УДК: 004

ЦИФРОВАЯ ГИГИЕНА В СОВРЕМЕННОМ МИРЕ ИЛИ КАК НЕ БЫТЬ ИСПОЛЬЗОВАННЫМ СОЦИАЛЬНЫМИ СЕТЯМИ

Лихаева М.А., Горбачева Д.С., Панкова Н.Г.

Брянский государственный университет имени академика И.Г.Петровского, Россия, Брянск, email: bryanskgu@mail.ru

Рассматривается проблема цифровой гигиены как одной из ведущих проблем современности. Приводятся статистические данные, связанные с измерениями в области информационного пространства. Приведены основания опасности неосознанного использования социальных сетей и сети Интернет. Представлены рекомендации по правильному и эффективному использованию современного Интернет-пространства.

Ключевые слова: цифровая гигиена, социальные сети, цифровая безопасность, информационное пространство, Интернет-пространство

Ежегодно время, проведенное людьми в социальных сетях, возрастает: если в 2013 году каждый тратил в среднем около 90 минут в день, в 2021 году эта отметка достигла 150 минут. Задумайтесь, как часто мы бездумно пролистываем ленту вместо того, чтобы начать заниматься действительно важными и неотложными делами? Сколько времени таким образом тратиться в пустую? Попробуем рассмотреть способы организации осознанного интернет-присутствия, и таким образом использовать соцсети с пользой.

Распространено мнение, что информационные технологии не могут принести вреда, и многие люди используют и, даже не подозревая о всех возможностях ИКТ как положительных, так и отрицательных. И эта непредвзятость может дорого обойтись. Современные девайсы в прямом смысле этого слова окружают нас информационной средой, которая влияет на наше мышление, убеждение, мировосприятие и даже здоровье.

Никто не сомневается в том, что благодаря смартфонам наши познавательные возможности увеличились в значительной степени. Но зачастую они также крадут наше внимание и время: согласно исследованиям широко распространены симптомы, напоминающие симптоматику синдрома дефицита внимания, так молодые люди могут проверять свой телефон 87 раз за день.

Стоит напомнить, что в прошлом информация проходила огромное количество проверок качества, достоверности, обоснованности, до того как она попадет на заголовки

газет или будет передана по каналам радиосвязи. В современном же информационном сообществе производство информации стало настолько молниеносным и объемным, что отфильтровать ее и идентифицировать кажется почти невозможным. В результате задача распределения информации ложится на плечи простого потребителя.

Именно так и появилось понятие «цифровая гигиена». Если раньше слово «гигиена» использовалось только в области медицинских знаний, то на сегодняшний день его употребление распространилось даже на информационную область. Собственно, цифровая гигиена подразумевает действия пользователя, нацеленные на обеспечение безопасной и осознанной информационной среды.

Совершенно ясно, что несоблюдение таких правил может привести к печальным последствиям: потери конфиденциальных данных, материальных средств, доступа к личным аккаунтам и т.д.

Итак, какие же принципы цифровой гигиены и безопасности вам необходимо знать?

— Безопасность или практичность? Насколько вы готовы к внедрению каких-либо элементов защищенности? Ответ на данный вопрос каждый определяет самостоятельно, принимая во внимание свои индивидуальные особенности и потребности. Ведь безопасность практически всегда идет вопреки удобству.

— Источники информации. Сперва следует изучить источники информации. Электронные почты, мессенджеры, социальные сети — это те средства, посредством которых человек и знакомится с определенной информацией. В целях безопасности необходимо постоянно отписываться от всех ненужных и бесполезных развлекательных подписок и рассылок. Среди всего этого многообразия информации можно с легкостью потерять что-то действительно нужное и полезное либо своевременно не заметить сообщение мошенников. В случае если вы прекратили использовать какой-либо сервис, вам следует удалить или заблокировать его. Неактивная в течении нескольких лет почта может быть атакована взломщиками, тогда с ее помощью взломают уже действующий почтовый ящик.

— Пароли остаются одним из главных средств аутентификации в Интернете. Для цифровой гигиены и безопасности сервиса является важным уникальность примененного кода доступа. Если подобрать простейший пароль — например, такой как password, 0000 или 1234 — у взломщиков будет больше шансов украсть ваши данные. То есть из-за слишком простого пароля сервис станет уязвимым, не важно сколько средств было бы вложено компанией-провайдером в его безопасность. Разделите сайты и сервисы на несколько категорий согласно уровню их критичности. В самую значимую необходимо включить

сервисы интернет-банков, почту, социальные сети. К менее критичным можно отнести, например, обычные интернет-магазины.

Почти на всех веб-сайтах есть возможность использовать вход через Open-ID, например, «войти через ВКонтакте / Twitter / Facebook / Google». С целью защиты своих данных рекомендуется воспользоваться именно ими, а аккаунты в этих сетях-провайдерах защитить максимально надежно. Необходимо понимать, что не стоит рассчитывать на память — менеджеры паролей позволяют сгенерировать сложный и надежный пароль для каждого критичного сервиса, а специальные плагины для браузеров смогут подставлять их автоматически. У многих нет доверия к таким программам, считая, что они собирают пароли в одном месте и предоставляют их в руки сторонних организаций. Это совершенно не так. Менеджеры паролей систематически проходят проверку на безопасность. Сама компания не может получить доступ к паролям, так как архитектура данной программы зачастую не позволяет это сделать, ведь данные хранятся в зашифрованном виде. Настоятельно рекомендуем использовать эти программы — таким образом будет значительно безопаснее, чем пользоваться одним и тем же паролем во всех ресурсах Интернета.

— Строгая аутентификация. Вне зависимости от сложности пароля всегда существует вероятность взлома сервисов первой категории критичности, например, почтовых ящиков, социальных сетей, мессенджеров. Чтобы защитить их от данной опасности, необходимо осуществлять еще один принцип цифровой гигиены — многофакторную (двухфакторную, строгую) аутентификацию. Фактором называют один из трех элементов: знание, владение, обладание. Знание — это конфиденциальная информация, то есть это сам пароль. Владение — это предъявление какого-либо объекта, который может быть только у владельца информации. К примеру, токены с криптографическими ключами, одноразовые коды, которые приходят на телефон. Обладание — это вопрос биометрии, например, отпечатки пальцев, голос, Face-ID. Как правило применяется только один из них, а сочетание двух из трех факторов уже будет называться многофакторной аутентификацией. В результате проведенных исследований, применение второго фактора сводит вероятность взлома аккаунта практически к нулю. Двухфакторная аутентификация необходима как на важных сайтах, так и на критичных сервисах, в частности менеджере паролей.

— Личные устройства. К самым главным правилам гигиены цифровых устройств относится обновлённая версия установок, которые предлагает ваша операционная система и программа. Таким образом, обновления помогают устранять бреши безопасности вашей системы и соблюдать важные правила цифровой гигиены.

Установка софта на современные смартфоны из неавторизованных магазинов и каталогов вызывают риск во всей системе безопасности устройства. Не нужно получать root-

доступы и делать jailbreak на ОС, если вы плохо разбираетесь в данной сфере. Ожидаемые преимущества могут превысить недостатки и отразиться в виде снижения уровня защищенности устройства.

— Частичные бекапы. Главный документ исчезает с рабочего стола компьютера. В такой момент не особо важно, что с ним стало — удалили вы, что-то наделали ваши друзья или смартфон подверглось хакерам. Самый главный вопрос, как же восстановить и вернуть файл. Нам могут помочь резервные копии данных, которые хранятся в облаке или на запасном диске. Вам нужно позаботиться о настройке этого копирования.

— Антивирусы. Сейчас установка таких программ вызывает споры. Но плохо разбирающему в цифровой технике пользователю, они позволяют почувствовать себя в интернете более защищенным.

— Сетевая безопасность. Вам нужно постараться избегать публичных сетей, не использовать их для доступа к сервисам. В такие моменты в сетях данные могут попасть к мошенникам. Для доступа они будут использовать подменные сертификаты безопасности. Таким образом, хакеры получат доступы к сервисам.

— Враждебные ссылки. Старайтесь не переходить по ссылкам от незнакомых отправителей. Хакер может взломать аккаунт в социальных сетях одного из ваших коллег и написать пост о несчастном случае с просьбой о сборе денежных средств.

— Личное vs публичное. К правилам цифровой гигиены и безопасности ещё относят разделение рабочего и личного пространства об информации. Не нужно использовать рабочий почтовый ящик для регистрации на внешних сервисах. Но лишним не будет просмотреть настройки конфиденциальности в социальных сетях.

Чтобы время, которое мы проводим в мировой сети, не стоило вам финансовых потерь, себя нужно приучать к цифровой гигиене. Правила очень легкие: обновлять ПО, ставить разные пароли, не делиться личной информацией. Быть внимательными к тому, что публикуем. Берегите себя и свои личные данные!

Список литературы:

1. Бабкин А.В., Буркальцева Д.Д., Костень Д.Г., Воробьев Ю.Н. Формирование цифровой экономики в России: сущность, особенности, техническая нормализация, проблемы развития. Научно-технические ведомости СПбГПУ Экономические науки, 2017, 10 (3), 9-25.

2. Бауэр В.П. Применение Блокчейн-технологии в разработке информационно-аналитической системы обеспечения национальной безопасности. В кн.: Стратегия экономической безопасности России: новые ориентиры развития. Сборник научных трудов I

научно-практической конференции «Сенчаговские чтения». М.: Институт экономики РАН, 2017. С. 152-155.

3. Горулев Д.А. Экономическая безопасность в условиях цифровой экономики // Технико-технологические проблемы сервиса, 2018, 1 (43), 77-84.

4. Капранова Л.Д. Цифровая экономика в России: состояние и перспективы развития. Экономика. Налоги. Право, 2018, No. 2, 58-69.

5. Лесных Ю.Г., Повойко И.В. Риски и угрозы экономической безопасности России со стороны мирового финансового рынка в новых геоэкономических условиях. Вестник КубГАУ 2015, 112 (08), 1462-1474.

6. Лопатин Ю.Н. Информационная безопасность в России. Проблемы, поиски решений. Гуманитарные исследования в Восточной Сибири, 2008, No. 2, 51-57.

7. Махалина О.М., Махалин В.Н. Цифровизация бизнеса увеличивает затраты на информационную безопасность. Информационные технологии в управлении, 2020, No. 1, 134-140.

8. Старостина Е., Хохлов А. Взгляд в будущее: система образования и воспитания кадров, успешно отвечающая на вызовы цифровой экономики. Информационная безопасность, 2018, No. 5. URL: https://lib.itsec.ru/articles2/job/vzglyad-v-buduschee-sistema-obrazovaniya-i-vospitaniya-kadrov--uspeshno-otvechayuschaya-na-vyzovy-tsifrovoy-ekonomiki (дата обращения: 28.01.2022).

9. Удалов Д.В. Угрозы и вызовы цифровой экономики. Экономическая безопасность и качество, 2018, 1 (30), 12-18.

10. Филин С.А., Якушев А.Ж. Организационно-управленческие инновации как основа цифровой экономики. Национальные интересы: приоритеты и безопасность, 2018, 14 (7), 1319-1332.

11. Хочуева Ф.А., Шугунов Т.Л., Жуков А.З., Ингушев Ч.Х. Информационная безопасность сквозь призму цифровой экономики. Современные наукоемкие технологии, 2018, 11 (1), 65-71.