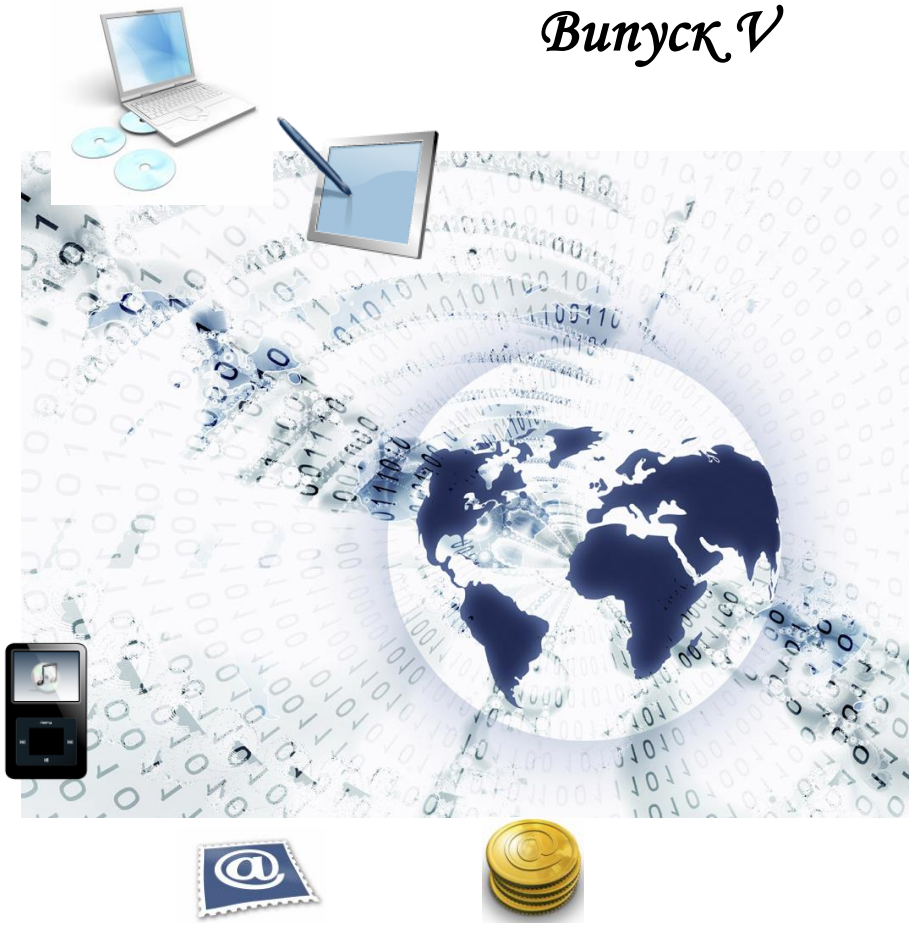
Міністерство освіти і науки України
ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут економіки, управління, права та інформаційних технологій

М А Т Е Р І А Л И

науково-практичної конференції
за підсумками проходження виробничих практик
здобувачів вищої освіти
спеціальності
126 Інформаційні системи та технології
Випуск V



кафедра інформаційних систем та технологій

28 вересня 2022 р.

Полтава – 2022

Матеріали науково-практичної конференції за підсумками проходження виробничих практик здобувачів вищої освіти спеціальності 126 Інформаційні системи та технології, кафедра інформаційних систем та технологій Полтавського державного аграрного університету, 28 вересня 2022 р. Вип. V. Полтава: ПДАУ, 42 с.

У збірнику надруковані матеріали досліджень, оприлюднених на науково-практичній конференції за підсумками проходження здобувачами вищої освіти виробничої практики «Організаційно-аналітична практика» за освітньо-професійною програмою «Інформаційні управляючі системи» спеціальності 126 Інформаційні системи та технології кафедри інформаційних систем та технологій Полтавського державного аграрного університету. У публікаціях зроблені узагальнення теоретичних знань та практичних навичок, набутих під час практики на базі підпрємств, організацій.

Відповідальність за зміст та редакцію тез несуть автори та наукові керівники.

ЗМІСТ

Синенко Владислав, здобувач СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Уткін Юрій

КРИТЕРІЇ АНАЛІЗУ САЙТІВ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

На сьогоднішній день Інтернет-ресурси вищих навчальних закладів є одним із потужних інструментів комунікаційної системи ЗВО у сфері вищої професійної освіти [1], забезпечує підвищення його рейтингу та конкурентоспроможності на ринку освітніх послуг. Інтернет-ресурс навчального закладу є його основною формою діяльності в мережі Інтернет і розуміння коректних критеріїв оцінки його функціонування допоможе уникнути помилок і багів при його використанні.

Одним з найважливіших напрямків використання Інтернет-ресурсу навчального закладу є залучення потенційних студентів, тому велика кількість інформації надається саме для абітурієнтів. У сучасних умовах головним комунікаційним інструментом виступає сайт вузу, який об'єднує в своїй структурі веб-сторінки структурних підрозділів університету, служб та співтовариств, громадських організацій та наукових спільнот, сторінок з інформаційно-довідковою інформацією, анкетування студентів і інше. Інформаційний ресурс ЗВО повинен передбачити наступні функції:

- виконувати комунікацію якісно і просто, надавати можливість зручного користування для відвідувачів;
- надавати актуальну і своєчасну інформацію та поповнення;
- рекламна функція при роботі приймальної комісії;
- система персоналізації для використання специфічної інформації через використання власних кабінетів користувача;
- забезпечувати доступ до навчальних матеріалів і наукових публікацій.

Існує багато методик оцінки роботи Інтернет-ресурсів, які розрізняються за критеріями аналізу, їх кількості тощо, в залежності від різної спрямованості конкурсів або досліджень. Оскільки на якість Інтернет-ресурсу ВНЗ впливає безліч різноманітних факторів, до оцінки ефективності роботи подібних ресурсів, необхідно підходити комплексно. На рисунку 1 представлено схематичний варіант критеріїв аналізу забезпечення якості сайту вищого навчального закладу.

Показники якості, представлені на рисунку 1 можна представити наступним чином:

1. Дизайн, стиль та графіка Інтернер-ресурсу - це набір дій, спрямованих на компетентну конструкцію вмісту, візуального дизайну сторінок, поєднання всіх його графічних елементів. Візуальне оформлення сайту - це комплекс картинок, фото, графіки, шрифтів та кольорів, які складають веб-ресурс. Важливим є вибір рішення головної сторінки сайту. Серед рекомендованих варіантів рішень можна назвати наступні:

- використання корпоративного стилю з додаванням анімаційних ефектів;

- використання неформальних ідей та/або яскравих елементів;
- дотримання балансу «текст-графіка»;
- використання кольорової гами, комфортної для сприйняття великої кількості інформації.

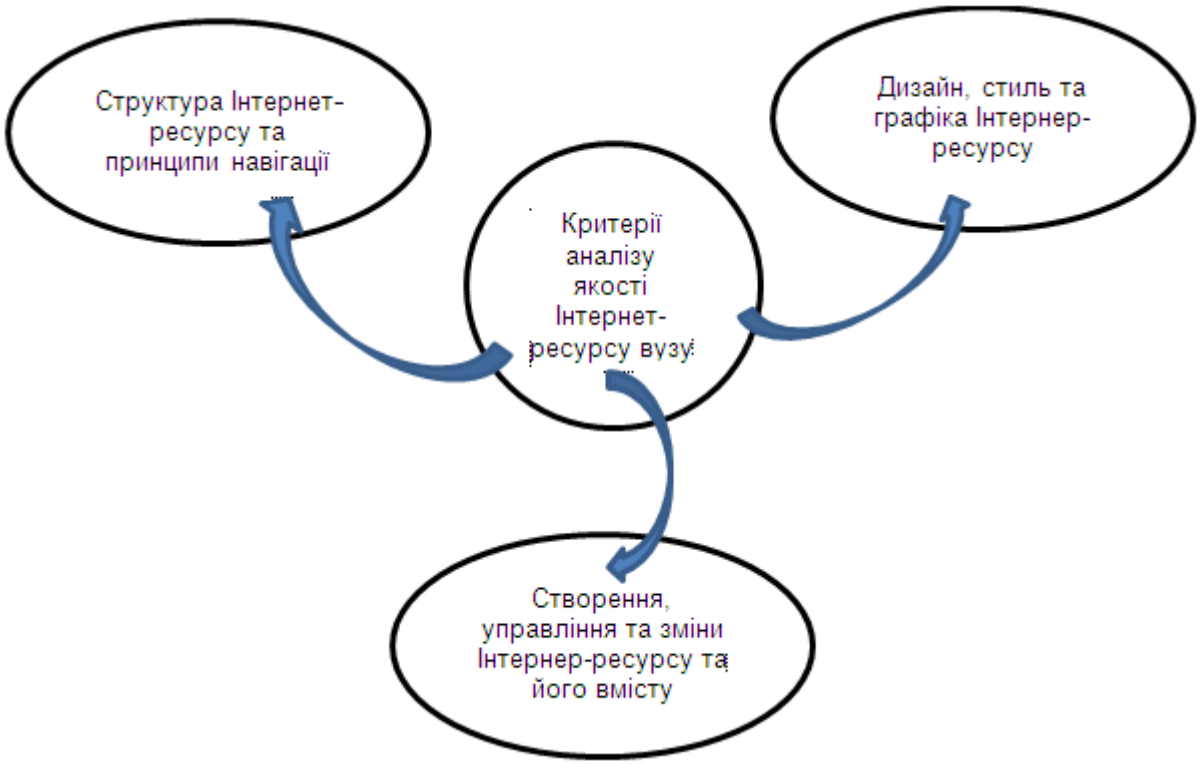


Рисунок 1 – Критерії аналізу якості Інтернет-ресурсу навчального закладу

2. Система управління вмістом (CMS) - це програмне забезпечення, яке працює у браузері [2]. Це дозволяє створювати, керувати та змінювати вміст Інтернет-порталу, сайту, ресурсу, не передбачаючи наявності специфічних знань у галузі програмування. Система управління вмістом пропонує графічний інтерфейс користувача, який дозволяє керувати всіма аспектами власного сайту: можна створювати та редагувати вміст, додавати зображення та відео, а також налаштувати загальний дизайн сайту. WordPress, Magento та Drupal - найпопулярніші CMS, які зараз присутні на ринку. CMS ще називають движком сайту. Якщо говорити просто – це основа сайту, яка керує усіма процесами, що відбуваються на веб-майданчику.

3. Структура сайту - це логічна побудова всіх сторінок сайту, категорій та підкатегорій [3]. Також можна сказати, що це логічна схема, згідно з якою всі сторінки та ділянки сайту розташовані відносно один одного та принципом, за яким вони взаємопов'язані між собою. Навігаційна структура сайту виконує важливі завдання: логічно поєднує різні інформаційні блоки, відображає поточне розташування відвідувача на сайті, забезпечує елементи управління для переїздів на сторінках сайту тощо, як правило, виділяють основну та додаткову навігацію в структурі сайту.

Організований комунікативний процес на вузівському сайті буде досягати своїх цілей і сприятливо сприйматися контактною аудиторією і відображати

позиції вузів конкурентів. Використання високотехнологічних комунікацій дозволяє переглянути ставлення до систем інформації та її прозорості, що дозволяє не тільки більш чітко визначити цільову аудиторію (абітурієнти та батьки, роботодавці, студенти, викладачі), але й значно збільшувати її кількість.

Список використаних джерел

1. Головко О. А. (2018). Інтернет-ресурс навчального закладу як освітнє медіакомунікаційне середовище. Технологія і техніка друкарства, (4(58), 2018. С. 91–98. https://doi.org/10.20535/2077-7264.4(58).2017.132674

2. Платонов І.В. Системи керування вмістом для веб-ресурсів. URL: https://vseosvita.ua/library/sistemi-keruvanna-vmistom-dla-veb-resursiv-416955.html

3. Правильна структура веб сайту під SEO: приклади, види і рекомендації з розробки структури. URL: https://www.bmb.com.ua/2021/02/seo.html

Олійник Богдан, здобувач вищої освіти СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Дегтярьова Лариса

АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ АТ КБ «ПРИВАТБАНК»

Сьогодні більшість банків працюють в Інтернеті та використовують сучасні технології інтерент-банкінгу, що дозволяють обслуговувати одночасно велику кількість клієнтів, проте такий підхід вимагає підвищених рівнів захисту інформації, бо рівень інформаційної безпеки безпосередньо впливає на популярність, надійність, кількість клієнтів та інвесторів, прибуток тощо. Тому питання безпеки в банку є одним із головних завдань та напрямків роботи ПриватБанку ним займається ІТ-відділу, який не тільки створює програмні додатки та підтримує їх, але й займається захистом ПЗ, СДО «Приват24» та банком в цілому.

Щоб з’ясувати наскільки захищений банк від кібератак, загроз витоку інформації та взагалі його безпечність. Для цього потрібно проаналізувати потенційні загрози та небезпеки за наступними факторами, як-от:

– джерела інформаційної безпеки;
– аспекти інформаційної безпеки;
– види небезпек та загроз;
– методи захисту та забезпечення інформаційної безпеки;
– рекомендації, які надає банк для необхідного рівня безпеки користування та додаткові можливості для її захищеності в разі необхідності та потреби.

Але перед тим, як приступити до налізу слід з’ясувати, що таке атака та зловмисник. Спроба реалізації загрози називається атакою, а той, хто робить таку спробу, – зловмисником. Потенційні зловмисники називаються джерелами загрози, що можуть негативно вплинути на роботу банку. І їх можна

класифікувати або поділити на різні групи залежно від різних чинників, що спричиняють надзвичайну ситуацію. Але всіх їх можна поділити на 3 чинники технічний, людський та природній (рисунок 1).

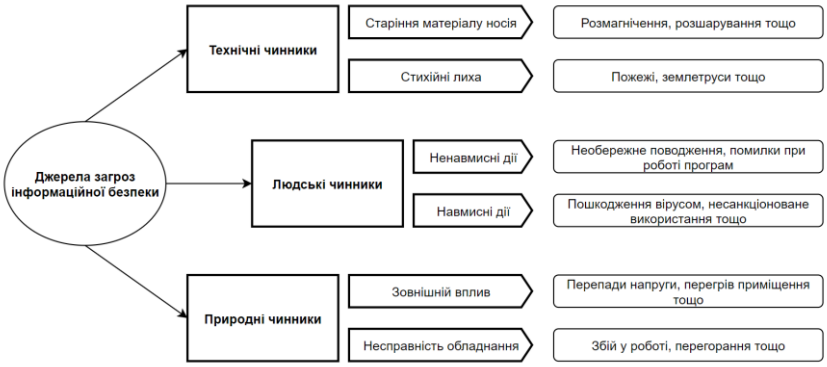


Рисунок 1. – Вигляд джерел інформаційної безпеки

Загроза інформаційної безпеки – це потенційна причина небажаного інциденту інформаційної безпеки, які може завдати шкоду банку.

За аспектом інформаційної безпеки, на який спрямовані загрози:

– загрози конфіденційності (неправомірний доступ до інформації);
– загрози цілісності (неправомірна зміна даних);
– загрози доступності (здійснення дій, що унеможливлюють чи ускладнюють доступ до ресурсів інформаційної безпеки).

Найчастішими і небезпечними є ненавмисні помилки користувачів, операторів і системних адміністраторів, які обслуговують інформаційні системи банку. Іноді такі помилки призводять до прямого збитку, а іноді створюють слабкі місця, якими можуть скористатися зловмисники (рисунок 2).

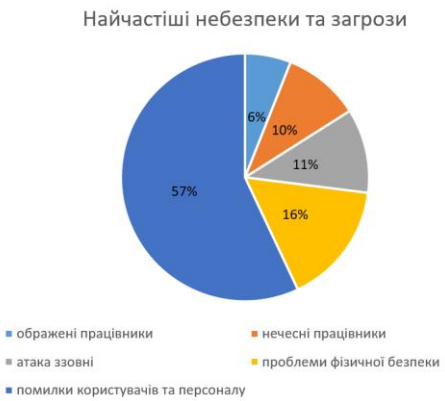


Рисунок 2. – Вигляд найчастіших небезпек та загроз

Однак, найбільші помилки все-таки роблять самі користувачі, коли повідомляють свої контактні дані злочинцям. Серед найпоширеніших прикладів шахрайства на які ведуться користувачі є [1]:

– перекази на рахунки шахраїв під їх тиском;
– телефонне шахрайство;

– інтернет-шахрайство;
– підробка сайтів;
– зняття коштів з викраденої або загубленої картки.

Щоб зменшити кількість та частоту таких небезпек банк використовує різні методи для боротьби із ними, які наведені на рисунку 3.

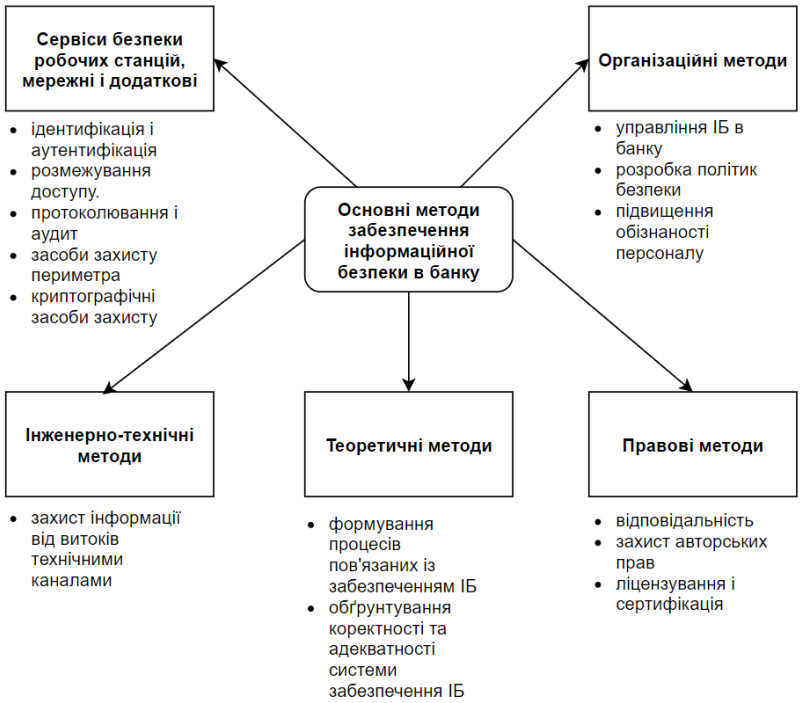


Рисунок 3. – Вигляд основних методів забезпечення інформаційної безпеки в банку

Для того, щоб протидіяти таким випадкам та ситуаціям «ПриватБанк» створює рекомендації, поради, відповіді на запитання для користувачів з привиду безпеки даних, захисту від шахрайства, фінансів тощо, які зібрані тут:

– про порядок і процедуру захисту персональних даних клієнтів ПриватБанку доступний за посиланням https://privatbank.ua/personal-information#gads-2612144;
– про захист від шахрайства та можливість її оформлення доступне за писанням https://privatbank.ua/strahovaniye/zakhyst-vid-shakhraystva;
– про захист від шахрайства для Premium користувачів доступне за URL: https://privatbank.ua/vip/fraud-protection;
– про заходи безпеки при використанні банківських продуктів надається за посиланням https://privatbank.ua/safeness;
– про інформаційну безпеку та 10 рекомендацій клієнтам надані у вільному за електронною адресом https://privatbank.ua/informational-security;
– про те як зручно та безпечно купувати в інтернеті через картки ПриватБанку тут https://privatbank.ua/udobno-bezopasno-pokupki-internet.

Дані поради в першу чергу необхідні для користувачів та нових клієнтів, щоб вони могли захистити себе від злочинних намірів, як шантаж або

шахрайства тощо. І також щоб ніхто не мав доступу до вашого рахунку на картках. Вони направлені на різні напрямки Для того, щоб протидіяти ним банк рекомендує пройти гру «Здолай Шахрая» за URL посиланням: https://game.ema.com.ua/ (рисунок 4) [2].

Рисунок 4. – Вигляд гри «Здолай Шахрая»

Гра на даний час налічує 57 рівнів (шахраїв), які необхідно пройти, щоб перевірити на скільки ви довірливі та безпечні під час покупок, замовлень та кредитування тощо. Після проходження гри у вас буде можливість витратити віртуальні монети на призи, а саме: сертифікат, який дає право на екскурсією Національним банком з відвідуванням Музею грошей та пам'ятний сувенір та доступ до курсу з фінансової грамотності «Знай про гроші».

Окрім цього, «ПриватБанк» пропонує використовувати унікальний сервіс страхування та захисту від безлічі видів шахрайства та обману клієнтів всього за 29 грн на місяць на суму 50 тисяч грн. Користувачі карток Premium курток є можливість страхувати 100 тисяч грн. за програмою Premium та 200 тисяч грн. за програмою Exclusive всього за 70 та 140 грн. відповідно [3]. Дані пропозиції допоможуть в найкоротші терміни повернути фінанси, що вкрали злочинці.

Також «ПриватБанк» дає винагороду за встановлення місця перебування шахрая, який завдав значних збитків і розшукується правоохоронними органами. За цю допомогу ви можете отримати 10 тисяч грн., а також гарантується ваша анонімність та безпека. Щоб повідомити про місце злочинця слід звернутися до найближчого відділення або написати на адресу antifraud@privatbank.ua [4].

Отже, таким чином ми дізналися про інформаційну безпеку ПриватБанку та методи захисту, які він рекомендує використовувати та застосовувати у житті, щоб не стати жертвою злочинця та зберегти свою інформацію та кошти в безпеці.

Список використаних джерел

1. Захист від шахрайства. PrivatBank : веб-сайт. URL: https://privatbank.ua/strahovaniye/zakhyst-vid-shakhraystva (дата звернення: 20.06.2022).
2. «Здолай шахрая». Game.ema : веб-сайт. URL: https://game.ema.com.ua/?utm_source=google&utm_medium=cpc&utm_campaign=game (дата звернення: 20.06.2022).
3. Захист від шахрайства. PrivatBank : веб-сайт. URL: https://privatbank.ua/vip/fraud-protection# (дата звернення: 21.06.2022).
4. Заходи безпеки при використанні банківських продуктів. PrivatBank : веб-сайт. URL: https://privatbank.ua/safeness (дата звернення: 21.06.2022).

Гладка Анастасія, здобувач вищої освіти СВО Бакалавр,
Спеціальність126 Інформаційні системи та технології
Науковий керівник – д.т.н., професор Поночовний Юрій

ЗАСОБИ ДІАГНОСТИКИ ПІДКЛЮЧЕННЯ ДО ІНТЕРНЕТУ

Оскільки на сьогоднішній день багато підприємств займається наданням послуг підключення до інтернету, то процес діагностики підключення є актуальним. Кожна людина стикається з погіршенням або навіть з зникненням сигналу Інтернету.

Спочатку розберемося, що таке інтернет. Інтернет – це велика, розгалужена (розподілена) мережа, що включає комп'ютерні вузли, розміщені у світі. Коли наш девайс підключається до мережі Інтернет, то він стає частиною всесвітньої мережі копм'ютерів. Доступ до Інтернету - це можливість користувачів та організацій підключатися до Інтернету за допомогою комп'ютерних терміналів, комп'ютерів та інших цифрових пристроїв, а також для доступу до таких служб, як електронна пошта та месенджери Глобальної мережі. [1].

Існує два важливих правила для з'єднання мереж із Інтернетом:

-усі мережі згодні використовувати єдині умовні позначки, щоб вирішити яким чином дані будуть переміщені, і як будуть оброблені помилки;

-усі мережі мають загальний спосіб адресації повідомлень і спеціальну ідентифікацію комп'ютерів, що знаходяться в системі Інтернет [2].

Для того щоб налагодити з'єднання з Інтернетом, є різні способи. Але спочатку, слід розглянути причину проблеми, діагностувати та усунути її. Близько 80% проблем із підключенням залежить від самого користувача, найбільш часто зустрічаємо є неправильні або збиті налаштування та несправне обладнання.

Іншими проблемами є: програмний збій або апаратна помилка, механічне пошкодження кабелю скрученої пари, пошкодження мережевого обладнання або проблеми провайдера.

Першим рішенням проблеми може стати діагностика неполадок стандартної програми Windows. Для застосування цього варіанту треба вибрати: Пуск > Настройки > Мережа та Інтернет > Стан (рисунок 1). Потім треба застосувати Засіб усунення неполадок мережі (рисунок 2).

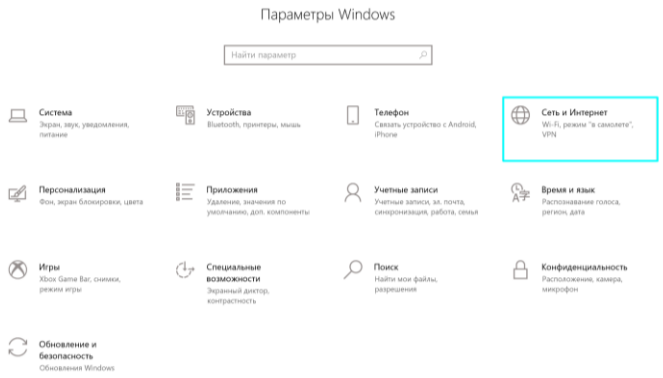


Рисунок 1. – Засіб діагностики за допомогою Windows

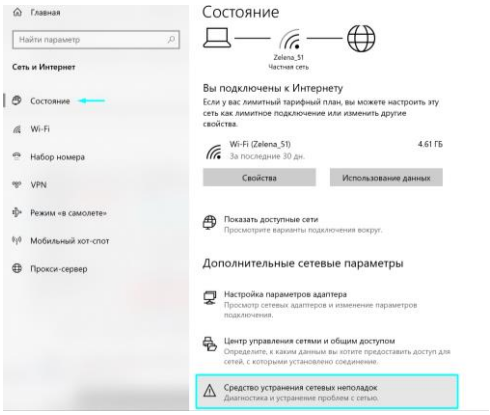


Рисунок 2. – Діагностика неполадок на мережі Windows 10

Ще один варіант діагностики це підключення іншого пристрою до мережі Інтернет. Якщо все ж таки підключення є, то проблема була в першому пристрої. В такому випадку може допомогти скидання налаштування мережі.

Також є спосіб підключення через кабель Ethernet, якщо користувач використовує бездротову мережу. Якщо все ж таки провідний інтернет є, то вся проблема може бути в налаштуваннях роутера.

Також часто зустрічаються такі проблеми як: різко знизилась швидкість доступу до інтернету (до окремих сайтів та для усіх сайтів). Якщо ця проблема стосується усіх сайтів, то Можлива причина: механічна проблема – неповний контакт на роз’ємах, пошкодження кабелю. Усунення проблеми: Вимкнути торрент-клієнт або інше програмне забезпечення, що завантажує канал зв’язку. Перевірити додатки, які можуть активно використовувати канал зв’язку – вимкнути їх або перезавантажити комп’ютер.

Якщо ж швидкість знизилась до окремого сайту, можливою проблемою є перевантаження сайту в даний момент, через велику кількість відвідувачів, що роблять закачування, або на сервері сайту встановлено обмеження швидкості передачі даних, а усунути проблему можна відклавши на деякий час

завантаження або перегляд файлів з цього сайту на інший не піковий час, або ж знайти цю інформацію на іншому сайті [3].

Отже, продіагностувавши усі можливі проблеми виникнення підключення до інтернету, можна скористуватись варіантами усунення цих проблем за допомогою вище зазначених інструкцій.

Список використаних джерел

1. Tripathy B. Internet of Things (IoT): TeChnologies, AppliCations, Challenges and Solutions (англ.) / B. Tripathy, J. Anuradha. Florida: CRC Press, 2017. 334 с.
2. Кудрявцева С.П., Колос В.В., Навчальний посібник. К.: Видавничий Дім «Слово», 2005. 400с
3. Діагностика та усунення несправностей. Магнус : веб-сайт. URL: https://magnus.net.ua/rekomendatsii/diagnostika-ta-usunennya-nespravnostej (дата звернення: 20.06.2022).

Омельченко Денис, здобувач вищої освіти СВО Бакалавр
спеціальність 126 Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Дегтярьова Лариса

АНАЛІЗ МОЖЛИВИХ ДЖЕРЕЛ І КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

Канали витоку інформації – методи та шляхи витоку інформації з інформаційної системи; паразитний (небажаний) ланцюг носіїв інформації, одним або кількома з яких (можуть бути) злочинець або його спеціальне обладнання [1].

Витік інформації відбувається відповідним каналом витоку. Оскільки засоби розвідки хакерів, як правило, технічні, то і канали витоку також називають технічними.

Технічний канал витоку інформації (ТКВІ) – сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засобу технічної розвідки (рисунок 1).

Якщо коротко сказати то, технічний канал витоку інформації є фізичним шляхом небезпечного сигналу (носієм інформації) від джерела небезпечного сигналу.

Небезпечний сигнал – це певний сигнал, який є паразитним або побічним, його компоненти містять інформацію про будь-яке фізичне походження, які мають інформацію з обмеженим доступом [2].

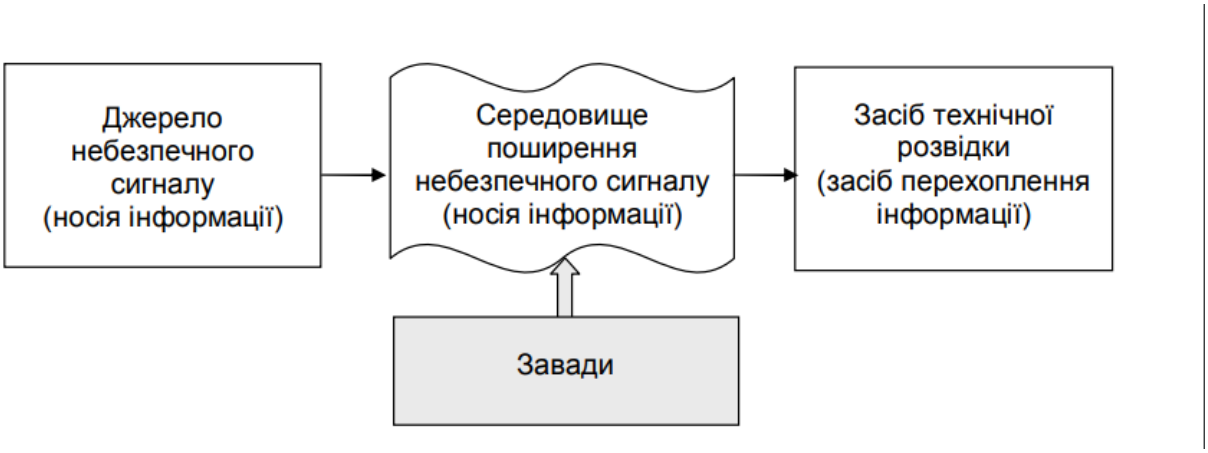


Рисунок 1. – Технічний канал витоку інформації

Носії інформації – це певні дані, які містять інформацію з обмеженим доступом. Носіями інформації можуть бути [3]:

1. електричний струм;
2. електромагнітне поле;
3. лазерний промінь;
4. вібраційне поле;
5. інші носії.

Для витоку інформації використаєм засоби технічної розвідки. Це засоби які призначені, для перехоплення інформації. Допустимо, що об’єкт інформаційної діяльності всі види робіт з інформацією: зберігання інформації, обробка інформації технічними засобами Схематично витік інформації зображено на (рисунку 2).

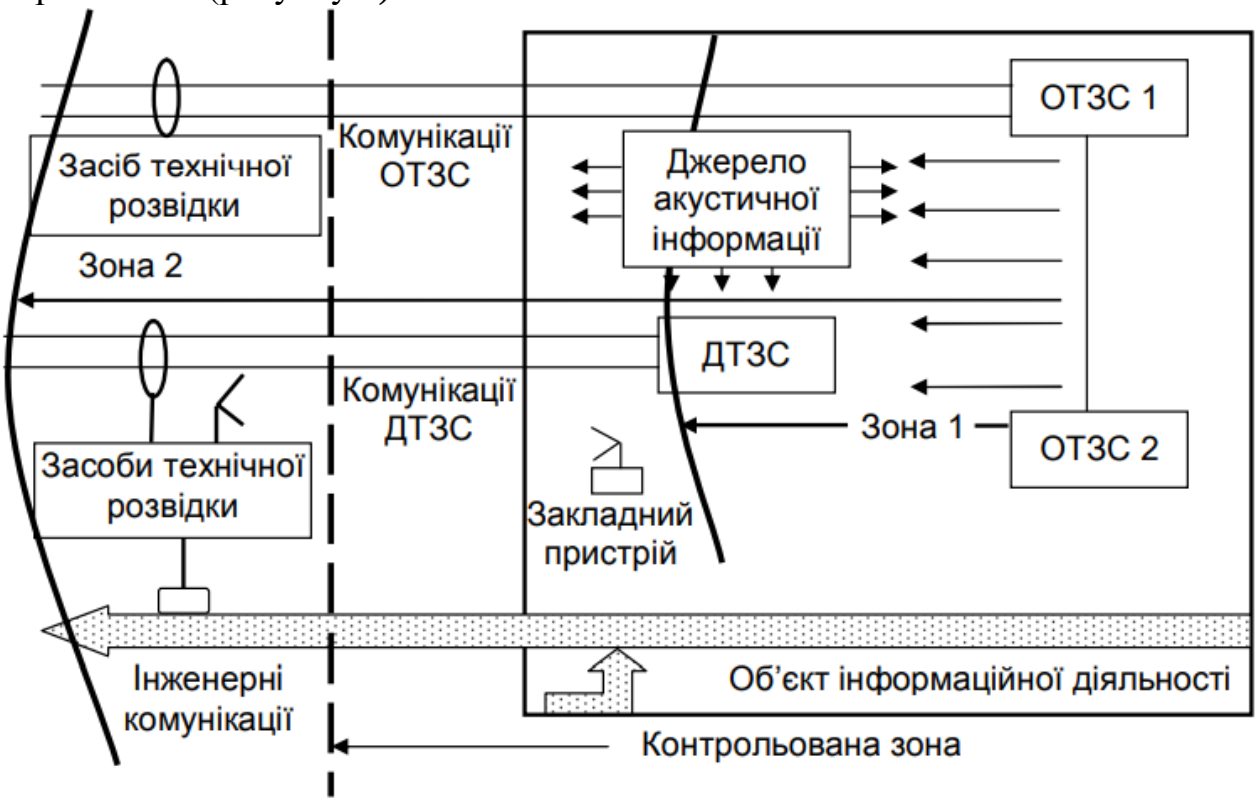


Рисунок 2. – Приклад зображення витоку інформації

Основні технічні засоби та системи (ОТЗС**)**, розташовані на об’єкті інформаційної діяльності технічні засоби та їх комунікації, які здійснюють обробку секретної інформації.

Допоміжні технічні засоби та системи (ДТЗС), розташовані на об’єкті інформаційної діяльності технічні засоби та системи і їх комунікації, які не здійснюють обробку секретної інформації, але перебувають під впливом небезпечних сигналів основних технічних засобів або небезпечних акустичних полів.

Зона 1 – територія (сфера) навколо основних технічних засобів, в межах якої здійснюється наведення небезпечних сигналів на інші технічні засоби, системи та їх комунікації, характеризується радіусом R1, що визначає граничну відстань від основних технічних засобів до межі, за якою вважається неможливим наведення небезпечних сигналів до технічних засобів.

Зона 2 – територія (сфера) навколо технічних засобів обробки інформації, за межами якої вважається неможливим перехоплення небезпечного сигналу 3 метою відтворення інформації, характеризується радіусом R2, що визначає найбільшу відстань від технічних засобів обробки інформації до межі, за якою напруженості електричного та магнітного полів небезпечного сигналу відносно шумових завад не перевищують нормованого значення. В Зоні 2 можливе перехоплення інформації, а за її межами ні (дивись рисунок 1. 2).

Зона 1 та Зона 2 є фізичними характеристиками (показниками) ОТЗС та визначаються експериментально-розрахунковим методом при спеціальних дослідженнях ОТЗС.

Таким чином слід зазначити, що для перехоплення небезпечного сигналу у вигляді електромагнітних полів необхідно навколо об’єктів інформаційної діяльності організаційно створити і забезпечити контрольовану зону, найменша відстань до межі якої від основних технічних засобів має бути більшою за радіус Зони 2 (R2).

Список використаних джерел:

1. Шевцов А. С., Іванченко С. О., Гавриленко О. В. Технічні канали витоку інформації. К: ЖІСЗЗІ НТУУ "КПІ", 2016. 104 с.

2. Рибальский О.В., Хахановський В.Г., Кудінов В.А Основи інформаційної безпеки та технічного захисту інформації. К.: Посібник для курсантів ВНЗ МВС України, 2012. 104 с.

3. Остін Т., Таненбаум Е. С. Архітектура комп’ютера. К.: Пітер Прес, 2019. 816 с.

Багрій Максим, здобувач вищої освіти СВО Бакалавр,
спеціальність «Інформаційні системи та технології»
Науковий керівник – к.ф.-м.н., професор Копішинська Олена

МОЖЛИВОСТІ WUSTPAGE

В даний час на ринку послуг веб-розробок існує доволі велика кількість різних конструкторів веб-сайтів. Проаналізувавши, можна побачити що серед найбільш популярних й відомих конструкторів Tilda, Wix, Jimdo з'явилася й чисто українська розробка під назвою WUSTpage, розробником якої саме і є ТОВ «ВЮСТ». Зокрема конструктор був створений саме як альтернатива російському конструктору Tilda, яким, за аналізованою статистикою, користувалася доволі велика кількість українських веб-розробників. В цей доволі складний час подібне рішення є доволі вдалим, а саме завдяки масовій українізації послуг на ринку, також є доволі прибутковим.

Аналізуючи складову даного конструктора, с першого погляду можна зробити висновок про доволі великий функціонал його можливостей.

Як саму головну особливість, можна вирізнити безкоштовний доступ до конструктору й безкоштовне створення сайту в ньому. Тому користувачу, який хотів би лише спробувати даний конструктор в дії, не потрібно витрачати зайві кошти на ознайомлення з WustPage.

Сам конструктор є доволі містким та функціональним. В ньому налічується 304 шаблони на різну тематику. Конструктор не обійшов практично ні одну галузь, до якої можна обрати шаблон (рисунок 1).

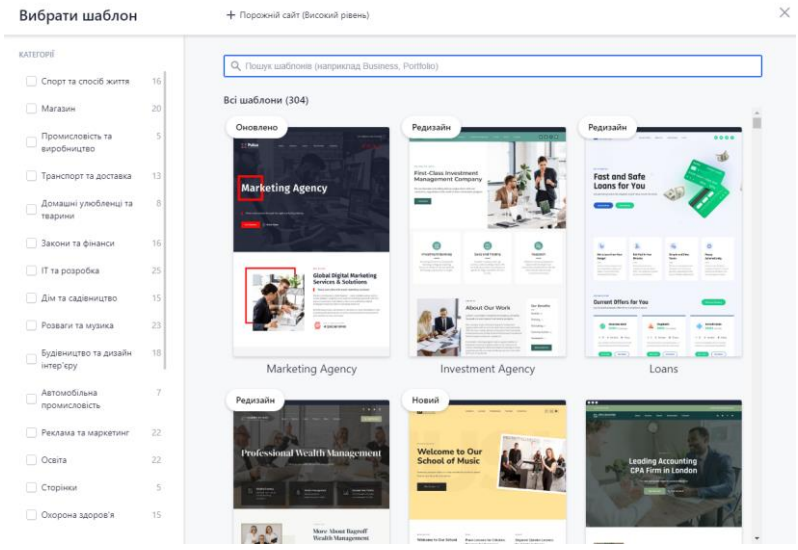


Рисунок. 1. – Вид макетів в конструкторі

Обравши потрібний макет, користувачу надається повний доступ до функціоналу вибраного шаблону. Надається можливість змінити або додати абсолютно будь-який параметр, починаючи зі звичайних фото та відеоматеріалів, закінчуючи анімаціями та, різного функціоналу і направлення,

кнопками (рисунок 2). Також, потрібно зазначити, що сайт має функцію автоматичного переводу сайт в мобільну версію.

Маючи настільки широкий спектр можливостей в самому конструкторі, що вирізняє його на фоні інших, більш простих та примітивних конструкторів, WustPage окрім створення звичайних інформативних сайтів дозволяє створювати й більш місткі та складні проекти, на кшталт інтернет магазину.

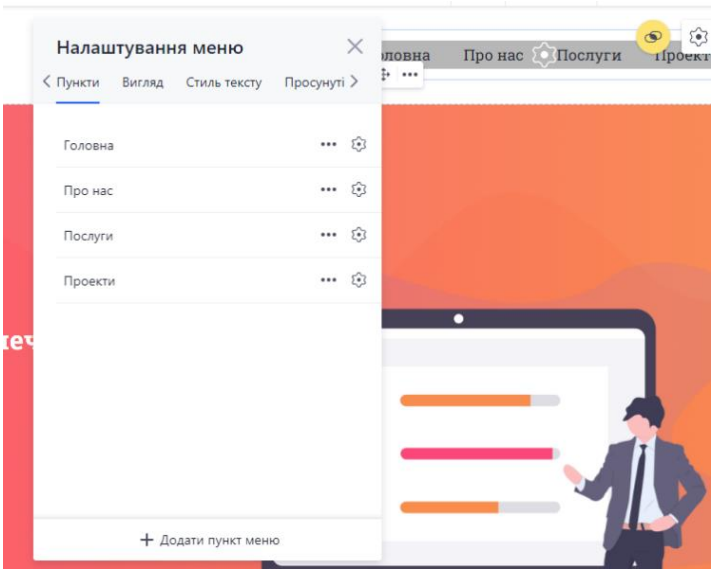


Рисунок. 2. – Вид налаштування компонентів створюваного сайту

Перевагою конструктору також можна вважати вбудовану CRM-систему, що має на меті повноцінний облік клієнтів та угод в одному місці з особистим кабінетом, окремим для кожного інтернет-магазину. Ще одною перевагою WustPage є SEO-оптимізація. Тобто, відбувається вдосконалення сайту для пошукових систем та користувачів, що відбувається шляхом проведення заходів по внутрішній та зовнішній оптимізації, а саме метою цієї функції є збільшення трафіку на сайт та його подальшої монетизація (для інформаційних ресурсів) або перетворення в клієнтів (для комерційних ресурсів) [2].

Також, не можна не вирізнити створення сайтів на замовлення. Розробка сайту займає не більше 2 днів. WustPage створює зрозумілі та прості у використанні веб-сайти для будь-якої ніши, а ціна за створення дорівнює якості [1].

Отже, можна зробити висновок, що WUSTpage є доволі вдалим та зручним додатком, що виконує свій заявлений функціонал на більш ніж достатньому рівні, та спрощує створення сайту як для тих, хто вперше в цій сфері, так і для вмілих розробників.

Список використаних джерел

1. Конструктор сайтів WustPage. URL: https://wustpage.com/ (дата звернення 23.05.2022).

2. SEO-оптимізація. URL: https://www.taina.com.ua/shho-take-seo-optymizacija/ (дата звернення 24.05.2022).

Рудь Максим, здобувач вищої освіти СВО Бакалавр,
спеціальність «Інформаційні системи та технології»
Науковий керівник – к.т.н., доцент Дегтярьова Лариса

ТЕХНІЧНІ ЗАСОБИ ОХОРОНИ НА ПІДПРИЄМСТВІ, УСТАНОВІ, ОРГАНІЗАЦІЇ

Офіційні дані свідчать про постійне зростання злочинності, тож ігнорувати цей факт не варто. Наслідком збільшення кількості правопорушень є підвищена вразливість будь-якого місця, у якому крадії отримують можливість чимось поживитися. Винятком не стають навіть державні установи.

Один зі основних способів захисту майна – установка сучасного охоронного обладнання та сигналізації. Головною умовою створення ефективної системи безпеки на об'єкті є використання цілого комплексу сучасних технічних засобів охорони.

Для того, щоб визначитися й обрати тип технічного охоронного засобу, потрібно ознайомитися з їхньою класифікацією.

Основні засоби – це:

– відеонагляд;
– охоронна сигналізація;
– контроль доступу;
– пожежна сигналізація.

Технічна охорона – це використання на об’єкті досягнень науки й техніки в галузі охоронних пристроїв. І однією з умов створення ефективної системи безпеки на об'єкті є використання цілого комплексу сучасних технічних засобів охорони.

Сьогодні серед охорнних систем є багато доступних і дієвих засобів.

Тривожна кнопка. Монтується на стіні, під стільницею або іншою поверхнею, може бути переносна. Передає сигнал на пульт для виклику групи захоплювання.

Тривожна кнопка може бути як доповненням до системи охоронної сигналізації, так і служити єдиним засобом охорони в разі цілодобової роботи охороняємого об'єкта. Підприємство «АЙ ТИ ГРАНД» завжи обирає якісну апаратуру, тому вибір спеціалістів лежить на пульті для керування охоронною системою AJAX SpaceControl (рисунок 1).

Пульт оснащений ефективною бездротовою системою радіозв'язку, яка використовує шифрування повідомлень та захист від підлоги. Це забезпечує відмінну захищеність сигналізації від спроб злому зловмисниками.

Крім того, він має ультрасучасну високонадійну систему зв'язку, що дозволяє йому успішно працювати в межах кількох поверхів бізнес-центру або на відстані до 800 м-коду на відкритій місцевості від центрального блоку сигналізації.

Рисунок 1. – Зовнішній вигляд пульта керування охоронною системою AJAX SpaceControl

Технічні засоби пожежної охорони. Мають пожежні датчики, сповіщувачі та інші елементи системи. У разі виявлення продуктів горіння передають сигнал тривоги на пульт. Підприємство встановлює Комплект пожежної сигналізації на базі ППКП Артон–2П (рисунок 2).

Рисунок 2. – Зовнішній вигляд комплекта ППКП Артон–2П

Потужна звукова сирена С-03-12 приверне увагу всіх відвідувачів та працівників цього приміщення. У разі відсутності основного живлення, система пожежної безпеки буде працювати автономно, від акумулятора, більше доби в режимі очікування і одну годину в режимі пожежної тривоги.

Чутливим елементом системи є димовий датчик СПД-3, встановлений на стелі в кожному приміщенні по одному в загальному коридорі, для підвищення надійності два датчики. Всі датчики рекомендуємо поєднати в один шлейф, а другий шлейф залишити резервним.

Використовуючи релейні виходи “Пожежа” та “Несправність”, пожежну систему можна інтегрувати в іншу систему безпеки, наприклад охоронну підключивши релейні виходи як зони охоронної централі. Також можна підключити GSM-дозвонювач на мобільний телефон власника приміщень.

Технічні засоби охоронної сигналізації. Мають датчики, що встановлюються на рухомі частини вікон і дверей, датчики руху, сигнальні пристрої, контрольну панель і клавіатуру. Спрацьовують при спробі проникнення в приміщення. Було виявлено, що на підриємстві встановленно Комплект охоронної сигналізації Ajax Cam Plus (рисунок 3).

Рисунок 3. – Зовнішній вигляд Ajax Cam Plus

Хаб контролює роботу системи безпеки, зв'язуючись з підключеними пристроями .Дальність зв'язку – до 2000 метрів за відсутності перешкод (наприклад, стін, дверей, міжповерхових перекриттів). У разі спрацювання датчика система піднімає тривогу за 0,15 секунд, активує сирени, а також оповіщає пульт охоронної організації та користувачів. За наявності перешкод на робочих частотах або при спробі глушіння Ajax переходить на вільну радіочастоту та надсилає повідомлення на пульт охоронної організації та користувачів системи. Отже, таким чином ми дізналися про всі охоронні системи ТОВ «АЙ ТІ ГРАНД».

Список використаних джерел

1. Комплект охоронної сигналізації Ajax StarterKit Cam Plus чорний. Moyo: веб-сайт. URL: https://www.moyo.ua/ua/komplekt_okhrannoy_signalizatsii_ajax_starterkit_cam_plus_chernyy/481437.html (дата звернення: 23.06.2022).
2. Комплект пожарной сигнализации ОФИС-минимальный на базе ППКП Артон-2П. Ohran : веб-сайт. URL: https://ohrana.ua/pozharnaya-bezopasnost/komplekt-pozharnoy-signalizatsii-ofis-minimalnyy-na-baze-ppkp-arton-2p.html?feed=gm&utm_source=google&utm_medium=cpc&utm_campaign=18372974564&utm_term=&utm_content=&utm_position=&utm_matchtype=&utm_placement=&utm_network=x&gclid=CjwKCAjwvsqZBhAlEiwAqAHElUwyF_UibAIdpBOGS9vN3wEk4aI4J_H-nV24xccBGAXgc6TuSiA_PRoCxnUQAvD_BwE (дата звернення: 23.06.2022).
3. Руководство пользователя Hub 2 Plus Moyo : веб-сайт. URL: https://www.moyo.ua/ua/pub/files/instructions/10511_1635408745.pdf (дата звернення: 23.06.2022).

Влох Тарас, здобувач вищої освіти СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н, доцент Дегтярьова Лариса

РЕДИЗАЙН САЙТУ ПІДПРИЄМСТВА

Якісний візуальний дизайн – одна з речей, яка утримує людей залишитися на порталі. Перше, що цікавить відвідувачів сайту, це дизайн. Тому потрібно зробити все можливе, щоб люди залишалися на вашому веб-сайті.

Кожен сайт потребує оновлення. Це можуть бути зовнішні покращення, «косметичні виправлення» або глибокі зміни, пов'язані з покращенням зручності використання та впровадженням нових функцій. Для цього потрібен редизайн.

Редизайн – це модернізація, яка передбачає зміни в оформленні, в контенті, функціональності ресурсу та інше [1].

Першим етапом редизайну послужив аналіз сайту. Важливо оцінити поточні сторінки веб-сайту, щоб визначити, чи слід зберегти, оновити або видалити контент на сторінці. Визначив сильні та слабкі сторони поточного веб-сайту.

Сильною стороною сайту є детальна інформація про користувача та його витрати.

Серед слабких сторін можна виділити недостатнє відведення часу на публікації новин в соціальних мережах та на сайті. Просування в інтернеті на низькому рівні: немає залучення клієнтів на сайті, якщо користувач не має профілю на сайті ТОВ «ТЕРА НЕТ» [2], з'являється форма входу на сайт, і ця форма буде на будь-якій сторінці сайту (рисунок 1).

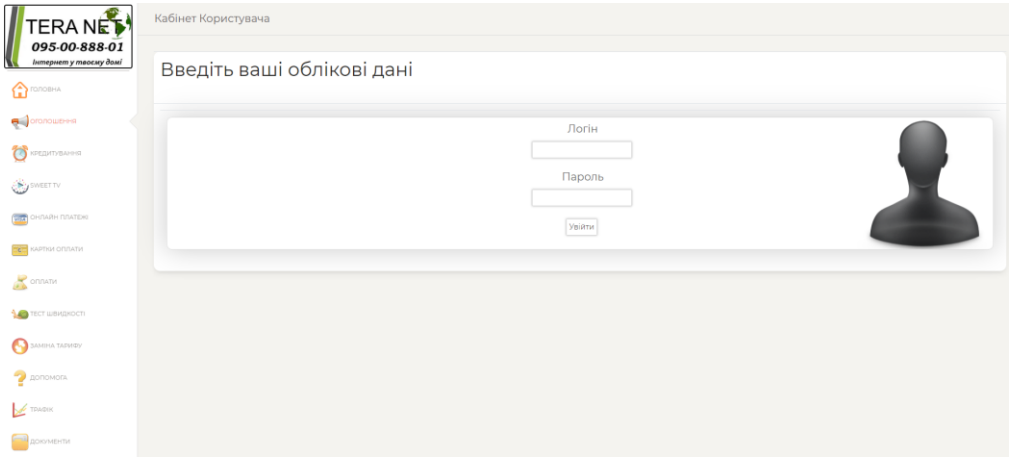


Рисунок 1. – Форма входу на сайт підприємства

Через це, потенційний клієнт, який зайде на сайт і захоче щось дізнатися, він цього не зможе зробити. Моя пропозиція в тому, щоб розробити головну сторінку сайту принаймні з основною інформацією: новинами і тарифами і

головне видимою (без форми входу), це дасть змогу відвідувачам прозоро оцінити, що пропонує дане підприємство.

Наступний етапом є створення візуального супроводу сайту. Розробляв редизайн в програмі Figma.

Figma – це багатоплатформовий онлайн-сервіс для веб-дизайну. З його допомогою можна створювати векторні ілюстрації, інтерактивні дизайни сайтів і мобільних додатків, а також елементи інтерфейсу [3].

Для початку визначив кольорову палітру сайту, щоб придержуватися певного стилю. В якості основного кольору вибрав зелений колір з різними відтінками (рисунок 2), виходячи з назви підприємства «ТЕРА НЕТ», слово «terra» з латинської це грунт, земля або земна поверхня, що асоціюється із зеленим або коричневим кольором, но на мій погляд коричневий колір не підходить, через те, що він важко сприймається на зір.

Рисунок 2. – Основна кольорова палітра сайту

Розробив логотип сайту. Далі продумав, що буде знаходитися на сайті, а саме: Головна сторінка, де є слайдер з основними новинами (до цього вони знаходились в розділі «Договір публічної оферти») та усіма тарифами (рис. 3), Тарифи, Контакти, Вибір мови (українська, російська, англійська), Мій кабінет (Профіль користувача, Кредитування, Онлайн платежі, Заміна тарифу, Статистика), Підтримка, Договір публічної оферти, Соціальні мережі (посилання на Instagram, Facebook, Telegram), Тест швидкості, Про нас. Визначився с шрифтом для сайту – Roboto.

Рисунок 3 – Вигляд головної сторінки

Видалив розділ «Онлайн платежі», «Оплати», «Документи» (там нічого не знаходиться) та «SWEET TV», замінив «Трафік» на «Статистика», «Головна» на «Профіль користувача», додав «Контакти».

Порівняв вигляд розділів сайту з моїм редизайном (рисунки 4 – 5).

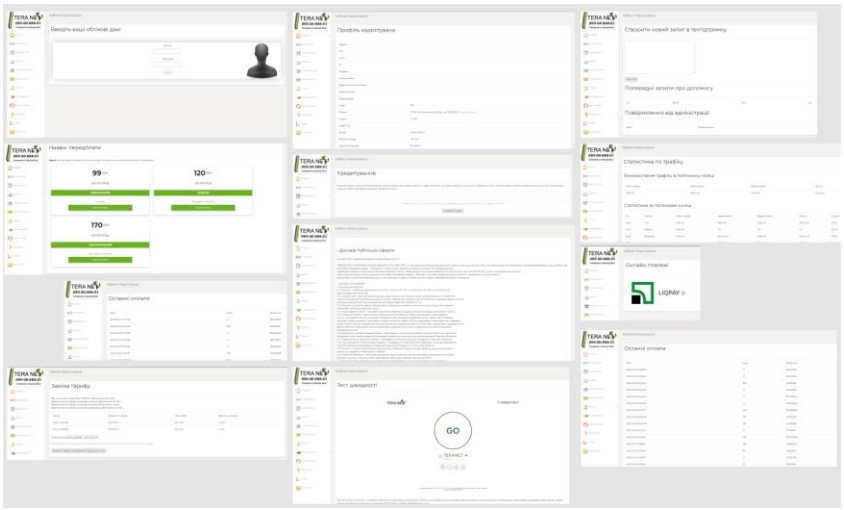


Рисунок 4. – Наявний дизайн сайту

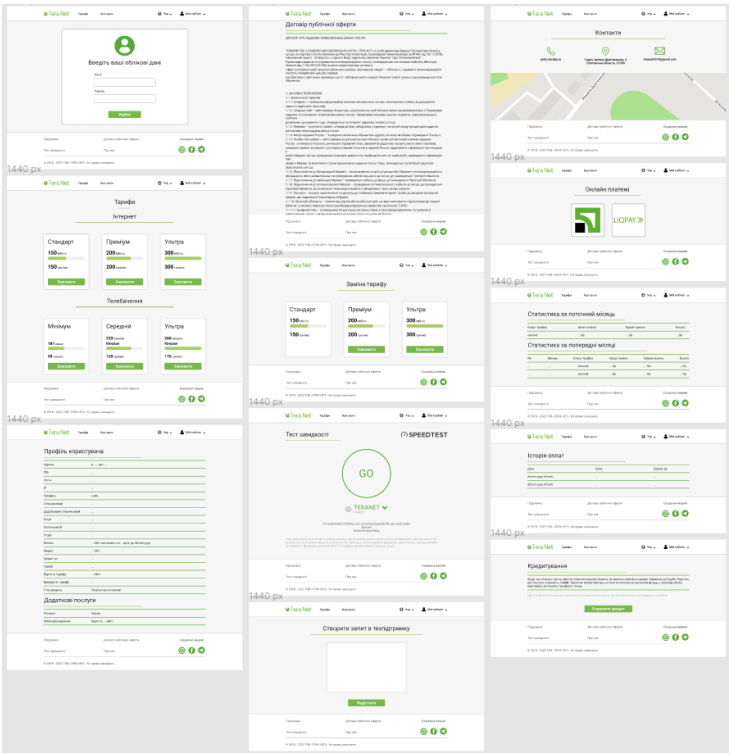


Рисунок 5 – Створений дизайн сайту

В результаті можна сказати, що редизайн перетворився в тренд, який властивий багатьом підприємствам. Бренди змінюють логотипи, розробляють стратегії, впроваджують нові технології – роблять все, щоб зберегти і підвищити популярність на ринку.

Список використаних джерел

1. Як робиться редизайн сайту? URL : https://brainlab.com.ua/uk/blog-uk/yak-robitsya-redizajn-sajtu (дата звернення: 22.09.2022).

2. ТОВ «ТЕРА НЕТ». URL: http://teranet.com.ua/ (дата звернення: 22.09.2022).
3. ЩО ТАКЕ FIGMA? URL: https://avada-media.ua/ua/figma/ (дата звернення: 22.09.2022).

Єрьомін Артур, здобувач вищої освіти СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н, доцент Уткін Юрій

ЗАСОБИ ДІАГНОСТИКИ ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ІНТЕРНЕТ

Велика кількість користувачів стикаються з проблемами мережі. Кожна проблема може бути різна та індивідуальна. Припустимо що, погіршився стан та якість мережі, сервери стали не доступними. Або після змін налаштувань в комп’ютері або заміни провайдера взагалі не вдається встановити доступ до мережі. Це все може виявити критичний вплив на онлайн сервіси та активних користувачів мережі.

В різних випадках потрібно проводити діагностику підключення та шукати відповідні засоби для цього. Щоб запобігти проблем які можуть бути.

Серед знайомих утиліт для діагностики мережі є Tracert, Ping. Це прості в користуванні та ефективні команди. Вони є засобом вбудованим в Windows, а також є вільний доступ до команд в мережі Інтернет.

За допомогою команди Tracert можливо оцінити з якою швидкістю надсилається текстовий пакет, настільки довгий шлях він пройшов, де була затримка пов’язана з передачею даних. Відповідно Tracert надсилає текстовий пакет в казаний вузол мережі, відображаючи всю інформацію про проміжних маршрутизаторів які він проходить [1].

За допомогою команди Ping, можливо з’ясувати час відгуку сервера, тобто він надсилає запит на сервер і фіксує час відповіді та надсилання. Відповідно чим менший час тим швидший обман даними між серверами.

Для одноканального підключення і для індивідуальних підключень у багатоканальному підключенні швидкодія визначається під час підключення. Для багатоканальних підключень швидкодія дорівнює сумі швидкостей індивідуальних підключень. Для багатоканальних підключень швидкодія може змінюватися, якщо підключення, що входять в його склад, будуть вилучені чи будуть додані нові підключення.

Якщо комп'ютер настроєний на прийом вхідних підключень, значок підключення з ім'ям користувача, привласненим цьому підключенню, автоматично з'являється в папці Мережні підключення (Сетевые подключения або Network Connections), як тільки даний користувач підключається до комп'ютера. Можна переглядати стан вхідного підключення, вибираючи в його контекстному меню пункт Стан (Состояние або Status).

Для використання засобами потрібно знати відповідні, параметри, які потрібно занотувати, або звернутися до довідки. Звісно тут немає ніяких

проблем, але з технічного плану може здатися що це незручно. Результати виконання цих команд висвітлено на зображенні [2], [3] (рисунок. 1), (рисунок 2).

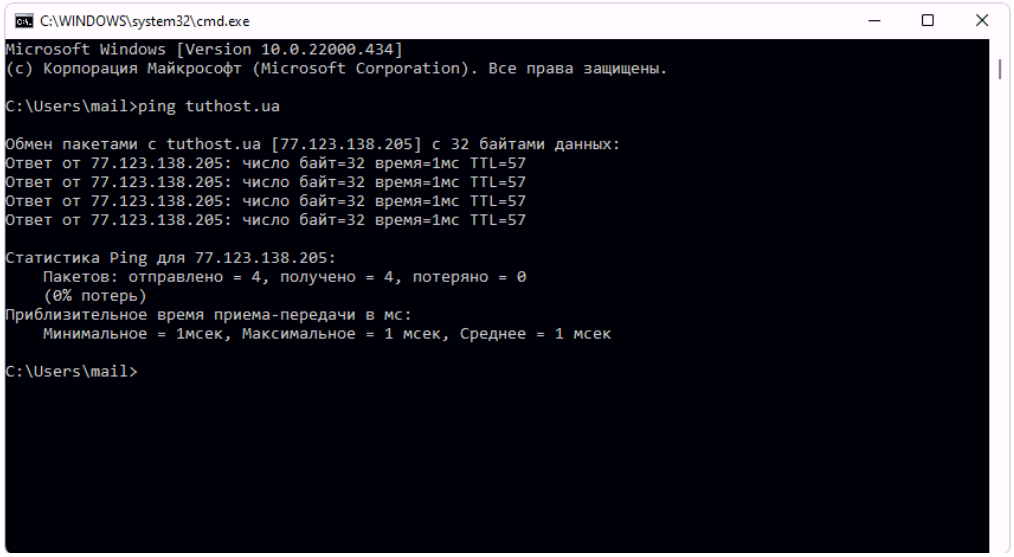


Рисунок 1. – Зовнішній вигляд виконання команди Ping

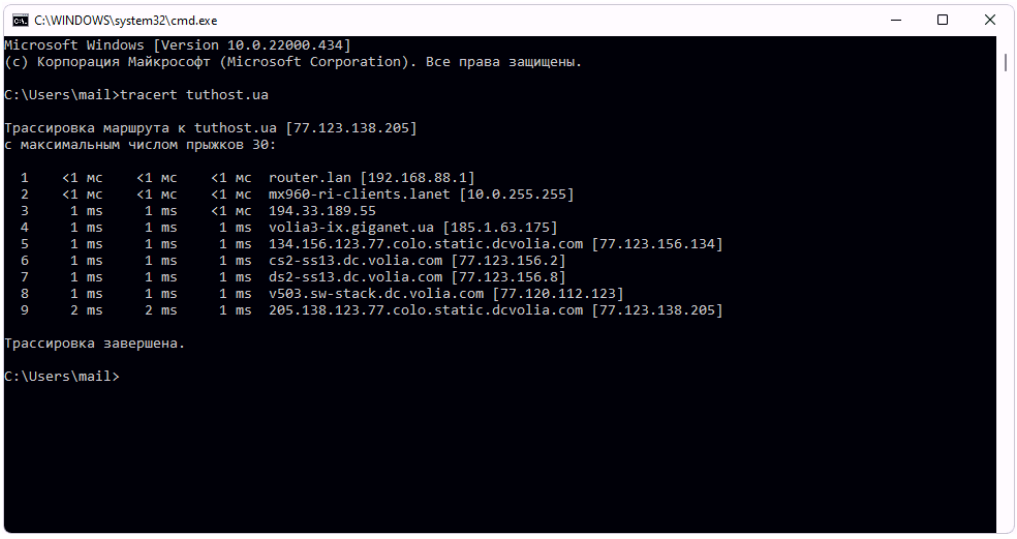


Рисунок 2. – Зовнішній вигляд виконання команди Tracert

На певних прикладам розглянемо результати відповідних команд. Наприклад у випадку коли потрібно з’єднатися з відповідним сервером та щоб сервер вашого інтернет – провайдера був ближче. Команди повідомляють про те що, деякі пакети не проходять далі провайдера, ймовірно через проблеми на його стороні. Також можливо привести приклад коли відсутній відгук сервера, це означає що він зараз недоступний, або адміністратор заблокував його.

Є декілька методів для усунення можливих проблем мережі:

- увімкнути пошук мережі;
- вийдіть з системи, перезавантаження комп’ютера або вимкніть комп’ютер;

– відключити і включити роутер, в рідшому випадку оновити прошивку;
– перевірити кабелі та роз’єми.

Отже засобів діагностики мережі досить багато, так само багато і програм які мають багатий функціонал для цього. Розглянуті мають самий простий в використанні а також доступний.

Список використаних джерел

1. Діагностика та усунення проблем з мережевим підключенням в Windows 7 URL: http://softik.net.ua/diagnostyka-ta-usunennya-problem-z-merezhevym-pidklyuchennyam-v-windows-7/
2. УКРАЇНСЬКИЙ ХОСТИНГ TUTHOST. URL: https://tuthost.ua/wp-content/uploads/2022/05/ping-1.png
3. Програмні засоби діагностики мережі. URL:https://tuthost.ua/wp-content/uploads/2022/05/tracert.png

Филь Владислав, здобувач вищої освіти СВО Бакалавр,
спеціальність «Інформаційні системи та технології»
Науковий керівник – к.т.н., доцент Уткін Юрій

КОМПЛЕКС ОРГАНІЗАЦІЙНИХ ЗАХОДІВ У СТРУКТУРІ БЕЗПЕКИ ЗАХИСТУ ДАНИХ

Захист інформації – тема, яка розглядається паралельно з питаннями обробки інформації в системах, поширення і т. ін. Стосовно захисту інформації приймаються закони, розробляються стандарти, оновлюються технічні рішення та нормативні акти. Згідно з Законом України «захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі». У статті 1 цього ж закону визначається, що «комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації».

Згідно з ДСТУ 3396.1-96 організаційні заходи захисту інформації – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення ТЗІ.

Організаційні заходи із захисту інформації – це комплекс адміністративних і обмежувальних заходів, спрямованих на оперативне виконання завдань захисту інформації шляхом регламентації діяльності персоналу і функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення захисту інформації. До плану можуть бути долучені такі заходи:

– розроблення документів (інструкцій, методик, правил, розпоряджень тощо) з різних напрямів захисту інформації в АС;

– внесення змін і доповнень до чинних в АС документів з урахуванням змінення умов (обставин);

– розроблення й впровадження нових організаційних заходів із захисту інформації;

– обґрунтування необхідності застосування та впровадження нових засобів захисту інформації;

– координація робіт з іншими підрозділами організації або зовнішніми організаціями на всіх етапах життєвого циклу АС;

– перегляд результатів виконання затверджених заходів і робіт із захисту інформації.

Входами системи захисту інформації є такі явища:

1) вплив зловмисників у процесі фізичного проникнення до місцезнаходження джерел конфіденційної інформації з метою її викрадення, внесення змін або знищення;

2) різноманітні фізичні поля, електромагнітні сигнали, які створюються технічними засобами зловмисників і впливають на засоби обробки й збереження інформації;

3) стихійні лиха (насамперед пожежі), що призводять до знищення або перекручування інформації;

4) фізичні поля та електричні сигнали з інформацією, які передаються функціональними каналами зв’язку;

5) побічні електромагнітні наведення й акустичні поля, а також електричні сигнали, що виникають у процесі діяльності об’єктивного захисту та несуть у собі конфіденційну інформацію.

Виходами системи є заходи щодо захисту інформації, адекватні вхідним впливам. Алгоритм процесу перетворення вхідних впливів (загроз) на заходи захисту визначає варіант системи захисту.

Побудова системи захисту інформації суб’єкта господарювання здійснюється поетапно:

1 етап – визначення й аналіз загроз;

2 етап – розроблення системи захисту інформації;

3 етап – реалізація плану захисту інформації;

4 етап – контроль функціонування та керування системою захисту інформації.

На першому етапі побудови системи захисту інформації необхідно здійснити аналіз об’єктивного захисту, ситуаційного плану, умов функціонування підприємства, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати дані для побудови окремої моделі загроз. Джерелами загроз може бути діяльність іноземних розвідок, а також навмисні чи ненавмисні дії юридичних і фізичних осіб.

Ефективна протидія загрозам інформації досягається винятково за умови комплексного застосування засобів та організаційнотехнічних методів із метою

захисту охоронюваних відомостей про об’єкт. Причому вказані засоби й методи мають застосовуватись відповідно до мети й завдань протидії, етапів життєвого циклу об’єкта та способів протидії. Суттєвим моментом є необхідність реалізації захисту інформації вчасно, активно, різноманітно, безперервно, раціонально, комплексно й планово. Одна з основних вимог – вчасність прийняття рішення щодо організації захисту інформації. Процес прийняття рішення потрібно прискорити з певних причин: по-перше, щоб вчасно розв’язати проблеми, що виникли, і не давати їм «розростатись» до такого стану, коли їх вирішення стане неможливим чи марним; по-друге, щоб відповідальні виконавці мали достатньо часу для виконання поставлених перед ними завдань. Активність протидії передбачає насамперед наступальний, активний її характер, ґрунтується на аналізі обставин, умінні зробити правильні висновки про можливі дії потенційного супротивника, що дадуть змогу запобігти та наполегливо реалізувати ефективні заходи протидії. Різноманітність протидії спрямовується на унеможливлення шаблонного підходу до організації й проведення заходів щодо захисту інформації. Комплексність передбачає вжиття комплексу заходів, спрямованих на своєчасне перекриття всіх можливих каналів витоку інформації. Неприпустимим є застосування окремих технічних засобів або методів, спрямованих на захист окремих серед загального числа можливих каналів витоку інформації.

Порядок проведення перевірок і контролю ефективності захисту інформації встановлюється нормативними документами, перелік яких також встановлює Стандарт.

Список використаних джерел

1. Про захист інформації в інформаційно-комунікаційних системах. Закон України. Чинний від 01.07.2022. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
2. Микитишин А. Г. Комп’ютерні мережі: навч. посіб. Львів : Магнолія, 2006. 256 с.

Богомольний Олександр, здобувач вищої освіти СВО Бакалавр,
спеціальність «Інформаційні системи та технології»
Науковий керівник – д.т.н., професор Поночовний Юрій

ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ MICROSOFT ACCESS ДЛЯ ВВОДУ ТА ПОКАЗУ ІНФОРМАЦІЇ

Велика кількість інформації залишається в письмовому вигляді, для зручності пошуку та використання цієї інформації раціонально перенести в електронний вигляд, і коли доходить питання про перенесення, то йде вибір між базами даних для зберігання цієї інформації і щоб була можливість фільтрувати потрібну інформацію.

Головною метою є ознайомлення з можливостями програмного продукту Microsoft Access та способу введення та виведення інформації з БД та порівняння його з іншою базою даних.

Найпростішим використання у порівнянні з іншими базами даних є Microsoft Access. Програмне забезпечення доступне відразу всім користувачам Windows, легко заповнювати інформацію та є багато можливостей виведення інформації в різних видах.

Для порівняння можна взяти також продукт Microsoft – SQL Server.

Порівняння Microsoft Access з SQL Server в табл. 1:

Таблиця 1 – порівняння двох баз даних.

MS Access	SQL Server
Microsoft Access – це настільна система управління реляційними базами даних (СУБД), призначена для роботи на автономний персональний комп'ютер (ПК) або локальної обчислювальної мережі під управлінням сімейства операційних систем Microsoft Windows.	Microsoft SQL Server - система управління реляційними базами даних (СУБД). Основна мова мови запитів – Transact SQL. Використовується для роботи з базами даних розміром від персональних до великих баз даних масштабу підприємства.
Можливості	
Створення, модифікація та використання похідних об'єктів (Запитів, форм та звітів);	Розділяти дані між платформами, додатками та пристроями для полегшення з'єднання внутрішніх та зовнішніх систем;
Створення зв'язків між таблицями, з підтримкою цілісності даних, каскадного оновлення полів та каскадного видалення записів.	Автоматизація рутинних адміністративних завдань. Наприклад, управління блокуванням та пам'яттю, редактор розмірів файлів. У програмі продумано налаштування, можна створювати профілі користувачів.
Переваги	
Є можливість експортувати дані та імпортувати дані з файлів текстової обробки, електронних таблиць або файлів бази даних безпосередньо[1];	Зручний пошук. Його можна здійснювати за фразами, словами, текстом чи створювати ключові індекси[4];
Також може вставляти або зв'язувати безпосередньо з даними, що зберігаються в інших програмах та базах даних[1];	Розмір сторінок – до 8 Кб. Дані отримуються швидко, а складну інформацію зручніше зберігати. Система обробляє транзакції в інтерактивному режимі, є динамічне блокування[4];

Access може працювати безпосередньо з даними з інших джерел, включаючи багато популярних програм баз даних на ПК, з багатьма базами даних SQL[1];	Масштабування системи. Взаємодіяти з нею можна як на простих ноутбуках, так і на ПК з потужним процесором, який здатний обробляти великий обсяг запитів[4].
Безкоштовне використання.	
Безпека даних	
Захист лише на рівні доменних політик;	Схеми, які не мають відношення до користувачів;
Захист за допомогою макросу AutoExec та блокування Shift;	Ролі;
Захист із використанням пароля БД;	Шифрування трафіку та даних;
Захист за допомогою термінального доступу до сервера (найвищий рівень захисту в Access, тому що І клієнтська частина та база з таблицями знаходиться на сервері).	Підтримка Kerberos.

При порівнянні двох баз даних можна помітити що у деяких моментах SQL Server трохи краще ніж Microsoft Access, але для використання SQL Server потрібно хоч мінімальне знання мови SQL, в Access не потрібно знання мови. Також Microsoft Access має широкий вибір між способами виведення інформації.

Способи виведення інформації [2]:

- таблиці;
- форми;
- звіти;
- запити;
- макроси;
- модулі.

Розповсюдженим способом виводу інформації є таблиці, але не завжди в них легко знайти потрібну інформації. Раціональніше використовувати спосіб виводу запит.

Запит дозволяє виконувати перелічені нижче завдання [3]:

– переглядати значення лише з полів, які цікавлять. Ви можете зберегти запит, який видає лише деякі з них;

– об'єднувати дані з кількох джерел. Запит дозволяє вибрати поля з різних джерел та вказати, як саме потрібно поєднати інформацію;

– використовувати вирази як поля. Наприклад, у ролі поля може виступити функція, яка повертає дату, а за допомогою функції форматування можна керувати форматом значень із полів у результатах запиту;

– переглядати записи, які відповідають вказаним умовам. Під час відкриття таблиці відображаються всі записи. Можемо зберегти запит, який видає лише деякі з них.

Отже, ми дізналися про переваги використання програмного забезпечення Microsoft Access, та його спосіб виводу інформації, запит, завдяки якому можна легко фільтрувати та обирати які саме данні він повинен демонструвати як підсумок.

Список використаних джерел

1. MS Access – Краткое руководство. веб-сайт. URL: https://coderlessons.com/tutorials/microsoft-technologies/izuchite-microsoft-access/ms-access-kratkoe-rukovodstvo (дата звернення: 21.06.2022).
2. Основні відомості про бази даних. Microsoft: веб-сайт. URL: https://support.microsoft.com/ru-ru/office/%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%D1%8B%D0%B5-%D1%81%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F-%D0%BE-%D0%B1%D0%B0%D0%B7%D0%B0%D1%85-%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85-a849ac16-07c7-4a31-9948-3c8c94a7c204 (дата звернення: 21.06.2022).
3. Знайомство із запитами. Microsoft Access: веб-сайт. URL: https://support.microsoft.com/ru-ru/office/%D0%B7%D0%BD%D0%B0%D0%BA%D0%BE%D0%BC%D1%81%D1%82%D0%B2%D0%BE-%D1%81-%D0%B7%D0%B0%D0%BF%D1%80%D0%BE%D1%81%D0%B0%D0%BC%D0%B8-a9739a09-d3ff-4f36-8ac3-5760249fb65c#__toc355883440 (дата звернення: 21.06.2022).
4. Головна інформація про SQL Server. Microsoft SQL Server: веб-сайт. URL: https://www.microsoft.com/en-us/sql-server/sql-server-2017?ranMID=24542&ranEAID=TnL5HPStwNw&ranSiteID=TnL5HPStwNw-JTahfmu9EoBwnUOg4y4nnQ&epi=TnL5HPStwNw JTahfmu9EoBwnUOg4y4nnQ&irgwc=1&OCID=AID2200057_aff_7593_1243925&tduid=%28ir__x0vzaeenhwkfbnc0c9wglse2if2xqodj0tno9cp900%29%287593%29%281243925%29%28TnL5HPStwNw JTahfmu9EoBwnUOg4y4nnQ%29%28%29&irclickid=_x0vzaeenhwkfbnc0c9wglse2if2xqodj0tno9cp900

Онищенко Ростислав, здобувач вищої освіти СВО Бакалавр,
спеціальність «Інформаційні системи та технології»
Науковий керівник – к.ф.-м.н., професор Копішинська Олена

ВАРІАНТ РОЗШИРЕННЯ ФУНКЦІОНАЛУ WEBHMI

Згідно, реалізація концепції «Індустрія 4.0» передбачає дотримання кількох принципів побудови цифрових екосистем: сумісність і прозорість взаємодії через IoT, технічна підтримка і децентралізація управлінських рішень.

Як наслідок, досить актуальним є питання забезпечення збору даних з сенсорів і датчиків і обліку контексту, в якому вони генеруються, для отримання повної інформації про всі процеси, які відбуваються з обладнанням, «розумними» продуктами, виробництвом в цілому та ін. На сьогодні зазначені фактори призвели до зростання попиту на різні варіанти SCADA.

Їх впровадження стає особливо актуальними в ситуаціях відсутності єдиної технічної політики щодо приладів обліку і витрат енергоресурсів; їх різних типів, відсутності комунікаційних інтерфейсів або доступу до них; відокремленого розміщення вузлів обліку на об’єктах або значної відстані розміщення один від одного. Одним з вдалих прикладів подібного роду систем є вітчизняний продукт – WebHMI [2].

Це система SCADA з вбудованим веб-сервером, що дозволяє керувати будь-якими засобами автоматизації по локальній мережі і через Інтернет з комп’ютера і мобільних пристроїв. Система поставляється у вигляді готового пристрою з усім необхідним програмним забезпеченням. WebHMI містить всі необхідні засоби для вирішення більшості типових задач збору і візуалізації даних, а також віддаленого доступу до них.

Система збирає, накопичує і обробляє ці дані, дозволяє експортувати їх в сторонні програми через API, відображати історичні графіки та тренди. Вбудоване середовище розробки дозволяє швидко створити інтерфейс для відображення технологічного процесу. Таким чином, в системі управління на базі WebHMI оператор, який обслуговує, персонал або розробник може легко організувати віддалену роботу або обслуговування через Інтернет.

Це дозволяє отримати доступ до системи, переглянути графіки та статистику, занести зміни у проект з будь-якого місця. Один з варіантів використання WebHMI реалізується на базі бездротових модулів збору даних і хмарної системи диспетчеризації IV Міжнародна науково-практична конференція «Інтеграція інформаційних систем і 98 21-22 жовтня 2021 р, м. Полтава, ПДАУ та аналітики (Level2 WebHMI). Використовуючи стандартні промислові протоколи на основі ModBus, автономні модулі зчитують дані з приладів обліку і відправляють їх через шлюзи по радіоканалу в мережу LoRa. Дані від шлюзів передаються через Інтернет на сервер WebHMI по протоколу MQTT. Сервер як набір готових сервісів забезпечує роботу з цими даними, їх зберігання, побудову звітів і аналітику.

Як відомо [3], до переваг протоколу MQTT слід віднести наступні фактори.

1. Протокол нейтральний до змісту пакета. Приймач повинен вміти інтерпретувати та декодувати повідомлення відповідно до формату, що використовується передавачем.

2. Пакет даних має невеликий розмір і може використовуватися для додатків з низькою пропускною здатністю. 3. Протокол забезпечує низьке енергоспоживання батареї.

4. MQTT використовує параметри QoS для забезпечення гарантованої доставки та може бути призначений для доставки повідомлень відповідно до шаблонів: «максимум один раз», «мінімум один раз» і «рівно один раз».

5. Масштабованість завдяки моделі «публікації / підписки».

6. Протокол пропонує незв'язану конструкцію, в якій легко розділити пристрій і сервер (вдало підходить для розподілених комунікацій «один до багатьох» і для окремих додатків).

7. Пристрій публікації може відправляти дані на сервер в будь-який час, незалежно від його стану.

8. Має функцію LWT («Остання воля» і «Заповіт») для повідомлення сторін про ненормальне відключення клієнта.

9. Для основних завдань зв'язку використовує TCP/IP. Разом з тим, MQTT має такі недоліки: не підтримує потокову передачу відео; має проблеми з затримкою (у MQTT можуть бути повільні цикли передачі); відсутні вбудовані механізми безпеки (MQTT використовує TLS/SSL); централізований брокер може привести до збою, оскільки клієнтські з'єднання з брокерами постійно відкриті. Як наслідок, доцільно розширити функціонал WebHMI за рахунок інтеграції альтернатив протоколу MQTT [4].

Одним з кандидатів є MQTT-SN (версія для сенсорних мереж) Він має деякі переваги у порівнянні з MQTT, особливо для вбудованих пристроїв. До них відносяться такі положення. MQTT-SN використовує тему ID замість імені теми. Перший клієнт відправляє брокеру запит на реєстрацію з ім'ям теми і темою ID (два октети). Після того, як реєстрація прийнята, клієнт використовує тему ID для посилання на ім'я теми. Це економить пропускну здатність і пам'ять пристрою. Ім'я для теми ID можна налаштувати в шлюзі MQTT-інтелектуальних технологій в умовах трансформації інформаційного суспільства» 50 РОКІВ КАФЕДРІ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ 99 SN, щоб повідомлення про реєстрацію теми можна було пропустити перед публікацією. MQTT-SN не вимагає стека TCP/IP. Його можна використовувати по послідовному каналу, де за допомогою простого протоколу зв'язку (для ідентифікації різних пристроїв на лінії) накладні витрати дійсно невеликі. В якості альтернативи його можна використовувати над UDP. Ще одним варіантом є застосування Data Distribution Service (DDS) [5]. Він використовується у мережах реального часу за принципом видавець/підписник. У комбінації з протоколом MQTT або MQTT-SN сервіс DDS може бути використаний для IoT. До того ж, впровадження DDS дозволить розширити сфери використання WebHMI на архітектури транспортних засобів NGVA, забезпечення обміну даними з бортовими мережами транспортних засобів і групове управління кількома роботами. Особливої уваги заслуговує версія

DDSTSN (застосування DDS у чутливих до часу мережах). Подальший розвиток даної тематики може бути розширений за рахунок використання ZeroMQ (ZMQ) [6].

Список використаних джерел:

1. Цифровая Индустрия 4.0. URL: https://www.forbes.ru/brandvoice/sap/345779-chetyre-nol-v-nashu-polzu.
2. WebHMI. URL: http://webhmi.com.ua.
3. MQTT. URL: https://www.navixy.com/ru/docs/academy/besprovodnijetechnologii/mqtt.
4. Слюсар В.И., Слюсарь И.И. Дрон-ретранслятор как элемент системы сбора данных сенсорных сетей. Застосування Сухопутних військ ЗС України у конфліктах сучасності: зб. тез доп. наук.-практ. конф., Львів, Україна, листопад 2020 р. С. 63, 64.
5. DDS. URL: https://uk.wikipedia.org/wiki/Data_Distribution_Service.
6. ZeroMQ. URL: https://en.wikipedia.org/wiki.

Нікітюк Максим, здобувач вищої освіти СВО Бакалавр,
спеціальність «Інформаційні системи та технології»
Науковий керівник – к.т.н., доцент Дегтярьова Лариса

МЕТОДИ ЗАХИСТУ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Повний захист - це інформація на комп'ютері, відключеному від усіх мереж, навіть електричних, у повністю броньованому сейфі, який, у свою чергу, знаходиться в кімнаті з не тільки охороною, але й усілякими різними оповіщеннями. Насправді така інформація має 100% рівень захисту. Але він не може бути використаний і тому не відповідає вимогам доступності. І як зазначалося раніше, порушення хоча б однієї властивості інформації призведе до порушення всієї системи.

Тому абсолютну систему захисту інформації можна створити лише за умови усунення в процесі створення людського фактору, який є основною причиною всіх помилок. Очевидно, що на сучасному етапі розвитку технологічної інформатизації це неможливо.

У результаті всі підприємства зазвичай змушені погоджуватися на відносний захист інформації – вони обіцяють захищати її протягом періоду часу, поки несанкціонований доступ не призведе до будь-яких наслідків. Тобто секретна інформація має бути недоступною до тих пір, поки вона не стане очевидною і зрозумілою, або нікому не потрібна.

Але як захистити інформацію за такий короткий термін? Звичайно, у сучасному світі існує безліч способів запобігти витоку чи втраті інформації.

Але загалом використовується лише перераховані методи захисту даних:

- бар’єр
- шифрування

- керування
- регламентація
- антивіруси
- пісочниця
- групова політика.

Під бар’єром розуміють спосіб фізичного захисту інформаційної системи, щоб зловмисники не мали можливості отримати доступ до захищеної зони (обладнання, носія інформації тощо). Бар'єри є одним із найпростіших і відносно надійних засобів захисту інформації. Так, на будь-якому великому підприємстві все обладнання, яке містить якусь конфіденційну інформацію, знаходиться в одному приміщенні, що суворо охороняється. Також такі приміщення можуть охоронятися людьми (охороною) і спеціальними системами захисту, для проходу через які потрібно знати спеціальні коди або паролі.

Маскування - спосіб захисту інформації, перетворення даних у форму, непридатну для сприйняття сторонньою особою. Якщо говорити про приховування інформації, то не можна сказати, що такою давньою наукою є криптографія. Формально криптографія (або криптографія) визначається як наука про забезпечення секретності повідомлень. Розшифровка такого повідомлення вимагає розуміння принципів. З давніх часів люди навчилися шифрувати інформацію, щоб ніхто не міг здогадатися про її значення. Цей спосіб захисту інформації активно використовується у військових конфліктах.

Наприклад, під час Другої світової війни кораблі ВМС США спілкувалися мовою невеликого густонаселеного індіанського племені. На кожному кораблі було кілька індіанців-«криптологів», і ворог мав мало шансів зробити собі таких «криптологів». Однак у цього способу захисту є і недоліки. Важко встежити за всіма людьми, які починають використовувати мову, і рано чи пізно мова стане зрозумілою для тих, хто намагається приховати розмову. У цьому випадку її потрібно замінити іншою мовою, а розробити досить потужну мову і навчити їй потрібну кількість людей дуже складно і дорого, та й не можливо зробити це швидко.

Шифрувальне програмне забезпечення — це ПЗ яке дозволяє зашифровувати данні використовуючи певні стандарти шифрування.

Існують наступні стандарти шифрування які використовують власний алгоритм шифрування даних:

- MD5 128-bit
- SHA 160-512 bit
- AES 128-256
- base64

Керування – метод захисту інформації, при якому контроль здійснюється над усіма компонентами інформаційної системи. Контроль доступу включає такі функції безпеки, як:

- Ідентифікувати користувачів, людей і ресурси системи (призначити персональний ідентифікатор кожному об'єкту);

– Ідентифікувати (аутенфікувати) об'єкти або суб'єкти за ідентифікаторами, які їм пред'являються;
– перевірка авторизації;
– допускати та створювати умови праці в межах встановлених норм;
– реєструвати звернення до захищених ресурсів;
– Реєстрація на випадок спроби несанкціонованої дії.

Регламентація є найважливішим методом захисту інформаційних систем і передбачає введення спеціальних директив, відповідно до яких повинні виконуватися всі операції із захищеними даними.

Антивіруси – програма яка сканує файли на наявність шкідливого коду, лікування програм що заражені вірусом, а також допомагає запобігати зараження файлу вірусом.

Основні функції:
– Сканування Інтернет трафіка
– Сканування ПК
– Відновлення пошкоджених файлів
– Емуляція запуску програми для відслідковування вірусної поведінки
– Сканування електронної пошти

Приклади антивірусного ПЗ:
– Avast
– Kaspersky
– Eset Nod32
– McAfree
– AVG
– BitDefender

Пісочниця – це ПЗ для запуску програми в обмеженому віртуальному середовищі з чітко обмеженим набором ресурсів, для виконання невідомої програми без загрози для операційної системи.

Приклади ПЗ:
– Sandboxie
– Avast
– Sandbox
– Honeypot
– VirtualBox
– Vmware.

Мотивація — це метод захисту інформації, який заохочує користувачів і персонал системи не порушувати встановлених порядків, дотримуючись встановлених морально-етичних норм, як встановлених, так і неписаних.

Наприклад, жодна всесвітньо відома компанія не буде нахилятися, щоб незаконно отримати необхідну інформацію про компанію конкурента.

Усі ці методи спрямовані на створення ефективної технології захисту інформації для усунення втрат через ненавмисні та успішного відбиття різного роду загроз.

Групова політика — це набір правил та параметрів за допомогою яких відбувається налаштування робочого місця в Windows Групову політику можливо використовувати наприклад для:

- Управління оновленням Windows, настроїти політику перезапуску, коли вона не буде виконуватися, період активності.
- Розподіленням рівнів користувачів (Користувач, адміністратор, ін)
- Затримка автоматичного перезапуску.

Висновок: Технології і можливості по захисту даних не стоять на місці, перелічені можливості не дають 100% гарантії що інформація не потрапить до рук зловмисників, адже головною небезпекою є людський фактор.

Криптографія є одним з найкращих засобів забезпечення конфіденційності і контролю цілісності інформації. Вона займає центральне місце серед програмно-технічних регулювальників безпеки, є основою реалізації багатьох з них і, в той же час, останнім захисним рубежем.

Список використаних джерел

1. Информационные системы и технологии управления: Учебник / ВЗФЭИ; Под ред. Г.А.Титоренко. 3-е изд. М.: ЮНИТИ, 2011. 591с.
2. Гужва В.М., Постєвой А.Г. Інформаційні системи в міжнародному бізнесі: Навч. посібник. К.: КНЕУ, 2002. 458с.
3. Карпенко С. Г., Іванов Є. О. Основи інформаційних систем і технологій. К.: МАУП, 2002. 264 с.

Кулінченко Ірина, здобувач вищої освіти СВО Бакалавр,
спеціальність «Інформаційні системи та технології»
Науковий керівник – к.т.н., доцент Дегтярьова Лариса,

АНАЛІЗ ТА ЗАХИСТ СУЧАСНИХ БАЗ ДАНИХ

У ході збільшення та поширення інформації, якою може володіти людина, з’явилась необхідність обробки, структуризації та зберігання інформації. Оптимальною моделлю бази даних, яка зможе повноцінно функціонувати та захищати користувацькі дані є електронні варіанти баз даних [1]. Проте, серед сучасних засобів керування базами даних важко зустріти програмний засіб, який може запропонувати користувачеві максимально можливу захищеність інформації від зловмисника. Вони мають низку криптографічних методів, які можуть шифрувати та гешувати інформацію, проте вони мають проблему, яка зв’язана з отриманням авторизованим користувачем відповідних йому прав, а саме ті випадки, коли зловмисник отримав необхідну йому автентифікаційну інформацію [2]. Мова йде про програмний засіб, який запропонує компаніям, не тільки функції, які є у більшості СУБД, а і покращення наявних засобів та перетворення усіх їх у кращий комплексний підхід.

Метою даної роботи є аналіз проблем захисту у сучасних СУБД. Для досягнення мети необхідно розв’язати такі задачі: порівняти декілька програм

баз даних; проаналізувати проблеми у захисті сучасних СУБД. Для зрівняння візьмемо програми MySQL Workbench і Microsoft Access.

MySQL – це потужна база даних корпоративного рівня, яка використовується багатьма сайтами та магазинами в світі. MySQL – це СУБД на основі SQL, яка розрахована на велику кількість користувачів, буде працюватиме надійно і продуктивно, та обмежена лише доступною оперативною пам'яттю, швидкістю диска і швидкістю обладнання, а не властивими програмними обмеженнями.

Microsoft Access – досить хороший для домашніх користувачів, але не може працювати з більш, ніж 2 гігабайтами даних і не повинен використовуватися на такому рівні. Microsoft Access – це інструмент, в основному, для роботи з базами даних, який ідеальний для доступу до різних корпоративних систем управління базами даних SQL, електронних таблиць Excel, CSV-файлів та інших джерел даних, також є можливість створення зручних форм, запитів, звітів і навіть цілих зовнішніх програм. У Microsoft Access вбудована СУБД SQL, яка, зазвичай, розрахована на одного користувача. Вона може використовуватися багатьма користувачами СУБД, але реальний максимум – шість користувачів, хоча при такій кількості, вона буде повільна та ненадійна.

Сучасні СУБД можна характеризувати як програмні засоби з високим ступенем захищеності інформації, яка зберігається в базах даних під їх управлінням, проте у ході аналізу баз даних було виявлено один з недоліків [3], а саме використання одного бар’єру для підтвердження користувачем наданих йому привілеїв.

При представленні проблеми було виділено таку ситуацію при використанні будь-якої з популярних на сьогодні СУБД користувачі мають певні ролі, які надають їм привілеї [4], зображені у табл. 1.

Таблиця 1 – ролі користувачів у сучасних СУБД

Роль	Можливості	Загрози
Власник	Усі дії по налаштуванню та обслуговуванню БД та видалення	Втрата даних у зв’язку з некомпетентністю чи халатністю,
Адміністратор	Адміністрування бази даних, надання привілеїв.	Цілісність даних, ненавмисне надання прав іншим користувачам.
Редактор	Редагування та видалення даних у таблицях	Цілісність та конфіденційність даних
Читач	Зчитування даних	Конфіденційність даних
Користувач без прав на доступ	Не може виконувати дії з БД	-

Проаналізувавши загрози, було виявлено ті, що можуть бути реалізовані відповідними користувачами. Сучасні бази даних надають права по користуванню базою даних після автентифікації користувача з необхідним рівнем доступу, тобто зловмиснику стає доступним рівень доступу користувача, в якого він міг отримати автентифікаційні дані, що на сьогодні не є найкращим рішенням у зв’язку з великою низкою каналів витоку та несанкціонованого отримання користувацьких даних.

Для роботи з базою даних, з точки зору безпеки в реальних умовах, створюється достатня кількість проблем, які зв'язані з користувацькою авторизацією. Це можуть бути, як проблеми звичайного підглядання паролю, так і проблеми крадіжок необхідних даних шляхом використання власних користувацьких автентифікаційних даних з невідповідною високою користувацькою роллю.

З цього можна зробити висновок, що сучасні СУБД, які мають слабкий парольний захист чи потребують більшого рівня захисту, потребують покращення автентифікаційної системи, яка буде мати на меті розбиття рівнів доступу користувачів і рівнів автентицікації.

Для аналізу та висування пропозицій слід перелічити деякі з реалізацій загроз, наведених у табл. 1. Загроза отримання зловмисником автентифікаційних даних відповідної ролі:

1) Читач бази даних дасть змогу зловмиснику вкрасти інформацію.

2) Редактор дасть змогу відредагувати інформацію у БД.

3) Адміністратор дасть змогу приховано надати права користувачам, що не мають відповідного рангу.

4) Власник ставить під загрозу існування бази даних в цілому.

Отже, можна зробити висновок, що однорівневий захист є проблемою, яку необхідно вирішити. Особистою рекомендацією є використання підходу, який передбачає включення багатошарового захисту інформації шляхом використання засобів криптографії, графічного паролю, що збільшить час, але дозволить відслідковувати та керувати доступом користувачів і захищати, перш за все, цілісність даних краще, чим це було реалізовано до цього.

Список використаних джерел

1. Зрюмов, Е. А., Зрюмова А. Г. Базы данных для инженеров: Навчальний посібник. Алт. держ. техн. ун-т им. И. И. Ползунова. Барнаул: Видав-во АлтГТУ, 2010. 131 с.

2. Полтавцева М. А., Хабаров А. Р. Безопасность баз данных: проблемы и перспективы //Программные продукты и системы, 2016. №. 3 (115).

3. Микитюк І.С., Баришев Ю.В. Підхід до захисту баз даних: тези на наукову конференцію, Вінницький національний технічний університет, 2017 р.

4. Microsoft Docs. Роли уровня баз даных. [Електронний ресурс]. Режим доступу: URL: Роли уровня базы данных - SQL Server | Microsoft Learn

Кибкало Володимир, здобувач вищої освіти СВО Бакалавр,
Спеціальність 126 Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Рябий М.О.

ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ МОДЕЛЕЙ ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНИХ РЕСУРСІВ

При аналізі інформаційних ризиків необхідно використовувати моделі системи інформаційної безпеки, засновані на міжнародних стандартах.

Розглянемо певну модель, побудовану відповідно до стандарту (ISO 15408 "Загальні критерії оцінки безпеки інформаційних технологій" [1]) і даних аналізу ризиків (ISO 17799 "Стандарт побудови ефективної системи безпеки"). Ця модель відповідає спеціальним нормативним документам із гарантування інформаційної безпеки, прийнятих в Україні, міжнародному стандарту ISO/IEC 15408 "Інформаційна технологія - методи захисту, критерії оцінки інформаційної безпеки", стандарту ISO/IEC 17799 "Управління інформаційною безпекою" і враховує тенденції розвитку вітчизняної нормативної бази з питань інформаційної безпеки.

Деталізований опис загальної мети побудови системи безпеки об'єкта замовника виражається сукупністю чинників або критеріїв, які уточнюють мету. Сукупність чинників є основою визначення вимог до системи (вибір альтернатив).

Модель інформаційної безпеки відображує сукупність об'єктивних зовнішніх і внутрішніх чинників та їх вплив на стан інформаційної безпеки на об'єкті і на збереження матеріальних або інформаційних ресурсів. Чинники безпеки можна поділити на технологічні, технічні й організаційні.

У процесі оцінки інформаційної системи та необхідно визначити ресурси інформаційної системи. При цьому необхідно розділити ці ресурси і зовнішні елементи, з якими здійснюється взаємодія. Ресурсами можуть бути засоби обчислювальної техніки, програмне забезпечення, дані. Прикладами зовнішніх-елементів є мережі зв'язку та інші засоби.

Визначення взаємозв’язків між ресурсами є основою побудови моделі організації з огляду на інформаційну безпеку.

Об'єктивні чинники моделі:

- загрози інформаційній безпеці підприємства, що характеризуються вірогідністю реалізації;
- вразливі місця інформаційної системи або системи контрзаходів (системи інформаційної безпеки);
- ризик - чинник, що відображує можливий збиток організації в результаті реалізації загрози інформаційної безпеки: просочування інформації та її неправомірного використання (ризик відображає вірогідні фінансові втрати - прямі або непрямі).

Принципами побудови збалансованої системи інформаційної безпеки підприємства є:

- аналіз ризиків у сфері інформаційної безпеки;
- визначення оптимального рівня ризику для підприємства на основі заданого критерію;
- вибір таких контрзаходів, які можуть забезпечити досягнення заданого рівня ризику;

Дана методика дає змогу проаналізувати вимоги щодо гарантування інформаційної безпеки підприємства. Для досягнення поставленої мети необхідне вирішення певних завдань [2]:

- розподілення інформації за рівнями доступу;

- прогнозування і своєчасне виявлення загроз безпеці інформаційних ресурсів;

- створення умов, при яких найменш вірогідна загроза безпеці інформаційних ресурсів;

- створення механізму і умов оперативного реагування на загрози інформаційній безпеці, забезпечення проведення робіт в короткі терміни;

- створення механізму і умов для максимально можливого відшкодування і локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб;

- забезпечення оптимального вибору заходів протидії;

- оцінити ефективність контрзаходів, порівняти різні їх варіанти захисту.

Необхідним елементом роботи є вимога замовника до допустимого рівня ризику.

Перед розробкою системи технічних рішень необхідно розробити організаційну політику безпеки. Ця політика, перш за все, повинна описувати порядок надання і використання прав доступу користувачів.

Побудова організаційної політики безпеки складається з декількох етапів:

- внесення до опису об'єкта автоматизації структури цінності і проведення аналізу ризиків;

- визначення правил будь-якого процесу користування цим видом доступу до ресурсів об'єкта автоматизації, що мають цей ступінь цінності.

Всі вимоги до функцій безпеки можна поділити на два типи: управління доступом до інформації і управління потоками інформації[3].

Перелік вимог до системи інформаційної безпеки, ескізний проект, план захисту (далі - технічна документація, ТД) - це вимоги безпеки інформаційного середовища об'єкта замовника, які можуть містити посилання на відповідний профіль захисту, а також чітко сформульовані вимоги.

У загальному вигляді ТД передбачає:

- уточнення функцій захисту;

- вибір архітектурних принципів побудови системи інформаційної безпеки;

- розроблення логічної структури системи інформаційної безпеки (чіткий опис інтерфейсів);

- уточнення вимог функцій забезпечення гарантоздатності системи інформаційної безпеки;

- розроблення методики і програми випробувань на відповідність сформульованим вимогам.

На етапі оцінки досягнутої захищеності оцінюють рівень гарантування безпеки інформаційного середовища об'єкта автоматизації на основі оцінки, за якої після виконання рекомендованих заходів можна довіряти інформаційному середовищу об'єкта.

Базові положення цієї методики припускають, що ступінь гарантування залежить від ефективності зусиль, докладених до оцінювання безпеки.

Список використаних джерел

1. Вітлінський, В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємництві. К.: КНЕУ, 2004. 480 с.

2. Завгородний, В. И. Системный анализ информационных рисков. Вестник Финансовой академии, № 4, 2008. С. 102–109.

3. Зегжда, П. Д. Теория и практика обеспечения информационной безопасности. М.: Яхтсмен, 1996. 192 с.