УДК 35.078.3

Гордієнко С.Б., к.т.н.; **Микитенко О.С.; Данильчук В.Г.**
(Державний університет інформаційно-комунікаційних технологій)

МЕТОДИ ТА РЕКОМЕНДАЦІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОНСАЛТИНГОВОЇ КОМПАНІЇ

Гордієнко С.Б., Микитенко О.С., Данильчук В.Г. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії. В роботі проведено аналіз діяльності консалтингової компанії по забезпечення інформаційної безпеки, визначено методи її забезпечення від зовнішніх і внутрішніх загроз та надано рекомендації по їх попередженню.

Ключові слова: КОНСАЛТИНГОВА КОМПАНІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ШИФРУВАННЯ

Гордиенко С.Б., Микитенко О.С., Данильчук В.Г. Методы и рекомендации обеспечения информационной безопасности консалтинговой компании. В работе проведен анализ деятельности консалтинговой компании по обеспечению информационной безопасности, определены методы её обеспечения от внешнихи внутренних угроз и предоставлены рекомендации по их предупреждению.

Ключевые слова: КОНСАЛТИНГОВАЯ КОМПАНИЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ШИФРАЦИЯ

Hordienko S.B., Mykytenko O.S., Danyl'chuk V.H. Methods and recommendations of providing of informative safety of consulting company. The analysis of activity of consulting company is in-process conducted for providing of informative safety, the methods of her providing are certain, both from external and from internal threats and recommendations are given on their warning.

Keywords: CONSULTING COMPANY, INFORMATIVE SAFETY, ENCIPHERING

Вступ. Консалтингова діяльність компанії передбачає аналіз, обґрунтування перспектив розвитку і використання науково-технічних та організаційно-економічних інновацій з урахуванням предметної області і проблем клієнта. Це важливий суб'єкт інформаційної діяльності, від рівня захисту інформації якого залежить добробут компанії.

Постановка проблеми. Підприємницька діяльність, що здійснюється в компанії, пов'язана з одержанням і використанням різного роду інформації (економічна, юридична, інтелектуальна), оскільки без необхідного обсягу та якості інформації неможливо забезпечити розвиток суб'єкта господарювання. В сучасних умовах розвитку ринкових відносин в консалтинговій сфері інформація є особливого роду товаром, що має велику цінність. Як товар інформація може користуватися попитом, однак тут присутня специфіка, пов'язана з перетворенням людських знань в товар, що створює складності у визначенні її вартості. Важливим аспектом забезпечення безпеки інформації на підприємстві є вчасний та швидкий обмін даними щодо надання послуг, а також відповідей на запити клієнтів.

Сучасні інформаційні технології дають змогу підприємству пришвидшити процес обміну та співпраці в компанії та реалізовувати власні інтереси. Неефективне використання даних може послабити або завдати значної шкоди безпеці підприємства, яке не має дієвої системи захисту від негативних інформаційних впливів.

Від обсягу, швидкості та якості обробки інформації значною мірою залежить ефективність управлінських рішень, зростає значення методів управління (з використанням інформаційних технологій) соціальними та економічними процесами, фінансовими і товарними потоками, аналізу та прогнозування розвитку внутрішнього і зовнішніх ринків.

За умов високого рівня конкуренції серед українських консалтингових компаній інформація є головною ареною зіткнень і боротьби і має обмежений інформаційний простір. В даний час для захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає в себе комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.). Таким чином, інформаційна безпека є невід'ємною складовою ефективної діяльності підприємства і потребую досконалого вивчення та аналізу.

Мета та завдання. Основною метою даного дослідження є розкриття цілей та завдань забезпечення інформаційної безпеки в сфері надання консалтингових послуг.

Завдання роботи полягає у визначенні сутності та рівня безпеки на підприємстві, дослідженні ризиків, а також у формуванні рекомендацій щодо підвищення рівня інформаційної безпеки і методів усунення недоліків.

Викладення основного матеріалу. Інформаційна безпека підприємства – це стан захищеності інформації, якою володіє підприємство (виробляє, передає або отримує), щодо несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Крім того, під інформаційною безпекою розуміють захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку її власникам або підтримуючій інфраструктурі.

Прикладом є випадкове видалення важливого документу співробітником при необмеженому доступі до інформації, що впливає на результат роботи менеджерів з продажу та інших відділів компанії. В цьому випадку відновлення інформації, що знаходилась в локальній мережі, займає достатню кількість часу або не відновлюється взагалі.

Як комплекс заходів, інформаційна безпека надає нам наступні фактори [1]: *конфіденційність* – властивість, яка гарантує, що інформація недоступна і не може бути розкрита несанкціонованими особами, об'єктами чи процесами (можливість ознайомитись з інформацією мають лише ті особи, які володіють відповідними повноваженнями); *цілісність* – властивість, яка гарантує, що система повноцінно виконує свої функції без навмисних чи випадкових несанкціонованих втручань (можливість внести зміни в інформацію повинні мати лише ті особи, які на це вповноважені); *доступність* – можливість отримання авторизованого доступу до інформації з боку вповноважених осіб в відповідний санкціонований для роботи період часу.

Сутність загроз інформаційної безпеки зводиться, як правило, до нанесення того чи іншого збитку організації. Прояви можливого збитку можуть бути: *моральна* і матеріальна шкода діловій репутації організації; *моральний,* фізичний чи матеріальний збиток, пов'язаний з розголошенням персональних даних окремих осіб; *матеріальний* (фінансовий) збиток від розголошення конфіденційної інформації; *фінансовий* збиток від необхідності відновлення порушених інформаційних ресурсів, які захищаються; *матеріальні* збитки (втрати) від неможливості виконання взятих на себе зобов'язань перед третьою стороною; *моральний* і матеріальний збиток від дезорганізації в роботі всього підприємства.

Джерела зовнішніх загроз можуть бути випадковими і запланованими та мати різний рівень кваліфікації. До них відносяться: *кримінальні* структури; *потенційні* злочинці і хакери; *нечесні* партнери; *технічний* персонал постачальників послуг тощо [2].

Внутрішні суб'єкти (джерела), знайомі зі специфікою розв'язуваних завдань, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного устаткування і технічних засобів мережі. До них відносяться: *основний* персонал (користувачі, програмісти); *допоміжний* персонал (прибиральники); *технічний* персонал.

Джерелами потенційних загроз безпеці інформації можуть бути і технічні засоби: *зовнішні* (засоби зв'язку, мережі інженерних комунікації, транспорт) і *внутрішні* (неякісні технічні засоби обробки інформації; неякісні програмні засоби обробки інформації; допоміжні технічні засоби – охорони, сигналізації, телефонії; інші технічні засоби, що застосовуються в установі).

Відповідно, дії, які можуть завдати шкоди інформаційній безпеці організації, можна також розділити на кілька категорій:

1. Дії, які здійснюються авторизованими користувачами. У цю категорію потрапляють: *цілеспрямована* крадіжка або знищення даних на робочій станції або сервері; *пошкодження* даних користувачів у результаті необережних дій.

2. Електронні методи впливу, які здійснюються хакерами. До таких методів відносяться: несанкціоноване проникнення в комп'ютерні мережі, DOS-атаки.

3. Комп'ютерні вірусита інші шкідливі програми. Це окрема категорія електронних методів впливу. Проникнення вірусу на вузли корпоративної мережі може призвести до

порушення їх функціонування, втрат робочого часу, втрати даних, викраденні конфіденційної інформації і навіть прямим розкраданням фінансових коштів. Вірусна програма, яка проникла в корпоративну мережу, може надати зловмисникам частковий або повний контроль над діяльністю компанії. Наприклад: при користуванні програмою Skype співробітнику надсилають посилання на сторонній ресурс. При "кліку" на цей ресурс на комп'ютер потрапляє вірус, що є загрозою для інших комп'ютерів локальної мережі, а також є небезпекою цілісності даних и паролів.

Таким чином, в сучасних умовах наявність розвиненої системи інформаційної безпеки стає однією з найважливіших умов конкурентоспроможності і життєздатності компанії.

Методи забезпечення інформаційної безпеки в компанії. Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні "знати" про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

На сьогоднішній день існує великий арсенал методів забезпечення інформаційної безпеки: *засоби* ідентифікації і аутентифікації користувачів (так званий комплекс ЗА); *засоби* шифрування інформації; *віртуальні* приватні мережі; *засоби* антивірусного захисту та інші.

Методи попередження основних загроз безпеці інформації в компанії:

1) Аутентифікація (або ідентифікація), авторизація і адміністрування. Ідентифікація та авторизація – це ключові елементи інформаційної безпеки. При спробі доступу до інформаційних активів функція ідентифікації дає відповідь на питання: чи ви є авторизованим користувачем мережі. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ [3].

2) Системи шифрування дозволяють мінімізувати втрати у випадку несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії. Завдання даного засобу захисту – забезпечення конфіденційності.

3) Говорячи про криптографію, слід згадати про захищені віртуальні приватні мережі (Virtual Private Network ─ VPN). Їх використання дозволяє вирішити проблеми конфіденційності і цілісності даних при їх передачі по відкритим комунікаційних каналам.

Використання VPN можна звести до вирішення трьох основних завдань: *захист* інформаційних потоків між різними офісами компанії (шифрування інформації проводиться тільки на виході у зовнішню мережу); *захищений* доступ віддалених користувачів мережі до інформаційних ресурсів компанії; *захист* інформаційних потоків між окремими додатками всередині корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється з внутрішніх мереж).

4) Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворювані вірусні програми.

Результатом дотримання порядку перевірки норм в компанії є збереження інформаційної системи підприємства, захист і гарантування повноти і точності виданої нею інформації, мінімізація руйнувань і модифікація інформації, якщо такі трапляються.

Висновки. На даний момент рівень захисту інформації є високим і досить стабільним. Зі збільшенням кількості інформації та співробітників з'являються нові загрози витоку інформації, збільшується ризик передачі інформації конкурентним організаціям. Звідси постає необхідність перегляду доступу співробітників до всіх ключових файлів з цінною інформацією, а також їх контрактних умов з метою захисту матеріальних інтересів компанії.

До нинішніх методів захисту є необхідність введення заборони на відвідування сторонніх ресурсів, своєчасне оновлення антивірусної програми, а також розділення інформації, що знаходиться в мережі, на різні паролі доступу.

Література

1. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К.: ТИД Диа Софт, 2002. –688 с.

2. Бєгун А.В. Інформаційна безпека / А.В. Бєгун. – К.:КНЕУ, 2008. –280 с.

3. Домарев В.В. Управління інформаційною безпекою в банківських установах / В.В. Домарев, Д.В. Домарев. . – Донецьк: Велстар, 2012. – 146 с.

УДК 621.391

Дьоміна Л.О., *асп. (Державний університет інформаційно-комунікаційних технологій)*

ДОСЛІДЖЕННЯ ОПТИМАЛЬНОГО РЕЗЕРВУВАННЯ ДЛЯ ВИЗНАЧЕННЯ НАДІЙНОСТІ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

Дьоміна Л.О. Дослідження оптимального резервування для визначення надійності інфокомунікаційних мереж. Сформульовано задачі оптимального резервування, визначені алгоритми пошуку кількості резервних елементів для показників надійності. Розглянуті методи проектування мереж та їх характеристики.

Ключові слова: ІНФОКОМУНІКАЦІЙНА МЕРЕЖА, НАДІЙНІСТЬ, РЕЗЕРВУВАННЯ

Дёмина Л.О. Исследование оптимального резервирования для определения надежности инфокоммуникационных сетей. Сформулированы задачи оптимального резервирования, определены алгоритмы поиска количества резервных элементов для показателей надежности. Рассмотрены методы проектирования сетей и их характеристики.

Ключевые слова: ИНФОКОММУНИКАЦИОННАЯ СЕТЬ, НАДЕЖНОСТЬ, РЕЗЕРВИРОВАНИЕ

Diomina L.O. Study to determine the optimal redundancy information and communication networks reliability. The problems of optimal redundancy, defined search algorithms of standby units for reliability. The methods of designing networks and their characteristics.

Keywords: INFOCOMMUNICATION NETWORK, RELIABILITY, RESERVATION

Вступ. Одним з основних критеріїв якості є надійність, тобто це властивість системи зберігати протягом певного проміжку часу значення параметрів, що характеризують функціонування системи. Це комплексна властивість системи, залежна від її безвідмовності, ремонтопридатності, довговічності і т.д. Тобто, це властивість системи зберігати в часі у встановлених межах значення всіх параметрів, що характеризують здатність виконувати необхідні функції в заданих режимах і умовах експлуатації [1]. Теорія надійності використовує апарат теорії ймовірностей і математичної статистики.

Особливий інтерес викликають методи, які дають можливість передбачити критичні ситуації для інфокомунікаційної мережі. Однією з найбільш ефективних теорій, що дозволяє оцінити параметри мережі, за яких можуть виникнути критичні ситуації, є теорія катастроф. Як відомо, “катастрофа” – це стрибкоподібна зміна, що виникає при плавній зміні зовнішніх умов [2]. Як правило, методи проектування мереж зводяться до того, щоб маючи на вході різні характеристики компонент мережі, у тому числі й характеристики їх надійності, визначити топологію мережі й обчислити надійність у цілому. Телекомунікаційні системи можна віднести до систем, що складаються з великої кількості підсистем. Зі збільшенням складності системи зв'язку імовірність виходу з ладу будь-якого її компонента збільшується. Сучасні системи зв'язку використовують велику кількість елементів, що робить необхідним використання обхідних маршрутів і резервування для підвищення коефіцієнта готовності системи зв'язку в цілому. Резервування – метод підвищення надійності об'єкта шляхом введення додаткових елементів і функціональних можливостей понад мінімально необхідних для нормального виконання об'єктом заданих функцій [3]. Підвищувати якість функціонування телекомунікаційних систем і мереж можна різними способами.

Тому дослідження оптимального резервування, а саме, визначення пошуку кількості резервних елементів для показників надійності *R*- і *T*-типів із заданою кількістю обмежень