Тезисы доклада на тему: «СоХран: защита хронологического приоритета в цифровую эпоху»

В.А. Перепёлкин, г. Новосибирск

Введение

О важности хронологического приоритета говорить не приходится. В современную цифровую эпоху объёмы информации, существующие в Сети, огромны и растут экспоненциально во времени. Уже давно пропала необходимость для массового пользователя Сети стирать, например, электронные письма, чтобы освободить место. Огромные массивы информации хранятся в различных социальных сетях. Само по себе это уже существенно затрудняет переписывание истории, хотя лишь отчасти. Но, одним из важнейших факторов современных мировых общедоступных хранилищ информации является то, что привелегированный доступ к этой информации имеет то или иное меньшинство. Самовольная блокировка пользователей в социальных сетях (вплоть до президента США), блокировка обсуждения неугодных тем, продвижение вниманию массового пользователя материалов помимо его выбора (будь то рекламных или политически значимых) – это и многое другое является следствием толпо-элитарной организации информационного пространства глобальной Сети.

Несмотря на это в современных условиях имеются все необходимые инструменты для того, чтобы выдвинуть альтернативу сложившемуся положению вещей, соответствующую концепции общественной безопасности, и существенно затрудняющей атаки на общество по хронологическому приоритету власти в форме переписывания или уничтожения истории. В своей основе предлагаемая идея проста – это введение в жизнь общества глобального облачного хранилища хронологической информации, основанного на одноранговых (пиринговых или p2p) сетях [1]. Одноранговые сети уже десятилетиями доказывают свою устойчивость к внешнему управлению и атакам. Сеть ещё до-Интернетного периода FIDONet [2], десятилетиями существующие BitTorrent-сети [3], анонимизирующие сети TOR [4], блокчейн-сети [5] – это лишь немногие общепризнанные яркие примеры, бесспорно демонстрирующие сильные стороны одноранговых сетей на самом высоком уровне значимости. (См. менее известные проекты, основанные на родственных идеях: [6–9].)

Что делает одноранговые сети значимыми с точки зрения хронологического приоритета власти в соответствии с концепцией общественной безопасности? То, что благодаря этому подходу сообщество людей может обеспечить себе соборное хранилище информации, защищённое от внешнего влияния. В качестве иллюстрации можно представить себе, например, блог – публичный Интернет-дневник, где каждый может писать заметки. Такие сервисы сегодня не редкость. Но принципиальная разница состоит в том, что в таком блоге не будет центрального управления. Все пользователи такого блога являются одновременно и предоставителями этого сервиса. Каждый пользователь на своём компьютере хранит часть данных других пользователей, а его записи, в свою очередь, распределены по компьютерам многих других пользователей. Существующие механизмы и инструменты цифрового подписывания данных предотвратят модификацию хранимых данных и обеспечат их подлинность.

Внешние атаки на такую одноранговую сеть крайне затруднены, потому что для этого необходимо скомпрометировать подовляющее большинство компьютеров пользователей сети, которых могут быть миллионы по всему миру. Даже если уничтожить все эти компьютеры физически, через некоторое время в Интернете начнут появляться бэкапы, сделанные в разное время, и припрятанные в чуланах, которые приведут к восстановлению уничтоженных данных, причём с криптографически доказанной их достоверностью.

Внедрение такого банка информации в жизнь общества позволит защитить его историческую память в значительной степени. Это, разумеется, не является панацеей, позволяющей закрыть вопрос защиты исторической памяти, но существенно укрепить позиции общества, построенного в соответствии с концепцией общественной безопасности, представляется возможным и целесообразным.

Однако наивная реализация этой идеи наталкивается на широкий спектр проблем, хотя и разрешимых, но требующих системного подхода к их решению. Рассмотрению по крайней мере значительной их части в первом приближении и посвящена настоящая работа.

2. Ключевые вопросы

Первостепенной важностью в реализации идеи глобального защищённого хранилища исторической информации на основе одноранговых сетей (далее в тексте – СоХран, Соборное Хранилище) является, на взгляд автора, создание и распространение информации о том, что такое хранилище полезно и возможно на современном технологическом уровне. Сегодняшний пользователь Сети не понимает, что он не обязан доверять непонятным дядям, владеющим социальными сетями и популярными Интернет-порталами, хранение своих данных. Он не знает, что может в рамках простой социальной инициативы обеспечить себе доказательно безопасное и защищённое от влияния любого меньшенства хранилище исторически значимой информации. Одно только заполнение этого пробела информацией о том, как это можно осуществить, у достаточно большого количества людей неизбежно повлечёт последствие в виде реализации этой идеи в жизнь. Люди, оценившие эту возможность, организуются в экспертное сообщество, которое проработает все необходимые теоретические и технологические вопросы создания СоХрана, разработает необходимый программный и социальный инструментарий и, что более важно, встроит в культуру общества необходимые элементы, обеспечивающие присутствие вышеупомянутой ключевой информации в поколениях.

Поясним, культурный аспект на частном примере разработки программного обеспечения. Известно, что во многие программы, позиционируемые как безопасные, делаются «закладки» – вредоносный код, который может быть использован злоумышленником. Действенным инструментом противодействия таким закладкам в рамках СоХрана представляется наличие активного сообщества программистов, разрабатывающих программное обеспечение с открытым исходным кодом в соответстви с правилом «каждая строка кода должна проверяться многими независимыми программистами». Это можно обеспечить лишь в том случае, если достаточное кличество пользователей СоХрана, которые являются программистами подходящей квалификации, активно вовлечены в работу над его программным обеспечением. И если каждый пользователь СоХрана будет иметь в личных друзьях хотя бы одного такого программиста, то, начиная с определённого количества пользователей, внести вредоносную «закладку» в программный код станет практически невозможно.

Другим важнейшим аспектом является социальный аспект СоХрана. Для его демонстрации рассмотрим проблему флуда и спама – две вероятные атаки, которые будут осуществляться представителями ветхозаветно-библейской концепции на проект. И то и другое представляет собой замусоривание информационного пространства нерелевантной информацией. Например, если на одну единицу полезной исторической информации, внесённой в СоХран будет приходиться тысяча единиц спама и флуда, то ценность СоХрана будет сведена на нет, а ресурсы пользователей этой одноранговой сети будут расходоваться зря. Примером эффективной меры противодействия флуду и спаму является использование внешних по отношению к СоХрану социальных связей

пользователей. А именно, программное обеспечение СоХрана возможно разработать таким образом, чтобы на каждом компьютере пользователя в большем объёме хранились данные его реальных знакомых, и знакомых их знакомых, и в меньшем – менее социально связанных с ним пользователй. Так бремя хранения спама и флуда ляжет лишь на самих спаммеров и флудеров, т.к. их будут «удалять из друзей» благонамеренные пользователи. Таким образом, СоХран должен не просто быть, а должен быть вплетён в социальную жизнь людей для максимальной эффективности.

В целом, ключевым тут является активное использование принципа прозрачности. Принцип прозрачности – это возможность любого человека ознакомиться с любым аспектом организации СоХрана, начиная от основополагающих принципов и заканчивая программным кодом. Активное его использование означает, что каждый пользователь в меру своих возможностей, квалификации и текущей целесообразности целенаправленно проверяет, что в СоХране всё в порядке. Именно такая активная позиция пользователей является гарантом тех сильных свойств, что СоХран потенциально предлагает по защите и обеспечению доступности хронологически значимой информации.

3. Методологические вопросы

Управление реализацией СоХрана в соответствии с принципами концепции общественной безопасности должен заниматься соборный интеллект социальной суперсистемы пользователей. Для этого целесообразным представляется проведение регулярного форума, прорабатывающего необходимые вопросы из затронутого в данной работе спектра и других вопросов, которые вскроются в процессе проработки. Результатами работы форума будут являться теоретическое и методологическое обеспечение СоХрана. В том числе, форум должен выявлять изменения в среде, например, в сфере компьютерной безопасности. Такой форум может иметь форму конференции, круглого стола и т.п., проводиться, например, в рамках «Зазнобинских чтений» или как самостоятельные мероприятия, в зависимости от масштаба вовлечённости сообщества.

В числе прочего форум должен вырабатывать стандарт СоХрана, то есть, как должен быть устроено программное обеспечение узла этой сети, а также организовывать разработку и поддержку референтной реализации узла (т.е. собственно программного обеспечения). Важно поддерживать разработку многих альтернативных реализаций программного обеспечения, чтобы повысить устойчивость системы в целом. Для этого форум должен вырабатывать методические указания по разработки альтернативных программных реализаций узла. Также форум должен заниматься вопросами организации информационной работы, т.е. организовывать просвятительскую деятельность и встраивать в ткань социокультурной жизни общества необходимые элементы для поддержания СоХрана как социокультурного явления, наращивания его ресурсной устойчивости.

Заключение

Вопрос создания честного глобального общедоступного хранилища данных для защиты хронологически значимой информации – это вопрос времени. СоХран неизбежно будет создан вследствие закона времени. СоХран – это процесс, который в конечном счёте реализуется в масштабах всего мирового сообщества, но начат он может быть в малых масштабах уже сегодня силами нескольких энтузиастов в свободное от работы время. Настоящая работа является, по сути, постановкой задачи и привлечением внимания к её решению. Учитывая широкий спектр связанных вопросов свой вклад могут внести специалисты самых разных профилей. В первую очередь, конечно, создание СоХрана – это проблема управления.

Литература

1. https://ru.wikipedia.org/wiki/Одноранговая_сеть
2. https://www.fidonet.org/
3. https://ru.wikipedia.org/wiki/BitTorrent_(протокол)
4. https://www.torproject.org/
5. https://ru.wikipedia.org/wiki/Блокчейн
6. https://en.wikipedia.org/wiki/Dat_(software)
7. Case, Amber (4 October 2015). "Why The Internet Needs IPFS Before It's Too Late". TechCrunch. Retrieved 16 July 2019. https://techcrunch.com/2015/10/04/why-the-internet-needs-ipfs-before-its-too-late/
8. http://netsukuku.freaknet.org/