Вінокурова О. О.

УДК 004.239:355.404.51:005

Магістр 1 року навчання
факультету обліку і аудиту ХНЕУ ім. С. Кузнеця

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Анотація. Розглянуто рівень розвитку і відповідність потребам сучасності системи забезпечення інформаційної безпеки на підприємствах України. Проаналізовано основні проблеми захисту інформації на підприємствах, показано основні напрями та методи покращення інформаційної безпеки.

Аннотация. Рассмотрен уровень развития и соответствие потребностям современности системы обеспечения информационной безопасности на предприятиях Украины. Проанализированы основные проблемы защиты информации на предприятиях, показаны основные направления и методы улучшения информационной безопасности.

Annotation. The information security management system at enterprises of Ukraine has been considered in terms of the level of its development and how it meets the modern needs. The main problems of information security at enterprises have been analysed, the main trends and methods to improve information security have been shown.

Ключові слова: інформаційна безпека, загроза, програмне забезпечення, кіберзлочин.

Інтенсивний розвиток і використання сучасних інформаційних технологій вже нині призвели до серйозних якісних змін у всіх сферах суспільного життя. Сучасне суспільство вступає в постіндустріальний період свого розвитку, який на загальну думку можна назвати інформаційним.

Бізнес залежить від інтернету, який таїть в собі безліч загроз. Не варто забувати і про внутрішні загрози: витік даних, уразливості у використовуваному програмному забезпеченні, шпигунстві і т. д. Весь спектр зовнішніх і внутрішніх загроз ставить перед невеликими компаніями непросту задачу по створенню системи IT-безпеки, яка дозволить ефективно протистояти сучасним загрозам.

Ці проблеми вважаються одними з найбільш актуальних і невідкладних завдань суспільства. Для їх вирішення в останні роки ведуться вельми інтенсивні і великомасштабні дослідження і розробки.

Дослідженням різних аспектів захисту інформації займались: Малюк А. А., Ажмухамедов І. М., Круглов А. А., Шолохова М. А., Лисенко М. С. та ін. Але потрібне подальше дослідження проблем захисту інформації з боку програмного та технічного забезпечення.

Метою даного дослідження є удосконалення можливостей забезпечення захисту інформації на підприємстві.

Пересилання електронних повідомлень, пошук нових клієнтів та партнерів у мережі, використання IM-месенджерів та соціальних мереж для спілкування, і, що найважливіше, використання банк-клієнтів для проведення фінансових операцій – так виглядає робочий день у невеликій компанії.

У зв'язку з цим особливої актуальності набуває проблема забезпечення інформаційної безпеки, і насамперед, надійного захисту інформації (попередження її перекручування чи знищення, несанкціонованої модифікації, зловмисної отримання та використання) [1].

Загостренню проблеми організації інформаційної безпеки сприяє також поява у величезних кількостях дешевих персональних комп'ютерів і побудованих на їх основі локальних і глобальних національних і транснаціональних мереж ЕОМ, що використовують супутникові канали зв'язку, повсюдна і масова комп'ютеризація інформаційних процесів, створення високоефективних систем розвідки і видобутку інформації.

Інформаційні системи є одним із системоутворюючих факторів життя сучасного суспільства, а вплив інформаційної безпеки на всі сторони життя суспільства з плином часу буде тільки зростати. Процес забезпечення безпеки інформації повинен носити комплексний характер і ґрунтуватися на глибокому аналізі можливих негативних наслідків. Такий аналіз передбачає обов'язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їх прояву і, як наслідок, визначення актуальних загроз безпеки інформації [2].

У невеликих компаніях керівна ланка не надає особливої значущості питань інформаційної безпеки, вважаючи кіберзагрози несуттєвим ризиком для бізнесу, і, як наслідок, виділяє недостатньо часу і коштів на вирішення питань безпеки. Обмеженість бюджету змушує компанії переходити на безкоштовне або неліцензійне програмне забезпечення. Особливо гостро проблема відсутності коштів і використання неліцензійного програмного забезпечення відчувається в регіонах. Навчання персоналу компанії основам роботи з IT-системами особливо важливо, оскільки людський фактор часто відіграє вирішальну роль у ході проведення атаки на компанію. Однак у 2013 році інтерес до інвестицій в навчання персоналу роботі з IT-системами знизився на 7 % [3].

Уразливості в програмному забезпеченні, витік даних або крадіжка мобільних пристроїв співробітників компанії приносить багато проблем фахівцям з інформаційної безпеки. Для мінімізації інцидентів, пов'язаних з внутрішніми загрозами, на середніх і великих підприємствах використовуються програмно-апаратні DLP-системи, які дозволяють здійснювати комплексні заходи щодо запобігання витоку даних із компанії. Шифрування ділового листування, папок і файлів, контроль знімних носіїв – невеликий перелік дій необхідних для мінімізації витоку даних. Управління оновленням програмного забезпечення – один із ключових аспектів внутрішньої безпеки, оскільки пере

важна більшість атак починається з експлуатування вразливостей в ПО [4].

Слід усвідомити ту ступінь залежності від комп'ютерної обробки даних, у яку потрапило сучасне суспільство. Акцент слід робити не на військовому чи кримінальному боці справи, а на цивільних аспектах, пов'язаних з підтриманням нормального функціонування апаратного та програмного забезпечення, тобто концентруватися на питаннях доступності та цілісності даних.

На процедурному рівні можна виділити такі класи заходів: управління персоналом; фізичний захист; підтримка працездатності; реагування на порушення режиму безпеки; планування відновлювальних робіт [5].

У рамках управління персоналом для кожної посади повинні існувати кваліфікаційні вимоги з інформаційної безпеки. У посадові інструкції повинні входити розділи, що стосуються захисту інформації. Кожного співробітника підприємства необхідно навчити заходам забезпечення інформаційної безпеки теоретично і відпрацювати виконання цих заходів практично.

Інформаційна безпека інформаційних систем (далі ІС) підприємства залежить від оточення, в якому вона працює. Необхідно вжити заходів для забезпечення фізичного захисту будівель та прилеглої території, підтримуючої інфраструктури і самих комп'ютерів.

У ході розробки проекту системи організації інформаційної безпеки передбачається адекватна реалізація заходів фізичного захисту офісних будівель та інших приміщень, що належать підприємству, за такими напрямами: фізичне управління доступом; протипожежні заходи; захист підтримуючої інфраструктури.

Передбачається також адекватна реалізація таких напрямів підтримки працездатності: підтримка користувачів ІС; підтримка програмного забезпечення; конфігураційне управління; резервне копіювання; управління носіями; документування; регламентні роботи.

Програма інформаційної безпеки повинна передбачати набір оперативних заходів, спрямованих на виявлення і нейтралізацію порушень режиму безпеки. Важливо, щоб у подібних випадках послідовність дій була спланована заздалегідь, оскільки заходи потрібно приймати термінові і скоординовані.

Реакція на порушення режиму інформаційної безпеки переслідує дві головні цілі: блокування порушника і зменшення завдається шкоди; недопущення повторних порушень.

На підприємстві повинен бути виділений співробітник, доступний 24 години на добу, що відповідає за реакцію на порушення. Усі користувачі ІС повинні знати координати цієї людини і звертатися до нього за умов перших ознаках небезпеки. У разі неможливості зв'язку з даним співробітником, повинні бути розроблені та впроваджені процедури первинної реакції на інформаційний інцидент [6].

Отже, революція в науково-технічній сфері призвела до появи нових видів інформаційно-комунікаційних технологій, що стали матеріальним підґрунтям глобалізаційних процесів. Інформатизація усіх сфер життєдіяльності змінила розуміння сутності феномену безпеки, джерел та характер загроз, значення та роль міжнародних інститутів.

Інформаційна безпека є невід'ємною складовою безпеки національної. Саме тому різні органи державної влади мають приділяти особливу увагу гарантуванню цієї безпеки, особливо в контексті неухильного руху розвинених суспільств до всеохоплюючої інформатизації всіх сфер їх життєдіяльності. Особливо це стосується органів безпеки, які мають не лише протидіяти інформаційним атакам всередині підприємства та держави, в контексті інформаційної війни, а й бути готовими до боротьби з новою категорією злочинів: кіберзлочинами – правопорушеннями в сфері інформаційних технологій.

До сьогоднішнього дня питанню захисту інформаційної безпеки на підприємствах не приділялося належної уваги. У той же час ефективність діяльності підприємств безпосередньо залежить від стану їх інформаційної безпеки. В умовах жорсткої конкуренції все частіше зустрічаються ситуації з витоку важливої для діяльності підприємств інформації. Саме тому виникає необхідність у розробці та впровадженні комплексної системи захисту інформації кожного підприємств. Для цього слід застосовувати методики аналізу ризиків, які дозволяють обрати оптимальний за ефективністю варіант захисту.

Наук. керівн. Петряєва З. Ф.

Література: 1. Малюк А. А. Защита информации: современные проблемы / А. А. Малюк // Безопасность информационных технологий. – 2010. – № 1. – С. 5–9. 2. Ажмухамедов И. М. Принципы обеспечения комплексной безопасности информационных систем / И. М. Ажмухамедов // Вестник АГТУ. Серия: "Управление, вычислительная техника и информатика". – 2011. – № 1. – С. 7–11. 3. Круглов А. А. Об информационной безопасности / А. А. Круглов, Б. И. Скородумов // Вестник Российского нового университета. – 2007. – № 2. 4. Смирнов Г. Особенности обеспечения информационной безопасности малого и среднего бизнеса / Г. Смирнов // Small Business Securuty, 2013. 5. Шолохова М. А. Процедурный уровень информационной безопасности / М. А. Шолохова // Информационная безопасность. – 2010. 6. Концепция обеспечения информационной безопасности предприятия [Электронный ресурс]. – Режим доступа : http://securitypolicy.ru/in dex.php. – Название с экрана. 7. Лисенко М. С. Особливості забезпечення інформаційної безпеки підприємств / М. С. Лисенко // Бізнес та безпека. – 2008. – № 7. – С. 30–35.