МАТЕРІАЛИ V МІЖНАРОДНОЇ СТУДЕНТСЬКОЇ НАУКОВОЇ

КОНФЕРЕНЦІЇ

СУЧАСНІ АСПЕКТИ ТА ПЕРСПЕКТИВНІ НАПРЯМКИ РОЗВИТКУ НАУКИ

М. ЖИТОМИР, УКРАЇНА

9 ЧЕРВНЯ 2023 РІК

МОЛОДІЖНА НАУКОВА ЛІГА

МАТЕРІАЛИ V МІЖНАРОДНОЇ СТУДЕНТСЬКОЇ НАУКОВОЇ

КОНФЕРЕНЦІЇ

СУЧАСНІ АСПЕКТИ ТА ПЕРСПЕКТИВНІ НАПРЯМКИ РОЗВИТКУ НАУКИ

м. Житомир, Україна
9 червня 2023 рік

Вінниця, Україна
«Європейська наукова платформа»
2023

УДК 001(08)
С 89

Голова оргкомітету: Коренюк І.О.

Верстка: Зрада С.І.
Дизайн: Бондаренко І.В.

Конференцію зареєстровано Державною науковою установою «УкрІНТЕІ» в базі даних науково-технічних заходів України та бюлетені «План проведення наукових, науково-технічних заходів в Україні» (Посвідчення №83 від 17.01.2023).

С 89 **Сучасні аспекти та перспективні напрямки розвитку науки**: матеріали V Міжнародної студентської наукової конференції, м. Житомир, 9 червня, 2023 рік / ГО «Молодіжна наукова ліга». — Вінниця: ГО «Європейська наукова платформа», 2023. — 224 с.

ISBN 978-617-8126-54-4
DOI 10.36074/liga-inter-09.06.2023

Викладено матеріали учасників V Міжнародної мультидисциплінарної студентської наукової конференції «Сучасні аспекти та перспективні напрямки розвитку науки», яка відбулася 9 червня 2023 року у місті Житомир, Україна.

УДК 001 (08)

ISBN 978-617-8126-54-4

СЕКЦІЯ 11.
ЕЛЕКТРОНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

СЕКЦІЯ 12.
КОМП'ЮТЕРНА ТА ПРОГРАМНА ІНЖЕНЕРІЯ

Чупахін Денис Олександрович, здобувач вищої освіти факультету інформаційних радіотехнологій і технічного захисту інформації
Харківський національний університет радіоелектроніки, Україна

Науковий керівник: Штих Інна Анатоліївна, старший викладач кафедри радіотехнологій інформаційно-комунікаційних систем
Харківський національний університет радіоелектроніки, Україна

ОСНОВНІ ПРАВИЛА ЗАБЕЗПЕЧЕННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ

Захист інформації в комп'ютерній мережі ефективніше в тому випадку, коли проектування і реалізація системи захисту проходить в три етапи [1]:

- аналіз ризику;
- реалізація політики безпеки;
- підтримка політики безпеки.

На першому етапі аналізуються вразливі елементи комп'ютерної мережі, визначаються і оцінюються загрози і підбираються оптимальні засоби захисту. Аналіз ризику закінчується прийняттям політики безпеки. Політикою безпеки (Security Policy) називається комплекс взаємопов'язаних заходів, спрямованих на забезпечення високого рівня безпеки. У теорії захисту інформації вважається, що ці заходи повинні бути спрямовані на досягнення такого [1]:

- конфіденційність (засекречена інформація повинна бути доступна тільки тому, кому вона призначена);
- цілісність (інформація, на основі якої приймаються рішення, повинна бути достовірною та повною, а також захищена від можливих ненавмисних і злочинних спотворень);
- готовність (інформація і відповідні автоматизовані служби повинні бути доступні і в разі необхідності готовності до обслуговування).

Оцінка ймовірності появи даних загроз і очікуваних розмірів втрат - важке завдання. Ще складніше визначити вимоги до системи захисту. Політика безпеки повинна визначатися наступними заходами [2]:

- ідентифікація, перевірка справжності та контроль доступу користувачів на об'єкт, в приміщення, до ресурсів автоматизованого комплексу;
- поділ повноважень користувачів, що мають доступ до обчислювальних ресурсів;
- реєстрація та облік роботи користувачів;
- реєстрація інформації на основі криптографічних алгоритмів високої стійкості;
- зміна цифрового підпису для передачі інформації по каналах зв'язку; забезпечення антивірусного захисту (у тому числі і для боротьби з невідомими вірусами) і відновлення інформації, зруйнованої вірусними впливами;
- контроль цілісності програмних засобів та оброблюваної інформації;
- відновлення зруйнованої архівної інформації, навіть при значних втратах;
- наявність адміністратора (служби) захисту інформації в системі;

- вироблення і дотримання необхідних організаційних заходів;
- застосування технічних засобів, що забезпечують безперебійну роботу устаткування.

Другий етап - реалізація політики безпеки. Починається з проведення фінансових витрат і вибору відповідних засобів для виконання цих завдань. При цьому необхідно врахувати такі фактори як безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість отримання повної інформації про механізми захисту і надані гарантії. Крім того, слід враховувати принципи, в яких відображені основні положення з безпеки інформації [1].

Підтримка політики безпеки - третій, найбільш важливий, етап. Заходи, що проводяться на даному етапі, вимагають постійно спостереження за що відбуваються вторгненнями в мережу зловмисників, виявлення "дірок" в системі захисту об'єктів інформації, обліку випадків несанкціонованого доступу до конфіденційних даних. При цьому основних відповідальність за підтримання політики безпеки мережі лежить на системному адміністраторі, який повинен оперативно реагувати на всі випадки злому конкретної системи захисту, аналізувати їх і використовувати необхідні апаратні і програмні засоби захисту з урахуванням максимальної економії фінансових коштів [1].

Список використаних джерел:

1. Максименко В. Н., Даньков А.П., Шекурова Е. Е. Методы защиты систем и сетей от несанкционированного доступа. / «Институт сотовой связи», 2004. – 358 с.
2. Филин С.А. Информационная безопасность: учебное пособие. / С.А. Филин – М.: «Вильямс», 2006. – 246 с.

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ V МІЖНАРОДНОЇ
СТУДЕНТСЬКОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ

«СУЧАСНІ АСПЕКТИ ТА ПЕРСПЕКТИВНІ НАПРЯМКИ РОЗВИТКУ НАУКИ»

9 червня 2023 рік • м. Житомир, Україна

Українською та англійською мовами

Всі матеріали пройшли перевірку на плагіат та експертизу за формальними ознаками (форматування, стиль мови, оформлення цитувань та списку використаних джерел). За точність викладеного матеріалу відповідальність несуть автори та їх наукові керівники. Організаційний комітет не завжди поділяє позицію авторів.

Підписано до друку 09.06.2023.
Папір офсетний. Цифровий друк. Формат 60×84/16.
Гарнітура Times New Roman, Poiret One та Arial.
Умовно-друк. арк. 13,02. Замовлення № 378.
Тираж: 100 екземплярів. Віддруковано з готового оригінал-макету.

Контактна інформація організаційного комітету:
Громадська організація «Молодіжна наукова ліга»
21037, Україна, м. Вінниця, вул. Зодчих, 40, офіс 103
Телефони: +38 098 1948380; +38 098 1526044
E-mail: info@liga.science | URL: www.liga.science

Видавець: ГО «Європейська наукова платформа».
21037, Україна, м. Вінниця, вул. Зодчих, 18, офіс 81. E-mail: info@ukrlogos.in.ua
Свідоцтво суб'єкта видавничої справи: ДК № 7172 від 21.10.2020.