Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

14. Что такое блокчейн и зачем он нужен [Электронный ресурс] /– Москва – 2017 – Режим доступа: https://habrahabr.ru/company/bitfury/blog/321474/, свободный. – Загл. с экрана.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В КОНТЕКСТЕ БОЛЬШИХ ДАННЫХ

В.А. КУРБАЦКИЙ

Белорусский Государственный Университет

В докладе рассматриваются основные принципы обеспечения Личной Информационной Безопасности с учетом влияния больших данных в условиях современного кризиса информационной безопасности, предлагается концептуальный подход и концептуальная архитектура Личной Информационной Системы со встроенным средством персональной защиты информации «защищенный криптоконтейнер».

Человек стремительно погружается в киберпространство, ведет в нем бизнес, финансовые операции, активно получает образовательные и другие социальные услуги. При этом уже становится очевидным, что эти процессы приводят к формированию Больших данных, связанных с человеком. Возникает вопрос: так ли это безопасно для человека? И обеспечиваем ли мы безопасную среду личного информационного пространства в должной мере? Очевидна потребность в исследовании способов защиты личного информационного пространства и разработке перспективных средств обеспечения личной информационной безопасности с учетом влияния Больших данных. Мы привыкли думать, что знаем больше, чем знаем на самом деле. Наше понимание эффектов технологии отстает от неумолимых последствий ее применения на десятилетия [1].

Всегда 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 прогнозирования. Дело в том, что единожды собранные данные, в современных условиях могут храниться практически неограниченное время и быть подвергнуты повторному анализу с приходом новых, более совершенных аналитических алгоритмов, уточняя результаты прогнозирования и открывая новые, до этого невидимые, свойства. Это означает, что все больше средств будет вкладываться в инструменты сбора и анализа Больших данных, а тема безопасности Личного Информационного Пространства будет становиться все актуальнее [2].

Системы сбора и анализа Больших данных должны основываться на тщательно обдуманных принципах, с учетом необходимости защищать частную жизнь и гражданские свободы, с учетом того факта, что эти системы создаются по определенным правилам. Однако, правила, создаваемые людьми, со всеми их изъянами и недостатками, иногда порождают аномалии с невообразимым исходом. Не стоит питать надежд, что одних лишь нормативно-правовых мер и стандартизации хватит для того, чтобы обезопасить человека от возможных рисков Личной Информационной Безопасности.

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 тех или иных программных продуктов (средств хранения, обработки и передачи данных; протоколов и т.д.) и выработки эффективной стратегии защиты информации (как персональной, так

и корпоративной, государственной), основываясь на специфике доступного набора инструментов. Традиционно мы привыкли, что в первую очередь нужно обеспечить информационную безопасность государства, информационную безопасность крупного, в первую очередь транснационального, бизнеса, личная же информационная безопасность остается в тени. Однако, при таком подходе, велика вероятность, что построенная система начнет разваливаться снизу, ведь все равно конечным пользователем любой, даже самой сложной системы, является человек. На сегодняшний день доступно достаточное количество инструментов для разграничения и контроля доступа, фильтрации сетевого трафика и борьбы с вредоносными программами, но так ли они эффективны в руках среднестатистического пользователя без должной настройки и понимания специфики их работы?

Мы жертвуем безопасностью информации ради удобства ее обработки, переходя от узкоспециализированных информационных систем к смешанным даже в тех секторах, где этого не стоило бы делать из соображений безопасности. Говоря простым языком: на сегодняшний день в одной среде, мы можем работать с закрытой государственной или корпоративной информацией, параллельно имея неограниченный доступ в глобальную сеть и используя посторонние носители информации. Мы смешиваем наше личное пространство с рабочим, а это вещи далеко несовместимые. Расширяя возможности информационной системы, мы так же увеличиваем объем ресурсов, необходимых для качественной экспертизы на предмет ее устойчивости к актуальным угрозам и соответствующей инженерной модификации. В реалиях современного мира обычно доступно меньше ресурсов, чем необходимо для покрытия всех поставленных задач аудита безопасности, что и рождает потенциальные проблемы. Личная информационная безопасность и информационная безопасность всех механизмов системы в целом тесно связаны и без должного обеспечения одной части, нельзя говорить об эффективном обеспечении других.

Из-за недостатка внимания разработчиков, сложности и недоступности удобных средств для разграничения сред, организации и защиты информации в личной информационной системе, а также недостатка понимания со стороны пользователей, личное информационное пространство формируется хаотично, недостаточно организованно и небезопасно. Для краткого описания нашего подхода к концептуальному проектированию личного информационного пространства представим, что личное информационное пространство каждого человека может формироваться двумя составляющими: личными информационными системами обычного пользователя и личными информационными системами эксперта. Мы специально делаем такое разделение. Первые - традиционно формируются достаточно хаотично, в определенной мере по остаточному принципу как следствие разработки корпоративных информационных систем, без особой ориентации на обеспечение информационной безопасности каждого пользователя (личности). Проще говоря: обеспечение корпоративных интересов первично, интересы личности - вторичны. Вторые - мы предлагаем формировать целенаправленно, с ориентацией на личность. Интересы информационной безопасности личности должны быть первичными. Анализ потенциальных информационных угроз позволил выработать определенные принципы концептуального проектирования личного информационного пространства. Исходя из этих принципов, мы предлагаем, что в идеале любая личная информационная система, формирующая личное информационное пространство, должна строится как экспертная и постепенно вытеснять традиционные. Личные информационные системы экспертного типа, как правило, рассматриваются как точки входа в сложные интегрированные информационные системы. Соответственно, для обеспечения конфиденциальности, целостности и доступности пользовательской ин-

формации в неоднородной мультиконтекстной среде, которой являются корпоративные и глобальные сети, возникает потребность в надежном техническом решении, способном обеспечить безопасную синхронизацию данных между пользовательскими средами. Одним из таких решений является концепция «защищенного криптоконтейнера», соединяющего в себе передовые технологии хранения, синхронизации и защиты данных. Криптоконтейнер представляет из себя набор программного обеспечения, реализующий кроссплатформенный интерфейс управления пользовательскими данными и предоставляющий 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. 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 использование облачных сервисов. Криптоконтейнер использует изолированную область памяти в процессе работы, так называемую песочницу. Это позволяет разбить пользовательскую среду на самодостаточные не конфликтующие области для безопасной работы с различными категориями задач и данными даже на не доверенных средах. Криптоконтейнер реализует программный интерфейс для внешних расширений, с помощью которых возможно «заточить» функционал под любые задачи и требования. В частности, реализуется модуль активного мониторинга выделенной области памяти с целью исключить внешнее вмешательство в процесс работы криптоконтейнера. В данном случае можно провести аналогию с активной защитой для военной техники: в то время как криптоконтейнер предоставляет крепкую броню для пользовательской информации, модуль активной защиты не позволяет угрозам даже подобраться к безопасной зоне. Для наглядности, проиллюстрируем работу криптоконтейнера на примере синхронизации пользовательского программного обеспечения и генерируемых в процессе его использования данных:

Пользователь, работая на некотором устройстве, помечает программу П1 как элемент криптоконтейнера.

В настройках криптоконтейнера пользователь отмечает Яндекс.Диск, Dropbox и локальную сеть в качестве «целей» для синхронизации. Криптоконтейнер создает репликацию бинарного файла программы П1, 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.

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.

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

Клиент, как правило, самое слабое звено системы. В большинстве случаев пользователь работает из недоверенной среды - его рабочее место используется для разных задач, в том числе и для тех, которые требуют повышенной защищенности рабочей среды. Клиент часто значительно экономит на средствах защиты и даже отказывается от многих требований безопасности (включая требования регулятора) в пользу удобст-

ва. Для повышения уровня безопасности личного информационного пространства эксперта для доступа к информационным системам, обрабатывающим информацию ограниченного распространения, интересным представляется защищенное программно-аппаратное устройство на основе Гарвардской архитектуры, предложенное В. Конявским и В. Степановым, описанное в патенте №118773.27.07.12. Основное отличие новой Гарвардской архитектуры от архитектуры фон Неймана заключается в том, что в компьютере с использованием новой Гарвардской архитектуры процессор может читать инструкции и выполнять доступ к памяти данных одновременно, без использования кэш-памяти. Таким образом, компьютер с новой Гарвардской архитектурой при определенной сложности схемы быстрее и безопаснее, чем компьютер с архитектурой фон Неймана, поскольку шины инструкций и данных расположены на разных, не связанных между собой физически, каналах. Исходя из физического разделения шин команд и данных, разрядности этих шин (следовательно, и адресные пространства) могут иметь различные значения и физически не могут пересекаться друг с другом [3,4].

Таким образом, объединяя удачные технические и программные решения, становится возможной безопасная работа с конфиденциальной информацией без потери мобильности и удобства современных вычислительных сред. Благодаря данному подходу к проектированию личного информационного пространства, человек получает компромиссный вариант управления персональной информацией в условиях современного кризиса личной информационной безопасности.

Список литературы

1. Таненбаум Э. Распределенные системы. Принципы и парадигмы. – СПб.: Питер, 2003. – 877 с.

2. Фрэнкс Б. Укрощение Больших данных. М.: Манн, Иванов и Фербер, 2014. 352 с.

3. Конявский В. А., Кузнецов Д., Волчков А., Афанасьев А. Специализированные компьютеры – панацея от хакеров? // Аналитический банковский журнал. – No12 (224) декабрь 2014. – С. 66–69.

4. Конявский В. А., Степанов В. Б. Компьютер типа «тонкий клиент» с аппаратной защитой данных. Патент на полезную модель No 118773.27.07.12, бюл. No21

КЛАССИФИКАЦИЯ И РАЗМЕТКА ЭЛЕМЕНТОВ ТЕКСТА НА УРОВНЕ ПРЕДЛОЖЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ НУЛЕВОГО ДНЯ

Е.Д. МАТЯШ

Московский технологический университет

Введение

Сейчас стало популярным использование таких систем, которые так или иначе имеют дело с понятием BigData – в данном случае имеется ввиду разметка текста в плане его разделения на различные элементы разных типов: слова, предложения, абзацы и т.д. Это разделение необходимо для поддержания работы многих систем, которые напрямую связаны с текстовой информацией. Текстовые редакторы, поисковики и любые другие информационные системы работают непосредственно за счет специальных алгоритмов обработки исходной текстовой информации. Все эти алгоритмы,