритмів найчастіше використовуються ключі?
2. Які алгоритми шифрування називаються симетричними, а які – асиметричними, які відкритими, а які – закритими?
3. Яке призначення відкритих ключів?
4. Де і навіщо зберігаються закриті ключі?
5. Як і навіщо використовується ключова фраза, задана при формуванні ключа?

6. Що необхідно встановити і отримати на комп’ютері для стандартизованої передачі зашифрованих повідомлень?
7. Чому розмір зашифрованих файлів може бути меншим від вхідного файла?

Практичне завдання:

1. Самостійно створіть привітання одногрупнику з нагоди приходу осені, зашифруйте та надішліть його адресату електронною поштою. Розшифруйте надіслані вам привітання.
2. Створіть електронний лист з формулюваннями та відповідями на контрольні запитання у своїй поштовій скриньці. Приєднайте до цього листа архів з наявних у вас відкритих ключів та довільний отриманий зашифрований і відповідний розшифрований документ. Тему листа сформуйте за шаблоном *<група>_PGP_<прізвище ім’я>*, наприклад: *ТЕХ31_PGP_Величко Володимир*. Надішліть створений лист на адресу min_max@i.ua.
3. Оформіть результати роботи у звіті.

Практична робота № 7

Тема: Оцінка ризиків інформаційної безпеки згідно стандарту ISO/IEC 27001:2013

Загальні відомості

У вересні 2013 року було опубліковано нову версію стандарту ISO/IEC 27001:2005, це - ISO/IEC 27001:2013 – Інформаційні технології – Метеди безпеки – Системи менеджменту інформаційної безпеки – Вимоги. А також разом із основним стандартом було створено ще один - ISO/IEC 27002:2013 – Інформаційцні технології – Методи бузпеки – Зведення практик для керування інформаційною безпекою.

Ознайомитись зі змістом стандартів можна за такими посиланнями:

http://www.pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf

http://www.amu.kz/inf-bezopasnost/ISO27001.pdf

http://www.almaz-art.com/docs/dstuISO_IEC27001_2015u.pdf

Через великий об’єм зміст стандартів не наводиться.

Теоретичні питання:

1. Які саме забов’язання відносно системи інформаційної безпеки має керівництво компанії, відповідно стандарту ISO/IEC 27001:2013?
2. Які характеристики повинна мати політика інформаційної безпеки?
3. Перелічіть основні етапи процеса оцінювання ризиків інформаційної безпеки?
4. Що є цілями інформаційної безпеки?
5. Що, згідно стандартів, розуміють під поняттями "обізнаність" та "комунікація"?
6. Як повинен проводитись контроль документованої інформації?
7. Які етапи включає в себе внутрішній аудит?
8. Яким чином згідно стандарту організація повинна реагувати на невідповідності й які корегувальні дії проводити?

Практичне завдання:

Детально ознайомитись зі змістом стандартів ISO/IEC 27001:2005 та ISO/IEC 27001:2013. Виконати порівняльний аналіз версій 2005 та 2013 років. Результати аналізу викласти у вигляді таблиці у звіті до практичної роботи.

Список рекомендованої літератури

Основна

1. Нечаев В. И Элементы криптографии М.: Высшая школа, 1999.
2. Ященко В.В. Введение в криптографию М.: МЦНМО—ЧеРо, 2000
3. Шапошников И.В Web- сервисы Microsoft .Net СПб.: БХВ-Петербург, 2002.-336 с
4. Кормич В.А. Інформаційна безпека: організаційно-правові основи: Навчальний посібник./МОН.-К.:Кондор, 2008.-283с.
5. Юдін О.І., Корченко О.Г., Конахович Г.Ф., Захист інформації в мережах передачі даних – К.: Вид-во ТОВ "НВП"Інтерсервіс", 2009.-716с.

Допоміжна

1. Хенлі Ернест Джон, Кумамото Хиромицу Надійнісне проектування технічних систем і оцінка ризику./ пер. з англ. О.Ю.Зареніна, В.Ф. Хмеля; під ред. Ю.Г.Зареніна.-К.: Вища школа, 1987.-544 с.

Інформаційні ресурси

1. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657
2. http://www.dut.edu.ua/uploads/l_1359_89216009.pdf

Методичне видання

МЕТОДИЧНІ ВКАЗІВКИ
ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ
З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
“Основи управління кібербезпекою”

для студентів денної та заочної форми навчання
за напрямом підготовки
освітнього ступеню "Бакалавр",
за спеціальністю 125 “Кібербезпека”

Видання оновлене та доповнене

Укладач
Лисенко Ірина Анатоліївна