Sciences and Humanity Studies. – 2011. – Vol. 3, No 1. – P. 307–321.

Бурлаков Олександр
к.е.н., доцент
Подільський державний аграрно-технічний університет
м. Кам'янець-Подільський, Україна

ВНУТРІШНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНИХ ПІДПРИЄМСТВ В УМОВАХ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Комплексний підхід до забезпечення IT-безпеки підприємства передбачає ефективний і збалансований захист як від зовнішніх, так і від внутрішніх загроз. В той же час результати досліджень показують, що служби інформаційної безпеки суб'єктів господарювання приділяють достатньо уваги лише зовнішнім загрозам (шкідливим кодам, мережевим атакам і спаму), у той час як дії самих співробітників підприємства взагалі не контролюються. Такий дисбаланс призводить до серйозних фінансових втрат через нецільове використання ресурсів підприємства і, що набагато важливіше, до витоку конфіденційної інформації. В останньому випадку часто страждає імідж компанії – а це часто складніше виміряти в економічних показниках [2].

За даними моніторингу, проведеного групою компаній InfoWatch, у першому півріччі 2015 року в світі (оприлюднено у ЗМІ та інших джерелах) зафіксовано 723 випадки витоку конфіденційної інформації, що на 10% перевищує кількість витоків, зареєстрованих за аналогічний період 2014 року [2].

В межах досліджуваного періоду розподіл витоків інформації за вектором впливу подано на рис. 1.

До внутрішніх загроз відносяться:

- несанкціонований доступ у приміщення;
- несанкціонований доступ до даних усередині корпоративної мережі;
- можливість запису інформації на переносні пристрої: флеш-накопичувачі, CD і DVD-диски;
- пересилання фотознімків паперових носіїв і екранів моніторів за допомогою мобільних телефонів;
- програмні віруси і «троянські» програми, а також неконтрольовані повідомлення електронної пошти.

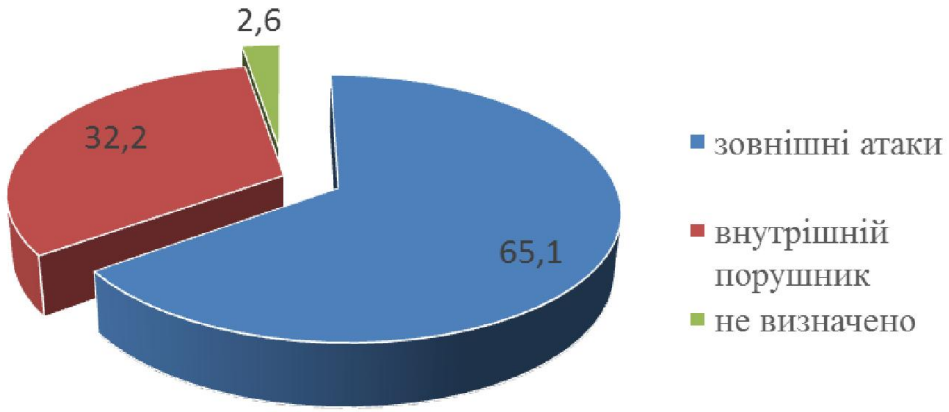

Рис. 1. Розподіл витоків інформації по вектору впливу, I півріччя 2015 р., %

Джерело: http://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2015_half_year.pdf

Для захисту від зовнішнього несанкціонованого доступу розроблені і постійно удосконалюються технічні засоби, програмні продукти та рішення інформаційно-технічної безпеки. При грамотній настройці і супроводі вони досить ефективно протистоять вторгненням в корпоративну мережу підприємства ззовні.

Боротьба з внутрішніми загрозами безпосередньо залежить від дії керівництва компанії. У цьому випадку необхідний випуск адміністративних інструкцій і заходів щодо упорядкування використання корпоративних ресурсів компанії.

Для мінімізації інцидентів, пов'язаних з внутрішніми загрозами, на середніх і великих підприємствах використовуються програмно-апаратні DLP-системи, що дозволяє здійснювати комплексні заходи щодо запобігання витоку даних з компанії. Шифрування ділового листування, папок і файлів, контроль знімних носіїв – невеликий перелік дій необхідних для мінімізації витоку даних [3].

Захист від внутрішніх загроз забезпечується як технічними засобами, так і комплексом супутніх послуг. Слід зазначити, що брак уваги хоча б до одного з етапів може призвести до негативних наслідків. Саме тому слід з однаковою старанністю підходити як до впровадження засобів технічного контролю, так і до складання нормативної бази та періодичному аудиту IT-інфраструктури [1].

Загрози інформаційної безпеки підприємства абсолютно реальні, їх не можна недооцінювати. Крім протидії зовнішнім загрозам особливу увагу слід приділити загрозам внутрішнім. Важливо пам'ятати, що витоки корпоративних секретів трапляються не тільки зі злого наміру – як правило, їх причина в елементарній халатності і неуважності працівника. При виборі засобів захисту не потрібно намагатися охопити всі мислимі і немислимі загрози, на це просто не вистачить грошей і сил. Необхідним та достатнім буде побудова надійної модульної системи безпеки, закриту від ризиків вторгнення ззовні і з можливостями здійснення контролю та моніторингу за потоком інформації всередині інформаційної системи підприємства.

Список використаних джерел

1. Алексей Доля. Внутренняя ИТ-безопасность http://compress.ru /article.aspx?id=10495#Внутренние ИТ-угрозы (дата звернення 20.11.2015 р.)
2. Информационная безопасность предприятия: внутренняя угроза [Електронний ресурс]. – Режим доступу http://www.safensoft.ru/ security.phtml?c=775 (дата звернення 20.11.2015 р.). – Информационная безопасность предприятия. Информационная защита бизнеса.
3. Смирнов Г. Особенности обеспечения информационной безопасности малого и среднего бизнеса [Електронний ресурс]. – Режим доступу: http://www.anti-malware.ru/Small_Business_Security (дата звернення 20.11.2015 р.).

Василькова Анастасия
студентка специалитета
Могилёвский государственный университет продовольствия
г. Могилёв, Республика Беларусь

ПРОБЛЕМЫ АНАЛИЗА НЕМАТЕРИАЛЬНЫХ АКТИВОВ

Вопросы эффективного использования нематериальных активов являются в современных условиях актуальными. Это связано в первую очередь с тем, что количество операций с нематериальными активами увеличивается с каждым годом и они занимают значительный удельный вес в структуре активов организаций. Динамичные качественные технические изменения, распространение информационных технологий, усложнение и интеграция финансового рынка Беларуси – все это требует детального изучения и емкого, полного использования объектов нематериальных активов. В связи с этим важнейшим вопросом в активизации использования нематериальных активов на предприятиях является оценка их стоимости, учет которой необходим не только для оценки эффективности производственного процесса, но и при других хозяйственных операциях организации.

Разработка программы анализа нематериальных активов является самым важным и ответственным участком аналитической работы. Она должна четко отражать следующие элементы: 1) объект анализа; 2) цель анализа; 3) задачи анализа; 4) период, за который проводится анализ; 5) показатели, которые предполагается использовать в ходе анализа; 6) источники информации для проведения анализа [1].

Объектом анализа являются так называемые неосязаемые активы – объекты прав интеллектуальной собственности, авторских прав. Их экономическая сущность проявляется в том, что они являются одним из видов ресурсов предприятия, позволяющие собственнику осуществлять предпринимательскую деятельность с целью получения экономических выгод.