ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

«АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ»

Збірник тез доповідей науково – технічної конференції
26 жовтня 2018 року
(Частина 2)

Київ – 2018

«Актуальні проблеми інформаційної та кібернетичної безпеки»: тези доповідей науково – технічної конференції навчально-наукового інституту захисту інформації Державного університету телекомунікацій (Частина 2) – Київ: - ДУТ, 2018 – 9с.

Збірник містить тези доповідей науково – технічної конференції «Актуальні проблеми інформаційної та кібернетичної безпеки» від 26 жовтня 2018 року навчально-наукового інституту захисту інформації Державного університету телекомунікацій. Пропонує тези студентів, що висвітлюють перспективи розвитку інформаційної та кібернетичної безпеки в світі.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

ЗМІСТ

СУЧАСНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В КАБЕЛЬНИХ СИСТЕМАХ ЗВ’ЯЗКУ

Марунченко С.О., СЗДМ-61
Державний Університет Телекомунікацій
Савченко В.А.

Зараз мережа являється одним із основним засобів обміну інформацією, а отже її захист дуже важливий, бо втрата інформації може завдати неповторних збитків, а також тягти за собою важку відповідальність.

У сучасному суспільстві інформація може бути не тільки помічником, а й зброєю. Поширення комп'ютерних систем і об'єднання їх в комунікаційні мережі підсилює можливості електронного проникнення в них. У всіх країнах світу існує проблема комп'ютерної злочинності, що викликає необхідність залучення все більшої уваги і сил для організації боротьби з даним видом злочинів. Особливо великий розмах злочину отримали в автоматизованих банківських системах і в електронній комерції. За зарубіжними даними, втрати в банках в результаті комп'ютерних злочинів щорічно складають багато мільярдів доларів.

Для зменшення шкоди потрібно грамотно вибирати заходи і засоби забезпечення захисту інформації від крадіжки, навмисного руйнування, несанкціонованого доступу, псування, читання і копіювання. Необхідне знання основних законодавчих положень в цій галузі, економічних, організаційних та інших заходів.

Кабельна лінія зв'язку - лінія проводового зв'язку з передаванням повідомлень по кабелю.

Кабельні лінії зв'язку – лінії зв'язку, що складаються з направлених середовищ передачі (кабелі), призначені спільно з провідними системами [3].

Під організацією зв'язку тут мається на увазі організація каналів:

1. телефонного зв'язку
2. факсимільного зв'язку
3. передачі даних
4. технологічного зв'язку
5. інших.

Раціональне розташування апаратури та технічних засобів в енергетичному приміщенні може суттєво вплинути як на результуючу напруженість електромагнітного поля усередині приміщення, так і на результуюче електромагнітне поле за його межами. Раціональне розташування передбачає перестановку окремих елементів обладнання приміщень або окремих груп апаратів та технічних засобів з тим, щоб нове розташування приводило до взаємокомпенсації напруженості електромагнітних полів небезпечних сигналів в заданих зонах.

Раціональне розміщення апаратури в окремих випадках може бути визначальним.

Для реалізації заходів з раціонального розташування апаратури та іншого обладнання енергетичних приміщень з точки зору ослаблення ПЕМВН необхідно:

- мати методику розрахунку електромагнітних полів групи джерел небезпечних сигналів;

• мати методи формалізації та алгоритми розв’язання оптимізацій них задач розташування апаратури.

Захист від витоку інформації за рахунок побічних електромагнітних випромінювань найрізноманітнішого характеру передбачає:

• розташування джерел і засобів на максимально можливому віддалені від меж контрольованої (охоронної) зони;

• екранування будівель, приміщень, засобів кабельних комунікацій;

• використання локальних систем, що не мають виходу за межі території, що охороняється (у тому числі вторинних годинникових систем, систем радіофікації, телефонних систем внутрішнього використання, диспетчерських систем, систем енергоживлення і т.ін.);

• розв’язку по колах живлення та заземлення, розташованих в межах охоронної зони;

• використання фільтрів придушення в інформаційних колах та колах живлення.

Найближчим часом прогрес в області розвитку засобів обчислювальної техніки, програмного забезпечення і мережевих технологій дасть поштовх до розвитку засобів забезпечення безпеки, що потребують багато в чому переглянути існуючу наукову парадигму інформаційної безпеки. Основними положеннями нового погляду на безпеку повинні бути:

• Дослідження і аналіз причин порушення безпеки комп'ютерних систем;

• Розробка ефективних моделей безпеки, адекватних сучасної ступеня розвитку програмних і апаратних засобів, а також можливостям зловмисників і руйнують програмних засобів;

• Створення методів і засобів коректного впровадження моделей безпеки в існуючі обчислювальні системи, з можливістю гнучкого управління, безпекою в залежності від висунутих вимог, допустимого ризику та витрати ресурсів;

• Необхідність розробки засобів аналізу безпеки комп'ютерних систем за допомогою здійснення тестових впливів (атак).

Список літератури:

1. Володин А.В., Устинов Г.Н., Алгулиев Р.М. Как обеспечить безопасность систем передачи данных.//Технологии и средства звязи: Каталог. - С. 90-92.
2. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Связьиздат, 1962. – 390 с.

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В ERP-СИСТЕМАХ ПРОГРАМНИМ СПОСОБОМ

Тринєєв Н., СЗДМ-61
Державний Університет Телекомунікацій
Савченко В.А.

Багато компаній по мірі зростання бізнесу приходять до розуміння, що їм потрібні спеціалізовані системи для автоматизації їх роботи. Таким програмним продуктом є ERP-система. Якщо в малому бізнесі вдається обійтися без цього інструменту, то середній бізнес з кожним днем активніше користується подібними засобами. Але щоб вибрати ERP-систему, і навіть для того, щоб розуміти, чи потрібно в бізнесі цей продукт і які переваги принесе його використання, важливо правильно розуміти, що це таке.

ERP (англ. Enterprise Resource Planning, планування ресурсів підприємства) - організаційна стратегія інтеграції виробництва і операцій, управління трудовими ресурсами, фінансового менеджменту і управління активами, орієнтована на безперервну балансування і оптимізацію ресурсів підприємства за допомогою спеціалізованого інтегрованого пакета прикладного програмного забезпечення, що забезпечує загальну модель даних і процесів для всіх сфер діяльності.

Розмірковуючи про інформаційну безпеку в ERP, можна почати з визначення цілей, яких ми хочемо досягти в своїй системі. Отже, цілі і завдання інформаційної безпеки:

• зменшення ризиків втрати / розкриття інформації;

• відповідність державним і внутрішньо корпоративних нормам захисту інформації;

• захист цілісності даних;

• гарантія конфіденційності внутрішньої інформації підприємства.

Сучасна ERP-система має триланкову клієнт-серверну архітектуру.

Три рівня такої системи - це:

• рівень бази даних (БД);

• рівень додатків;

• рівень представлення (призначений для користувача).

Зберігання даних здійснюється в базі даних (рівень БД), їх обробка - на сервері додатків (рівень додатків) і, нарешті, безпосередню взаємодію з користувачем відбувається через програму «Клієнт» з графічним інтерфейсом (рівень представлення). У ролі такої клієнтської програми останнім часом часто використовується веб-браузер.

Забезпечення тій чи іншій мірі захищеності інформації можливо на кожному з цих рівнів, питання лише у вимогах, пропонованих до кінцевої системі. У роботі ми познайомимося з існуючими механізмами захисту інформації на рівнях ERP, а які з них використовувати - залежить від конкретного проекту.

Сполучним середовищем для компонентів, що знаходяться на різних архітектурних рівнях ERP, є мережева інфраструктура. У підсумку, розмірковуючи про інформаційну безпеку, умовно можна виділити наступні основні аспекти:

• мережева безпека;

• безпеку БД;

• безпеку на рівні сервера додатків;
• захист інформації на клієнтському комп'ютері.

Висновок: в роботі буде розглянуто поняття ERP – системи, особливості та види захисту ERP-систем, також буде звернута увага на основні джерела безпеки та цілісності ERP – систем.

Список літератури:

1. Юрий Зырянов – 2009. - http://citcity.ru/16501/
2. Columbus– 2016. - https://sites.columbusglobal.com/ru-ru/news/2016/09/statya-ob-ugrozah-erp

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЛАСУ 2 НА ОСНОВІ СУЧАСНИХ ТЕХНОЛОГІЙ ВІДЕОСПОСТЕРЕЖЕННЯ

Сенченко О., СЗДМ-61
Державний Університет Телекомунікацій
Савченко В.А.

В теперішній час в провідних країнах світу склалася досить чітко окреслена система концептуальних поглядів на проблеми забезпечення інформаційної безпеки. Проте, як свідчить реальність, злочинні дії над інформацією не тільки не зменшуються, але і мають досить стійку тенденцію до зростання. Розуміючи це, більшість керівників підприємств і організацій вживають заходи щодо захисту важливої для них інформації за рахунок створення комплексних систем захисту інформації на основі сучасних технологій відеоспостереження.

Метою є: обґрунтувати важливість інтегрування систем відеоспостереження у комплексні системи захисту інформації в автоматизованих системах класу 2.

Задачею є: обґрунтування необхідності створення КСЗІ в АС; обґрунтування необхідності інтегрування систем відеоспостереження в КСЗІ.

У даному питанні розглядається вплив систем відеоспостереження в комплексній системі захисту інформації для запобігання несанкціонованого доступу та зняттю секретної інформації.

Для вирішення завдань захисту інформації створюється комплексна система захисту інформації (КСЗІ). Під інформаційною безпекою будемо розуміти стан захищеності інформаційного середовища підприємства, який забезпечує його функціонування і розвиток в інтересах організації. Управління інформаційною безпекою – це сукупність заходів, призначених для досягнення і підтримання стану захищеності. Проблема створення системи захисту інформації включає два взаємодоповнюючі завдання: 1) розроблення системи захисту інформації (її синтез), 2) оцінка розробленої системи захисту інформації. Друге завдання вирішується шляхом аналізу її технічних характеристик з метою встановлення, чи задовольняє система захисту інформації комплексу вимог до даних систем. Таке завдання в даний час вирішується майже виключно експертним шляхом за допомогою сертифікації засобів захисту інформації та атестації системи захисту інформації в процесі її впровадження.

Для підвищення ефективності роботи КСЗІ в АС потрібно впроваджувати встановлення в них прихованих систем відеоспостереження з детектором руху. Серед переваг прихованих систем відеоспостереження с детектором руху слід виділити в першу чергу той факт, що її камери непомітні сторонньому оку, а це означає, що контроль безпеки буде вище, як і шанси виявити зловмисника. Іншою перевагою використання систем відеоспостереження є можливість збереження та відтворення записаної інформації з камер.

Так як злочинні дії над інформацією не тільки не зменшуються, але і мають досить стійку тенденцію до зростання, мають розроблятися комплексні системи захисту інформації в автоматизованих системах, актуальність яких була обґрунтована в даному питанні. Для підвищення ефективності роботи КСЗІ в АС в них мають встановлюватися приховані системи відеоспостереження з детектором руху. Серед переваг яких слід виділити в першу чергу той факт, що їх

камери непомітні сторонньому оку, а це означає, що контроль безпеки буде вище, як і шанси виявити зловмисника. Іншою перевагою використання систем відеоспостереження є можливість збереження та відтворення записаної інформації з камер.

НАУКОВЕ ВИДАННЯ

«АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ»

Збірник тез доповідей науково – технічної конференції 26 жовтня 2018 року
(Частина 2)

Адреса оргкомітету:
Україна, 03680, Київ, вул. Солом'янська, 7, тел. (044) 249-25-91
Державний університет телекомунікацій, Київ
e-mail: amina.zidan13@gmail.com