

obnaruzheniya-vtorzheniy-v-korporativnoy-informatsionnoy-sisteme-predpriyatiya-s-ispolzovaniem.

4. Соціальна інженерія в інтернет-просторі. [Електронний документ]. – URL: http://chtei-knteu.cv.ua/herald_ru/content/download/archive/2016/v3-4/NV-2016-v3-4_13.pdf.

5. Мохаммед Ф. О. Межсетевые экраны. *Доклады БГУИР*. 2009. № 5 (43). [Электронный документ]. URL: <https://cyberleninka.ru/article/n/mezhsetevye-ekrany>.

Ключові слова: RAT вірус, структура RAT вірусу, віртуальна машина, мережевий екран, захист від RAT вірусів.

Ключевые слова: RAT вирус, структура RAT вируса, виртуальная машина, сетевой экран, защита от RAT вирусов.

Keywords: RAT virus, RAT virus structure, virtual machine, firewall, protection against RAT viruses.

Научный руководитель: доцент Задерейко А. В.

Соловийов Артем Сергійович

Національний університет «Одеська юридична академія»,
студент 3 курсу факультету кібербезпеки
та інформаційних технологій

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕРНЕТЕ

В настоящее время существует проблема кражи персональных данных. В условиях глобализации пользования человека всё больше приобретает связь с глобальной сетью Интернет. За последние десятилетие количество пользователей возросло. Работая в интернете человек получает множество полезной информации, но иногда он может не заметить то как его персональные данные оказываются под большой угрозой. Вопрос о защите персональных данных является очень актуальным, особенно является актуальной информация защита персональных данных, попавшая в интернет. Личные данные – это любые данные, идентифицирующие человека. Ваше имя, адрес электронной почты, местоположение, биометрические данные, логин [1].

В современном мире практически у каждого человека есть электронная почта, профили в различных социальных сетях. В любом случае взлом аккаунтов может привести в потере персональных данных. Отдельным вопросом защиты персональных данных в интернете возникает, если обратить внимание на электронную коммерцию, ведь онлайн покупки стали естественным явлением для большинства людей.

При совершении платёжных операций, стоит особо внимательно изучить сайт, на котором будет производиться покупка товара, нежелательно привязывать свою банковскую карту к платёжной системе банка. В повседневной жизни люди оставляют за собой. Цифровую информацию о том: где живут, какую еду предпочитают, что и где покупают и другие данные о личной жизни. По этим элементам жизни человека, можно узнать больше, чем они сами хотели бы о себе рассказать.

Узнав такую информацию о человеке, мошенник может воспользоваться методом социальной инженерии и получить ещё больше персональных данных чем человек мог оставить в интернете.

Угроза потери персональных данных может привести к подмене данных для выполнения входа в социальные сети. Из-за потери персональных данных могут появляться фейковые аккаунты в социальных сетях для проведения мошеннических операций. Получение финансовых данных: номера кредитных карт, электронных кошельков, аккаунтов платных онлайн игр. А также мошенник, получив персональные данные человека может их удалить.

Пользуются персональными данными не только злоумышленники. Личными данными человека также активно интересуются специалисты по таргетинговой рекламе. Главный источник получения сведений для данного вида рекламы – файлы cookie, которые передаются браузером пользователя на сервер таргетингового агентства [2].

Методы самостоятельной защиты персональной информации. Защиту от вирусов, которые могут овладеть личными

данными могут обеспечить только лицензированные антивирусные программы, которую нужно постоянно обновлять. Перед установкой программ из не проверенных источников или регистрацией на сайтах с введением персональных данных, требуется внимательно прочитать пользовательское соглашение, поскольку одним из его условий может быть обработка и использование личной информации.

Пользователи мобильных устройств имеют функцию, разрешения или запрета получения приложением личной информации, например: геолокация, список записной книжки, фотогалерея, камера и внутренние файлы устройства. Важно иногда проверять какие личные файлы вы доверили приложению на своём устройстве. При появлении подозрительных действий со стороны приложения рекомендуется отказаться от установки и пользования таким приложением.

Для предоставления лучшей защиты в социальных сетях или других электронных сервисах, советуется использовать сложные пароли. Для создания паролей можно использовать генератор паролей. Для каждого сервиса рекомендуется использовать отдельный пароль, чтобы они не повторялись. Менять пароли следует менять каждые пару месяцев.

А также для большей защиты своих данных и аккаунтов, требуется использовать двойную аутентификацию. Каждый раз для входа будет требоваться код, который будет случайно генерироваться в стороннем приложении для большей надёжности.

В местах где вы можете подключиться к бесплатным точкам доступа к интернету, часто сидят злоумышленники, которые могут перехватить ваш трафик и получить ваши личные данные. Для этого можно использовать VPN сервисы, которые будут шифровать ваш трафик, и злоумышленнику будет сложнее получить ваши данные.

В заключение можно выделить правила для пользования интернетом, которых следует придерживаться, чтобы обеспечить свои персональные данные.

1. Следить за тем что и кому пересылается в сообщениях.

2. Внимательно изучать лицензионное соглашение на наличие пункта об обработке персональных данных.

3. При пользовании электронной коммерции, не привязывать свои банковские карты в непроверенных сервисах.

Таким образом, можно обеспечить достаточную защиту персональных данных. Существует множество способов обезопасить свои данные через генераторы паролей, двух этапная аутентификация и различные приложения для шифровки трафика в интернете, так как защита личной информации в современном мире это большая проблема, много злоумышленников пытаются украсть вашу информацию, прикрываясь поддельными сервисами очень похожими на настоящие.

Список використаних джерел:

1. Юрист и закон [Електронний ресурс] – Режим доступу до ресурсу: https://uz.ligazakon.ua/magazine_article/EA012189.

2. SEARCHINFORM [Електронний ресурс] – Режим доступу до ресурсу: <https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-internete/>.

Ключові слова: Персональні дані, особиста інформація, інтернет, захист.

Ключевые слова: Персональные данные, личная информация, интернет, защита.

Key words: Personal data, personal information, internet, protection.

Науковий керівник: к.т.н., доцент Бойко В. Д.

Степанов Денис Вікторович

Національний університет «Одеська юридична академія»,
студент 2-го курсу факультету кібербезпеки
та інформаційних технологій

ІНСТРУМЕНТАРІЙ QT ДЛЯ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У наш час існує величезна кількість цікавих технологій і рішень в IT-сфері і початківцям доволі важко обрати шлях, яким