УДК 004
https://doi.org/10.38086/2522-9613-2019-1-66-75

Активная защита криптоконтейнера как элемент противодействия пассивному сбору персональных данных

В. А. Курбацкий, магистр прикладной математики и информационных технологий, инженер-программист

E-mail: i1954@xe.am

ЗАО «Институт информационных инновационных, инвестиционных технологий», пл. Свободы, д. 23, 220030, г. Минск, Республика Беларусь

Аннотация. Статья посвящена исследованию проблем обеспечения личной информационной безопасности с учетом влияния Больших данных в условиях современного кризиса информационной безопасности. Человек стремительно погружается в киберпространство, ведет в нем бизнес, проводит финансовые операции, активно получает образовательные и другие социальные услуги. Эти процессы приводят к формированию цифрового следа. В статье рассмотрено явление возникновения цифрового следа человека и процессы, с этим связанные. В частности, рассмотрен процесс формирования новой символической среды повседневной жизни. В результате анализа актуальных проблем личной информационной безопасности в рамках инициативы по созданию защищенной платформы был спроектирован и разработан программный комплекс защиты информации «Криптоконтейнер», принципы которого рассмотрены в данной статье. Предложен альтернативный подход к обеспечению информационной безопасности с учетом личного информационного пространства человека.

Ключевые слова: личная информационная безопасность; личное информационное пространство; криптоконтейнер; цифровой след; защищенная платформа

Для цитирования: Курбацкий, В. А. Активная защита криптоконтейнера как элемент противодействия пассивному сбору персональных данных / В. А. Курбацкий // Цифровая трансформация. – 2019. – № 1 (6). – С. 66–75. https://doi.org/10.38086/2522-9613-2019-1-66-75

Cryptocontainer's Active Protection as an Element of Countering the Passive Collection of Personal Data

V. A. Kourbatski, Master of Applied Mathematics and Information Technology, software engineer

E-mail: i1954@xe.am

CJSC «Institute of Information Innovation, Investment Technologies», 23 Svobody Sq. 220030 Minsk, Republic of Belarus

Abstract. The article is devoted to the study of the problems of personal information security, taking into account the impact of Big data in the current crisis of information security. A person is rapidly immersed in cyberspace, conducts business in it, conducts financial operations, actively receives educational and other social services. These processes lead to the formation of a digital footprint. The article considers the phenomenon of the digital footprint appearance and the processes associated with it. In particular, considered the formation of a new symbolic environment. The cryptocontainer, complex information protection software, was designed and developed as a result of the actual personal information security problems analysis and as a part of the secure platform creation initiative. Its principles are discussed in this article. An alternative approach to providing information security was proposed, taking into account the personal information space.

Key words: personal information security; personal information space; cryptocontainer; digital footprint; secure platform

For citation: Kourbatski V. A. Cryptocontainer's active Protection as an Element of Countering the passive Collection of personal Data. *Cifrovaja transformacija* [Digital transformation], 2019, 1 (6), pp. 66–75 (in Russian). https://doi.org/10.38086/2522-9613-2019-1-66-75

Введение. Большие данные обладают огромным потенциалом, и в каждое мгновение собирается все больше и больше данных о людях, которые делятся информацией о себе как осознанно (например, через публикации в социальных сетях), так и неосознанно (используя всевозможные «умные» устройства и датчики). Активно способствуют процессу накопления

больших данных и быстроразвивающиеся методы социальной инженерии. На основе этих данных специализированные аналитические алгоритмы могут рассказать очень многое [1].

При анализе социальных процессов традиционно ключевым являлось понимание важности связей между людьми. Сейчас к этому добавляется еще и следующее: связь людей и умных устройств со множеством встроенных механизмов сбора пользовательских данных оказывает огромное влияние практически на все современные сферы общественной жизни, предоставляя потенциально широкие возможности для автоматизированного анализа и прогнозирования процессов, связанных с человеком. Дело в том, что единожды собранные данные в современных условиях хранятся практически неограниченное время и могут быть подвергнуты последующему многократному анализу с появлением новых, более совершенных аналитических алгоритмов, уточняя результаты анализа и открывая новые, до этого неизвестные свойства. Все больше средств вкладывается в инструменты сбора и анализа больших данных, а тема безопасности личного информационного пространства с течением времени становится все актуальнее.

Основная часть. Синтетическая реальность. Информационные ресурсы, включающие социальные медиа, конструируют новую символическую среду повседневной жизни. Они моделируют отношение людей к действительности и предлагают эмоциональные, интеллектуальные и поведенческие шаблоны, в той или иной степени оказывающие влияние на человека и общественные ритмы. Доступ к информационным ресурсам имеет свою цену. Человек делится сведениями о себе при регистрации аккаунтов во всевозможных социальных сетях, на форумах и других онлайн-сервисах, и это лишь небольшая часть цифровых следов, которые каждый день оставляет обычный пользователь глобальной сети. Рабочие документы, фотографии, электронные сообщения, данные о контактах, история поисковых запросов, геолокационные метки — все это накапливается на серверах транснациональных компаний, т. к. человек использует их цифровые сервисы. К примеру, в обычном прикладном ПО может быть встроен механизм контроля лицензий, который требует активного сетевого соединения для защиты от несанкционированного распространения. Подобный алгоритм обычно формирует отпечаток информационной системы, связанной с конкретным человеком или группой людей. Данный отпечаток передается владельцу приложения и может храниться неограниченное время. Понятно, что без анализа (обратного инжиниринга) подобного программного обеспечения и модификаций, включающих удаление или блокировку соответствующих элементов программной логики, избавиться от необходимости периодического «выхода в сеть» не представляется возможным. Однако, обратный инжиниринг считается прямым нарушением лицензионного соглашения при работе с большинством закрытого ПО, требует специальных навыков и практически неприменим в реальных условиях. Таким образом, разработчики программного обеспечения, загоняют нас в выстроенные ими рамки, ограничивающие поле для построения персональной безопасной информационной среды. С точки зрения разработчика это преподносится как вынужденная мера, а вот с точки зрения пользователя — как существенная угроза личной информационной безопасности. Таким образом компании получают возможность использовать собранные данные по своему усмотрению (например, анализируя их в совокупности с другими собранными данными и предлагая пользователю контекстную рекламу на их основе и т. д.), а при желании даже продать или передать их третьим лицам. Могут существовать теневые биржи больших данных, о которых мы не догадываемся [2].

Можно рассмотреть известные случаи одностороннего ультимативного принуждения человека к раскрытию персональной информации со стороны компаний-владельцев популярных сетевых сервисов. Так, к примеру, в рамках очередной версии пользовательского соглашения сервисов Google [3], было постановлено, что согласно новой политике обработки персональных данных, компания может собирать и хранить: личную информацию о пользователях, оставленную при создании учетной записи, информацию из служб, с которыми работает пользователь, а также поисковые запросы, IP-адреса, сведения о местоположении пользователя, информацию о маршруте мгновенных сообщений, cookie-файлы, пользовательские идентификаторы. С внесением изменений, которые были сделаны в одностороннем порядке (у пользователя, имеющего почту, документы и другие данные на серверах Google,

попросту не оставалось другого выхода), претерпела изменения и политика конфиденциальности. С этого момента пользователю стало доступно «удаление» своей личной информации из электронных сервисов компании, однако Google оставляет за собой право хранить ее копии. Собираемые данные, с точки зрения компании, используются только в «благих целях»: для предоставления информации другим пользователям, а также для повышения эффективности работы различных сервисов. Однако серия публичных событий, связанных с Google, говорит об обратном. В частности, в 2012 году компания выдала американским спецслужбам содержание электронных писем, метаданные, сведения о подписках, а также другие данные сотрудников Wikileaks и лишь спустя два с половиной года уведомила их об этом [4].

Компания Facebook, владелец одноименной социальной сети, пошла еще дальше и, согласно пользовательскому соглашению, владельцы аккаунтов теперь обязаны иметь только актуальную информацию на своей странице. Например, номер телефона должен быть актуализирован в течение двух суток после его редактирования. Это свидетельствует о «диктаторском» отношение компаний к пользовательскому контенту. Так, Instagram, согласно правилам использования, которые опубликованы для пользователей только на английском языке, фиксирует передачу всех авторских прав на опубликованные фото и видео компании Facebook, официально являющейся владельцем ресурса Instagram [5].

Человек, пожелавший удалить персональные данные из баз данных социальной сети или, например, сервиса электронной почты, не всегда может сделать это в полной мере. Пользовательские соглашения многих цифровых сервисов позволяют «удалить» аккаунт, скрыв информацию, но сами данные о человеке так и останутся на серверах.

Данные, образующие цифровой след личности, можно условно разбить на четыре типа, представленные в таблице 1. Предложенная автором классификация отражает субъективный взгляд на разбиение персональных данных по типам.

Таблица 1. Примеры данных, формирующих цифровой след личности
Table 1. Examples of data forming a digital footprint

Тип	**Примеры данных**
Статические	– ФИО – Место рождения – Серия и номер паспорта – Информация о водительском удостоверении – Страховой номер индивидуального лицевого счета
Непостоянные	– Номер телефона – Адрес места жительства – Идентификатор в социальной сети – Адрес электронной почты
Побочные	– Информация о сессии доступа в глобальную сеть – Список использованных IP-адресов
Связи	– Контакты – Информация о семейных связях – Рабочие связи – Список контактов электронной почты

Совокупность таких сведений представляет собой семантическую сеть, содержащую относительно подробную информацию о личности. Эти данные формируют виртуальный прообраз личности, являющийся частичным отражением реальной личности человека.

Во времена глобальной геополитической нестабильности, огромных усилий стоит сохранение государственного суверенитета, в том числе и информационного. Однако, как и в случае с обеспечением кибербезопасности, важной составляющей государственного цифрового суверенитета является цифровой суверенитет человека, но, похоже, человек его утратил [6; 7].

Помимо вопроса о безопасности персональных данных, существует и другой: а принадлежат ли еще нам наши мысли? Часто можно услышать заявления, начинающиеся со слов «я думаю», «я считаю», «по-моему». Обычно человек практически уверен в том, что то, что он думает и говорит является прямым отражением его сущности. Сегодня, когда скорость обмена информацией возросла на порядки, короткие посты со смешными картинками в социальных сетях заменили книги, доступ к миллиардной аудитории находится на расстоянии одного нажатия, а грань между человеком реальным и его виртуальным прообразом стремительно разрушается. Можем ли мы быть так уверены в том, что наше мысли все еще наши? Цифровые социальные сервисы в большинстве своем не служат цели кристаллизации общественной морали и ценностей, а преследуют коммерческие интересы и становятся площадками, используемыми для манипулирования общественным мнением, политическими взглядами и даже могут повлиять на выбор того, что мы будем есть на обед. Проникновение в личное информационное пространство сегодня тотально, а репутация в онлайн-среде для многих неотделима от реальной жизни. Среднестатистический пользователь социальных медиа не аналитичен и зачастую склонен не подвергать каким-либо сомнениям подготовленный для него легкоусваиваемый информационный контент. В то же время, интеллектуальные алгоритмы социальных сетей научились адаптивно подбирать каждодневный информационный «рацион». Благодаря обратной связи и анализу реакции, алгоритмы со временем могут все точнее определять «то, что нам нужно», подобно хорошему врачу-диетологу. В умелых руках такой инструментарий может быть использован как угодно: от банального извлечения коммерческой выгоды до элемента геополитической стратегии.

А что обычный человек может противопоставить всем этим цифровым инструментам шпионажа и манипуляции, разработка которых профинансирована из многомиллиардных бюджетов гигантских корпораций при поддержке спецслужб [1; 8; 9; 10]? Привычные для всех артефакты личной кибербезопасности, такие как антивирусные сканеры, уже не спасут, так как борьба за цифровой суверенитет уже давно вышла за рамки цифрового пространства и ведется в рамках глобального геополитического противостояния [2]. Возникает потребность в разработке совершенно иной доктрины цифровой безопасности и эффективного инструментария, способного дать ответ на новые вызовы.

Криптоконтейнер. Защищенная платформа. Программный комплекс защиты информации (ПКЗИ) «Криптоконтейнер» создается как элемент вышеупомянутого инструментария и призван выполнять функцию обеспечения личной информационной безопасности при различных сценариях взаимодействия пользовательской среды с информационными экосистемами предприятий и государства. При этом не исключается возможность полностью автономного использования данного комплекса для персональных нужд защиты информации. Ряд элементов криптоконтейнера и защищенной платформы нацелен на снижение информационного шума, создаваемого в процессе взаимодействия человека и информационной среды, тем самым способствуя подавлению цифрового следа, за которым «охотятся» вышеупомянутые механизмы сбора и анализа данных, интегрированные в повседневно используемые человеком программные продукты. Ниже предлагается таблица потенциального влияния криптоконтейнера в совокупности с другими элементами защищенной платформы на цифровой след человека (таблица 2).

«Криптоконтейнер» призван заполнить нишу обеспечения личной информационной безопасности при различных сценариях взаимодействия пользовательской среды с информационными экосистемами предприятий и государства.

Технически ПКЗИ «Криптоконтеийнер» представляет из себя набор программных

Таблица 2. Потенциальное влияние криптоконтейнера и других элементов защищенной платформы на цифровой след человека
Table 2. Potential impact of the crypto container and other elements of the secure platform on the digital footprint of a person

Элементы защищенной платформы	**Эффекты**
Криптоконтейнер	– Криптографически защищенная репликация и контроль целостности пользовательских данных при хранении, использовании и синхронизации ограничивает доступ к ним третьих лиц, исключая возможность внешнего анализа на уровне содержания – Использование только встроенного механизма децентрализованной синхронизации может целиком исключить потребность в передаче данных на сервера третьей стороны – Встроенный механизм обмена данными позволяет избежать компрометацию сведений об информационном окружении человека, убирая потребность в раскрытии данных об адресатах третьей стороне
Сетевой анализатор + экран	– Постоянный анализ и контроль сетевой активности позволяет ограничить «выбросы» пользовательских данных, тем самым снижая вероятность пассивной утечки потенциально значимой для идентификации сведений о человеке информации
Обозреватель	– Сигнатурное сканирование и удаление трекеров, всевозможных счетчиков, виджетов социальных сетей и прочих сторонних элементов из загружаемого кода веб-страниц позволяет снизить заметность пользовательской сетевой активности для сторонних сервисов – Обновляемая база небезопасных ресурсов в совокупности с использованием эвристического анализа и возможностями настройки ограничений как на уровне отдельного клиента, так и на уровне предприятия, позволяет найти компромиссный вариант между безопасностью и потенциалом глобальной сети
Почтовый сервис	– Использование децентрализованной сети криптоконтейнера для хранения писем и вложений в совокупности с возможностью использования децентрализованного SMTP позволяет использовать привычные почтовые сервисы лишь в качестве точек сбора почты, приходящей на уже закрепленные за пользователем адреса – Поддержка шифрования позволяет организовать безопасный обмен почтовыми сообщениями, затрудняя возможность проведения анализа содержания писем и вложений третьей стороной

Продолжение таблицы 2
Table 2 (continuation)

Элементы защищенной платформы	Эффекты
Система обмена мгновенными сообщениями	– Асимметричное шифрование и одноранговая архитектура сети позволяют исключить наличие централизованного сервера третьей стороны для организации обмена мгновенными сообщениями – Шифрование сведений о человеке в рамках децентрализованной сети и возможность персонального разграничения уровней доступа к этим сведений самим человеком за счет использования отдельных криптографических ключей для каждого элемента социального профиля позволяет избежать раскрытия данных об адресатах при обмене мгновенными сообщениями

средств, реализующих кроссплатформенный инструментарий для безопасного хранения, управления и обмена пользовательскими данными и приложениями. Инструмент предоставляет пользователю безопасную интегрированную среду с низким порогом входа. Криптоконтейнер позволяет создать криптографически защищенную репликацию любых пользовательских данных и обеспечить их доступность на всех пользовательских устройствах, независимо от используемой операционной системы (рис. 1).

Криптоконтейнер использует изолированные области памяти в процессе работы, так называемые песочницы. Это позволяет разбить пользовательскую среду на самодостаточные не конфликтующие зоны для безопасной работы с различными категориями данных даже в недоверенных средах [11].

Система хранения данных в рамках криптоконтейнера спроектирована таким образом, что позволяет использовать для синхронизации практически любые доступные решения. Это может быть как p2p-обмен между устройствами в рамках локальной пользовательской или корпоративной сети, так и облачные сервисы. Для этой цели была разработана кроссплатформенная библиотека синхронизации, которая реализует базовый функционал синхронизации данных и предоставляет универсальный программный интерфейс синхронизации для приложений, построенных на базе защищенной платформы (рис. 2) [12].

Криптоконтейнер реализует программный интерфейс для внешних расширений, с помощью которых возможно подстроить функционал под различные задачи и требования. В частности, реализован модуль активного мониторинга выделенной области памяти с целью исключения внешнего вмешательства в процесс работы криптоконтейнера. В данном случае можно провести аналогию с активной

Рис. 1. Общая схема логических слоев криптоконтейнера
Fig. 1. General scheme of logical layers of the crypto container

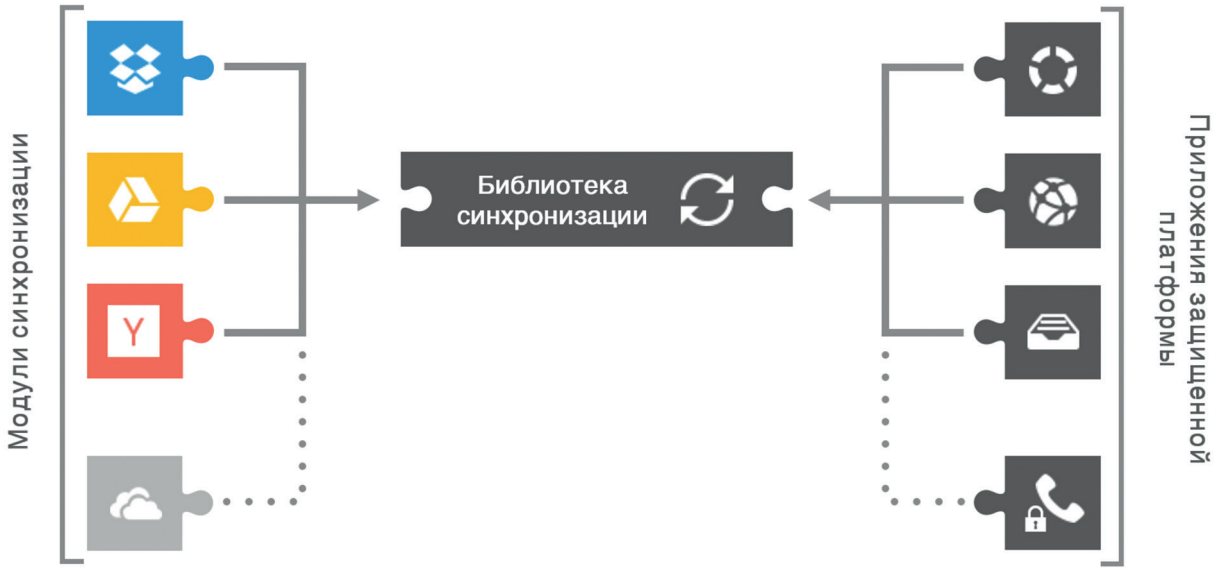

Рис. 2. Модульная подсистема синхронизации
Fig. 2. Modular synchronization subsystem

защитой для военной техники: в то время как криптографические средства в рамках криптоконтейнера предоставляют крепкую «броню» для размещенной под ней информации, модуль активной защиты не позволяет угрозам даже подобраться к безопасной зоне.

При этом в основе пользовательского интерфейса «криптоконтейнера» лежит идея максимальной доступности технологий защиты информации для человека, которая, при этом, не ограничивает возможности глубокой конфигурации инструментов по мере необходимости. В качестве примера, на рисунках 3 и 4 приведены изображения интерфейса управления хранилищами криптоконтейнера, главного окна основного приложения.

Для наглядности, проиллюстрируем работу криптоконтейнера на примере синхронизации пользовательского программного обеспечения и генерируемых в процессе его использования данных:

1. Пользователь, работая на некотором устройстве, помечает программу X как элемент криптоконтейнера.

2. В настройках криптоконтейнера пользователь отмечает Яндекс.Диск, Dropbox и локальную сеть в качестве целей для синхронизации.

3. Криптоконтейнер создает репликацию бинарного файла программы X, директории с конфигурацией программы и директории с пользовательскими данными внутри криптографически защищенного хранилища, создает изолированную область памяти для исполнения программы, разбивает данные на части и применяет обработчики для выбранных целей синхронизации. В результате данные синхронизируются между пользовательскими устройствами в локальной сети, а также размещаются в зашифрованном виде в облачных хранилищах.

4. При использовании другого устройства, пользователь будет иметь актуальную версию данных, самой программы, ее конфигурации и сможет продолжить работу прямо с того места, на котором закончил.

5. После завершения работы, криптоконтейнер шифрует хранилище на личном ключе пользователя и очищает выделенную область памяти.

Заключение. В эпоху цифровой трансформации, одна из основных проблем безопасности информации заключается в том, что при интенсивном развитии информационно-коммуникационных технологий существует ощутимый недостаток времени и ресурсов для экспертной оценки повсеместно используемых программных продуктов (средств хранения, обработки и передачи данных; протоколов и т. д.) и выработки эффективной стратегии защиты информации (как персональной, так и корпоративной, государственной). Традиционно мы привыкли, что в первую очередь необходимо обеспечить информационную безопасность государства и предприятий, а личная информационная безопасность обеспечивается по остаточному принципу и зачастую это полностью ложится на плечи самого человека (как правило, не являюще-

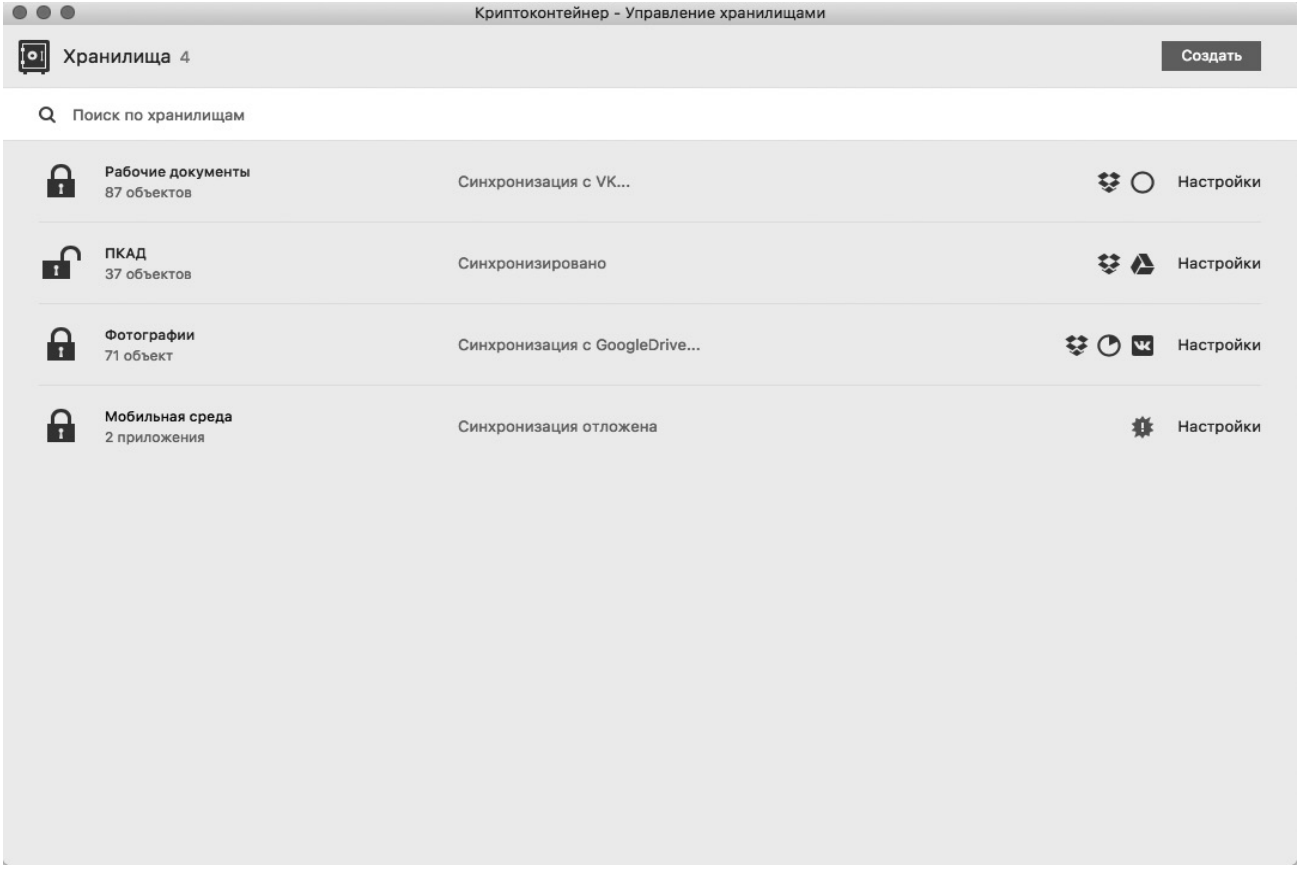

Рис. 3. Интерфейс управления хранилищами криптоконтейнера
Fig. 3. Control interface stores crypto container

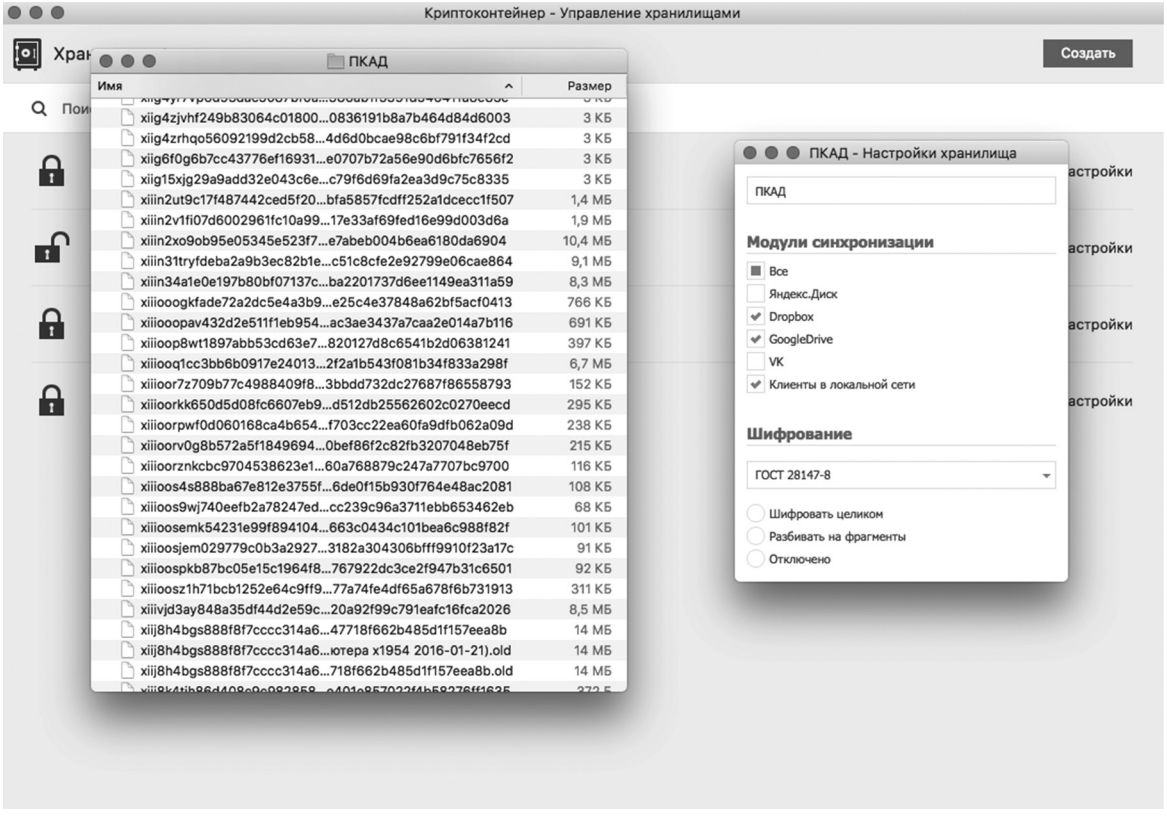

Рис. 4. Окно управления хранилищем и отображение блоков хранилища в файловой системе
Fig. 4. Storage management window and display of storage blocks in the file system

гося экспертом в области информационной безопасности). Как следствие — мы тратим множество ресурсов на создание сложных информационных систем для предприятий и государства, которые во многих реальных сценариях все равно остаются крайне уязвимыми из-за необходимости взаимодействия с персональными информационными средами, безопасность которых пока не может гарантировать ни одна подобная система. С течением времени, развитие информационных технологий не только открывает перед нами очередные возможности, но и формирует новые, все менее прогнозируемые и потенциально очень серьезные вызовы с точки зрения информационной безопасности. Нам необходимо заложить концептуальный фундамент обеспечения комплексной информационной безопасности систем различного масштаба, и подкрепить его эффективным инструментарием, учитывая при этом и личную информационную безопасность. В противном случае, если продолжать игнорировать информационную безопасность на уровне личного информационного пространства, последствия для цифрового суверенитета могут стать катастрофическими.

Список литературы

1. Гриняев, С. Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. – Москва: Издательство Харвест, 2004. – 448 с.
2. Коровин, В. М. Третья мировая сетевая война / В. М. Коровин. – Санкт-Петербург: Издательство Питер, 2014. – 352 с.
3. Условия использования Google [Электронный ресурс]. – 2019. – Режим доступа: https://policies.google.com/terms?hl=ru&gl=ru. – Дата доступа: 16.03.2019.
4. Google hands data to US Government in WikiLeaks espionage case [Electronic resource]. – 2019. – Mode of access: https://wikileaks.org/google-warrant/Letter-to-Google.html – Date of access: 16.03.2019.
5. Instagram Terms of Use [Electronic resource]. – 2019. – Mode of access: https://instagram.com/about/legal/terms/ – Date of access: 16.03.2019.
6. Курбацкий, А. Н. Системная актуализация проблемы информационной безопасности личности / А. Н. Курбацкий // Проблемы безопасности и противодействия терроризму. – Москва: МЦНМО, 2008. – С. 110–117.
7. Курбацкий, А. Н. Личная информационная безопасность и правила поведения в виртуальном пространстве / А. Н. Курбацкий // Вопросы защиты информации. – 2014. – No 4. – С. 218–224.
8. Project «Weeping Angel» specification [Electronic resource]. – 2019. – Mode of access: https://wikileaks.org/vault7/#Weeping%20Angel – Date of access: 25.03.2019.
9. Project «Pandemic» specification [Electronic resource]. – 2019. – Mode of access: https://wikileaks.org/vault7/#Pandemic – Date of access: 25.03.2019.
10. Project «Angelfire» specification [Electronic resource]. – 2019. – Mode of access: https://wikileaks.org/vault7/#Angelfire – Date of access: 25.03.2019.
11. Харин, Ю. С. Криптология / Ю. С. Харин, С. В. Агиевич, И. Л. Васильев, Г. В. Матвеев; под ред. Ю. С. Харина. – Минск: Изд. центр БГУ, 2013. – 511 с.
12. Таненбаум, Э. Распределенные системы. Принципы и парадигмы / Э. Таненбаум. – Санкт-Петербург: Издательство Питер, 2003. – 877 с.

References

1. Grinyaev S. N. Pole bitvy – kiberprostranstvo: Teoriya, priemy, sredstva, metody i sistemy vedeniya informacionnoj vojny [Cyberspace: Theory, Techniques, Means, Methods and Systems of Information Warfare]. Moscow: Harvest Publ., 2004. 448 p. (in Russian).
2. Korovin V. Tret'ya mirovaya setevaya vojna [The Third World Network War]. St. Petersburg: Piter Publ., 2014. 352 p. (in Russian).
3. Usloviya ispol'zovaniya Google [Google Terms of Use]. Available at: https://policies.google.com/terms?hl=ru&gl=ru (accessed: 16.03.2019) (in Russian).
4. Google hands data to US Government in WikiLeaks espionage case. Available at: https://wikileaks.org/google-warrant/Letter-to-Google.html (accessed: 16.03.2019).
5. Instagram Terms of Use. Available at: https://instagram.com/about/legal/terms/ (accessed: 16.04.2019).
6. Kourbatski A. N. The system actualization of information security problems of the personality. Problemy bezopasnosti i protivodejstviya terrorizmu [Problems of safety and counteraction to terrorism]. Moscow: MCCME, 2008, pp. 110–117 (in Russian).
7. Kourbatski A. N. Personal information security and code of conduct in the virtual space. Voprosy zashchity informacii [Information security issues], 2014, no. 4, pp. 218–224 (in Russian).
8. Project «Weeping Angel» specification. Available at: https://wikileaks.org/vault7/#Weeping%20Angel (accessed: 25.03.2019).

9. Project «Pandemic» specification. Available at: https://wikileaks.org/vault7/#Pandemic (accessed: 25.03.2019)
10. Project «Angelfire» specification. Available at: https://wikileaks.org/vault7/#Angelfire (accessed: 25.03.2019)
11. Kharin Y. S., Agiyevich S. V., Vasiliev I. L., Matveyev G. V. Kriptologiya [Cryptology]. Minsk: BSU Publ., 2013. 511 p. (in Russian).
12. Tanenbaum E. Raspredelennye sistemy. Principy i paradigmy [Distributed systems. Principles and paradigms]. St. Petersburg: Piter Publ., 2003. 877 p. (in Russian).

Received: 18.03.2019 *Поступила: 18.03.2019*