ЗБІРНИК МАТЕРІАЛІВ XI ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ МОЛОДИХ ВЧЕНИХ «НАУКОВА МОЛОДЬ-2023»

21 листопада 2023 року

scientific YOUTH

Рада молодих вчених НАПН України,
Рада молодих учених при МОН України,
Рада молодих вчених Інституту цифровізації освіти НАПН України,
Рада молодих вчених Інституту соціальної та політичної психології НАПН України,
Рада молодих вчених Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України,
Рада молодих вчених Івано-Франківського національного технічного університету нафти і газу,
Рада молодих вчених Державного науково-дослідного інституту МВС України,
Рада молодих вчених Міжрегіональної Академії управління персоналом,
Офіс підтримки вченого,
Рада молодих вчених ДНУ «Український інститут науково-технічної експертизи та інформації»,
Рада молодих вчених Інституту педагогічної освіти і освіти дорослих імені Івана Зязюна НАПН України,
Рада молодих вчених Національного наукового центру «Інститут аграрної економіки» НААН України,
Державний університет «Житомирська політехніка»

ЗБІРНИК МАТЕРІАЛІВ XI ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ МОЛОДИХ ВЧЕНИХ «НАУКОВА МОЛОДЬ-2023»

21 листопада 2023 року

м. Київ

УДК 378: 044 : 001.37

З 18

Збірник матеріалів XI Всеукраїнської науково-практичної конференції молодих вчених «Наукова молодь-2023» (Київ, 21 листопада 2023 р.). / упоряд.: А. Яцишин. К.: ЦП «КОМПРИНТ», 2023. 338 с.

ISBN 978-617-8282-02-8

Матеріали надруковані в авторській редакції. За достовірність фактів, посилань, відповідальність несуть автори публікацій та їх наукові керівники.

Рекомендовано до друку Вченими радами
Державної наукової установи «Український інститут науково-технічної експертизи та інформації» та Інституту цифровізації освіти НАПН України.

Збірник матеріалів містить наукові статті та тези доповідей поданих на XI Всеукраїнську науково-практичну конференцію молодих вчених «Наукова молодь-2023», що відбулася 21 листопада 2023 року. Матеріали подані на конференцію були розглянуті під час роботи таких секцій: сучасний стан і перспективи використання цифрових технологій в освіті та інших галузях; актуальні проблеми соціальної та політичної психології; освітній процес в умовах воєнного стану: проблеми та шляхи вирішення; сучасні проблеми в галузі енергетики; інтеграція молодих вчених у міжнародний науковий простір: досвід та перспективи. В рамках конференції було проведено різні заходи для молодих вчених: дискусія «Співпраця Рад молодих вчених для оптимізації зусиль у формуванні молодих дослідників»; презентація проєктів для молодих вчених; круглий стіл «Штучний інтелект для вченого: можливості та перспективи»; майстер-клас «Застосування штучного інтелекту для наукових досліджень».

Збірник адресовано всім хто цікавиться сучасними науковими дослідженнями.

Подяка. Автори публікації вдячні захисникам України за можливість продовжувати працювати та займатися науковою і викладацькою діяльністю у період війни.

З вдячністю Збройним силам України!
З вірою у перемогу України!

ISBN 978-617-8282-02-8

КІБЕРБЕЗПЕКА В СУЧАСНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ: ЗАГРОЗИ ТА ЗАХИСТ

Коломоєць Данило,
Таврійський державний агротехнологічний університет
імені Дмитра Моторного

Науковий керівник:
Холодняк Ю.В.

Актуальність та постановка проблеми. Сучасний світ заснований на обміні інформацією та використанні комп'ютерних систем. Ця залежність викликає серйозні виклики для кібербезпеки, оскільки існують безліч загроз, які ставлять під загрозу як особисті дані, так і діяльність корпорацій та держав.

Споживачі та підприємства зберігають величезні обсяги конфіденційних даних на цифрових пристроях та серверах. Це включає в себе особисті дані, фінансову інформацію, медичні записи, корпоративні секрети та багато іншого. Несанкціонований доступ до цих даних може призвести до крадіжки ідентифікаційних даних, фінансового обману, обману в інтернеті та інших злочинів [1-2].

Все більше аспектів нашого життя відбувається в онлайн-середовищі. Це стосується покупок, роботи, освіти, медицини, громадського обслуговування та багатьох інших сфер. Збільшення кількості цифрових послуг і пристроїв, що підключені до мережі, створює безліч можливостей для атак і порушень приватності.

Серйозною загрозою є інтернет-кримінальні групи та хакери, які постійно знаходять нові шляхи для атак на користувачів та організації. Не менш небезпечні загрози існують і з боку держав, які можуть використовувати кіберзброю для ведення кібервійни, розвідки та інших агресивних дій [3]. Інформаційна безпека стає не лише питанням комерції, але й національної безпеки.

Актуальність теми дослідження визначається швидким розвитком технологій і постійними змінами у сфері загроз. Незважаючи на постійний розвиток заходів для кіберзахисту, злочинці також посилюють свої атаки. В цьому контексті, дослідження кібербезпеки стає критично важливим для розробки ефективних стратегій та технологій для захисту інформації та критичної інфраструктури.

Метою дослідження є аналіз основних проблем у галузі кібербезпеки, а також основних методів та засобів для захисту інформації в сучасних комп'ютерних системах, а також розробка рекомендацій для підвищення рівня кібербезпеки в сучасних комп'ютерних системах.

Основні матеріали дослідження. Сучасна динаміка технологічного розвитку та росту використання цифрових систем відкриває широкий спектр загроз у сфері кібербезпеки. Заслуговує на увагу те, що ці загрози мають потенціал завдати серйозних шкідливих наслідків для користувачів, організацій та навіть національної безпеки. Проаналізуємо найактуальніші загрози в галузі кібербезпеки, які потребують уваги та вивчення [4]:

Віруси та Малваре. Серйозні загрози представляють віруси, троянські коні, черви та інші форми шкідливого програмного забезпечення (малваре). Ці вектори атаки намагаються вразити комп'ютери та цифрові пристрої, завдаючи шкоди даним, крадучи конфіденційну інформацію та негайно розповсюджуючи загрози.

Фішинг. Систематична загроза фішингу включає в себе соціальну інженерію, спрямовану на обман користувачів та виклик довіри. Ця форма атаки намагається витягти від користувачів конфіденційну інформацію, таку як паролі та кредитні дані, шляхом імітації надійних джерел.

Хакерські атаки. Злочинці, які впроваджують хакерські атаки, використовують різноманітні методи для проникнення в комп'ютерні системи та мережі. Це може призвести до втрати даних, фінансових збитків та навіть нелегального доступу до конфіденційної інформації.

DoS та DDoS-атаки. Атаки DoS та DDoS мають на меті перевантаження серверів та мереж, що призводить до недоступності веб-сайтів та онлайн-сервісів. Це може призвести до серйозних фінансових втрат для організацій та підприємств.

Злам паролів та аутентифікаційних даних. Незаконний доступ до системи часто досягається шляхом злому паролів або крадіжки аутентифікаційних даних, таких як логіни та паролі. Це може загрожувати конфіденційності та безпеці користувачів.

Кібершпигунство та кібервійна. Держави та кіберкримінальні групи ведуть активне кібершпигунство, спрямоване на отримання конфіденційної інформації та великих обсягів даних. Крім того, кібервійна включає в себе атаки на інфраструктуру та системи критичного інтересу, загрожуючи національній безпеці.

Інтернет речей (IoT) та підключені пристрої. Збільшення кількості підключених до мережі IoT-пристроїв створює нові вектори для атак. Недостатньо захищені IoT-пристрої можуть стати слабкими ланками у кіберзахисті та потенційними точками входу для злочинців.

Соціальні мережі та онлайн-платформи. Соціальні мережі, надаючи платформи для взаємодії та обміну інформацією, також стають ідеальними місцями для поширення дезінформації, кібербулінгу та інших форм онлайн-атак на приватність та безпеку користувачів.

Аналіз цих загроз відзначається їх надзвичайною різноманітністю і потенційною небезпекою для користувачів, підприємств та суспільства в цілому. У відповідь на ці загрози необхідно надавати відповідну увагу, розробляючи та впроваджуючи ефективні засоби кіберзахисту, що забезпечують безпеку в цифровому світі.

Забезпечення кібербезпеки в сучасних умовах вимагає постійного вдосконалення підходів та інструментів для боротьби з загрозами. Нижче ми розглянемо деякі з сучасних стратегій та підходів до кіберзахисту, а також їхню ефективність:

Сучасні системи кіберзахисту активно використовують методи виявлення загроз, які включають в себе аналіз подій, моніторинг мережі та використання розвинутих алгоритмів машинного навчання. Ці методи дозволяють виявляти надзвичайну активність, яка може свідчити про атаку, та реагувати на неї в реальному часі. Існують різні методи виявлення загроз, які можна класифікувати на кілька основних категорій [5, 6]:

Сигнатурний аналіз – метод, який використовує попередньо визначені сигнатури атак, тобто характерні патерни чи відомі аномалії. Система порівнює вхідні дані з відомими сигнатурами, і якщо знайдено співпадіння, то відбувається

сповіщення адміністратора або запускаються відповідні заходи для захисту. Один із недоліків цього методу полягає в тому, що він може бути неефективним у виявленні нових атак, які не мають відомих сигнатур.

Аналіз аномалій – метод, який базується на виявленні незвичайних або аномальних активностей, які відрізняються від звичайних моделей поведінки системи чи користувачів. Використовуються алгоритми машинного навчання для створення профілів поведінки. Цей підхід дозволяє виявити нові загрози, але може також генерувати багато хибних позитивів, що ускладнює відсіювання дійсних атак від помилок системи.

Системи відслідковування та ідентифікації користувачів – підхід передбачає моніторинг активності користувачів, включаючи їхню авторизацію, вхідні та вихідні дії. Системи відслідковування і ідентифікації можуть виявляти незвичайні спроби входу або зміни в користувацькому аккаунті, що може бути індикатором атаки або несанкціонованого доступу.

Деякі методи виявлення загроз аналізують вміст передачі даних, шукаючи патерни, які можуть вказувати на аномалії або загрози. Цей підхід часто використовується для виявлення загроз в мережах передачі даних.

Методи виявлення загроз можуть бути застосовані окремо або в поєднанні для покращення ефективності. Важливо враховувати специфічні потреби та особливості організації при виборі методів виявлення загроз і встановленні їхніх параметрів та правил.

Методи виявлення загроз виявилися дуже корисними для попередження атак та вчасної реакції на них. Однак їхню ефективність обмежена, оскільки деякі атаки можуть залишити нульовий слід, інколи важко визначити нові типи загроз.

Ще одним важливим аспектом кіберзахисту є шифрування даних. Шифрування даних полягає в перетворенні інформації в незрозумілу форму для незаконних користувачів. Використання шифрування під час передачі та зберігання даних може запобігти їх незаконному доступу.

Шифрування даних є важливим заходом кіберзахисту, але воно не завжди гарантує стовідсоткову безпеку. Все залежить від коректного впровадження та управління ключами шифрування.

Для запобігання та пом'якшення впливу DDoS-атак (атак, які переповнюють мережі чи сервери запитами) використовуються спеціалізовані пристрої та послуги, які виявляють та відсікають шкідливий трафік. Виявлення та захист від DDoS-атак ефективні, однак рівень захисту може варіюватися в залежності від потужності та методів атаки. Сучасні DDoS-атаки стають все більш сильними та розподіленими, що може призвести до обмеженого успіху виявлення та захисту.

Наступним інструментом кіберзахисту є двофакторна аутентифікація, яка вимагає від користувача надання двох видів ідентифікаційних даних для доступу, зазвичай пароля та одноразового коду. Цей підхід підвищує рівень безпеки, оскільки навіть при витоку паролів злочинцям буде важко отримати доступ, однак ефективність двофакторної аутентифікації залежить від коректного впровадження та ретельності користувачів при використанні цієї технології.

Вчасно виявляти потенційні загрози та реагувати на них допомагають системи відслідковування та ідентифікації, які використовуються для моніторингу діяльності

користувачів та виявлення аномалій у поведінці. Але успішність таких систем залежить від якості алгоритмів та точності моніторингу.

Системи кіберзахисту повинні постійно оновлюватися та навчатися виявляти нові загрози та атаки. Це включає в себе оновлення сигнатур антивірусного програмного забезпечення, аналіз нових методів атаки та вдосконалення методів виявлення. Цей підхід є критичними для ефективного кіберзахисту, оскільки загрози постійно еволюціонують. Недолуге оновлення може призвести до вразливостей.

Усі ці підходи мають свої переваги та недоліки, і вони часто використовуються в поєднанні для максимального захисту. Ефективність будь-якого підходу до кіберзахисту залежить від його правильної реалізації, а також від постійного моніторингу та оновлення для відповіді на зростаючі загрози.

В нашому аналізі ми звернули увагу на різноманітність кіберзагроз, включаючи віруси, фішинг, хакерські атаки, DDoS-атаки, злам паролів, кібершпигунство та інші. Методи виявлення загроз та системи відслідковування і ідентифікації можуть бути ефективними в виявленні широкого спектру аномалій в мережі, але їхнім недоліком є обмежена здатність реагувати на абсолютно нові типи атак, що можуть не мати відомих сигнатур.

З іншого боку, шифрування даних та двофакторна аутентифікація виявляються ефективними проти багатьох типів атак, таких як злам паролів і незаконний доступ до даних. Однак ці підходи не надають захист від інших видів загроз, наприклад, DDoS-атак, які можуть переповнити ресурси системи та мережі.

Під час порівняння різних підходів до кіберзахисту, слід враховувати складність їх впровадження. Методи виявлення загроз та системи відслідковування та ідентифікації можуть вимагати значних зусиль для налаштування і інтеграції з існуючими системами. Вони часто потребують постійного оновлення баз даних та алгоритмів для забезпечення ефективного виявлення нових загроз.

З іншого боку, впровадження двофакторної аутентифікації та шифрування даних може бути менш витратними з точки зору інтеграції з існуючими системами. Ці підходи можуть бути реалізовані швидше і дозволяють швидше покращити рівень кібербезпеки.

Для забезпечення ефективності кіберзахисту важливо постійно оновлювати методи виявлення загроз та системи відслідковування і ідентифікації. Системи цих підходів потребують постійного оновлення алгоритмів та баз даних для виявлення нових типів атак і загроз.

Двофакторна аутентифікація та шифрування даних менш залежні від постійного оновлення, оскільки їх ефективність базується на сильних криптографічних принципах. Тобто вони можуть забезпечити стійкий захист інформації і даних без постійних оновлень.

Важливим аспектом при виборі підходу до кіберзахисту є його вплив на продуктивність та зручність використання системи. Методи виявлення загроз та системи відслідковування і ідентифікації можуть призвести до підвищеного навантаження на системи та мережу через постійне моніторинг та аналіз великої кількості даних.

Використання двофакторної аутентифікації та шифрування даних може бути менш впливовим на продуктивність і зручність використання, оскільки вони в основному застосовуються на рівні індивідуальних користувачів і точно на вимогу.

Порівнюючи різні підходи до кіберзахисту, важливо враховувати різноманітність загроз та конкретні потреби організації. Жоден підхід не є універсальним, і найкращий вибір може полягати в комбінації різних методів для забезпечення комплексного захисту інформації та даних. Важливо також враховувати складність впровадження та постійне оновлення підходів для забезпечення ефективного кіберзахисту.

Висновки. Забезпечення кібербезпеки у сучасних комп'ютерних системах є критично важливим завданням, оскільки зростаюча залежність від технологій та інтернету створює нові можливості для кіберзлочинців і загроз. У світлі непередбачувого росту кібератак та інцидентів безпеки, важливо приділити належну увагу проблемі кібербезпеки та вжити заходів для захисту інформації та даних.

Аналізуючи сучасні загрози в галузі кібербезпеки, ми розглянули широкий спектр атак, включаючи віруси, фішинг, хакерські атаки, DDoS-атаки, злам паролів, кібершпигунство, а також загрози, пов'язані з Інтернетом речей та соціальними мережами. Ці загрози створюють серйозні ризики для конфіденційності, цілісності та доступності даних.

Для ефективного захисту комп'ютерних систем і мереж важливо застосовувати сучасні підходи до кіберзахисту, включаючи методи виявлення загроз, шифрування даних, виявлення та захист від DDoS-атак, двофакторну аутентифікацію, системи відслідковування та ідентифікації, постійне навчання та оновлення. Важливо розробляти і впроваджувати ефективні політики та процедури безпеки, а також мати плани реагування на інциденти та контингентності.

Захист від кіберзагроз вимагає постійного зусилля, співпраці та залучення всіх учасників у процес забезпечення безпеки. Важливо створювати культуру кібербезпеки та надавати навчання персоналу для ефективного виявлення та захисту від загроз. Крім того, обов'язково слід створювати та підтримувати системи автоматизованої ідентифікації та аутентифікації, які допомагають контролювати доступ до ресурсів та даних.

Загалом, забезпечення кібербезпеки вимагає комплексного підходу та постійного удосконалення. Тільки шляхом поєднання технологій, освіти та свідомості можна забезпечити надійний захист в цифровому світі. Насамкінець, запитання кібербезпеки стає новим актуальним завданням, яке необхідно розглядати серйозно і приділяти йому належну увагу для забезпечення стійкого функціонування сучасних комп'ютерних систем.

Список використаних джерел:

1. Bellekens X., Jayasekara G., Hindy H., Bures M., Brosset D., Tachtatzis C., Atkinson R. From cyber-security deception to manipulation and gratification through gamification. In International Conference on Human-Computer Interaction. Springer: Berlin/Heidelberg, Germany, 2019. P. 99–114.

2. Ukwandu E., Ben-Farah M.A., Hindy H., Bures M., Atkinson R., Tachtatzis C., Andonovic I., Bellekens X. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. Information. 2022. Vol. 13. No. 146. https://doi.org/10.3390/info13030146

3. Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту. Наука і оборона. 2020. № 16. С. 356-358.

4. Холодняк Ю.В., Мірошниченко М.Ю. Технології захисту інформації. Запоріжжя: ТДАТУ, 2023. 150 с.

5. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Кропивницький: Видавець Лисенко В. Ф., 2020. 295 с.

6. Дудикевич В. Б.,Хорошко В.О., Яремчук Ю.Є. Основи інформаційної безпеки. Вінниця: ВНТУ, 2018. 316 с.

****

НОВІТНІ ТЕХНОЛОГІЇ ДОПОВНЕНОЇ РЕАЛЬНОСТІ ТА ВІРТУАЛЬНОСТІ В ОСВІТНЬОМУ ПРОЦЕСІ

Кошарський Віталій, Жук Інна,
ННІУЕБ МАУП

Технології доповненої реальності (Augmented Reality, AR) здатні проєктувати цифрову інформацію (зображення, відео, текст, графіку) поза екранами пристроїв та об'єднувати віртуальні об'єкти з реальним середовищем. Популярна кілька років тому гра Pokemon GO є яскравим прикладом AR технологій. Віртуальна ж реальність (Virtual Reality, VR) за допомогою 360° картинки переносить людину в штучний світ, де навколишнє середовище повністю змінене. Познайомитись з доповненою реальністю можна за допомогою одного лише смартфона, проте для занурення у віртуальний простір вам знадобиться спеціальний шолом або окуляри [6].

На сьогодні кожен учасник освітнього процесу нашої країни так чи інакше ознайомився з використанням новітніх інформаційних технологій під час навчання. Використання месенджерів, створення груп у соціальних мережах, викладення наочного матеріалу у програмах відеоконференцій, використання все більше інструментів мультимедіа не є для когось новим чи незрозумілим. Цікавим фактом стало висвітлення у новинах інформації про приклад навчання зі застосування в VR грі «Half-Life:Alyx», що продемонстрував лектор із США. Він провів заняття з геометрії, використовуючи VR-простір: маркери, предмети оточення, скло, як інтерактивну дошку. На жаль, у вітчизняному інформаційному просторі дуже мало інформації щодо використання таких новітніх інформаційних технологій в освітньому процесі. Тематика використання AR-технологій, або ж VR-технологій не розкривається. Що це за технології і як саме їх можна використати в освітньому просторі України?

Варто зазначити, що AR-технологія давно не «ноу-хау», до прикладу, відома в усьому світі, особливо в Америці та Західній Європі, гра «Pokemon GO», яка використовує саме цю технологію, набула популярності з 2009 року. Прикладів використання, візуалізації AR-технологій було безліч в багатьох фільмах та іграх, зокрема, Batman: Arkham Asylum, де цю технологію розкривають через ігровий інтерфейс. В реальному житті ця технологія працює, по суті, таким же чином: тобто через пристрій (телефон, окуляри, проектор), який здатний сприймати цифрову інформацію (зображення, відео, текст, графіку) та проектувати додаткову цифрову інформацію поза екранами пристроїв, тобто