Тези доповідей 54-ї наукової конференції молодих дослідників ОНПУ-магістрантів «Сучасні інформаційні технології та телекомунікаційні мережі» // Одеса: ОНПУ, 2019, вип.54

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ ТА ЦІЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ И ЦЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

COMPREHENSIVE SYSTEM OF INFORMATION PROTECTION AT ENTERPRISES AND OBJECTIVES OF INFORMATION SECURITY

Науковий керівник – доцент кафедри РТП
Старцев В. І., Старцев В. И., Startsev V.I.,
Студент – Погоріла О.Д., Погорелая Е.Д., Pohorila O.D.

Анотація: розглянуто поняття інформаційної системи, створення комплексної системи захисту інформації на підприємстві та цілі інформаційної безпеки.

Ключові слова: інформаційна безпека, комплексна система захисту, конфіденційність, цілісність, доступність.

Аннотация: рассмотрено понятие информационной системы, создание комплексной системы защиты информации предприятия и цели информационной безопасности.

Ключевые слова: информационная безопасность, комплексная система защиты, конфиденциальность, целостность, доступность.

Abstract: the concept of an information system, the creation of an integrated enterprise information security system and the goals of information security are considered.

Keywords: information security, integrated security system, privacy, integrity, accessibility.

Інформаційна система представляє собою організаційно-технічну систему, в якій реалізується технологія збереження, збирання, пошук, оброблення та пересилання інформації з використанням технічних і програмних засобів.

При створенні комплексної системи захисту інформації необхідно враховувати, що інформацію слід захищати у всіх видах її існування — документальному, електронному, що міститься і обробляється в автоматизованих системах (АС) і окремих засобах обчислювальної техніки (ЗОТ); це відноситься і до персоналу, який обробляє інформацію.

Також необхідно вживати заходи щодо захисту інформації від витоку технічними каналами. При цьому необхідно захищати інформацію не тільки від несанкціонованого доступу (НСД), але і від неправомірного втручання в процес її обробки, зберігання та передачі на всіх фазах, порушення працездатності АС і ЗОТ, впливу на персонал і т.п.

Всі заходи інформаційної безпеки спрямовані на вирішення хоча б однієї з трьох цілей:

— захищати конфіденційність даних;

— зберігати цілісність даних;

— сприяти доступності даних для дозволеного використання.

Ці цілі формують тріаду конфіденційності, цілісності, доступності (КЦД), основу всіх програм безпеки. Фахівці з інформаційної безпеки, які створюють політики і процедури, повинні враховувати кожну мету при створенні плану захисту комп'ютерної системи.

Принцип захисту інформаційної безпеки, конфіденційності, цілісності та доступності неможливо переоцінити: він є центральним для всіх досліджень і практик в області інформаційної безпеки.

Моделі цілісності забезпечують чистоту і достовірність даних, захищаючи системні дані від навмисних або випадкових змін, та мають три мети:

— заборонити неавторизованих користувачам вносити зміни в дані або програми;

— забороняє авторизованим користувачам вносити неправильні або несанкціоновані зміни;

— підтримувати внутрішню і зовнішню узгодженість даних і програм.

Прикладом перевірок цілісності є балансування пакета транзакцій, для того, аби переконатися, що вся інформація присутня і точно врахована.

Моделі доступності дозволяють зберігати дані і ресурси для санкціонованого використання, особливо під час надзвичайних ситуацій або лих. В інформаційній безпеці зазвичай вирішуються три загальні проблеми доступності:

— відмова в обслуговуванні (DoS) через навмисні атаки або через невиявлені недоліки в реалізації (наприклад, програми, написаної програмістом, який не знає про нестачу, що може привести до аварійного завершення програми при виявленні певного несподіваного введення);

— втрата можливостей інформаційної системи через стихійні лиха (пожежі, повені, шторми або землетруси) або людські дії (бомб або ударів);

— відмови обладнання при нормальному використанні.

Деякі дії, які зберігають конфіденційність, цілісність і / або доступність, надають доступ тільки авторизованому персоналу, застосовують шифрування до інформації, яка буде відправлена через Інтернет або зберігається на цифровому носії, періодично перевіряють безпеку комп'ютерної системи для виявлення нових вразливостей, створюють програмне забезпечення для захисту і розробки плану аварійного відновлення, щоб гарантувати, що підприємство може продовжувати існувати в разі аварії або втрати доступу зі сторони персоналу.

Список літератури

1. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення.
2. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
3. Гайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. — К.: Вид. група BHV. - 2009. — 608 с.
4. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч.1 / С. В. Кавун, В. В. Носов, О. В. Мажай. – Харків: Вид. ХНЕУ. - 2008. – 352 с.
5. Ленков, С. В. Методы и средства защиты информации. В 2-х томах / Д. А. Перегудов, В. А. Хорошко. — К.: Арий, 2008, — Т. I. — 464 с.
6. Ленков, С. В. Методы и средства защиты информации. В 2-х томах / Д. А. Перегудов, В. А. Хорошко. — К.: Арий, 2008, — Т. II. — 344 с.
7. 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.
8. 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.

9. 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.
10. 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.
11. Сиропятов, О. А. Система контролю та управління доступом співробітниківпідприємства / О. А. Сиропятов, О. С. Стрєльцов // Сучасні інформ. технології та телекомунікац : тези доп. 53-ої наук. конф. молодих дослідників ОНПУ-магістрантів, м. Одеса, 2018 р. - Одеса, 2018. - Т.4, вип. 53. - С. 4-6.
12. Сиропятов, О. А. Сравнительный анализ теоретических подходов моделирования трафика с точки зрения соответствия сетям нового поколения / О. А. Сиропятов, В. Я. Чечельницкий // Інформатика та мат. методи в моделюванні. - 2013. - Т. 4, № 1. - С. 57-67.
13. Задорожнюк, Н. О. Дослідження методів стратегічного аналізу / Н. О. Задорожнюк, Г. В. Пустова // Економіка. Фінанси. Право. – Київ, 2017. – № 11/2. – С. 52–53.