

УДК 004.413

## ПРЕИМУЩЕСТВА КОНЦЕПЦИИ КИБЕРИММУНИТЕТА ПРИ РАЗРАБОТКЕ ПРОГРАММНЫХ ПРОДУКТОВ

Рыбаков С.Д. (Университет ИТМО, г. Санкт-Петербург)

Научный руководитель – кандидат технических наук, доцент Балакшин П.В.  
(Университет ИТМО)

**Аннотация.** В работе рассматриваются основополагающие принципы концепции кибериммунной подготовки программных продуктов. Раскрываются ее преимущества по сравнению с прочими популярными методологиями разработки ПО. Таким образом, показывается состоятельность кибериммунитета и оцениваются его перспективы.

**Введение.** В связи с активным развитием компьютерной техники и ее внедрением во все сферы окружающей нас жизни, люди потребляют все больше различных программных продуктов. Закономерно возникающая конкуренция в сообществе разработчиков приводит к тому, что в процессе разработки ПО наибольший акцент делается на скорость вывода продукта на рынок при снижении сопутствующих затрат, что негативно сказывается на безопасности кода. Кроме того, постоянное усложнение технологий приводит и к снижению возможностей программистов обеспечить наиболее действенную защиту программ, да и влияние человеческого фактора присутствует.

Вследствие существования указанной проблемы, встает необходимость в подготовке такой методологии разработки ПО, которая бы позволяла осуществлять достаточную защиту продуктов при наименьших издержках. Коротко говоря, необходим унифицированный способ эффективной разработки достаточно безопасных программных продуктов.

**Основная часть.** Для решения поставленной задачи АО «Лаборатория Касперского» провела анализ уже существующих решений и концепций, моделей. Результаты показали, что требуемые параметры эффективности и надежности не достигаются, поэтому была разработана собственная операционная система – KasperskyOS [1]. Она стала тем самым искомым инструментом для реализации достаточно надежных программ при соблюдении корректного «технологического процесса» [2].

Однако, во-первых, само использование еще не столь известной ОС связано с некоторыми сложностями для разработчиков, а во-вторых, принципы ее функционирования, такие как «Монитор безопасности», «Политики безопасности», модель «Нулевого доверия» (Zero Trust) и прочие аспекты оказались гораздо более самостоятельными, чем казалось изначально.

Возникло предположение о том, что, экстраполируя заложенные в KasperskyOS идеи [3][4] на процесс разработки, можно описать методологию подготовки достаточно защищенных программных продуктов от этапа формирования их концепции до финальной верификации результата.

Полученный процесс позволяет избежать наиболее популярных проблем разработки и кода за счет использования прозрачной методологии Secure By Design, принципов изоляции, контроля и минимизации доверенной кодовой базы, формирования понятных архитектурных требований и использования шаблонов обеспечения безопасности. В результате, обеспечивается наиболее эффективное решение проблемы построения решения, которому можно будет доверять при условии, что оно состоит из компонентов, меньшинству из которых можно однозначно доверять.

**Выводы.** В данный момент данная концепция активно развивается, формулируется и тестируется Лабораторией Касперского. Проходят курсы и семинары по ознакомлению с ней, хакатоны по практическому применению теоретических и практических аспектов на

различных площадках, в чем автор принимает участие, подтверждая заявленную эффективность методологии на практике.

**Список использованных источников:**

1. Блог «Лаборатории Касперского», «Операционная система с кибериммунитетом: кто, зачем и как создает KasperskyOS» [Электронный ресурс] – URL: <https://habr.com/ru/article/499746/> (дата обращения 05.03.2023)
2. Документация по KasperskyOS [Электронный ресурс] – URL: <https://support.kaspersky.ru/help/KCE/1.1/ru-RU/overview.htm> (дата обращения 05.03.2023)
3. Rushby, J.: Separation and integration in MILS (the MILS constitution). Technical report, Menlo Park, CA, February 2008
4. Flask: Flux Advanced Security Kernel [Электронный ресурс] – URL: <https://www.cs.utah.edu/flux/fluke/html/flask.html> (дата обращения 25.01.2023)

Рыбаков С.Д. (автор)

Подпись

Балакшин П.В. (научный руководитель)

Подпись