УДК 004.056.5
Сніжной Г.В. [1], Харибін Г.Ю. [2]

[1] проф. НУ «Запорізька політехніка»
[2] студ. гр. БК-813 НУ «Запорізька політехніка»

РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ НА КОМЕРЦІЙНОМУ ПІДПРИЄМСТВІ СИСТЕМИ БЕЗПЕКИ РОБОЧИХ СТАНЦІЙ

В умовах стрімкої цифровізації бізнес-процесів інформаційна безпека підприємства стає визначальним фактором його стабільності. Для компанії захист комерційної таємниці, клієнтських баз, фінансової звітності та логістичних ланцюгів є пріоритетом. Метою дослідження є розробка регламенту Системи безпеки робочих станцій (СБРС) на засадах конфіденційності, цілісності та доступності даних [1].

Технічне забезпечення робочих місць співробітників, а саме апаратне забезпечення розподіляється на основі принципу необхідної достатності для виконання посадових обов'язків. Усі ПК підключені до корпоративної локальної обчислювальної мережі (ЛОМ) з доступом до Інтернету через корпоративний шлюз безпеки. Керівництву підприємства пропонуються ноутбуки бізнес-класу (для забезпечення мобільності та роботи у відрядженні) із вбудованими модулями TPM 2.0 та апаратні токени для зберігання кваліфікованого електронного підпису (КЕП). Для відділу бухгалтерського обліку пропонуються настільні ПК стандартної продуктивності, монітори 24"-27" (для зручної роботи з таблицями), спільний мережевий лазерний принтер, апаратні токени (КЕП), джерела безперебійного живлення (ДБЖ). Відділ закупівель та продажів укомплектовується настільними ПК або корпоративними ноутбуками, гарнітурами для IP-телефонії, спільним мережевим БФП. Можливо додаткове обладнання, а саме спеціалізований промисловий ПК або захищений планшет, сканер штрих-кодів/QR-кодів, принтер етикеток. Робоче місце офіцер з інформаційної безпеки укомплектовується високопродуктивною

робочою станцією, двома моніторами (для моніторингу трафіку, подій безпеки). Важливим є наявність виділеного зашифрованого зовнішнього накопичувачу для резервного копіювання конфігурацій безпеки.

Програмне забезпечення робочих місць встановлюється виключно системним адміністратором за погодженням з Офіцером з ІБ на основі посадових інструкцій (Принцип найменших привілеїв). Усі робочі станції мають базовий набір: ОС (наприклад, Windows 11 Pro / Enterprise), корпоративний антивірус (EDR-агент), офісний пакет, корпоративний месенджер та поштовий клієнт. Відповідно до функціоналу співробітників на робочих станціях встановлюється наступне програмне забезпечення:

1. Керівництво: ERP-система (модуль аналітики та управління), ПЗ для підписання документів (M.E.Doc), захищений VPN-клієнт для віддаленого доступу.
2. Бухгалтерія: Спеціалізоване облікове ПЗ (наприклад, BAS ERP, BAS Бухгалтерія), система подачі звітності (M.E.Doc), ПЗ для роботи з Клієнт-Банком.
3. Відділ закупівель (Китай/Тайвань): ERP-система (модуль закупівель), спеціалізовані захищені месенджери для зв'язку з азійськими партнерами (WeChat, Signal), VPN-клієнт для забезпечення безпечного каналу зв'язку.
4. Відділ продажів: CRM-система, програмний клієнт IP-телефонії, поштовий клієнт.
5. Офіцер з ІБ: Консоль управління SIEM-системою (збір та аналіз логів), консоль антивірусного управління (EDR/XDR), сканери вразливостей (напр., Nessus), ПЗ для аналізу мережевого трафіку (Wireshark), консоль адміністрування Firewall.

Паролювання, ідентифікація та шифрування даних виконується за вимогами: довжина пароля — не менше 12 символів (великі, малі літери, цифри, спецсимволи). Зміна пароля кожні 90 днів. Заборонено використання попередніх 5 паролів.

З метою запобігання візуальному витоку даних встановлюється автоматичне блокування робочої станції через 5 хвилин неактивності. Заборонено залишати розблокований ПК без нагляду ("Політика чистого столу та екрану"). Усі накопичувачі на ноутбуках та ПК шифруються за допомогою технології BitLocker / FileVault.

У разі крадіжки ноутбука (наприклад, у директора) дані неможливо буде прочитати. Передача даних через мережу Інтернет здійснюється виключно зашифрованими протоколами (HTTPS, TLS, IPsec/OpenVPN). Загальне резервне копіювання виконується за правилом «3-2-1» (3 копії, 2 різні носії, 1 копія поза офісом). Резервне копіювання бази даних (ERP, Бухгалтерія) виконується за правилом: інкрементне копіювання – кожні 4 години, повне – щодня вночі.Дані користувачів зберігаються не на локальних дисках комп'ютерів

(робочі станції), а на захищених мережевих дисках (File Server). Серверні файли бекапляться щодня. Резервні копії перевіряються на можливість відновлення (Restore Test) Офіцером з ІБ щомісяця.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою (ISO/IEC 27001:2022, IDT). [Чинний від 2023-08-17]. Київ : ДП «УкрНДНЦ», 2023. 19 с.