ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

ENSURING THE INFORMATION SECURITY OF THE ENTERPRISE

Науковий керівник – доцент кафедри Радіотехничних пристроїв

Мельник М.О., Melnik M.

Виконав – Полоз М.Г., Poloz M.

Анотація: у даній статті розглядається актуальна на даний момент проблема захисту інформації на підприємствах, оскільки доступ до конфіденційної інформації і її зміна може завдати істотної шкоди фінансовому становищу компанії.

Ключові слова: інформаційна безпека на підприємстві, загрози, несанкціонований доступ, резервування, захист інформації.

Abstract: this article discusses the current at the moment the problem of information security in enterprises, as access to confidential information and its change can cause substantial damage to the financial situation of the company.

Keywords: information security at the enterprise, threats, unauthorized access, backup, information protection.

Однією з найбільш нагальних проблем інформаційного суспільства є захист інформації, оскільки всілякі дані, що обробляються і накопичуються обчислювальною технікою, стали останнім часом визначати напрямок діяльності і багато інших аспектів життя сучасного соціального організму.

За допомогою незаконного володіння інформацією можна здійснювати найрізноманітніші протиправні діяння, наприклад, виробляти незаконний оборот фінансових коштів, отримувати доступ до секретної комерційної інформації і т.д. Слід зазначити, що конфіденційна інформація представляє величезний інтерес для конкуруючих фірм. Саме вона стає причиною посягань з боку зловмисників.

Багато проблем інформаційної безпеки пов'язані з недооцінкою важливості конфіденційність інформації. В результаті для підприємства це може обернутися банкрутством. Навіть одиничний випадок халатності персоналу підприємства може принести йому багатомільйонні збитки, втрату репутації фірми і довіри клієнтів. Щоб цього уникнути, фахівці служби безпеки підприємства використовують спеціальне обладнання, яке виробляє аналіз електромагнітних випромінювань, одержуваних під час роботи на комп'ютері.

Технології забезпечення інформаційної безпеки можна поділити на дві групи:

—1-а група – захищають програмні і апаратні засоби для обробки і зберігання інформації від відмов, порушень, здатних виникнути в результаті випадкової помилки;

—2-а група – захищають програмні і апаратні засоби обробки інформації від всіляких навмисних загроз, які заздалегідь плануються зловмисниками.

Повноцінне забезпечення інформаційної безпеки на підприємстві повинно бути стандартизовано і перебувати під повним контролем цілий рік, в реальному часі, в цілодобовому режимі. При цьому система враховує весь життєвий цикл інформації, починаючи з моменту появи і до повного її знищення або втрати значущості для підприємства.

Цілями системи захисту інформації підприємства є:

—запобігання витоку, розкрадання, втрати, спотворення, підробки інформації внаслідок її розголошення;

—запобігання загрозам безпеки особистості, підприємства, суспільства, держави внаслідок розголошення або спотворення інформації;

—запобігання несанкціонованим діям зі знищення, модифікації, спотворення, копіювання, блокування інформації, що може привести до зменшення її потенційної ефективності;

—запобігання різних форм незаконного втручання в інформаційні ресурси і системи підприємства;

—забезпечення правового захисту інформації як об'єкта власності (виключення можливості її незаконного тиражування);

—захист конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних, наявних в інформаційних системах підприємств;

—збереження конфіденційності документованої інформації відповідно до законодавства (грифи секретності, прав доступу і поширення і т.д.).

Слід зауважити, що з метою захисту інформації кожен користувач зобов'язаний знати і здійснювати наступні заходи:

—контролювати доступ як до інформації в комп'ютері, так і до прикладних програм. Необхідно мати гарантії того, що тільки авторизовані користувачі зможуть мати доступ до інформації і додатків;

—процедури авторизації. Адміністратору слід розробити процедури авторизації, що визначають, хто з користувачів може мати доступ до тих чи інших прикладних програм та інформації, і передбачити відповідні заходи щодо впровадження в організацію таких процедур;

—захист файлів. Слід розробити процедури по обмеженню доступу до файлів: для вказівки типу інформації, що міститься в файлах, і необхідного рівня безпеки використовувати зовнішні та внутрішні мітки; обмежувати доступ в ті приміщення, в яких зберігаються архіви, файли і бібліотеки даних; для обмеження доступу до файлів тільки авторизованих користувачів використовувати організаційні заходи і програмно-апаратні засоби;

—захист цілісності інформації. Інформацію слід піддавати перевіркам на помилки, вона повинна бути авторизованої, повною і точною. Точність

інформації необхідно перевіряти за допомогою процедур порівняння отриманих результатів обробки з передбачуваними;

—захист системних програм. При розробці програм заходи захисту повинні включати в себе процедури щодо внесення змін до програми, її приймання і тестування до введення в експлуатацію;

—становлення заходів захисту більш адекватними за рахунок залучення спеціалізованих організацій;

—розгляд питання про комунікаційної безпеки. Дані, що передаються по незахищених лініях, можуть бути перехоплені.

На державному рівні правовий захист регулюється державними та відомчими актами. У нашій країні регуляторами є: Конституція, закони України, нормативні документи, цивільне, адміністративне і кримінальне право. Відомчі нормативні акти визначаються наказами, інструкціями, положеннями та інструкціями, які видаються самими відомствами, організаціями, а також підприємствами, що діють в рамках певних структур.

Насамкінець слід зазначити, що комплексний захист організацій сьогодні здійснює значна кількість спеціалізованих охоронних підприємств і служб безпеки. Вони проводять різні види робіт з фізичної, економічної та інформаційної безпеки, оскільки в сучасній обстановці без вирішення цих питань будь-який вид діяльності не зможе бути ефективним і прибутковим.

Список літератури

1. ISO/IEK27032 2012. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности»
2. Аналіз побудови моделі політики інформаційної безпеки підприємства / М. О. Мельник, Г. Д. Нікітин, К. О. Мезенцева // Системи обробки інформації. - 2017. - Вип. 2. - С. 126-128.

3. МЕТОДИ АНАЛІЗУ РИЗИКІВ ТА МОДЕЛІ ОЦІНКИ РИЗИКІВ З БЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ / М. О. Мельник, А. В. Тихонова // Сучасні інформаційні технології та телекомунікаційні мережі.-2019
4. Использование альтернативного метода ведения интернет-бизнеса, как одной из составляющих развития малого бизнеса Украины / М. А. Мельник, А. С. Сафронов, А. А. Рура // Системи обробки інформації. - 2017 — № 2(148). – С. 192-194. - http://www.hups.mil.gov.ua/periodic-app/article/17418
5. Сафронов, А. С. Применение организационно-технических методов для развития системы информационной безопасности организации / А. С. Сафронов, О. Е. Плачинда, Ю. И. Венедиктов // Пр. Одес. політехн. ун-ту. - Одеса, 2011. - Вип. 1 (35). - С. 263-267.
6. Сафронов, А. С. Анализ критериев для классификации ИТ-компаний / А. С. Сафронов, А. В. Мороз, С. В. Николайчук // Вост.-Европ. журн. передовых технологий. - 2011. - № 1 (6). - С. 44-46.
7. Кобозева, А. А. Общий подход к анализу состояния информационных систем как теоретический базис для стеганоалгоритмов, устойчивых к атаке сжатием / А. А. Кобозева, М. А. Мельник, П. Е. Баранов // Інформатика та мат. методи в моделюванні. – 2014. – Т. 4, № 2. – С. 99-104.
8. Востров, Г. Н. Распределенные технологии в построении и управлении динамическими системами сетевых коммуникаций / Г. Н. Востров, М. Г. Годынский, А. Атие // Цифрові технології. - 2012. - Вип. 11. - С. 153-158.
9. Задорожнюк, Н. О. ІТ-аутсорсинг та перспективи його розвитку в Україні / Н. О. Задорожнюк // Економіка. Фінанси. Право : інформ.-аналіт. журн. – Київ, 2017. – № 5/3. – С. 9–11.