DOI: https://doi.org/10.36910/6775-2524-0560-2020-41-22
УДК: 004.7.056.5
Бортник Катерина Яківна, к. ф.-м. н., доцент
https://orcid.org/0000-0001-5282-099X
Делявський Михайло Володимирович, д. т. н., професор
Кузьмич Олена Іванівна, к. ф.-м. н., доцент
https://orcid.org/0000-0002-8717-4497
Багнюк Наталія Володимирівна, к. т. н., доцент
https://orcid.org/0000-0002-7120-5455
Чернящук Наталія Леонідівна, д. п. н., професор
https://orcid.org/0000-0002-3178-8377
Луцький національний технічний університет, м. Луцьк, Україна

ОСНОВНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЙНИХ СИСТЕМ

Бортник К.Я., Делявський М.В., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л. Основні загрози безпеці інформаційних систем. В даній статті проведено актуальний аналіз основних загроз безпеці інформаційних систем, серед яких - загрози порушення конфіденційності інформації, порушення цілісності інформації, загрози порушення працездатності системи. Виконано дослідження підходів реалізації безпеки інформації автоматизованих систем, наведено відповідні статистичні дані. Проаналізовано шляхи перешкоджанню витоку інформації, забезпечення її цілісності, розроблено принципи проектування ефективної системи захисту даних.
Ключові слова: загроза безпеці, інформаційна система, кібербезпека, система захисту даних

Бортник К.Я., Делявский М.В., Кузьмич А.И., Багнюк Н.В., Чернящук Н.Л. Основные угрозы безопасности информационных систем. В данной статье проведен актуальный анализ основных угроз безопасности информационных систем, среди которых - угрозы нарушения конфиденциальности информации, нарушение целостности информации, угрозы нарушения работоспособности системы. Выполнены исследования подходов реализации безопасности информации автоматизированных систем, приведены соответствующие статистические данные. Проанализированы пути препятствия утечки информации, обеспечения ее целостности, разработаны принципы проектирования эффективной системы защиты данных.
Ключевые слова: угроза безопасности, информационная система, кибербезопасность, система защиты данных

Bortnyk K.Ya., Deliavskyi M.V., Kuzmych O.I, Bahniuk N.V, Chernyashchuk N.L. The main threats to the security of information systems. This article provides an up-to-date analysis of the main threats to the security of information systems, including - threats to the confidentiality of information, violation of the integrity of information, threats to the system. The research of approaches of realization of information security of automated systems is carried out, the corresponding statistical data are presented. Ways to prevent information leakage, ensure its integrity are analyzed, the principles of designing an effective data protection system are developed.
Key words: security threat, information system, cybersecurity, data protection system.

Постановка проблеми та аналіз досліджень. Перевід інформаційних комунікацій в електронну форму останнім часом призвів до створення самостійного типу активу – інформацію, і як будь-яка цінність, вона підлягає захисту від шахраїв. У зв'язку з цим виникають суттєві ризики в галузі безпеки інформації. Ігнорування таких проблем призводить до втрати конкурентоспроможності на державному і на корпоративному рівнях. Таким чином, актуальність загроз збереження і конфіденційності інформації вимагає уважного ставлення до питань її захисту.

Актуалізуючи завдання виявлення загроз інформаційної безпеки зауважимо наступне. Суб'єкт інформаційних відносин може постраждати чи отримати шкоду як від поломки системи, так і від зловмисного доступу несанкціонованого користувача. Таким чином, інформаційна безпека є одним з найважливіших аспектів на всіх рівнях - національному, галузевому, корпоративному, персональному. Саме тому дослідження основних загроз безпеці інформації є актуальною задачею, яка має практичну цінність та потребує рішення. Найбільш небезпечні загрози інформаційної безпеки - це внутрішні загрози. Проведемо аналіз досліджень [7-9], які відображають стан інформаційної безпеки в організаціях. Індекс небезпеки витоку внутрішньої інформації в організаціях на 50% випереджає аналогічний показник для будь-якої з зовнішніх загроз. Державні структури і представники приватного сектора заявляють про витік інформації, наслідком чого є прямі фінансові збитки (46%), удар по репутації (42,3%) і втрата клієнтів (36,9%). В цьому контексті, як зазначено в дослідженнях [10] найбільш ефективним засобом захисту від загроз інформаційної безпеки є комплексні інформаційні продукти (44,8%), на другому місці - організаційні заходи (25,3%), тренінги персоналу (21,6%) і обмеження зв'язку з зовнішніми мережами становлять 18,1%.

© Бортник К.Я., Делявський М.В., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л.

Таким чином, проблеми кібербезпеки набувають все більшої актуальності. За останній час кількість витоків і крадіжок даних зросла, причому це трапляється на робочих місцях, мобільних, IoT-пристроях. Результати останніх досліджень [1-3] показують, що зростає не тільки кількість витоків даних, але і їх масштабність. В цьому контексті, в даній роботі проведено актуальний аналіз основних загроз безпеці інформації сучасної інформаційної системи та дослідження підходів забезпечення їх безпеки. Розглядаються шкідливі програми, віруси-шифрувальники, витік інформації, цільові атаки (APT), злом сайтів, DDoS, нові загрози для мобільних пристроїв, віртуальних і хмарних середовищ.

Виклад основного матеріалу дослідженя. Інформаційна система — це сукупність організаційних і технічних засобів для збереження та обробки інформації для забезпечення потреб користувачів. Тому реалізація інформаційної безпеки підрозуміває захист інтересів суб'єктів інформаційних відносин. При найактуальнішими напрямками є конфіденційність, цілісність та доступність. Тому важливим є захищеність інформації та інфраструктури від випадкових або навмисних впливів. Такі впливи можуть завдати неприйнятного збитку суб'єктам інформаційних відносин. Зауважимо, що правильний з методологічної точки зору науковий підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем.

Аналіз типів загроз безпеці інформаційної системи. Важливим чинником класифікації загроз безпеці інформації інформаційно-технічних систем є сучасна статистика, яка відіграє в цьому контексті визначальну роль. Згідно звіту корпорації Microsoft в 2007 році приблизно 60% всіх комп'ютерних систем були атаковані програмними загрозами [3]. Наведемо деякі статистичні дані. У 2016 році з'ясувалося, що дані 3 мільярдів акаунтів Yahoo потрапили в руки зловмисників. До цього дня цей витік вважають одним з найсерйозніших за останній час. Також в 2016 році Uber повідомила, що кіберзлочинці отримали доступ до інформації клієнтів і водіїв, ці дані налічували понад 57 мільйонів записів. В 2017 році 412 мільйонів облікових записів користувачів сервісу для дорослих FriendFinder були також викрадені в ході кібератаки. 2017 рік також відзначився найбільшою компрометацією даних 147,9 мільйонів американців через злом бюро кредитних історій Equifax. Зловмисники використовували вразливість у системі безпеки програми на веб-сайті компанії і отримали доступ до номерів соціального страхування, дат народження, адрес і в ряді випадків до номерів водійських посвідчень.

За статистикою 2017 року компанії Cisco, в США сталося понад 130 великомасштабних витоків в результаті націлених кібератак, і цей показник за рік виріс на 27%. Крім того, 31% організацій зіткнулися з кібератаками на інфраструктуру експлуатаційних технологій. Більше 400 000 комп'ютерів щонайменше в 150 країнах були вражені вірусом WannaCry в 2017 році. Цей вірус-вимагач коштував світу збитків, які оцінюються в 4 мільярди доларів. Більш того, 5,4 мільярда атак WannaCry були заблоковані за весь 2017 рік. Близько 24 000 шкідливих мобільних додатків блокуються щодня. У 2017 році середня кількість скомпрометованих даних по світу становила 24 089. Найбільша кількість витоків відбувалося в Індії (більше 33 тисяч файлів), на другому місці - США (28,5 тисяч). У березні 2018 року було викрадено дані користувачів мобільного додатку MyFitnessPal. Американська компанія Under Armour, якій належить цей додаток, повідомила про близько 150 мільйонів постраждалих. Також з 1 січня 2005 року по 18 квітня 2018 було зареєстровано 8 854 випадків витоків.

Проаналізуємо статистику найбільш поширених типів кібератак, а також джерела їх реалізації. Найбільше програм-вимагачів було зафіксовано в країнах з найбільш доступним для населення інтернетом. США тримає серед них перше місце з 18,2% від усіх атак шкідливих програм такого типу. Знаменитий троян Ramnit в значній мірі торкнувся фінансового сектору. Також, у 2017 році 53% атак Ramnit припали саме на цю галузь. Більшість шкідливих доменів (близько 60%) пов'язані зі спам-кампаніями. У 74% компаній є більше 1000 застарілих чутливих файлів. Шкідливі програми і мережеві атаки – це є два найбільш збиткових для компаній типи атак, і організації витратили в середньому $ 2,4 мільйона на захист від них. Файли Microsoft Office (наприклад, Word, PowerPoint і Excel) представляють найпоширенішу групу шкідливих розширень - 38% від загальної суми. Близько 20% шкідливих доменів є абсолютно нові, вони використовуються приблизно через тиждень після реєстрації. Більше 20% кібератак в 2017 році були здійснені з Китаю, 11% з США і 6% з Росії. Серед додатків для музики та аудіо зловмисних є 20%. У період з 2015 по 2017 рік від націлених кібератак найбільше постраждали США - були зареєстровані 303 великомасштабні атаки. У 2017 році загальний обсяг шкідливих програм зріс на 88%. У числі найбільш виявлених шкідливих

© Бортник К.Я., Делявський М.В., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л.

програм знаходяться Heur.AdvML.C, Heur.AdvML.B і JS.Downloader. До 2020 року кількість використовуваних людьми і машинами паролів зросла до 300 мільярдів.

За метою впливу розрізняють наступні типи загроз, а саме - *загрози порушення конфіденційності інформації; загрози порушення цілісності інформації; загрози порушення працездатності системи* (відмови в обслуговуванні).

Порушення конфіденційності, доступності і цілісності ресурсів можуть бути викликані небезпечними впливами на систему. Небезпечні впливи на ІС можна поділити на *випадкові* та *зловмисні*. Аналіз досвіду експлуатації інформаційних систем показує, що інформація піддається різним випадковим впливам на всіх етапах функціонування інформаційної системи.

Причинами *випадкових впливів* можуть бути: Аварії можуть бути спричинені: надзвичайними ситуаціями, пов'язаними зі стихійними лихами та перебоями в електромережі; несправності та несправності обладнання; помилки в програмному забезпеченні та роботі користувача; поломки в лініях зв'язку, спричинені впливом навколишнього середовища.

Умисні погрози пов'язані з навмисними діями злочинця. Порушником може бути працівник, відвідувач, конкурент, працівник і т. д. Дії порушника можуть бути викликані різними мотивами: невдоволення працівника своєю кар'єрою, матеріальна зацікавленість, цікавість, конкуренція, прагнення до самоствердження тощо.

Несанкціонований доступ є найпоширенішим та різнобічним видом шкідливих порушень, зокрема це: перехоплення паролів, «маскарад» - незаконне використання привілеїв.

Перехоплення паролів здійснюється спеціально розробленими програмами. Коли законний користувач намагається увійти в систему, програма-перехоплювач імітує на екрані логін користувача та пароль, які надсилаються власнику програми-перехоплювача, після чого відображається повідомлення про помилку і управління повертається в операційну систему. Користувач вважає, що допустив помилку при введенні пароля. Він повторює вхід і отримує доступ до системи. Власник програми-перехоплювача, отримавши логін та пароль законного власника, тепер може використовувати їх у своїх цілях. Є й інші способи перехоплення паролів.

«Маскарад» - це виконання деяких дій одним користувачем від імені іншого, який має відповідні повноваження. Метою «маскараду» є приписування деяких дій іншому користувачеві або надання повноважень та привілеїв іншому користувачеві.

Прикладами здійснення «маскараду» є:

- вхід під іменем та паролем іншого користувача (такому «маскараду» передує перехоплення пароля);
- надсилання повідомлень по мережі від імені іншого користувача.

«Маскарад» особливо небезпечний в електронних платіжних системах, де неправильна ідентифікація клієнта через "маскарад" зловмисника може призвести до великих втрат законного клієнта банку.

Незаконне використання пільг. Більшість систем безпеки встановлюють певні набори привілеїв для виконання певних функцій. Несанкціоноване вилучення привілеїв, таких як "маскарад", призводить до можливості правопорушнику виконати певні дії, щоб обійти систему захисту. Слід зазначити, що незаконне вилучення привілеїв можливе або за наявності помилок в системі захисту, або через недбалість адміністратора в управлінні системою та призначенні привілеїв.

Давайте розглянемо загрози, з якими можуть зіткнутися комп'ютерні мережі. Головною особливістю будь-якої комп'ютерної мережі є те, що її компоненти розподіляються в просторі. Коли зловмисник потрапляє в комп'ютерну мережу, зловмисник може використовувати як пасивні, так і активні методи вторгнення.

У разі пасивного вторгнення (перехоплення інформації) порушник лише спостерігає за проходженням інформації через канал зв'язку, не втручаючись в інформаційний потік або зміст інформації. Як правило, зловмисник може ідентифікувати пункти призначення та ідентифікатори або лише факт повідомлення, його довжину та частоту обміну, якщо вміст повідомлення неможливо розпізнати - для аналізу трафіку (потоку повідомлень) у цьому каналі.

Під час активного вторгнення порушник прагне замінити інформацію, передану в повідомленні. Він може вибірково модифікувати або змінювати повідомлення, затримувати або змінювати порядок повідомлень. Зловмисник може також скасувати та затримати всі повідомлення, передані по каналу. Такі дії можна кваліфікувати як відмову надсилати повідомлення.

Комп'ютерні мережі характеризуються тим, що крім звичних локальних атак, які здійснюються в рамках єдиної системи, на об'єктах мережі здійснюються так звані віддалені атаки. Зловмисник може знаходитися на відстані тисяч миль від об'єкта, який атакується, і не лише

© Бортник К.Я., Делявський М.В., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л.

конкретний комп'ютер може бути атакований, але й інформація, що передається через мережеві канали зв'язку. Віддалена атака означає зловмисний вплив інформації на розподілену комп'ютерну мережу, що здійснюється програмно за допомогою каналів зв'язку

Шляхи реалізації загроз. Дамо коротку характеристику розповсюджених загроз безпеці інформаційних систем, які систематизовані в Таблиці 1. Нижче показані основні шляхи реалізації загроз безпеці системи при впливі на її компоненти. Ця таблиця дає тільки загальну картину того, що може відбутися з системою, а конкретні обставини та особливості повинні розглядатися окремо.

Таблиця 1
Шляхи реалізації загроз безпеці ІС

Об'єкти впливу	**Порушення конфіденційності інформації**	**Порушення цілісності інформації**	**Порушення працездатності системи**
Апаратні засоби	Несанкціонований доступ – підключення; використання ресурсів; викрадення носіїв	Несанкціонований доступ – підключення; використання ресурсів; модифікація, зміна режимів	Несанкціонований доступ – зміна режимів; виведення з ладу; пошкодження
Програмне забезпечення	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – впровадження „троянських коней", „вірусів", „черв'яків"	Несанкціонований доступ – спотворення; знищення; підміна
Дані	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – спотворення; модифікація	Несанкціонований доступ – спотворення; знищення; підміна
Персонал	Розголошення; передача відомостей про захист; халатність	„Маскарад"; вербування; підкуп персоналу	Покидання робочого місця; фізичне усунення

«Троянський кінь» - це програма, яка, крім дій, описаних у його документації, виконує і інші дії, що призводять до порушень безпеки системи та руйнівних результатів. Небезпека "троянського коня" - це додатковий блок команд, вбудований в оригінальну утиліту, який надається користувачам. Цей блок команд може бути запущений, коли виникає умова (дата, стан системи). Користувач, який запускає таку програму, загрожує ресурсами.

Ось кілька руйнівних дій, реалізованих «троянськими конями»:

- знищення інформації. Вибір об'єктів і способів знищення визначається уявою та цілями автора шкідливої програми;
- перехоплення та передача інформації. Зокрема, існують програми, які перехоплюють паролі, набрані на клавіатурі;
- цілеспрямована модифікація тексту програми, що реалізує функції безпеки та захисту системи.

Загалом, «троянські коні» завдають збитків ІР, викрадаючи інформацію та чітко пошкоджуючи програмне забезпечення системи. Троянський кінь - одна з найнебезпечніших загроз безпеці ІВ. Радикальним способом захисту від цієї загрози є створення закритого середовища для програм, які необхідно зберігати та захищати від несанкціонованого доступу. Однак установка нового програмного забезпечення на ваш комп'ютер повинна дозволятися лише адміністраторам, чого зазвичай важко досягти.

Комп'ютерні «віруси» - це програми, які можуть заражати інші програми, модифікуючи їх, включаючи модифіковану копію програми, остання зберігає здатність до розмноження. Ключовими поняттями у визначенні комп'ютерного вірусу є здатність вірусу самостійно відтворювати та модифікувати код заражених програм.

Мережевий хробак - це тип вірусної програми, яка поширюється по глобальній мережі. Перші версії "черв'яків" були розроблені для пошуку в мережі інших комп'ютерів з безкоштовними

© Бортник К.Я., Делявський М.В., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л.

ресурсами для забезпечення розподілених обчислень. Мережеві хробаки - найнебезпечніший тип шкідливого програмного забезпечення, оскільки вони можуть атакувати будь-яку з величезної кількості комп'ютерів, підключених до Всесвітньої павутини або інших мереж. Для захисту від «хробака» використовуються засоби блокування несанкціонованого доступу до внутрішньої мережі.

Слід зазначити, що «троянські коні», комп'ютерні віруси та мережеві "хробаки" є одними з найбільш небезпечних загроз для ІР. Для захисту від шкідливих програм необхідно вжити низку заходів:

- виключення несанкціонованого доступу до виконуваних файлів;
- тестування нових програм;
- контролювати цілісність виконуваних файлів та системних областей;
- створення закритого середовища для виконання програми.

Впровадження безпеки інформаційних систем. Основною метою інформаційної системи є збір, зберігання, обробка та видача інформації, і тому проблема інформаційної безпеки є центральною для ІС. Забезпечення безпеки ІВ передбачає організацію протидії будь-якому несанкціонованому вторгненню в роботу ІВ, а також спроби модифікувати, викрасти, відключити або знищити його компоненти - захист усіх компонентів ІВ - апаратного забезпечення, програмного забезпечення, даних та персоналу. Існує два підходи до проблеми безпеки ІВ: фрагментарний та складний.

Фрагментарний підхід спрямований на протидію чітко визначеним загрозам у певних умовах. Прикладами такого підходу є індивідуальні засоби контролю доступу, окремі засоби шифрування, спеціалізовані антивірусні програми тощо. Перевагою цього підходу є висока селективність до конкретної загрози. Істотним недоліком цього підходу є відсутність єдиного захищеного середовища обробки інформації. Фрагментарні заходи інформаційної безпеки захищають конкретні об'єкти ІВ лише від конкретної загрози. Навіть невеликі модифікації загрози призводять до втрати ефективності захисту.

Комплексний підхід орієнтований на створення безпечного середовища обробки інформації в ІВ, яке поєднує в собі різноманітні заходи для боротьби із загрозами. Інтегрований підхід використовується для захисту ІВ великих організацій, а також для малих ІВ, які виконують відповідальні завдання або обробляють особливо важливу інформацію. Більшість державних та великих комерційних підприємств та установ дотримуються комплексного підходу. Комплексний підхід до безпеки базується на специфічній політиці безпеки щодо ІС. Політика безпеки реалізується за допомогою адміністративних та організаційних заходів, фізичних та програмно-апаратних засобів і визначає архітектуру систем безпеки.

Висновки.

Таким чином, при проектуванні ефективної системи захисту слід враховувати ряд принципів, що відображають основні положення з безпеки інформації. Серед них - економічна ефективність, мінімум привілеїв. Наступними є простота, можливість примусового відключення захисту, відкритість проектування та функціонування механізмів захисту, загальний контроль, незалежність системи від суб'єктів захисту, звітність та підконтрольність. Важливими принципами є відповідальність, ізоляція та розподіл, повнота та узгодженість. Надійна система захисту повинна бути повністю сертифікована і протестована. Найважливіші та критичні рішення повинні прийматися людиною. Існування механізмів захисту повинно бути, наскільки це можливо, приховане від користувачів, робота яких повинна контролюватися.

Все частіше фахівці з кібербезпеки під час аналізу систем безпеки інформації ІС більшість уваги, коштів і засобів спрямовують на запобігання атаки саме суб'єктивних (навмисних) програмних загроз. При цьому в більшості випадків апаратні джерела загроз майже не розглядаються. Експерти-розробники інтуїтивно покладаються на достатньо високий рівень надійності сучасних аналогових і цифрових пристроїв та, відповідно, малу ймовірність здійснення атаки об'єктивних апаратних загроз. Також враховується і висока надійність загальноприйнятих технічних обмеженнь безпосереднього доступу людини до ІС з метою засобів захисту інформації ІС, що майже повністю унеможливлює реалізацію апаратних загроз. Таким чином, прогнозуємо подальше зменшення впливу апаратних і стрімкий зріст програмних загроз безпеки інформаційних систем, що вимагає проведення аналізу, вдосконалення нормативної бази, розробки нових принципів побудови і організації сучасних системи безпеки інформації. Тому, при аналізі проблематики, пов'язаної з інформаційною безпекою, необхідно враховувати специфіку той факт, що інформаційна безпека є складовою частиною інформаційних технологій, що розвиваються надзвичайно високими темпами. Тут важливі як окремі

© Бортник К.Я., Делявський М.В., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л.

рішення, серед яких закони, навчальні курси, програмно-технічні засоби, так і механізми генерації нових рішень, що дозволяють їх реалізовувати в темпі сучасного технічного прогресу.

Список бібліографічного опису

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посібн. — К.: Видавн. дім. «КМ Академія», 2003. — 244 с.
2. Хорошко В.О., Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки / За ред. проф. В.О. Хорошка. - К.: ДУІКТ, 2008.- 186 с.
3. Беловєд Н.І., Петровська Н.А. Мережні атаки і захист від них // Збірник наукових статтей "Управління розвитком". – Вип. 7'2008. – Х.: ХНЕУ, 2008. – С. 21-22.
4. Бєлозьоров Є.В. Спосіб забезпечення цілісності та безпеки обробки даних користувача в інформаційних системах // Матеріали III Міжнародної науково-технічної конференції "Сучасні інформаційно-комунікаційні технології /COMINFO'2007/". – К.: ДУІКТ, 2007. – С. 261-264.
5. Дóренський О.П. Дослідження потенційних загроз безпеці інформації інформаційної системи та аналіз їх класифікаційного поділу // Збірник наукових праць Кіровоградського національного технічного університету. – Вип. 19. – Кіровоград: КНТУ, 2007. – С. 55-61.
6. Аналітика [Електронний ресурс] — Режим доступу https://www.anti-malware.ru/analytics/Threats_Analysis
7. Астахов А. Анализ защищенности корпоративных автоматизированных систем // Jet Info [Електронний ресурс] — Режим доступу: www.jetinfo.ru\2002\7\1\article1.7.2002.html
8. Доля А. Внутренние угрозы ИТ-безопасности. // Byte-Россия [Електронний ресурс] — Режим доступу:: www.bytemag.ru/?ID=603365
9. Доля А. Внутренние ИТ-угрозы в России 2006 // КомпьютерПресс N 5, 2007.
10. Грудзаев С. Полезные мелочи - Aladdin Security Solution // LAN [Електронний ресурс] — Режим доступу:: http://www.osp.ru/lan/2008/05/5068377/
11. V.Satsyk R.Grudetsky, O.Kuzmych, N.Bahniuk, L.Hlynchuk Y.Melnychuk Reduction of Server Load by Means of CMS Drupal // IEEExplore Digital Library, Published in: 2020 10th International Conference on Advanced Computer Information Technologies, Deggendorf, 16-18 September 2020.

References

1. Antonyuk A.O. Fundamentals of information protection in automated systems: Textbook. manual - K .: V. House. "KM Academy", 2003. - 244 p.
2. Khoroshko V.O., Cherednichenko B.C., Shelest M.E. Fundamentals of Information Security / Ed. prof. V.O. Horoshko. - K .: ДУІКТ, 2008.- 186 c.
3. Beloved N.I., Petrovskaya N.A., Network attacks and protection against them // Collection of scientific articles "Development Management". - No. 7'2008. - Kh .: KhNEU, 2008. - P. 21-22.
4. Belozerov E.V. The method of ensuring the integrity and security of user data processing in information systems // Proceedings of the III International Scientific and Technical Conference "Modern Information and Communication Technologies / COMINFO'2007 /". - K .: ДУІКТ, 2007. - pp. 261-264.
5. Dorensky O.P. Research of potential threats to information system information security and analysis of their classification division // Collection of scientific works of Kirovograd National Technical University. - No. 19. - Kirovograd: KNTU, 2007. - P. 55-61.
6. Analytics [Electronic resource] - Access mode https://www.anti-malware.ru/analytics/Threats_Analysis
7. Astakhov A. Analysis of security of corporate automated systems // Jet Info [Electronic resource] - Access mode: www.jetinfo.ru \ 2002 \ 7 \ 1 \ article1.7.2002.html
8. Share A. Internal threats to IT security. // Byte-Russia [Electronic resource] - Access mode :: www.bytemag.ru/?ID=603365
9. Share A. Internal IT threats in Russia 2006 // ComputerPress N 5, 2007.
10. Grudzaev S. Useful little things - Aladdin Security Solution // LAN [Electronic resource] - Access mode :: http://www.osp.ru/lan/2008/05/5068377/
11. V.Satsyk R.Grudetsky, O.Kuzmych, N.Bahniuk, L.Hlynchuk Y.Melnychuk Reduction of Server Load by Means of CMS Drupal // IEEExplore Digital Library, Published in: 2020 10th International Conference on Advanced Computer Information Technologies , Deggendorf, 16-18 September 2020.

© Бортник К.Я., Делявський М.В., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л.