УДК 004.056.

Кругляк В.В.,
Дегтярьова Л.М., к.т.н., доцент
Полтавський національний технічний
університет імені Юрія Кондратюка

МЕТОДИ ОЦІНКИ ПРОДУКТИВНОСТІ РОБІТ ПО ЗАХИСТУ ІНФОРМАЦІЙНИХ КАНАЛІВ В КОРПОРАТИВНИХ МЕРЕЖАХ

Анотація. *У статті проведено аналіз робіт по захисту каналів в корпоративних мережах. Розглянуті проблем , що виникають при роботі над захистом мережі. Визначено використання різних способів захисту інформації. Надано рекомендації як захиститися від витоку та втрати інформації. Досліджено методи оцінки продуктивності робіт по захисту інформаційних каналів в корпоративних мережах.*

Ключові слова: *Корпоративна мережа, захист інформації, інформаційна загроза, аналіз ризиків.*

Вступ

Сучасні умови соціально-економічного розвитку в Україні сприяють широкому впровадженню новітніх інформаційних технологій, створенню та використанню інфотелекомунікаційних систем, автоматизованих систем обробки і передачі інформації. Системи захисту інформації повинні відповідати запитам сьогодення в умовах росту числа інформаційних загроз, що виникають в процесі функціонування самих корпоративних мереж. Сучасні системи безпеки повинні захищати не окремі елементи мережі, а інформаційні потоки і ресурси незалежно від місця й часу їх виникнення. Рішення, як захищати інформацію і які засоби застосовувати, може бути складним. Це рішення

стосується й управління інформаційною безпекою, включаючи розробку політики безпеки і забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан подій.

Основна частина

Вирішення питання про оцінку рівня захищеності інформаційних активів компанії обов'язково пов'язано з проблемою вибору критеріїв і показників захищеності, а також ефективності корпоративної системи захисту інформації. Сама політика безпеки будується на основі аналізу ризиків, які визнаються реальними для інформаційної системи організації.

Сучасні методики управління ризиками, проектування і супроводу корпоративних систем захисту інформації повинні дозволяти вирішити ряд завдань перспективного стратегічного розвитку організації.

По-перше, кількісно оцінити поточний рівень інформаційної безпеки організації, що потребують виявлення ризиків, які виникають на всіх рівнях забезпечення захисту інформації: правовому, організаційно-управлінському, технологічному, а також технічному.

По-друге, розробити і реалізувати комплексний план дій з вдосконалення корпоративної системи захисту інформації для досягнення задовільного рівня захищеності інформаційних активів організації.

Такий підхід відповідає комплексному характеру забезпечення безпеки інформаційних мереж на всіх етапах їх життєвого циклу – від концептуальних схем та проектування до технічної експлуатації та використання.

Цілями захисту інформації є [1]:

- запобігання витоку, розкрадання, втрати, спотворення, підробки інформації;
- запобігання несанкціонованим діям зі знищення модифікації, спотворення, копіювання, блокування інформації;

– запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи.

Головна мета будь-якої системи інформаційної безпеки полягає в забезпеченні сталого функціонування об'єкта: запобігання загроз його безпеки, захисту законних інтересів власника інформації від протиправних посягань, у тому числі кримінально караних діянь у даній сфері відносин, забезпеченні нормальної виробничої діяльності всіх підрозділів об'єкта.

Для цього необхідно [2]:

– віднести інформацію до категорії обмеженого доступу;
– прогнозувати і своєчасно виявляти загрози безпеки інформаційних ресурсів, причини та умови, що сприяють нанесенню фінансового, матеріального і морального збитку, порушення його нормального функціонування і розвитку;
– створити умови функціонування з найменшою вірогідністю реалізації загроз безпеки інформаційних ресурсів і нанесення різних видів збитків;створити механізм і умови оперативного реагування на загрози інформаційної безпеки і прояву негативних тенденцій у функціонуванні, ефективне припинення зазіхань на ресурси на основі правових, організаційних і технічних заходів і засобів забезпечення безпеки;
– створити умови для максимально можливого відшкодування та локалізації збитку, що наноситься неправомірними діями фізичних і юридичних осіб, і тим самим послабити можливий негативний вплив наслідків порушення інформаційної безпеки.

Для того, щоб забезпечити надійний захист ресурсів корпоративної інформаційної системи на сьогодні і на найближче майбутнє, у системі інформаційної безпеки повинні бути реалізовані найбільш прогресивні й перспективні технології інформаційної безпеки.

При виконанні робіт можна використовувати наступну модель побудови корпоративної системи захисту інформації (рис. 1)

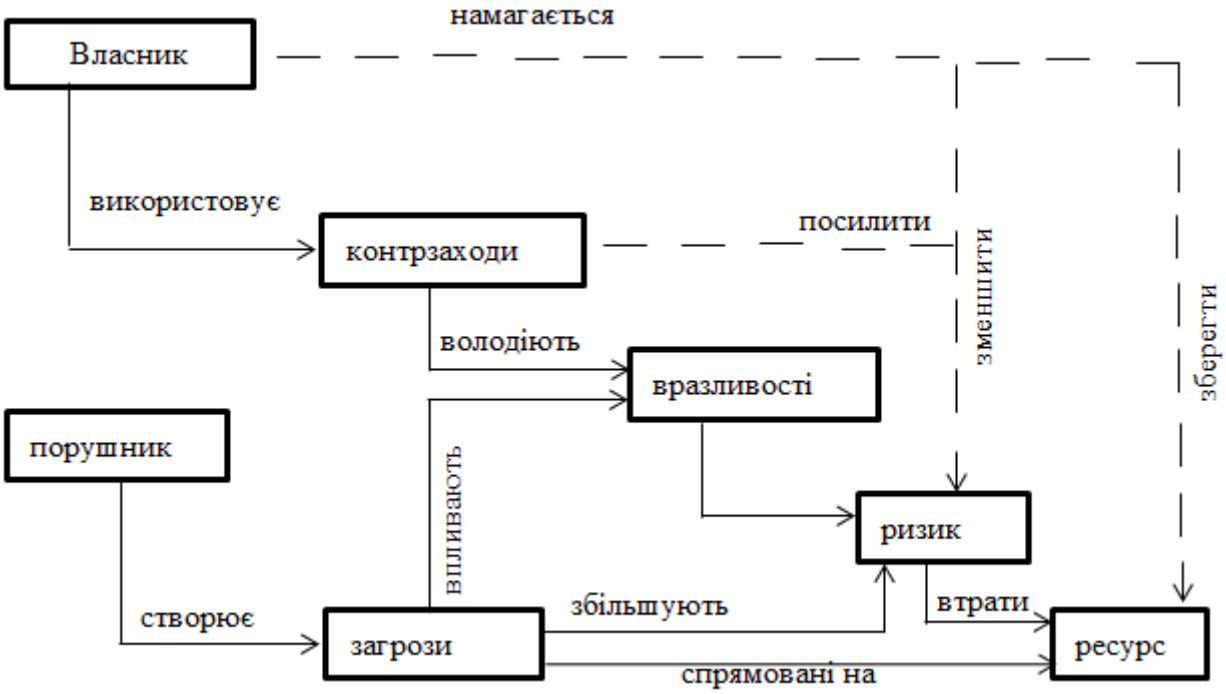

Рис. 1 Модель побудови корпоративної системи захисту інформації

Інформаційна безпека представляє собою багатогранну сферу діяльності, у якій успіх можливий тільки при систематичному, комплексному підході.

Продуктивність систем захисту інформації

На даний час фахівцями в галузі комп'ютерних технологій розроблено багато методів та способів захисту інформації. Системний підхід до захисту інформації вимагає необхідність обліку всіх взаємопов'язаних, взаємодіючих і таких, що змінюються в часі елементів, умов і чинників, істотно значущих для розуміння і вирішення проблеми забезпечення безпеки.

Інформаційний захист має забезпечуватися взаємопов'язаним комплексом заходів:

- оперативних;
- програмних;
- технічних;

– організаційних.

Ступінь впливу заходів тієї чи іншої групи на різні загрози відрізняється. Він залежить від багатьох умов, таких як характер загрози, характеристика середовища в якому ця загроза здійснюється, особистості порушника.

Зараз існують наступні методи та способи оцінки продуктивності систем захисту інформації:

– Метод порівняльного багатовимірного аналізу. Він створений для визначення ступеня взаємного впливу загроз та причин їх виникнення (і як результат – оцінка ефективності системи захисту інформації). Його суть можна звести до такого узагальненого алгоритму – складається перелік об'єктів, що оцінюються, і вибираються ознаки,за якими буде проводитись оцінка. В даному випадку під об'єктами оцінки розглядаються показники захищеності обчислювальної системи, а під ознаками – сукупність параметрів, що характеризують ці показники.

– Метод аналізу ризиків інформаційних систем. На даний час при побудові систем захисту інформації особливого значення набуває завдання побудови моделей загроз інформації. Існує чимало алгоритмів, які здійснюють аналіз ризиків інформаційних систем. До найбільш відомих алгоритмів належать CRAMM і RiskWatch. Зазначені алгоритми мають ряд переваг та набули широкого поширення.

Метод CRAMM був розроблений Службою Безпеки Великобританії за завданням Британського уряду і використовується як державний стандарт, починаючи з 1985 р., урядовими і комерційними організаціями Великобританії. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються один від одного своїми базами знань. Для комерційних організацій є Комерційний профіль, для урядових організацій – Урядовий профіль. CRAMM припускає поділ усієї процедури на три послідовних етапи. Завданням першого етапу є відповідь на питання: "Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції безпеки, чи необхідно провести більш детальний

аналіз?" На другому етапі проводиться ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується питання про вибір адекватних контрзаходів [3].

Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення запитів, списки перевірки і набір звітних документів. Якщо за результатами проведення першого етапу встановлено, що рівень критичності ресурсів є дуже низьким і існуючі ризики свідомо не перевищать деякого базового рівня, то до системи висувається мінімальний набір вимог безпеки. У цьому випадку велика частина заходів другого етапу не виконується, а здійснюється перехід до третього етапу, на якому генерується стандартний список контрзаходів для забезпечення відповідності базового набору вимог безпеки.

Метод RiskWatch розробляється американською компанією RiskWatch Inc. і є потужним засобом аналізу і управління ризиками. В сімейство RiskWatch входять програмні продукти для проведення різних видів аудиту безпеки. У методі RiskWatch як критерії для оцінки та управління ризиками використовуються "прогнозування річних втрат" (ALE) і "повернення від інвестицій" (ROI). Сімейство програмних продуктів RiskWatch має масу переваг. RiskWatch допомагає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту. Використовувана в програмі методика включає в себе 3 фази [3].

Перша фаза – визначення предмету дослідження. На даному етапі описуються параметри організації – тип організації, склад досліджуваної системи. Опис формалізується у ряді підпунктів. Далі кожен з обраних пунктів описується докладно. Для полегшення роботи аналітика в шаблонах даються списки категорій захищених ресурсів, утрат, загроз, уразливих місць і заходів захисту. З них потрібно вибрати ті, що реально присутні в організації.

Друга фаза – введення даних, що описують конкретні характеристики системи. Дані можуть вводитися вручну або імпортуватися зі звітів, створених інструментальними засобами дослідження вразливості комп'ютерних мереж. На

цьому етапі докладно описуються ресурси, втрати та класи інцидентів. Класи інцидентів отримуються шляхом зіставлення категорії втрат і категорії ресурсів. Для виявлення можливих уразливостей використовується опитувальник, база якого містить більше 600 питань. Питання пов'язані з категоріями ресурсів. Допускається коректування питань, виключення або додавання нових, встановити частоту виникнення кожної з виділених загроз, ступінь вразливості і цінність ресурсів. Усе це використовується і надалі для розрахунку ефективності впровадження засобів захисту.

Третя фаза – оцінка ризиків. Спочатку встановлюється зв’язок між ресурсами, втратами, загрозами і вразливими місцями, виділеними на попередніх етапах. Для ризику розраховуються математичні очікування втрат за рік (формула 1):

$$L = P \times V \quad (1)$$

де L – сума втрат від загроз інформації за рік;

P – частота виникнення загроз протягом року;

V – вартість ресурсу, який під загрозою.

Розглянуті методи дозволяють оцінити чи переоцінити рівень поточного стану інформаційної безпеки , розробити концепцію і політику безпеки , а також запропонувати плани захисту від виявлених загроз і вразливих місць.

Висновок

При створенні системи захисту інформації необхідно враховувати всі слабкі, найбільш вразливі місця інформаційної системи організації, а також характер, можливі об'єкти і напрями атак на систему з боку хакерів, ймовірні шляхи проникнення в систему і несанкціонованого доступу до інформації.

Система захисту інформації повинна будуватися з урахуванням не тільки всіх відомих каналів витоку інформації і несанкціонованого доступу до

інформації, але і з передбаченням можливості появи принципово нових шляхів реалізації загроз безпеці інформації.

Також для запобігання можливим втратам чи пошкодженню даних необхідно використовувати засоби призначені для аналізу захищеності корпоративних мереж та виявлення можливих каналів реалізації загроз інформації. Їх застосування дозволяє передавати інформацію про можливі атаки на корпоративну мережу, оптимізувати втрати та захист інформації і контролювати поточний стан захищеності мережі. Крім того, в межах організації обов'язковою вимогою є наявність централізованих засобів керування політикою інформаційної безпеки.

Посилання

1. *Биячуев Т.А. Безопасность корпоративных сетей – 2004*
2. *Арчилов Р. Построение защищенных корпоративных сетей – 2012*
3. *Хорев А.А. Оценка эффективности защиты информации от утечки по техническим каналам // Специальная техника. – 2006. - № 6. - С. 53 – 61. 3.Королев В.И. Морозова Е.В. Методы оценки*
4. *Методи проникнення в корпоративні мережі [Електронний ресурс]– Режим доступу до ресурсу: https://www.kitgsm.com.ua/stati/bezpeka/metodi-proniknennya-v-korporativni-merezhi.html*

Authors:
Vladislav Kruglyak , Larisa Degtyaryova

METHODS OF EVALUATION OF PRODUCTIVITY OF PROJECTS ON PROTECTION OF INFORMATION CHANNELS IN CORPORATE NETWORKS

Abstract. The article analyzes work on protection of channels in corporate networks. Considered the problems that arise when working on network protection. The use of different ways of protecting information is determined. Advice is given on how to protect against leakage and loss of information. The methods of estimation of work efficiency on protection of information channels in corporate networks are investigated.

Keywords: Corporate network, information protection, information threat, risk analysis.

Авторы:Кругляк Владислав Вадимович, Дегтярева Лариса Николаевна

МЕТОДЫ ОЦЕНКИ ПРОИЗВОДИТЕЛЬНОСТИ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИОННЫХ КАНАЛОВ В КОРПОРАТИВНЫХ СЕТЯХ

Аннотация. В статье проведен анализ работ по защите каналов в корпоративных сетях. Рассмотрены проблемы, возникающие при работе над защитой сети. Определены использования различных способов защиты информации. Даны рекомендации как защититься от утечки и потери информации. Исследованы методы оценки производительности работ по защите информационных каналов в корпоративных сетях.

Ключевые слова: Корпоративная сеть, защита информации, информационная угроза, анализ рисков.