МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКІЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Рижков Е.В., Гавриш О.С

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
Захист інформації у мережі Інтернет

Дніпро
2017

РЕЦЕНЗЕНТИ

С.В. Свириденко начальник Управління інформаційної підтримки та координації поліції «102» Головного управління Національної поліції в Дніпропетровській області, полковник поліції;

В.В. Сеник кандидат технічних наук, доцент, завідувач кафедри інформатики Львівського державного університету внутрішніх справ.

Методичні рекомендації по захисту інформації у мережі Інтернет / О.С. Гавриш, Е.В. Рижков.– Дніпро: Дніпропетровський державний університет внутрішніх справ, 2017. – __ с.

Проблеми інформаційних загроз та інформаційної власності для навчального середовища є дуже гострими в наш час. У методичних рекомендаціях розглянуто основні аспекти та напрямки пов'язані з інформаційною безпекою як дома так у вищих навчальних закладах, окреслено основні загрози інформаційної безпеки та інформаційної власності, прості методи та засоби захисту інформації при користуванні мережею Інтернет.

Методичні рекомендації можуть бути корисними для педагогів навчальних закладів, які застосовують інформаційні технології у навчальному процесі, для здобувачів вищої освіти та практичних працівників Національної поліції.

Рекомендовано Науково-методичною радою ДДУВС (протокол № від ___.___.2017).

ЗМІСТ

ВСТУП

В кінці XX - початку XXI ст. перехід до постіндустріальної епохи, для якої характерний вільний інформаційний обмін, висунув ряд завдань щодо інтелектуальної власності, і вони вимагають якнайшвидшого рішення. Пов'язано це, перш за все, з протиріччям взаємодії двох систем: інституту інтелектуальної власності, вже сталого протягом кількох десятиліть, і глобальною мережі Інтернет, яка на теперішній день є однією з ключових технологій, найбільшою мірою сприяє процесії переходу світової спільноти до вільного інформаційному обміну.

В цілому, основна функція Інтернету — це передача інформації в усіх її видах, всі інші функції цього комунікаційного каналу випливають з неї. Відповідно, особливості економічних відносин, що виникають у процесі використання Інтернету, безпосередньо пов'язані з передачею інформації. У XXI ст., коли інтелект стає вирішальним фактором суспільного розвитку, а плоди людського розуму (так званий "Інтелектуальний капітал") розглядаються як один з основних об'єктів економічного обороту, право інтелектуальної власності є серйозним стимулом для наукової, творчої, дослідницької діяльності і служить одним з двигунів науково-технічного прогресу.

Поява такого засобу передачі інформації, як Інтернет, відкрило нові перспективи для використання результатів людської думки і обміну ідеями, дало можливість користувачеві Мережі, з одного боку, донести свої ідеї творчі напрацювання до інших людей, а з другого - отримати доступ до продуктів творчої діяльності всієї світової спільноти. Щомиті в світі з'являються мільйони нових файлів, які успішно завантажуються в Мережу. Сотні тисяч доларів заробляють інформаційні стрічки на поширенні фактів у ЗМІ, Інтернет-бібліотеки реалізують інформацію в електронних книгах, музикальні портали транслюють і продають композиції, фотобанки торгують ілюстраціями. Світові бренди Microsoft, Yahoo, Apple, Google рахують свої нематеріальні активи мільярдами доларів - їх високотехнологічні інтелектуальні продукти продаються по всьому світу. Сила-силенна домашніх сторінок користувачів пропонують "творчі" послуги за гроші. Найпоширеніші з них можна без зусиль відшукати в пошуковій системі: "Пишемо сценарії, книги, статті на замовлення, продаємо фотографії, знімаємо відеоролики, створюємо гімни, девізи, назви для компаній, розробляємо дизайни сайтів і т.д. Все це дозволяє однозначно стверджувати, що інтелектуальна власність вийшла в Інтернет.

Створилася парадоксальна ситуація: з одної сторони, є право інтелектуальної власності (право власності є основою ринкової економіки), а з іншого боку, є необхідність широкого поширення інформації.

1.1 Протиріччя в системі охорони прав інтелектуальної власності в Інтернеті

В Інтернеті є ряд об'єктів правової відповідальності: поширення фактів подій та пригод в світі, робота журналістів з видобутку і публікації актуальної інформації зі сфери політики, економіки, соціального розвитку та ін. Згідно із законом, авторське право не поширюється на відомості про факти. Авторським правом охороняється лише форма, в якій ці відомості підносять (за умови, якщо форма носить оригінальний і творчий характер).

Ті, для кого новий текстовий контент - єдиний канал для залучення інвестицій, намагаються максимально обмежити себе від протиправних дій користувачів. Для захисту інформаційних продуктів, що публікується на стрічках новин, найбільші інформагентства попереджають: "Інформація" рейтер (www.reuters.com) є інтелектуальною власністю "Рейтер" і його інформаційних провайдерів. Будь-яке копіювання, передрукування чи наступне поширення інформації, в тому числі вироблене шляхом кешування, кадрування або з використанням аналогічних засобів, суворо забороняється без попередньої письмової згоди з боку "Рейтер". Логотип "Рейтер" і сферичний логотип "Рейтер" є зареєстрованими товарними знаками групи компаній "Рейтер" в усьому світі".

Істотно змінилися взаємодії відносини між володарем інтелектуальної власності та її споживачами. якщо роль посередника між автором і публікою традиційно виконував видавець, то тепер її здійснюють організації, що управляють майнові правами на колективній основі, і організатори колективної творчості — власники мережевих ресурсів. У той же час одне з досягнень сучасного людства - це проголошення прав на доступ до інформації та знанням. Громадські інтереси вимагають перегляду традиційної авторської монополії, і в першу чергу на наукові твори. Обмеження доступу до інформації суперечить також нормам законодавства, зобов'язаннями перед міжнародним співтовариством сприяти подоланню інформаційного розриву і забезпечення рівного доступу до інформації.

З правової точки зору, феномен Інтернету укладений в одну просту річ: даний універсальний майданчик зовсім не захищає правовласників від крадіжки безкоштовного, на перший погляд, контенту (змісту). Так, залишаються економічно і юридично беззахисними перед беззаконням власники домашніх сторінок і комерційних сайтів, фотографи, журналісти, програмісти, музиканти, поети, письменники і інші користувачі, що публікують свої авторські роботи.

У Західній Європі та США законодавство в цій сфері більш розвинене, ніж у нас (досить згадати хоча б Digital Millenium Copyright Act в США). Але злагоджено працюючої законодавчої системи, наприклад, такою, яка є щодо товарних знаків, патентів та інших "класичних" об'єктів інтелектуальної власності, за кордоном також немає. Поки що, це загальна для всього світу проблема.

Зрозуміло, що відсутність норм, які б враховували особливості Інтернету, і його слабка контрольованість дозволяють безкоштовно використовувати інтернет-ресурси, що знаходяться в вільному доступі, і в багатьох випадках безкарно ухилятися від економічної та правової відповідальності.

Має місце безпрецедентне протиріччя і складність регулювання відносин власності в Інтернеті. Однак необхідно встановити баланс між інтересами творців інтелектуальних результатів і суспільства.

1.2. Концептуальна основа прав власності в Мережі

Інтелектуальна власність в сучасному світі є найважливішим економічним ресурсом. У період трансформації сучасного суспільства і його переходу в постіндустріальну епоху пріоритетне значення починають купувати не природні ресурси і навіть не власне високотехнологічне виробництво, а інтелектуальний капітал і, відповідно, права на володіння і розпорядження тим чи іншим інформаційним ресурсом, значна частина якого зосереджена в мережі Інтернет . Саме тому інтелектуальна власність в Інтернеті повинна перебувати під захистом авторського права і розглядатися як нематеріальний актив її власника (автора).

Йде становлення інституту інтелектуальної власності в Мережі як комплексу економічних, соціальних, правових і культурних феноменів. Феномен інтелектуальної власності в мережі Інтернет - це комплекс відносин, який повинен будуватися на основі системи договірних зобов'язань.

Економічна складова відносин суб'єктів і об'єктів простору Інтернету полягає в праві володіти і розпоряджатися тим інтелектуальним капіталом, яким є інформаційні ресурси, розміщені в Мережі. Цей вид власності потребує чіткого визначення та нормативному оформленні.

Об'єкти авторсько-правової охорони в мережі Інтернет як об'єкти комерційного інтересу диференціюються залежно від того, на якому етапі дані об'єкти пов'язані з використанням Інтернету - на етапі створення або на етапі поширення тієї чи іншої інформації.

Інтелектуальна власність в Інтернеті стає основою великого сегмента "електронної комерції" - сегмента "творчого" бізнесу, що обумовлює необхідність створення нових форм економічних відносин між користувачами Мережі та правовласниками тих чи інших інтернет-ресурсів.

Таким чином, в Інтернеті формуються економічні взаємини нового типу в області інтелектуальної власності, отже, потрібні практичні пропозиції щодо захисту авторських прав на матеріали, розміщені в мережі Інтернет, необхідна розробка способів та стратегій захисту запобігання несанкціонованому доступу до використання інтелектуальної власності в мережі Інтернет.

2. Основні сучасні інформаційні загрози та методі боротьби з ними

1) Загрози для особистої безпеки
•Загроза ознайомлення з матеріалами небажаного змісту (порнографія, ненормативна лексика, суїцидального характеру, сектантські, расистські та ненависницькі, вибухові речовини, хакерські сайти)
• Загроза отримання недостовірної інформації
• Загроза залежностей (комп'ютерної, ігрової, Інтернет і т.д.)
• Загроза спілкування з небезпечними людьми (шахраями, збоченцями і т.д)
• Загрози вчинення протиправних дій (хакерство, порушення авторських прав і т.д.)

2) Загрози витоку персональної інформації
•Загроза розголошення конфіденційних даних (прізвища, імені, адреси, номерів кредитних карток, телефону і т.д).

3) Загрози для персональних комп'ютерів
• Загроза проникнення вірусів, черв'яків.
• Загроза завантаження шкідливого активного коду
•Загроза завантаження програм з прихованими функціями: троянців, клавіатурних шпигунів і т.д.

Розглянемо більш детально сучасні напрямки в сфері інформаційної безпеки та прості методи для запобіганню можливих злочинних дій з їх сторони.

Apps

Гороскоп, прогноз погоди, мобільні ігри, навігатор - сучасний смартфон чи планшет важко уявити без корисних додатків. Тут приховано пастку: деякі додатки надто "допитливі" та збирають конфіденційні дані, передаючи їх у мережу в незахищеному вигляді. Це можливо насамперед тоді, коли ми користуємося громадськими точками доступу до Wi-Fi.

Найбільші "прогалини" у сфері захисту інформації мають безкоштовні додатки. Завдяки ним дані про ваше місце перебування, паролі, контакти, пошукові запити, СМС, повідомлення в соцмережах осідають на серверах, розкиданих у всьому світі. На базі цих даних створюються профілі користувачів, які надзвичайно цікавлять рекламників. Перевірити надійність "Apps" можна на різноманітних сайтах, наприклад http://www.checkyourapp.de/.

E-Mail

Небезпечний електронний лист може виглядати просто. У темі вказано, наприклад, "відповідь на ваш запит". Ніби нічого підозрілого, тож ви відкриваєте лист і вкладений у нього файл. Раз, два - і в вашому комп'ютері поселився "троян" (троянський вірус) чи програма, що непомітно: зчитує дані, копіює паролі, під'єднує ваш комп'ютер до інших.

Деякі електронні листи закликають отримувачів вводити свої конфіденційні дані і виглядають так, мовби їх надсилає ваш банк. Цей вид інтернет-шахрайства зветься "phishing" (схоже на "fishing" - "риболовля" з англійської). Увівши дані своєї картки в підозрілому листі, незабаром ви можете дізнатися, що ваш банківський рахунок обікрали. Тому завжди уважно читайте, про що вас просять. Не відкривайте прикріплені файли, якщо відправник листа невідомий, та в жодному разі не вводьте фінансові дані. Пам'ятайте: банки не запитують клієнтів про їхні пін-коди, бо не повинні цього знати.

Facebook

Підчепити комп'ютерну заразу можна і в улюбленій соцмережі. Ви вже, напевно, отримували повідомлення нібито від друзів із текстом на кшталт "Ти повинен побачити це відео! Переходь за цим лінком!". Одним необережним "кліком" можна завантажити "троян". Іноді достатньо провести курсором мишки по отриманій картинці - і Facebook повідомляє в новинній стрічці, що ви "лайкнули" фото. Самі ви про це й не підозрюєте, а шкідницьке посилання поширюється. Розумники, які програмують такі хитрощі, знають, як працюють популярні антивірусні програми та як їх обійти.

Перш ніж нажимати на посилання, що обіцяє "надзвичайно смішне відео", придивіться, чи це справді Youtube-лінк. Не переходьте на все, що виринає на новинній стрічці. Будьте обережні з Facebook-додатками. Не лінуйтеся періодично перевіряти налаштування приватності.

Google

Найпопулярніша пошукова машина світу. Слово "гуглити" звучить не лише з народних вуст: приміром, у Німеччині воно було занесене до авторитетних словників видавництва Duden. Утім, Google нерідко критикують, адже до захисту приватних даних концерн ставиться без надмірного пієтету. Щоб користуватися певними сервісами, необхідно дозволити програмі "бачити" особисту інформацію, як-то, наприклад, місце перебування.

Cookies

Це текстові дані, які завантажуються на комп'ютер із веб-сайтів. Вони зберігають інформацію: паролі, адреси поштових скриньок, товари в "кошиках" інтернет-крамниць. Користувач не повинен щоразу заносити все це заново. Cookies практичні, але є нюанс: вони збирають про нас дані, які використовуються для кращого розміщення інтернет-реклами. Якщо вчора ви шукали в мережі "дамський годинник із леопардовим браслетом", не дивуйтеся, що сьогодні реклама годинників вас переслідує. Втішає те, що Cookies можна заблокувати в кожному інтернет-браузері (наприклад, функція "Disconnect Search").

IP-адреса

Це мов поштова адреса в реальному житті. Кожен пристрій із доступом до інтернету має власну IP-адресу. Таким чином його можна вирахувати. Абревіатура IP означає Internet Protocol - мережевий протокол, який уможливлює обмін інформацією між різними комп'ютерами. Ось як виглядає типова IP-адреса: 193.98.161.111. Знаючи її, можна зрозуміти, послугами якого інтернет-провайдера ви користуєтеся та в якому регіоні перебуваєте. Якщо на ваш запит Youtube відповідає: "На жаль, це відео недоступне для перегляду в Вашому регіоні", отже, система вирахувала, що ви знаходитесь в Україні та не маєте прав на перегляд ролика.

Jailbreak

Розрекламовані та зведені в культ IOS-пристрої, тобто iPhone, Ipad чи iPod Touch, мають обмеження. Програмне забезпечення на них можна встановлювати тільки з оригінальних App-Stores - інтернет-крамниць Apple. Ті, кому цього мало, давно знайшли вихід. Майже біля кожної станції київського метро можна знайти "точки" ремонту і продажу смартфонів, де вам пообіцяють "перепрошити" будь-який смартфон і планшет. Умілець проникає в систему і встановлює програму, яка дозволить завантажувати на планшет чи смартфон будь-які додатки. Користувачі називають це Jailbreak.

"Перепрошивка", на перший погляд, зручна. Але таким чином "природну" систему захисту комп'ютера чи смартфона "ламають". Після того пристрій легше інфікується вірусами та вже не може надійно захищати ваші конфіденційні дані. Операційна система вже не працює так злагоджено, як раніше. Про гарантійний ремонт теж доведеться забути.

QR-код

Квадратики з чорно-білими цятками можна знайти всюди. Це матриці з бінарними кодами, тобто багатьма одиницями й нулями, які можна фотографувати смартфоном і отримувати посилання на веб-сайти. Пастка є й тут, адже ніхто не може знати наперед, що приховує QR-код. Відкривши посилання, ви можете натрапити на сторінку, що "заразить" смартфон вірусом. Будьте обережні із невідомими QR-кодами, які, наприклад,

пропонують скорочений URL (bit.ly). Або встановіть захисний додаток, який працює за принципом антивірусної програми.

QR-код може спрямувати на небезпечний сайт

WhatsApp

Популярний безкоштовний додаток для обміну повідомленнями, фото, аудіо та відео стрімко витісняє СМС. Але й тут є над чим подумати. Додаток отримує доступ до вашої телефонної книги, бо тільки так можна побачити, хто з друзів теж користується WhatsApp. Ваші дані надсилаються на сервер, розташований у США. Що з ними там відбувається, достовірно невідомо. І хоча з серпня 2012 року повідомлення WhatsApp передаються в закодованому вигляді, прогалини в системі захисту додатка все ще існують. Чи має фірма WhatsApp офіс, точно невідомо. Та підозрілі факти не впливають на популярність додатка: за даними виробника, програмою вже користуються понад 400 мільйонів користувачів у всьому світі.

Дані для авторизації

Один із улюблених видів спорту для хакерів - зламувати особисті дані. Поштова скринька, Facebook- чи Twitter-акаунт, пароль для онлайн-банкінгу… Через "зламані" сторінки в соцмережах поширюється спам, а банківські рахунки "очищуються" від грошей. Чимало користувачів полегшують забаву хакерам, використовуючи для різних цілей ті самі паролі. Це зрозуміло, адже запам'ятати таку кількість паролів, яка нам сьогодні потрібна, нереально. Але чимало експертів радять саме це.

Вигадуйте складні паролі з малими й великими літерами, цифрами, знаками, транслітерацією. Не використовуйте дату народження, номер телефону, ім'я песика чи улюбленого актора. У всесвітній мережі можна знайти безліч "генераторів паролів", як-то, наприклад, http://www.heise.de/download/passwort-generator.html, а також поради для вигадування безпечних паролів.

Досить простою и популярною програмою для зберігання даних для авторизації є програма «LastPass»

LastPass – програма, що створена для зручності і надійної безпеки зберігання паролів. Програма є безкоштовною (виключенням є мобільні додатки, крім додатка для iPad).

Вона існує у вигляді плагінів для Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Maxthon і Apple Safari. Також є LastPass букмарклет для інших браузерів. Паролі в LastPass зашифровані алгоритмом AES-256, зберігаються в «хмарі» і можуть бути синхронізовані між пристроями. LastPass також має заповнювач форм, що дозволяє автоматизувати введення паролів і заповнення форм. Плагін підтримує генерацію безпечних паролів, має журнал входу на сайти.

Можливості програми LastPass :

• один головний пароль;
• синхронізація браузерів;
• генерація стійких паролів;
• шифрування паролів;
• заповнювач форм;
• імпорт і експорт паролів;
• дворівнева аутентифікація;
• google Authenticator;
• переносна;
• мобільний доступ через браузер

Програма виконана у вигляді плагіна (доповнення або надбудови) до багатьох відомих браузерів, включаючи Internet Explorer, Google Chrome, Mozilla Firefox, Opera і Apple Safari і т.д. Цікаво і те, що сам додаток не обмежується тільки операційними системами сімейства Windows. Існують спеціальні розробки для Mac OS X, Linux і навіть мобільні версії. Причому, між усіма цими варіантами суттєвої різниці немає, оскільки, вони можуть синхронізуватися між собою. Крім усього іншого, програма Lastpass поширюється абсолютно безкоштовно і не має обмежень по установці або часу використання.

Якщо говорити про основні можливості програмного пакету Lastpass, то серед основних функцій варто виділити максимальну безпеку зберігання паролів. Тут застосовується дворівневий захист. Іншими словами, можна зашифрувати кожен окремий пароль, а при доступі до всієї бази паролів, застосовується, так званий, майстер-пароль. Крім того, зовсім необов'язково придумувати власні паролі. Додаток Lastpass має вбудований генератор паролів, який здатний створювати досить складні комбінації з літер, цифр і символів. Само собою зрозуміло, що зламати такий пароль при всьому бажанні буде дуже непросто.

Однією з найголовніших функцій в системі безпеки можна назвати і захист від комп'ютерних шпигунських програм. Крім усього іншого, тут використовується локальне зберігання даних, якими можна поділитися з іншими користувачами.

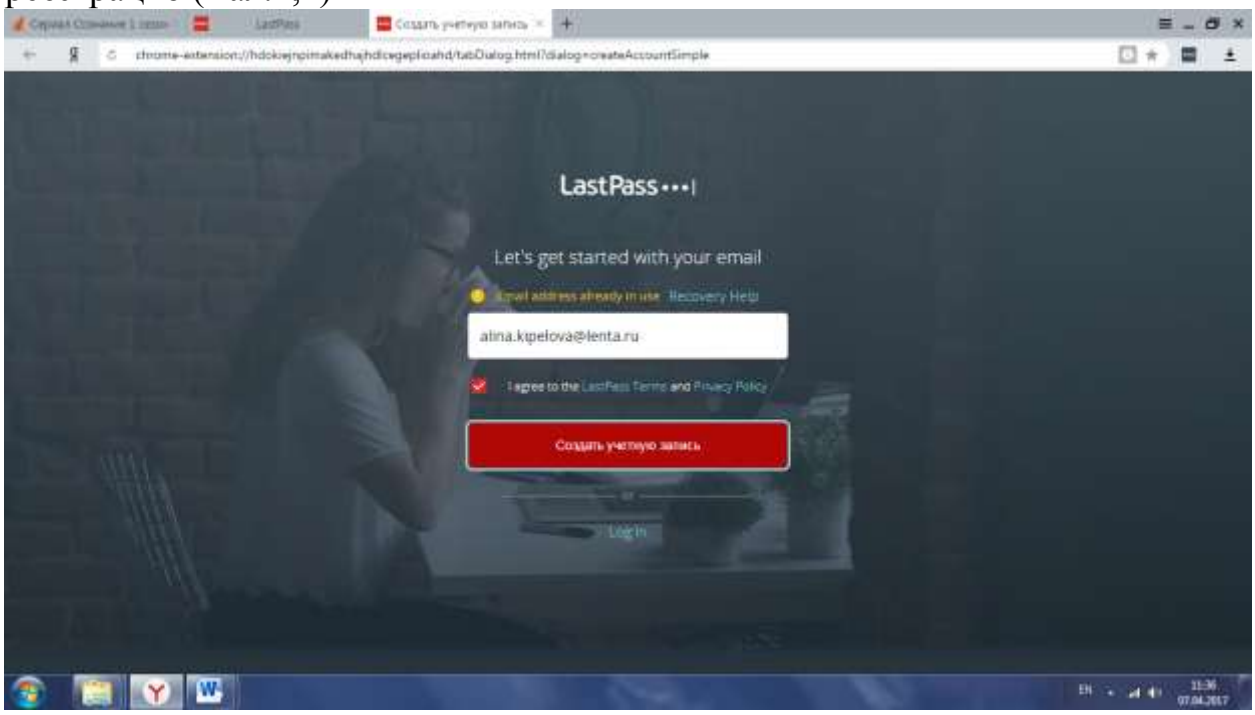
Серед найбільш затребуваних користувачами можливостей програма Lastpass пропонує систему автоматичного заповнення веб-форм. Тобто, користувачеві не потрібно кожен раз при доступі до того чи іншого веб-ресурсу вводити пароль заново. Досить зберегти (або згенерувати) його в програмі один раз. Згодом паролі буду введені автоматично.

Не менш важливим є і те, що додаток Lastpass здатне імпортувати раніше створені паролі з вище перерахованих браузерів. Власне, як і нові дані, такі паролі можна зберігати в самому додатку Lastpass.

Варто зазначити, що інтерфейс програми Lastpass досить простий і зрозумілий. Хоча тут і використовується англійська мова, навіть при мінімальному його знанні, з додатком Lastpass можна розібратися без праці.

Та й налаштувань тут, за великим рахунком не багато, практично всі вони автоматизовані. Хоча є і розширені можливості для досвідчених користувачів

Після встановлення програми вам насамперед потрібно пройти реєстрацію (мал.1,2)

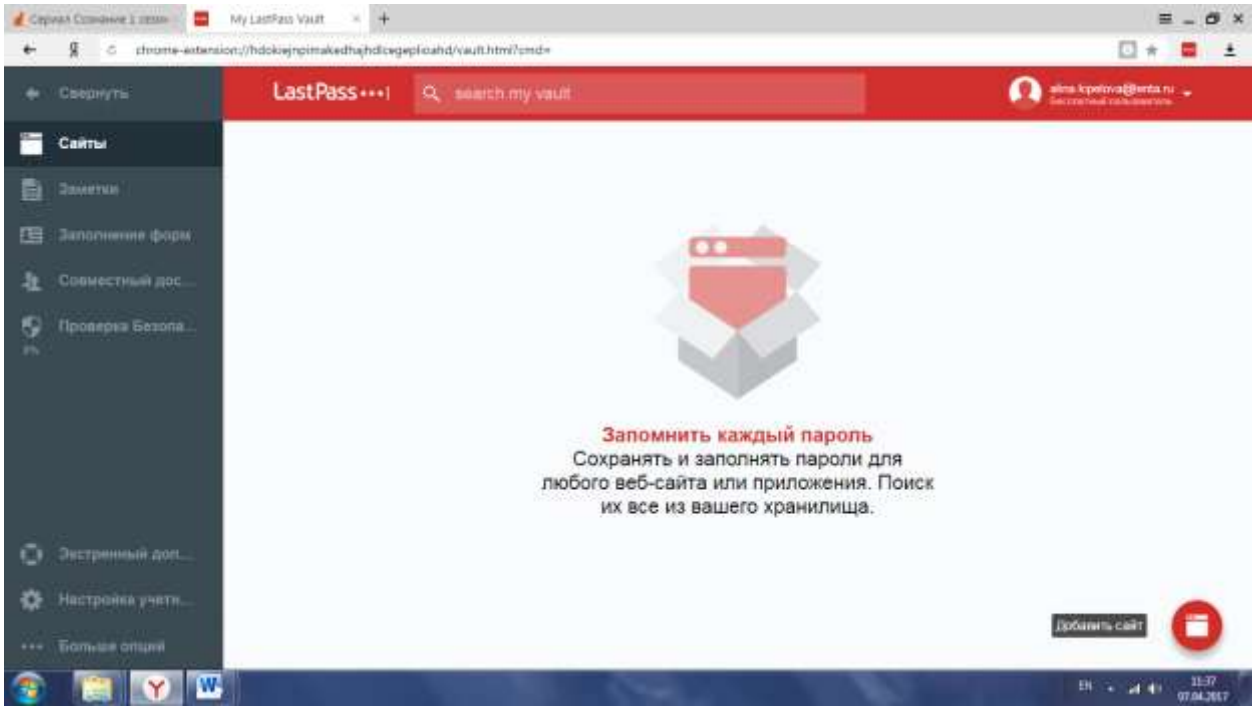


Мал.1

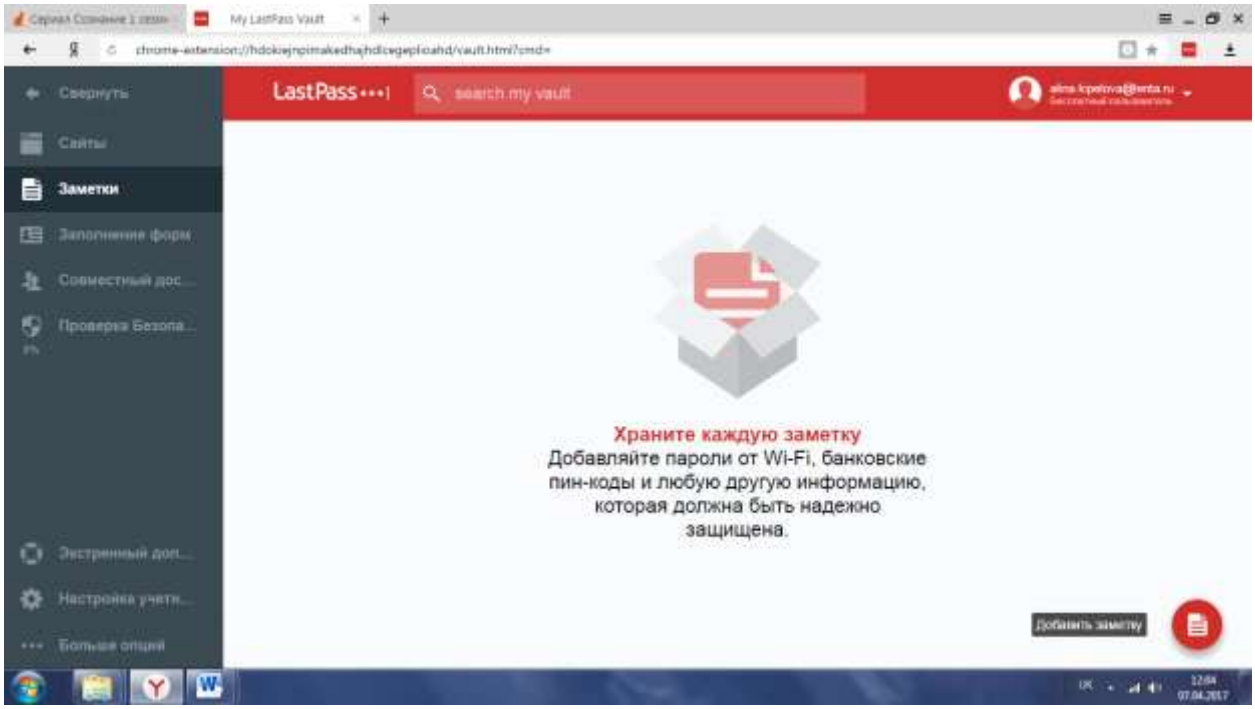
Мал.2

Це потрібно для того, щоб ви могли запам'ятати тільки один реєстраційний пароль від LastPass, а всі інші паролі будуть зберігатися всередині програми. Потім, додаток додасть розширення в усі ваші браузери, які встановлені на комп'ютері.

Інтерфейс програми-розширення цікавий, лаконічний і виконаний у flat-дизайні. Ліва частина відведена під меню навігації, а права - під вкладки з інформацією: сховище, профілі форм, загальний доступ, Enterprise, підручники. Тут же, за допомогою інтерфейсу, ви можете додавати паролі від сайтів вручну, якщо з якихось причин не хочете автоматично (мал.3,4)



Мал.3



Мал.4

При вході на будь-який сайт, який вимагає реєстрації, після авторизації на ньому, LastPass запросить у вас зберегти пароль чи ні. Нажавши по кнопці

«Зберегти» ви автоматично додаєте пароль в менеджер LastPass і вже при наступних авторизації LastPass сам знатиме, який пароль вводити.

Суть роботи LastPass схожа з функцією запам'ятовування паролів в браузерах, але з тим винятком, що в LastPass ви зможете синхронізуватися з усіма своїми пристроями, і працювати з веб-сайтами набагато швидше і безпечніше як на домашньому комп'ютері і планшеті, так і на роботі і телефоні.

Браузер

Іноді можна тільки дивуватися: як мій комп'ютер міг заразитися, якщо у мене були оновлені антивірус і операційна система? А між тим, багато вірусів в наші дні мутують із запаморочливою швидкістю. Тоді логічно поставити питання: як вірус виявився в моєму комп'ютері?

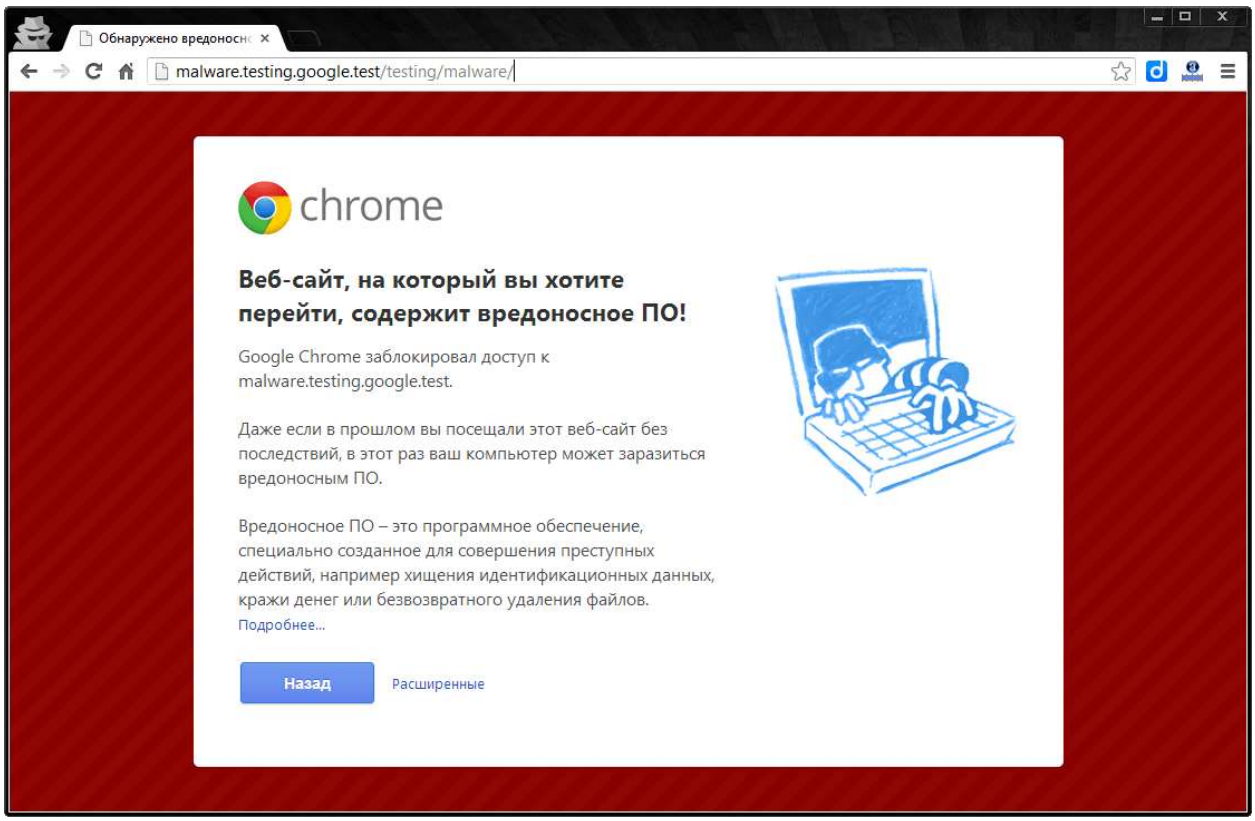
Ну, один з найбільш ймовірних способів проникнення - це браузер. Відразу виникає думка, що тоді потрібно завести окремий комп'ютер для роботи, другий - для ігор, а третій - для перегляду сайтів . Не кожен бюджет витримає такі витрати. Ось деякі способи безпечного перегляду веб-сайтів, якими Ви можете скористатися в більшості випадків абсолютно безкоштовно.

• Віртуальна машина

Віртуальна машина - це спеціальна машина, яка дозволяє Вам переглядати сайти прямо з вашого власного комп'ютера. Це як комп'ютер, який знаходиться всередині вашого комп'ютера, - якесь захищений простір, в якому Ви можете завантажувати інші операційні системи. Будучи ізольованою, віртуальна машина не може заразити Ваш комп'ютер. Прикладами безкоштовних віртуальних машин є VirtualBox для Windows і VMware Player для Windows.

• Браузер в «закритій коробці»

Трохи простіше ізолювати всередині себе роботу веб-браузера. Такий прийом відомий як «пісочниця» (sandbox). Еквівалентно запуску браузера в окремій «клітці», з якої нічого не може вийти за межі, поки ми самі цього не захочемо. Наприклад, Ви можете використовувати Panda SafeBrowser або безпечний браузер Google Chrome. (мал.5)



(мал.5)

• Встановлення додаткових плагінів

Навігація по сайтам без JavaScript, Flash-анімацій або Java-аплетів значно підвищує безпеку перегляду сайтів, але це також може привести до певних проблем. Щоб подолати і цю перешкоду, такі браузери як Firefox і Chrome мають додаткові плагіни для контролю того, що і коли завантажується: Flashblock (Firefox і Chrome) і такі додатки для видалення скриптів як Chrome NotScripts є кращими.

• Віртуальний перегляд

Існують сторінки, які виступають в якості посередника між Вашим браузером і тією сторінкою, яку Ви хочете відвідати, - щось на зразок проксі. Наприклад, Virtual-Browser.

Флешка

Річ, без якої не обійтися ні студенту, ні молодому фахівцю. Водночас вона може відправити в небуття весь жорсткий диск комп'ютера. Флешка складається з блоку пам'яті та контрольного чипа, який керує даними і "спілкується" з комп'ютером, до якого під'єднана флешка. Якщо отримати контроль над чипом, то можна маніпулювати й комп'ютером - змушувати видаляти дані та інше. Також флешка є ідеальним переносником шкідливих програм. Тому користуйтеся нею тільки на комп'ютерах, які захищені антивірусними програмами.

Для ефективного захисту необхідна не лише наявність антивірусного пакету на комп’ютері, але й правильна організація роботи по антивірусному захисту. В останні роки на ринку комплексних антивірусних пакетів на лідируючі позиції по багатьом параметрам вийшов Qihoo 360 Total Security від компанії Qihu 360 - відмінний безкоштовний антивірус, який захистить вас від більшості шкідливих програм, що чекають в віртуальному світі. Антивірус складається з 5 компонентів: антивірусного ядра Avira і Bitdefender, System Repair, який відповідає за відновлення системи, проактивного компонента QVM II і вбудованого хмарного сервісу 360 Cloud.

Всі ці «лицарські обладунки» дозволять вам користуватись Інтернетом і не відволікатись через «троянів» та інших «радощів». Як ми вже згадували, на будь-якому сайті можна скачати 360 Total Security безкоштовно, не побоюючись підступу.

Антивірус 360 Total Security очистить ваш комп'ютер від вірусів, підчистить «залишки» видалених програм і при необхідності відновить пошкоджену систему. Більш того, все це станеться швидко і без якихось додаткових маніпуляцій з вашого боку. До речі, щоб працювати з софтом було зручно, він досить приємно графічно оформлений, та має український інтерфейс.

Компанія також випустила 360 security essential - полегшена версія антивіруса, в якій відсутня перевірка безпеки WiFi, оптимізація системи і очищення тимчасових файлів комп'ютера.

Таким чином, якщо вам потрібен простий і в той же час надійний сканер безпеки, то 360 Total Security - це кращий варіант.

Список бібліографічних посилань та основних публікацій авторів

1. Положення про проведення професійно-орієнтованої ділової гри «Лінія – 102» // Затверджено Наказом ДДУВС від 24.02.2017 № 141.
2. Порядок проведення комплексних оперативно-тактичних навчань // Затверджено Науково-методичною радою ДДУВС протокол № 2 від 20.10.2016.
3. Золотоноша О.В., Рижков Е.В. Інноваційний підхід до вдосконалення практичної складової навчального процесу у вузах МВС на прикладі ДДУВС / О.В. Золотоноша, Е.В. Рижков // Науковий вісник Дніпропетровського державного університету внутрішніх справ : Збірник наукових праць. – 2016. - № 4 (84) . – С. 15-22.
4. Гавриш О.С., Махницький О.В., Прокопов С.О., Рижков Е.В. Навчальна інформаційно-технічна платформа Національної поліції в системі практичного навчання (Досвід Дніпропетровського державного університету внутрішніх справ) / О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков // Використання сучасних інформаційних технологій в діяльності Національної поліції: матеріали Всеукраїнського науково-практичного семінару (25 листопада 2016 р., м. Дніпро). – Дніпропетровський державний університет внутрішніх справ, 2016. – С. 12-19.
5. Прокопов С.О. Навчальне автоматизоване робоче місце оперативного працівника в інформаційно-технічній платформі

інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників національної поліції в ДДУВС / С.О. Прокопов // Юридична наука: сучасний статус, перспективи, інновації: матеріали всеукраїнської науково-практичної конференції (7 грудня 2016) / Редкол.: Краснощок А.В. (гол. ред.) та ін. – Кривий Ріг: КФ ДДУВС, 2016. – С. 83-88.

6. Прокопов С.О., Махницький О.В., Гавриш О.С. Інформаційно-технічна платформа інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників Національної поліції в ДДУВС / О.С. Гавриш, О.В. Махницький, С.О. Прокопов // Право і суспільство. – 2017. – № 1. – С. 182–190.