ровой материал легко копируется, распространяется и модифицируется, цифровые культурные продукты потенциально находятся в постоянном состоянии «становления», в некоторых отношениях более адекватно описываемого как процессы, а не как готовые продукты. Вот почему, авторство было проблематизировано в сетевых, связанных гиперссылками цифровых средах: продукты никогда не бывают завершенными, пути чтения связаны гиперссылками и сетью, а отношения между создателями и аудиторией часто антииерархичны, а продукт является объектом совместной деятельности, непрерывно изменяющемся во времени.

Цифровая культура рассматривается как понятие, сочетающее в себе противоречивые явления, вступающие во взаимодействие и образующие новые совокупности элементов, например: глобализация - локализация, индивидуальное авторство – нетворкинг. Специфические характеристики цифровой культуры можно объяснить видами вовлеченных технических процессов, типами возникающих культурных форм и видами опыта, которые влечет за собой цифровая культура.

Информационная безопасность в социальной сфере

Головнёва А.И., Дождикова Р.Н.

Возникновение вычислительной техники как средства сортировки информации привело к компьютеризации общества и появлению новых информационных технологий. Информационная безопасность – один из значимых компонентов комплексной безопасности на любом уровне – национальном, отраслевом, коммерческом или персональном. В. Н. Ильюшенко определяет информационную безопасность как защиту информации и защиту от информации. Это разграничение информационной безопасности было разработано, в частности, С. П. Расторгуевым.

Он отмечает, что информационная безопасность, как составляющая национальной безопасности, имеет два направления: защита информации и

защита от «опасной» информации. Ключом к информационной безопасности является мониторинг информации, распространяющейся в глобальном пространстве и возникновение возможностей и инструментов для отражения возникающих угроз.

Нынешняя информационная система представляет собой сложнейшую систему, состоящую из большого числа элементов с различной степенью автономности, которые соединяются между собой и обмениваются сведениями. Абсолютно все детали могут подвергаться внешним воздействиям или выходить из строя. Попытка реализации угрозы именуется атакой, а тот, кто совершает такую попытку – злоумышленником. Предположительные злоумышленники являются источниками угрозы. Чаще всего угроза связана с наличием слабых мест в защите информационных систем (таких, например, как способность доступа нежелательных лиц к важному оборудованию или ошибки в программном обеспечении).

Если вы хотите, чтобы ваши пароли и данные были достаточно защищены от хакеров, обязательно узнайте, как взломать ваш пароль. Если вы думаете, что такие правонарушители проходят мимо, или вы думаете, что они никогда не смогут угадать ваш пароль, вы можете узнать, насколько вы ошибаетесь. Простейший метод взлома – запросить пароль пользователя. Фишинговое сообщение принуждает ничего не подозревающего читателя подделывать сервисы онлайн-банкинга, платежные системы или другие сайты, которые требуют от вас предоставления личной информации «для решения какой-то ужасной проблемы безопасности».

Другой способ – это спросить напрямую или по телефону, нужно просто позвонить в компанию и спросить пароль для доступа к сети, вы будете поражены тем, как часто это работает. Есть ещё один способ, которым пользуются самые уверенные хакеры, они заходят в офис под видом курьеров, техников или любого другого сотрудника. Форма позволяет им сохранять пароли, введенные реальными сотрудниками, и предоставляет прекрасную способность для всех.

Итак, как вы можете себя защитить. Используйте пароли. Причина использования паролей состоит в том, что, если кто-то попробует получить доступ к вашим данным или оборудованию, пароли доставят массу неудобств. Чем труднее отгадать или «взломать» применяемый вами пароль, тем в наибольшей сохранности будет ваша информация. Протяжённость пароля значительно влияет на уровень защиты. Личные номера, безусловно, являются одним из наименее безопасных паролей, которые широко применяются (например, банковские карты для кассовых аппаратов банкоматов или телефонные карты). Числа от 0 до 9 могут использоваться в личных числах, то есть может быть десять тысяч вариантов числа.

Также, вы можете использовать другой метод, такой как шифрование. Шифрование – это способ превращения открытой информации в закрытую и наоборот. Он используется для хранения важной информации в ненадежных источниках или для ее передачи по незащищенным каналам связи. Используются следующие методы шифрования: 1) симметричное шифрование (алгоритм шифрования может быть известен посторонним, но неизвестна небольшая часть секретной информации – ключ один и тот же для отправителя и получателя сообщения); 2) асимметричное шифрование (третьи лица могут знать алгоритм шифрования и, возможно, открытый ключ, но не закрытый ключ, известный исключительно получателю).

Электронная цифровая подпись (ЭЦП) юридически равнозначна подписи бумажного документа. При регистрации ЭЦП в специальных центрах корреспондент получает два ключа: секретный и открытый. Процесс подписания электронного документа состоит из обработки текста сообщения с использованием секретного ключа.

Таким образом защита информации представляет собой взаимосвязь мер, совершаемых собственником информации для защиты права владения и распоряжения информацией, формирования условий, ограничивающих распространение информации, а также избежания или значительного препятствия несанкционированному доступу к ней. Концепция информацион-

ной безопасности заключается в защите информации и поддерживающей ее инфраструктуры от случайных или преднамеренных естественных или искусственных воздействий, наносящих вред владельцам или пользователям информации и поддерживающей ее инфраструктуре.

Социальные сети как способ дополнительного заработка

Бондаренко В.А., Храмкова А.С., Дождикова Р.Н.

Социальные сети – это тренд во всем мире. От Нигерии до Южной Африки, Индии, США, Великобритании и всего мира социальные сети играют большую роль в жизни большинства людей. Люди проводят большую часть своего дня в социальных сетях. От чата на Facebook до твитов в Twitter, обмена фотографиями в Instagram или просмотра видео на YouTube – социальные сети стали повседневным делом для миллиардов людей. Но помимо развлечений, в наше время социальные сети стали одним из источников дохода. В данной работе представлено несколько способов заработать деньги, не выходя из дома.

1. Станьте маркетологом в социальных сетях. Это один из лучших способов заработка в социальных сетях. Ваша работа в качестве маркетолога в социальных сетях заключается в продвижении услуг, продуктов и имиджа компаний или отдельных лиц на различных платформах социальных сетей, чтобы помочь им найти потенциальных клиентов или развить свой бренд [1]. Это очень прибыльная работа по всему миру. Можно даже создать компанию, специализирующуюся на маркетинге в социальных сетях. По оценкам Payscale, люди, работающие маркетологами в социальных сетях, зарабатывают более 49 000 долларов в год.

2. Зарабатывайте деньги, размещая рекламу в социальных сетях. Это очень распространенный способ заработка в социальных сетях. Заработать в социальных сетях на размещении рекламы может любой желающий. Объявления – это просто аббревиатура для рекламы. Чтобы заработать