УДК 004.725.5
DOI: 10.31673/2409-7292.2020.013741

Лагута В.В.

ПІДВИЩЕННЯ ЯКОСТІ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА

Проаналізовано принцип організації системи безпеки з використанням моделі OSI та рекомендації стандарту кібербезпеки ISO 27000. Показано переваги побудови системи безпеки з використанням доменного підходу. Розроблені рекомендації для побудови захищеної комп'ютерної мережі. Захист доцільно будувати по наступним напрямам: захист систем та пристроїв, безпека серверів, забезпечення захисту мережі та фізична безпека.

Ключові слова: інформаційно-телкомунікаційна система, інформація з обмеженим доступом, домен, хост, об'єкт інформаційної діяльності, корпоративна мережа.

Вступ

У теперішній час неможливо уявити собі серйозну компанію яка не використовує у своїй роботі сучасні інформаційні технології для роботи. Однією з неодмінних складових даних технологій є об'єднання обчислювальних ресурсів компанії в єдину розподілену інформаційно-телекомунікаційну систему.

Проблема кібернетичної безпеки у інформаційно-телекомунікаційних системах сьогодні дуже гостро стоїть перед організаціями будь-якого рівня. Витік критично важливої інформації, зростання обсягів паразитного трафіку, вимагання, шантаж і замовні атаки на інформаційні ресурси стали останнім часом частим явищем.

Основна частина

Основна мета концепції кібернетичної безпеки - визначення методів і засобів захисту та забезпечення безпеки інформації, що відповідають інтересам, вимогам і законодавству України в сучасних умовах необхідності використання ресурсів глобальних мереж передачі даних загального користування для побудови корпоративних захищених і безпечних мереж. Інформаційно-телекомунікаційної мережі підприємства це взаємопов'язана сукупність мереж, служб передачі даних і телеслужби, призначена для надання єдиного захищеного мережевого простору обмеженому рамками корпорації колу користувачів (рис. 1) [1].

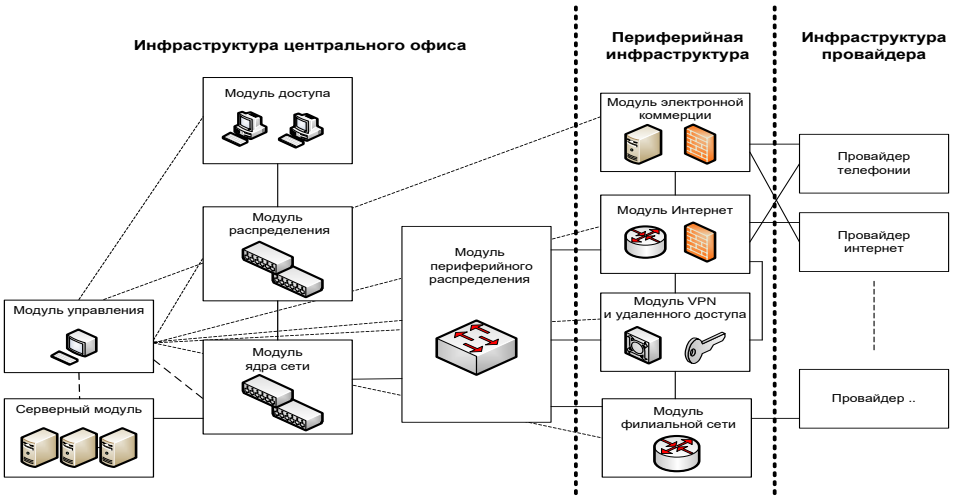

Рисунок 1. Блок-схема корпоративної мережі

Система забезпечення безпеки інформації повинна мати багаторівневу структуру і включати наступні рівні [2]:

рівень захисту автоматизованих робочих місць (АРМ);

рівень захисту локальних мереж та інформаційних серверів;

рівень захисту корпоративної АС.

На рівні захисту автоматизованих робочих місць повинна здійснюватися ідентифікація та аутентифікація користувачів операційної системи. Повинно здійснюватися управління доступом: надання доступу суб'єктів до об'єктів відповідно до матрицею доступу, виконання реєстрації та обліку всіх дій суб'єкта доступу в журналах реєстрації. Повинна бути забезпечена цілісність програмного середовища, періодичне тестування засобів захисту інформації. Такі засоби захисту повинні володіти гнучкими засобами налаштування і можливістю віддаленого адміністрування.

Рівень захисту локальних мереж і мережевих серверів повинен забезпечувати:

ідентифікацію користувачів і встановлення автентичності доступу в систему, до компонентів;

захист аутентифікаційних даних;

встановлення аутентичності при доступі до серверів;

пропуск аутентифікаційної інформації від одного компонента до іншого без перевстановлення аутентичності доступу.

Засоби захисту інформації повинні мати модульну структуру, кожен модуль повинен підтримувати область пам'яті для власного виконання. Для кожного модуля системи захисту інформації, кожного компонента системи захисту інформації, розділеного в автоматизовану систему, повинна забезпечуватися ізоляція ресурсів, що потребують захисту так, щоб вони підкорялися контролю доступу і вимогам ревізії.

Рівень захисту корпоративної автоматизованої системи повинен гарантувати:

1. Цілісність передачі інформації від її джерел до адресата:

аутентифікацію;

цілісність комунікаційного поля;

неможливість відмови партнерів по зв'язку від факту передачі або прийому повідомлень.

2. Безвідмовність у наданні послуг:

безперервність функціонування;

стійкість до атак типу «відмова в обслуговуванні»;

захищений протокол передачі даних.

3. Захист від несанкціонованого розкриття інформації:

збереження конфіденційності даних за допомогою механізмів шифрування;

вибір маршруту передачі.

На даний час в основному застосовується семірівнева модель OSI яка для опису кібербезпеки використовує рівні тобто це ієрархічна модель і це є недоліком. На противагу такому підходу у 2013 році був розроблений стандарт мережевої безпеки ISO 27000. Модель кібербезпеки ISO 27000 використовує для опису категорій безпеки, а не рівні як OSI. Модель кібербезпеки ISO не є ієрархічною, вона однорангова. В неї кожен домен напряму пов'язаний з іншим доменом. Усього таких доменів дванадцять. Ці дванадцять доменів служать для організації кібербезпеки крупних масивів інформації на високому рівні. Стандарт являє собою практичні рекомендації по наступних дванадцяти доменах що охоплюють всі аспекти мережевої безпеки [3]:

оцінка ризиків;

політика безпеки;

організація інформаційної безпеки;

послуга Asset Manadgement;

безпека кадрової служби;

фізична безпека і безпека умов роботи;

керування передаванням даних та операціями;

придбання, розробка та обслуговування інформаційних систем;

управління доступом;

управління розслідуванням подій інформаційної безпеки;

управління безперервністю бізнес-процесів;
відповідність нормативним вимогам.

Проаналізувавши домени я дійшов висновку, що рекомендації по забезпеченню інформаційної безпеки підприємства доцільно розробляти по чотирьох напрямах: захист систем та пристроїв, безпека серверів, забезпечення захисту мережі та фізична безпека. Розглянемо рекомендації детально.

Захист систем та пристроїв ґрунтується на укріпленні хоста, захист бездротових мереж, захист даних на хостах, керування вмістом і образами, фізичний захист робочих станцій. Засоби для виконання таких завдань наведені на рис. 3.

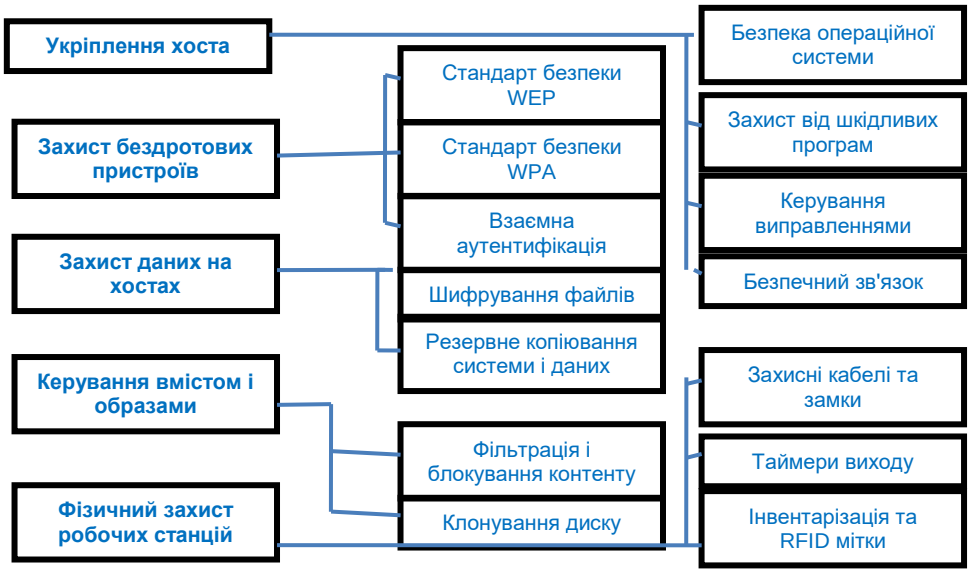

Рисунок 3. Організація захисту систем та пристроїв.

Укріплення захисту серверів полягає у відповідних адміністративних заходів, безпечний віддалений доступ та фізичний захист серверів. Засоби укріплення захисту серверів показано на рис. 4.

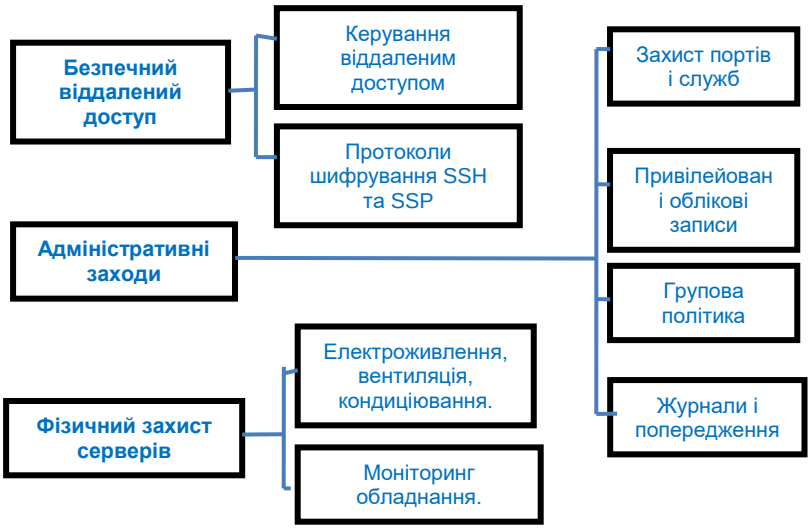

Рисунок 4. Рекомендації щодо укріплення захисту серверів

Рекомендації по укріпленню мережі схематично зображені на рис. 5.

Рисунок 5. Рекомендації по укріпленню мережі

Фізична безпека полягає у забезпеченні фізичного контролю та доступу і організації спостереження рис. 6.

Рисунок 6. Фізична безпека

Всі фізичні засоби контролю доступу, включаючи системи стримування та виявлення, в кінцевому підсумку залежать від персоналу, який повинен втручитися та припинити фактичний напад або вторгнення. На об'єктах з системою інформаційної охорони високого рівня, доступ до особливо важливих зон організації контролюється охоронцями. Перевага використання охоронців полягає в тому, що вони можуть адаптуватися краще, ніж автоматизовані системи. Це є кращим рішенням для контролю доступу, коли ситуація вимагає миттєвої і адекватної реакції. Однак охоронці не завжди є найкращим рішенням. Існують численні недоліки використання охоронців, включаючи витрати і неможливість контролювати і реєструвати великий обсяг трафіку. Використання охоронців також вносить фактор людської помилки.

Відеоспостереження і спостереження з використанням електронних засобів

Відеоспостереження і спостереження з використанням електронних засобів може доповнити, а в деяких випадках і замінити охоронців. Переваги відеоспостереження або

спостереження з використанням електронних засобів - це можливість відслідковувати зони навіть за відсутності охоронців або персоналу, здатність записувати та реєструвати відео та дані спостереження протягом тривалого періоду часу, а також можливість використання детекторів руху та сповіщення (рис. 3.19).

Крім того, можна забезпечити більш високу точність фіксації подій навіть після того, як вони відбулися. Іншою важливою перевагою цього типу забезпечення безпеки є можливість вести спостереження з точок, важкодоступних для охоронців. Також може бути набагато економічніше використовувати камери для моніторингу всього периметру об'єкта. В добре захищеній організації відеоспостереження або спостереження з використанням електронних засобів повинні бути розміщені на всіх входах, виходах, вантажних відсіках, сходах та місцях збирання сміття. У більшості випадків ці системи доповнюють охоронців.

Висновок

Підсумовуючи викладене необхідно відмітити, що застосування доменного підходу для побудови системи мережевої безпеки більш доцільніше ніж використання моделі OSI. Такий підхід дозволить глибше охопити складові інформаційно-телекомунікаційної системи.

Перелік посилань

1. А. Астахов. Аналіз захищеності корпоративних автоматизованих систем /А. Астахов. – Москва, 2010.
2.Standart ISO 27000 - https://intercert.com.ua/articles/regulatory-documents/210-iso-27000
3. Безпека корпоративних мереж - https://www.cisco.com/c/ru_ru/solutions/enterprise-networks/enterprise-network-security/index.html

Надійшла: 29.01.2020 Рецензент: д.т.н., професор Гайдур Г.І.