УДК 330

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЦИФРОВОЙ ЖИЗНИ

Арьков К.А.,
студент ЦОС22ПИ,
Коновалова Л. И.,
преподаватель,
ФГБОУ ВО Мичуринский ГАУ,
Мичуринск, Россия
lubakonovalova@yandex.ru

Аннотация: Вопросы безопасности цифровой жизни становятся острыми, многоплановыми и требуют более внимательного изучения и широкого обсуждения. Технологическое, цифровое, техническое и др. развитие общества ведет к новым угрозам и рискам, что требует формирования новых методов работы с ними.

Ключевые слова: безопасность, цифра, жизнь.

Цель работы – изучение обеспечения безопасности цифровой жизни.

Вопросы безопасности цифровой жизни становятся острыми, многоплановыми и требуют более внимательного изучения и широкого обсуждения. Технологическое, цифровое, техническое и др. развитие общества ведет к новым угрозам и рискам, что требует формирования новых методов работы с ними. Безопасность – состояние защищенности жизненно важных интересов личности, общества, государства от внутренних и внешних угроз. ФЗ от 28.12.2010 г. № 390-ФЗ «О безопасности» не содержит определения «безопасность», что является существенным упущением как юридическим, так и методическим.

Говоря о вопросах развития цифровизации и цифровой экономики, необходимо рассмотреть вопрос об обеспечении безопасности цифровой

жизни. Идеальной безопасности не существует. Раньше, примерно между 1780 и 1850 гг, был единственный период истории человечества, когда мы имели ту безопасность, что можно назвать идеальной. Она закончилась в 1851, когда Альфред Хоббс вскрыл «невскрываемый» замок.

Безопасность не существует просто в вакууме. Пока вы не знаете от кого защищаетесь, вы не сможете принять подходящие контрмеры. Хорошим примером - способ блокировки, например, iPad: либо пароль, либо отпечаток пальца. Ваше решение зависит - от кого собираетесь защитить устройство: от попутчиков или правительственного ведомства, или от органов правопорядка в целом.

Существует персональная модель угроз, например: владение личными криптовалютными активами; поддержание нескольких проектов открытого персонального оборудования; публичность человека; пассивные угрозы (например, взлом базы клиентов). Учитывая вышесказанное, хотелось бы озвучить следующие принципы: пароли, двухфакторная аутентификация, безопасность криптовалютных активов, мобильная безопасность, браузерная безопасность, сетевая безопасность, физическая безопасность. Рассмотрим их более подробно:

1) Пароли - всегда используйте менеджер паролей для всего. Рекомендуется использовать 1Password, но есть много других вариантов, как платных, так и бесплатных (открытых). 1Password - это отличный инструмент для устранения необходимости запоминать пароли, позволяет хранить наши учетные данные для нескольких служб.

Человек не знает своего мастер-пароля. Вместо этого, он запоминает его половину. Вторую половину ему предоставляет YubiKey4 - это простой USB-ключ, который выполняет функцию клавиатуры при подключении к компьютеру. Он имеет одну кнопку, которая при нажатии генерирует одноразовый пароль и обеспечивает безопасную двухфакторную аутентификацию. При этом следует помнить: никогда не пишите настоящие ответы к вопросам для восстановления пароля, никогда не пользуйтесь сервисами, которые требуют ввести учетные данные от другого сервиса.

2) Двухфакторная аутентификация – старайтесь всегда ее включать; избегайте использования СМС в двухфакторной аутентификации, особенно для чего-либо важного; используйте Google Authenticator или Authy.

3) Безопасность криптовалютных активов: пользуйтесь кошельком и используйте Ledger Nano S; распределяйте свои средства между холодным и горячим хранилищами; не храните свои средства в обменнике (на сегодняшний более день безопасным считается Coinbase); обходитесь с любыми средствами и токенами (которые не защищены мультиподписью или железным кошельком); используйте отдельные аккаунты для всего; используйте другую учетную запись для каждого типа токенов, которые есть у вас во владении; убедитесь, что у вас есть бэкапы каждого из ваших приватных ключей (ваш менеджер паролей хорошо подходит для этого); всегда отсылайте тестовую транзакцию перед отправлением крупной; никогда не вбивайте адрес вручную.

4) Мобильная безопасность. Она сложна. Если бы Black Phone от Silent Circle был совместим с вашим оператором связи, то лучше воспользоваться им. В настоящий момент iPhone, вероятно, лучше защищён, чем Android. Если вы пользуетесь Android, допускайте, что ваш оператор имеет полный доступ к вашему устройству. Не загружайте ни контейнер, ни связки ключей вашего менеджера паролей на смартфоне. Оставайтесь авторизованными в минимальном наборе аккаунтов.

5) Браузерная безопасность: установите блокировщик рекламы (рекомендуется ublock-origin); установите privacy badger, HTTPS Everywhere, Chrome и Firefox (они схожи с точки зрения безопасности, но предпочтительнее Firefox); не стесняйтесь сидеть в режиме «инкогнито»; не позволяйте вашему браузеру хранить пароли.

6) Сетевая безопасность: используйте VPN. При этом следует проверить, в какой юрисдикции находится ваш провайдер VPN. (рекомендуется использовать IPredator). Для дополнительной защиты настройте ваш домашний роутер так, чтобы он отправлял весь ваш трафик через VPN. Flashrouters — наиболее удобный вариант роутера.

7) Физическая безопасность: никогда не подключайте к вашему компьютеру устройство, которым вы не владеете, вроде USB-ключа или чужого телефона для зарядки; приобретите USB-блокатор для зарядки устройств.

Выводы:

1. Постоянно изучать актуальные вопросы развития цифровизации, ведущие к новым угрозам и рискам на современном этапе развития общества.

2. Формировать новые методы работы с рисками и угрозами цифровизации для обеспечения безопасности цифровой жизни.

Список использованных источников

1. Мамаева Л.Н. Характерные проблемы информационной безопасности в современной экономике // Информационная безопасность регионов. 2016. № 1 (22). С. 21–24

ENSURING THE SAFETY OF DIGITAL LIFE

Arkov K.A.,
Student TsOS22PI,
Konovalova L.I.,
Teacher,
Michurinsk State Agrarian University
Michurinsk, Russia
lubakonovalova@yandex.ru

Annotation: The security issues of digital life become acute, multifaceted and require more careful study and extensive discussion. Technological, digital, technical and other development of society leads to new threats and risks, which requires the formation of new methods of working with them.

Keywords: safety, figure, life.