И.В. Алябьев, З.З. Шарипов
Ташкентский университет информационных технологий им. Мухаммада Аль-Хорезми, г. Ташкент
УДК 004.056.5

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ЭТАП ПРОЕКТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация. В статье вводится понятие политики информационной безопасности программного обеспечения, а так же описана разработка подобной политики как этап проектирования.

Ключевые слова: политика информационной безопасности, проектирование программного обеспечения.

Проектирование программного обеспечения (далее ПО) может быть очень трудоемким процессом, в зависимости от его назначения и предъявляемых к нему требований отказоустойчивости, надежности и т.п. Информационная безопасность, в контексте работы разрабатываемого ПО, может быть обеспечена недостаточно, в зависимости от квалификации разработчиков ПО в области информационной безопасности. В данной статье описан подход, потенциально повышающий обеспеченность информационной безопасности, путем разработки политики информационной безопасности ПО в процессе проектирования.

Политика информационной безопасности ПО (далее ПИБПО), в контексте данной статьи, определяется как перечень требований и рекомендаций информационной безопасности, предъявляемых к ПО на всех этапах разработки. На рис.1 показана общая структура подобной ПИБПО.

ПИБПО, в общем случае, имеет два т.н. «уровня»: локальный и глобальный. Локальный уровень представляет собой ПИБПО, разрабатываемую и применяемую в рамках конкретного проекта по разработке ПО. Локальная ПИБПО включает в себя два базовых уровня: совокупность общих требований и рекомендаций ИБ и совокупность требований и

рекомендаций ИБ для конкретной предметной области (для которой, собственно, и разрабатывается ПО в конкретном случае).

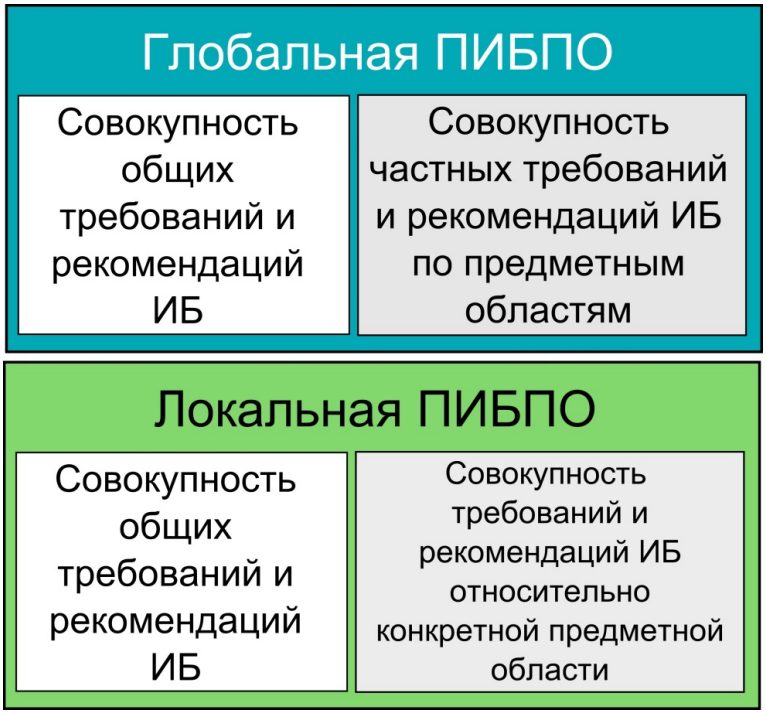

Рис.1. Общая структура политики информационной безопасности ПО.

Общие требования и рекомендации ИБ, в свою очередь, могут быть сформированы на основе различных стандартов в сфере ИБ, опубликованных результатов исследований в сфере ИБ и т.п. Частные же требования формируются в процессе исследования конкретной предметной области. Т.н. «глобальная» ПИБПО, формируется на основе локальных ПИБПО, и, также, имеет 2 уровня.

На рис.2 изображен процесс формирования глобальной ПИБПО. На этапе проектирования ПО происходит формирование локальной ПИБПО. Источником для локальной политики ПИБПО являются требования ИБ, описанные в техническом задании конкретного проекта (например, разработка системы планирования ресурсов предприятия). Далее происходит применение стандартов и других регламентирующих нормативных документов ИБ, имеющих отношение к предметной области конкретного проекта (например, FIPS200 - Минимальные требования безопасности для федеральной

информации и информационных систем). После чего применяются опубликованные результаты научных исследований. В конечном счете, знания, полученные в результате разработки политики ИБ в рамках проекта, накапливаются в глобальной ПИБПО. В последующих разработках, глобальная ПИБПО используется как один из источников для разработки локальной ПИБПО.

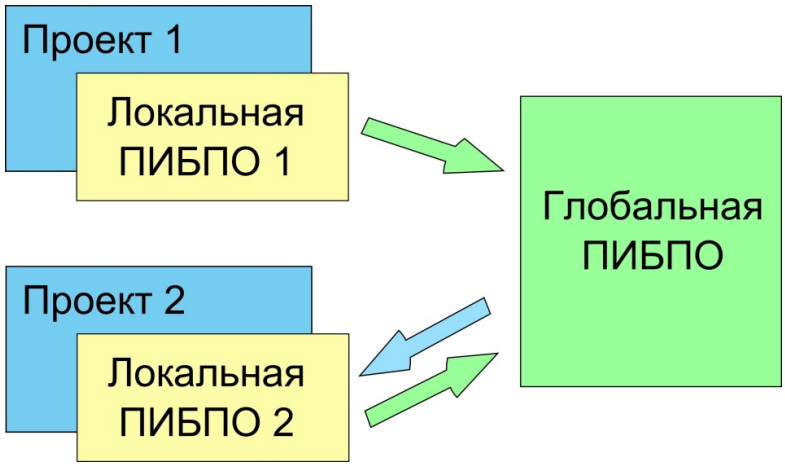

Рис.2. Процесс формирования политики информационной безопасности ПО.

ПИБПО рекомендуется описывать в виде тезисов, подкрепленных обоснованием того или иного требования или рекомендации. Кроме того, следует обеспечить контроль версий для глобальной ПИБПО.

Описанный выше подход потенциально повышает уровень обеспечения информационной безопасности в программных продуктах, реализованных с его использованием. Следует отметить, что с развитием глобальной ПИБПО, повышается и эффективность ее использования с каждой новой разработкой.

Также следует отметить пользу данного подхода с точки зрения образования (саморазвитие участников и повышение квалификации). При наличии ПИБПО новые члены той или иной команды разработчиков будут обучаться более эффективно (в контексте повышения квалификации в сфере информационной безопасности), что особенно актуально в исследовательских и прикладных проектах выполняемых командами, сформированными из студентов.