III. Проблемы обеспечения информационной безопасности

DOI: 10.25728/iccss.2022.75.12.017

Курако Е.А.

К вопросу безопасности отечественного программного обеспечения

Аннотация: Рассмотрена разработка программного обеспечения для отечественных операционных систем общего назначения с использованием документации и примеров, расположенных на сайтах операционных систем. Поднят вопрос о качественном подборе материалов для создания безопасного программного обеспечения.

Ключевые слова: программное обеспечение, документация, разработка, операционная система, безопасность

Количество задач, возникающих в области создания программного обеспечения, достаточно велико. Основными проблемами являются возрастающая сложность кода и архитектуры приложений, и, как следствие, высокий начальный порог вхождения в эту область. Непрерывное совершенствование и исследование новых методов разработки безопасности программного обеспечения [1] и обработки данных добавляет значительный объем необходимой для изучения информации. В то же время, в рамках импортозамещения [2], возникает срочная потребность в разнообразных программах для отечественных операционных систем (ОС) общего назначения. Процесс обучения в учебных заведениях, как правило, направлен на получение базовых фундаментальных знаний и не успевает за быстроменяющимися тенденциями.

Известно, что операционная система, сама по себе, без прикладных программ не интересна пользователям. И для развития ее окружения необходимо создание (адаптация) большого количества приложений. Как пример, можно рассмотреть мобильную операционную систему HarmonyOS, когда Huawei

провела огромную компанию по привлечению разработчиков на свою платформу [3].

Безопасность системы определяется самым слабым звеном. Таким образом, сторонние приложения должны советовать уровню операционной системы. Сторонний разработчик должен оперативно разобраться в организованной системе безопасности ОС для создания надежного программного продукта. Ввиду постоянного совершенствования ОС, основным источником сведений о ней и ее механизмах является официальный веб-сайт.

Рассмотрим раздел официальных сайтов основных отечественных операционных систем, посвященный разработке приложений и механизмам защиты.

Альт Линукс СПТ (Разработчики: ООО «Свободные программы и технологии», «Базальт СПО»)

На сайте присутствует раздел с документацией и есть описание некоторых особенностей при разработке программ для системы. К сожалению, раздел, посвященный разработке безопасных приложений, отсутствует. Хотя стоит отметить, что сообщество разработчиков приглашает вступить в их ряды, где новичку организуют помощь на начальном этапе. Так же есть раздел с книгами и тезисами докладов, посвящённый разработке ПО.

Astra Linux (НПО «Русские базовые информационные технологии»)

Портал Astra Linux достаточно объемный по содержанию, сложно структурирован, но в нем есть информация для разработки приложений интегрирующихся с механизмами безопасности системы, например, «Руководящие указания по конструированию прикладного программного обеспечения для операционной системы общего назначения Astra Linux Common Edition». На сайте есть форум и раздел с бюллетенями, содержащие обновляющиеся методики и обновления программного обеспечения для нейтрализации угроз уязвимостей в информационных системах.

Ред ОС и GosLinux (Разработчик: компания «Ред Софт»)

На сайтах этих систем никакой информации не представлено. Есть документация для пользователя и для администратора.

ROSA Linux (Разработчик: ООО «НТЦ ИТ РОСА»)

Сайт имеет ярко выраженную рекламную направленность. На главной странице присутствует ссылка на раздел «Разработчикам», где можно перейти на форум или на википедию, посвященную Rosa Linux. Дополнительно новичкам создали группу на сайте vk.com, где обещают помощь. Но раздела, повещённого методикам безопасного программирования, нет.

Эльбрус (Разработчик: АО «МЦСТ»)

Сайт операционной системы «Эльбрус» для разработчика лаконичен. Ему предлагается приобрести «Набор разработчика «Эльбрус Линукс» (PDK)», в котором есть примеры, документы и даже исходники компонентов системы. Для приобретения набора необходимо прислать официальный запрос в отдел продаж.

В целом можно сделать вывод о слабом распространении методик и результатов исследований, направленных на создание защищённого программного обеспечения. С одной стороны, идет исследование новых и усовершенствование существующих моделей, методов, алгоритмов, эти результаты отражаются в обновляющихся нормативных документах. С другой стороны, есть запрос разработчиков (как начинающих, так и переквалифицирующихся) на актуальную документацию, позволяющую вести разработку приложений для отечественных операционных систем с современными механизмами защиты. В то же время, разработчики отечественных систем, как правило, не спешат делиться наработанным опытом.

Литература:

1. *Девянин П.Н., Тележников В.Ю., Хорошилов А.В.* Формирование методологии разработки безопасного системного программного обеспечения на примере операционных систем // Труды ИСП РАН. – 2021. – Том 33. Вып. 5. – С. 25-40.

2. *Курако Е.А., Орлов В.Л.* К вопросу перевода информационных систем на отечественное программное обеспечение / Материалы 28-й Международной научной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС'2020, Москва). – М.: ИПУ РАН, 2020. – С. 246-249.

3. Huawei привлекает разработчиков в свой магазин

приложений. – URL: https://new-science.ru/huawei-privlekaet-razrabotchikov-v-svoj-magazin-prilozhenij/ (дата обращения 01.10.2022).

DOI: 10.25728/iccss.2022.52.24.018

Курако Е.А., Орлов В.Л.

Принципы обеспечения безопасности при использовании сервис-браузерной технологии

Аннотация: Рассматриваются вопросы защиты информации при использовании сервис-браузерной технологии. Выделяются уровни обеспечения безопасности. Определяется возможность использования сервис-браузера для защиты информационных систем.

Ключевые слова: сервис-браузер, клиент, сервер, средства защиты, безопасность, хранилище, аутентификация, авторизация

В качестве клиентов для информационных систем могут использоваться сервис браузеры [1, 2]. Сервис-браузер, в отличие от обычного браузера, имеет компонент, выполняющийся на клиенте (клиент браузера), и компонент (сервис браузера), выполняющийся на сервере (рисунок 1). Кроме того, на сервере (может быть отдельном) размещается хранилище данных браузера.

Причем каждый компонент включает три фрагмента.

- Фрагмент загрузки и обновления.
- Фрагмент обеспечения безопасности.
- Фрагмент организации запуска и завершения модулей.

В настоящей работе рассматривается фрагмент обеспечения безопасности, поэтому сосредоточимся на описании основных принципов, на которых базируется его разработка.