Web 3.0: когда произойдет глобальный переход?

Вестники новой цифровой эры пророчат, что Интернет на пороге великих потрясений. Децентрализация контроля и управления навсегда изменит наш мир – физический, а не только виртуальный! В деталях «новой реальности» попробуем разобраться вместе со старшим научным сотрудником Института кибербезопасности и защиты информации (ИКиЗИ) Андреем Дахновичем.

Марк Цукерберг, рекламируя идею метавселенной, демонстрирует в своих презентациях нам этот «дивный новый мир»: вы надеваете очки виртуальной реальности и запросто ходите в гости к своим друзьям по всему миру, или даже летите на другие планеты пообщаться с внеземным разумом. При этом установленные на компьютере различные девайсы позволяют испытывать всю гамму ощущений – движение, прикосновение, а в будущем, возможно, вкусы и запахи. Словом, виртуальный мир максимально подобрался к нашей реальности.

В 2007 году Тим О’Райли, идеолог предыдущей версии Интернета, выразил грядущие изменения еще более недвусмысленно: Web 3.0 – это про «взаимодействие Интернета с

физическим миром», про стирание грани между онлайн и офлайн, когда мы позабудем слова «войти в Сеть».

Но насколько соответствуют все эти рекламные лозунги действительности? Web 3.0 – по сути, обозначение нового витка технологий. А понятия Web 1,2,3 – лишь стадии процесса, описывающего Всемирную сеть в разные временные периоды: статическая, динамическая и децентрализованная. Чтобы понять, что собой представляет Web 3.0, кратко определимся с понятиями предыдущих версий.

Web 1.0 (1991-2004) был «Интернетом читателей» – в нем были только странички для чтения вроде Википедии. Дизайн был минималистичным, примитивным – кричаще-красочным или, наоборот, скучно-серым. Затем появились соцсети, месенджеры – и это ознаменовало приход и переход к продвинутой интерактивной версии Интернета (с 2004 по настоящее время). Появилась возможность публиковать свой контент на сайтах и в мессенджерах, хлынул обратный поток данных – от пользователя к сервису. А крупные корпорации стали «опекунами и распорядителями» этого контента.

Ядро «третьего поколения» Web – децентрализация управления. Резко снизится роль корпораций, владеющих серверами, на которых хранится информация. На сцену выйдет пользователь: теперь он не пассивный зритель – потребитель и генератор контента, а равноправный игрок, имеющий «контрольный пакет акций» на информацию.

Концепция Web 3.0 претерпевала изменения несколько раз. Изначально автор Всемирной паутины Тим Бернерс-Ли отождествлял Web 3.0 с «семантическим вебом» – сетью, где серверы общаются между собой по специальным протоколам для актуализации информации, так как множество сайтов со временем начинают устаревать. Позже уже упомянутый Тим О’Райли разделил эти два понятия и заложил в концепцию Web 3.0 «взаимодействие между физическим миром и виртуальным» с помощью различных датчиков и «умных» устройств. Последнее и легло в основу Web 3.0.

Web 3.0 стоит на фундаменте нескольких современных технологий и понятий: это блокчейн, искусственный интеллект, семантическая паутина (помогающая искусственному интеллекту понимать контекст) и «Интернет вещей» – «умные» тостеры, утюги и пылесосы, подключенные к Всемирной сети, которые будут буквально угадывать желания хозяина, включаясь в нужное время. Словом, «Интернет вещей» – та самая давно обещанная концепция «умного дома в “умных городах”».

Для чего нужен Web 3.0?

Попробуем разобраться в деталях «новой реальности» вместе со старшим научным сотрудником Института кибербезопасности и защиты информации (ИКиЗИ) Андреем Дахновичем.

Если Web 3.0 будет реализован теми же компаниями, на тех же условиях, что существует и

Web 2.0, то гаджеты смогут начать транслировать «новый дивный мир» – каждому свой, индивидуальный. Сегодня картину мира для нас формируют рекомендательные системы – лентами новостей, которые «подстраиваются под вас». Меняется интерфейс взаимодействия, но не сама сущность и основа, а главное, не меняются ценности.

Но, прежде чем обсудить угрозы «нового цифрового мира», попробуем разобраться, для чего нужен Web 3.0, каковы причины его появления, и кто бенефициары этого преобразования?

Нужно понимать, что речь идет создании копии физического мира, попытке оцифровать все процессы, протекающие в социуме, – это цифровые банки, цифровое сообщество, цифровая индустрия. Сейчас мы видим только его зачатки в виде отдельных продуктов, которые формализовались в виде концепции. Сначала появились понятия биткоин и блокчейн (распределенный реестр). Затем, на основе блокчейна, появились NFT – цифровые активы.

Кто же стороны этого процесса развития Интернета? Бенефициаров, чьи желания в одном совпадают, в другом – прямо противоположны, двое. Это, с одной стороны, мы сами, пользователи Интернета, или клиенты. С другой – корпорации, которые обслуживают серверы, хранят информацию, в том числе наши персональные данные. Поколение Интернет 2.0 называют «вебом контекстной рекламы»: вы заходите на сайты, оставляете информацию о себе, ваших интересах и предпочтениях, а далее корпорации обмениваются ею с другими компаниями. И далее на всех сайтах, которые вы посещаете, вам выдают рекомендации к просмотру контента – появляется более релевантная новость, чтобы удержать вас в соцсети. И чем больше вы просмотрите содержимое сайта иди соцсети, тем больше рекламы вам продемонстрируют, тем выше будут доходы компании.

Нам, пользователям, это не нравится – мы не знаем точно, что за информацию о нас собирают и какие именно сведения сохраняют. Кроме того, существует такое понятие, как «теневой профиль». Возьмем для примера самую популярную соцсеть. Допустим, у вас нет профиля в условной социальной сети. Но все ваше окружение уже зарегистрировалось в ней, и вы есть в контактной книге своего окружения. И когда соцсеть синхронизирует контакты, то ей уже известно, что такая персона, как вы – существует, и для нее необходимо создать «теневой профиль». Он, по сути, уже создан, но пока не активирован. Принцип подобен работе израильского приложения GetContact: вы синхронизируете контакты со своей телефонной книгой и можете увидеть, как та или иная персона записана в телефонных книгах других людей. Соцсети делают то же самое, но не считают нужным уведомлять вас об этом.

Таким образом, возникает вопрос о сохранении приватности персональных данных клиента и правообладании своим же контентом. И тогда пользователи задумались о необходимости установить контроль за потоком своих данных, которые они сами же и генерируют. Мы публикуем свой контент на сайтах, свои фотографии в соцсетях, но хотим, чтобы эта информация принадлежала нам, ее владельцам, а не соцсетям (причем сейчас даже

существующие законы о защите информации не исполняются, нет методик проверки, каким образом эти данные хранятся).

Второй бенефициар – компании, они заинтересованы в том, чтобы зарабатывать деньги и быть успешнее конкурентов. Корпорации сталкиваются с проблемой отсутствия роста. Напомним, что мы пользуемся соцсетями «условно бесплатно» – не платим копейкой, зато расплачиваемся своими данными. И если количество пользователей не растет, то просмотры рекламы, соответственно, тоже. Предприятие не развивается и появляются конкуренты. Решают эти проблемы компании по-разному. Например, тот же Facebook переименовался в корпорацию Meta* (запрещена в РФ) и продвигает технологию метавселенной (MB) как новаторскую идею для привлечения инвесторов и новых пользователей. Но пока на деле это лишь интерфейс взаимодействия с Web 3.0. Если раньше соцсети продавали идеи вроде «добавь музыку», то теперь предлагают блокчейны, метавселенную и технологию NFT (цифровые картинки).

Блокчейн и криптовалюты часто связывают с развитием Web 3.0, и это неслучайно. Блокчейн и есть та самая альтернатива централизованному узлу, которому нужно доверять безоговорочно (в наших примерах – соцсети). В этом случае сведения о вас доступны практически всем, каждый пользователь их видит и знает, что эти данные принадлежат только вам. При таком раскладе чужие данные невозможно использовать в своих целях или, например, удалить. Вы закрепились в этом блокчейне, и теперь эти данные хранятся на множестве серверов по всему миру.

Блокчейны – это распределенные по всему миру реестры, если хотите, бухгалтерские книги, каждая новая запись в этом реестре подтверждается вычислением (подсчетом хэша). Пример такого хранения данных – биткоин, информацию из которого нельзя изъять – однажды загруженная, она там хранится вечно. Таким образом, публичный блокчейн в Web 3.0 решает вопрос правообладания и приватности данных. Но остается проработать вопрос конфиденциальности – никто не станет загружать всю информацию о себе в публичный блокчейн. Также публичный блокчейн подразумевает, что каждый может стать его участником и строить соцсеть будущего.

Безопасный интернет: он возможен или нет?

И теперь, зная полную картину, можно переходить к проблеме безопасности Web 3.0. Итак, представим, что переход к новой модели прошел успешно и сервера распределены по всему миру. Но тут возникает главный вопрос – как обеспечить безопасность их пользователей? Ведь децентрализация сама по себе противоречит регулируемости.

В таком случае Web 3.0 – это модель, при которой все участники (каждый клиент и каждый сервер) равноправны в принятии решений с целью избежать регулируемости. Строго говоря, и сам по себе Интернет есть пиринговая сеть (peer-to-peer, «равный равному»), которую сложно регулировать. Это не просто провод, это распределенная сеть с

множеством узлов, передающих информацию.

Интернет в России, разумеется, пиринговый, но он же и суверенный – мы можем контролировать все границы нашего сегмента сети Интернет. У регулятора на сегодняшний день нет понимания, как контролировать Web 3.0 и какие проблемы будут возникать в процессе перехода. Наши исследования безопасности Web 3.0 начались относительно недавно. Хотя, на основе тех технологий, которые существуют, уже есть понимание, какие риски он несет.

Контроль децентрализованных систем – крайне сложная задача, особенно если эти системы распространяют информацию. Регулятору нужно исполнение законов, пользователю – свобода слова, системе – развитие. Поэтому вряд ли получится просто поставить на контроль все узлы Web 3.0, это может стать неподъемной задачей. Скорее всего, мы увидим некий компромисс между тремя участниками (пользователь, система, регулятор): пользователям необходимо будет регистрировать профили, которые в случае нарушений приведут регулятора к конкретному человеку, а системы Web 3.0 позволят участвовать в процессе так, чтобы участие в нем было максимально прозрачным для всех. Основное внимание уделено тому, что уже в процессе развития: децентрализованные приложения, изучение блокчейна, который основан на криптографических механизмах. Есть множество статей на эту тему, написанных в том числе и нашими политехниками-криптографами.

Баланс сил в плане безопасности может серьезно изменить квантовая криптография. И если появится квантовый компьютер (а он уже существует, но не набрал необходимой мощности), то он с легкостью взломает криптографический алгоритм – механизм, который сейчас защищает информацию на наших компьютерах. При этом часть блокчейнов будет подвержена уязвимостям, а часть из них продолжат работу как ни в чем не бывало – в зависимости от используемого механизма подтверждения (proof-of-stake, proof-of-work) и используемых криптографических алгоритмов.

Нам предлагается дополнить, а позднее – и во многом заменить, физический мир цифровым (криптовалюты, цифровые активы). Важно, чтобы при этом персональная информация стала общедоступной в плане верификации. Необходим так называемый «открытый протокол взаимодействия», чтобы каждый мог проверить лично, какая именно информация о вас хранится на сервере. Таким образом, для клиентов важен механизм реализации. Поэтому уровень приватности данных пользователя будет зависеть от организации процессов Web 3.0. Если ситуация останется той же, что и сегодня (все серверы и процессы подконтрольны корпорациям-гигантам), то архитектурно будет выстроена новая модель, но идеологически она останется прежней. Мы в итоге получим «прокачанный» Web 2.0. И тогда есть опасность, что если соцсеть перестанет существовать, то и вся информация о нас исчезнет.

Предстоит множество работы и регуляторам, и технологически – как обеспечить безопасность профиля, как хранить, чтобы данные не утекали в открытый доступ. Чтобы этого избежать, уже сейчас создаются консорциумы Web 3.0, куда входят компании таких

цифровых гигантов, как Adobe, Microsoft и прочие. Готовятся намерения о протоколах взаимодействия, чтобы не было ситуации, когда одна компания концентрирует всю информацию на своем сервере. Это самые зачатки новой модели.

Единый аккаунт – это еще один тренд Web 3.0. Единый идентификатор – на все сайты, соцсети и даже ключ к вашему электронному кошельку. И если мы говорим, что это проекция виртуального мира на реальный, то по идее это уже не просто ваш единый аккаунт, а некая ваша виртуальная идентичность. Это уже не просто пароль, чтобы войти на сайт, вы теперь существуете как виртуальная персона – целостный цифровой человек в едином экземпляре. Хорошо это или плохо, можно спорить, время покажет, а решение о его введении будет зависеть от того, как договорятся компании.

Еще одна ласточка нового мира – технология NFT (non-fungible token) – невзаимозаменяемые уникальные токены.

Продавцы воздуха **и «грустные обезьянки»**

NFT – это система цифровой собственности, подтверждающая, что вы владеете неким цифровым активом (картинкой, видео, музыкальным треком и так далее) – ценностью, существующей только в виртуальном мире. Суть в том, что реальную картину можно потрогать руками, а значит, ее трудно скопировать и легко отличить оригинал от копии. В Интернете это сделать проблематично, все аналоги абсолютно идентичны. Чтобы устранить эту несправедливость, придумали «подписывать» контент цифровой подписью, чтобы все знали, что именно вы автор или владелец данного цифрового продукта. Нечто вроде патентного права на социальных началах. Но как проверить, что цифровая подпись принадлежит именно вам?

Последние пару лет существуют специальные маркетплейсы, где авторы размещают свои произведения «цифрового искусства», а пользователи их покупают. Вы можете стать счастливым обладателем картинки двухпиксельной обезьянки, о чем все узнают из записей в блокчейне.

Благородная идея NFT заключалась в том, что ее использование должно было охраняться авторским правом. Но это оказалось призрачными надеждами и пока больше походит на финансовую пирамиду. Все сводится к тому, что заинтересованная компания штампует все новые картинки, купленный вами «шедевр» дорожает, и вы перепродаете его подороже.

NFT работает примерно как цифровая подпись, но данные для проверки хранятся, опять же, в блокчейне. Главная проблема в том, что NFT не дает гарантий от копирования контента, то есть не защищает авторство. NFT-токен дает только гарантию на владение конкретным экземпляром цифрового актива в конкретной эко-системе – маркетплейса и блокчейна, с которым маркетплейс умеет работать. И здесь кроется подводный камень: блокчейны не связаны между собой, и не факт, что, купив его в одном маркетплейсе (самые популярные –

Ethereum и Solana), в другом вас признают правообладателем. Да и владеете вы, по сути, не картинкой, а лишь ссылкой на нее, которая хранится, условно, в Web 2.0.

Весь шик NFT в том, что вы владеете чем-то дорогим. Потому что нарисовать картинку из двух пикселей на миллион долларов может каждый. Что, собственно, и произошло: все кому не лень создавали (или копировали), а потом их снова многократно перепродавали с возрастанием цены. И кстати, кто теперь ответит за эту мусорную лавину примитивных однотипных картинок, которые теперь будут похоронены в Интернете навечно? Не ждет ли нас новая экологическая катастрофа – информационный мусор, умножаемый в геометрической прогрессии?..

Бум прошел, рынок обвалился. Но факт остается фактом: все подобные маркетплейсы основаны на блокчейне. Это означает, что постепенный переход в новую реальность Web 3.0 уже стартовал, а ошибки, допущенные в организации NFT, будут учтены. Сама по себе технология никуда не уйдет, ее доработают и вернут нам для покупки «грустных обезьян» (Bored Apes Yacht Club – одна из самых известных NFT-коллекций 10 000 изображений, построена на блокчейне Ethereum).

Свобода? Равенство? Братство?

Процесс, скорее всего, не будет идти скачкообразно. Это будет плавный постепенный процесс перехода. По сути, мы уже существуем в Web 2,5: приложения, которыми мы привыкли пользоваться (мессенджеры, браузеры, соцсети, конференц-связь), заменяются на аналоги, которые умеют работать с чем-то на основе блокчейна. Например, существуют браузеры, которые поддерживают одновременно и Web 2.0 и Web 3.0 – Google Chrome можно заменить на Brave (браузер, настроенный на взаимодействие с криптокошельком). Или облачные хранилища типа Яндекс Диск, Google Drive тоже заменяются на аналоги децентрализованного хранения (такие как Storj, Sia) и хранят файлы распределенно по узлам сообщества.

Но принуждать переходить на новые технологии, конечно, никто не станет. Государственные органы, к примеру, часто используют версию Windows XP, которая уже перестала поддерживаться. Объекты критической инфраструктуры не подключены к открытому Интернету, что позволяет использовать устаревшие версии операционных систем.

Также будет и на этапе перехода к Web3.0. Однако если появятся новые ограничения, новые регламенты взаимодействия с Интернетом, то возникнет сложность с поддержанием устаревшего интерфейса с вебом предыдущей версии, и будет проще перейти на новый, чем поддерживать оба сервера. И тогда в Web 2.0 канет в небытие...

Шаги в светлое цифровое будущее

Резюмируя, можно выделить ряд вопросов Web 3.0, которые нужно решить в переходном

периоде:

Технологический (установка нового программного обеспечения, замена оборудования); это сложный процесс как с точки зрения создания новых технологий, так и технического обеспечения – потребуется новое оборудование, на котором будут работать эти программы, и продумывание системы регулирования.

Социальный (отлаживание новых схем взаимодействия людей); вопрос, не относящийся непосредственно к кибербезопасности, но косвенно влияющий на него – это вопрос управления. Считается, что Web 3.0 должны управлять не организации (заинтересованные корпорации), а ДАО – децентрализованные авторитетные организации. Что-то наподобие профсоюза или совета, состоящих из общественных организаций и людей. И возглавит его не генеральный директор, решение которого является определяющим и обязательным к исполнению для всех, а сообщество, в котором каждый из членов является «директором» и чье решение в споре может стать решающим.

- Энергетический – поиск энергоресурсов (уже сейчас Ethereum и Bitcoin потребляют столько же, сколько целая Австрия).

Кибербезопасность – решение проблемы цифровой приватности, авторства и киберпсихологических операций.

Важно проконтролировать опасности распространения информационного воздействия, характерные для Web 2.0. Известно, что через индивидуальную подборку новостной ленты «под клиента» можно формировать идеологическую картину мира и вынуждать покупать продукцию, выгодную владельцу сервера. Да, в новой системе будет решена проблема управления своими персональными данными – ты их владелец и распорядитель. Однако непонятно, кто будет нести ответственность за происшествия, инциденты с нарушением безопасности? Кто должен быть наказан, в конце концов, если система сработала не так, как предполагалось? Кто принял неправильное решение при голосовании? Все 50 с лишним голосов из 100, причастные к голосованию по проблеме? Неясно также, как будет осуществляться контроль за исполнением протоколов.

Ситуация примерно такая же, как с искусственным интеллектом. ИИ – это скрытая независимая нейросеть, и она сама принимает решение на основании усвоенных ею алгоритмов. Тогда возникает вопрос этического плана: если робот убьет человека, то кто виноват – сама машина, ее непосредственный владелец, корпорация-производитель или ее разработчик?

Пока сложно точно предположить, как скоро произойдет этот глобальный переход. Учитывая нынешние темпы экономического и технологического развития, эксперты прогнозируют его примерно к 2040 году. А пока будет идти плавная подстройка под эту масштабную трансформацию. Надеемся, что она действительно поможет решить извечную

дилемму между свободой слова и защитой частной жизни.

Защита персональных данных

А пока мы еще на пути к светлому будущему, напомним читателям несколько правил для защиты персональной информации:

1. Развивайте цифровую грамотность.
2. Старайтесь не оставлять одни и те же данные о себе в разных источниках. Следуйте принципу минимально необходимых сведений. К примеру, не указывайте водительские права, если нет необходимости.
3. Фильтруйте персональную информацию по критичности указания достоверных данных. Необходимо разделять источники информации минимум по двум категориям. Если речь идет о сайте Госуслуг, то, безусловно, важно максимально защитить свои данные: как правило, именно на подобных ему сайтах содержится наиболее полная информация о вас. Здесь необходима и двухфакторная идентификация, и очень надежный пароль, в идеале – для этого можно завести отдельную почту. А вот при регистрации на сайте магазина необязательно указывать полностью ФИО и точную дату рождения. Как вариант – можно указать даже номер телефона, который вы не используете для звонков, оставить его исключительно для целей регистрации на подобных сайтах и подтверждения заказа смс-кой, а звонки отключить.
4. Применяйте расширения для браузера, обеспечивающие безопасность. Вирусы чаще всего заносятся на ваше устройство не с цифровых носителей, а из Интернета, когда вы скачиваете какие-то файлы. И такие расширения обезопасят ваш компьютер от вредоносных сайтов. У некоторых роутеров тоже есть такие встроенные функции.
5. Используйте менеджер паролей. Пусть это будет не единый пароль везде, а для различных сайтов и разных браузеров – разные ключи. Помните, если в Google Chrome включена функция синхронизации устройств (или автоматический подбор пароля), то ваши пароли туда и утекают. И если вы заходите в Гугл-диск с другого устройства, то он, соответственно, сохраняется на чужом компьютере. Удачного и безопасного вам путешествия во Всемирной сети!