Устранение уязвимостей в сертифицированных СЗИ. Опыт российского разработчика и анализ ситуации в проектах по информационной безопасности

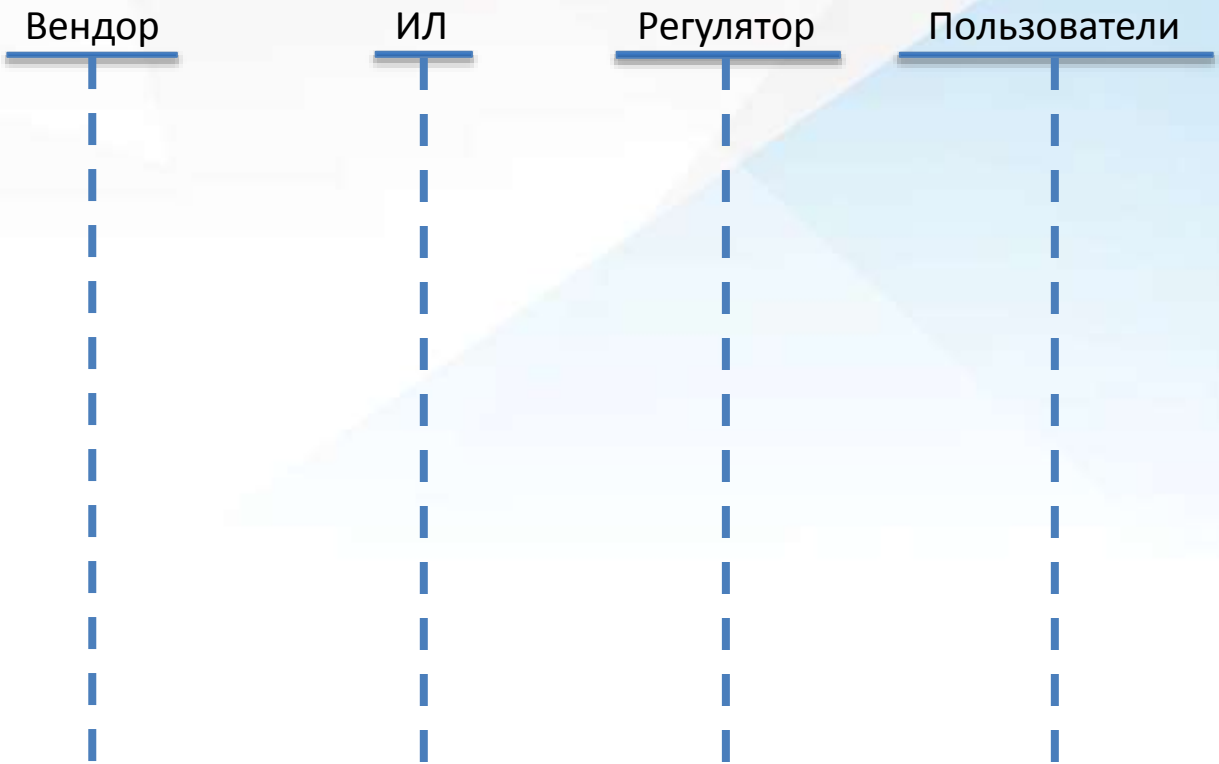

25
КОНФИДЕНТ
ГРУППА КОМПАНИЙ

Методика обновления сертифицированных средств защиты информации:

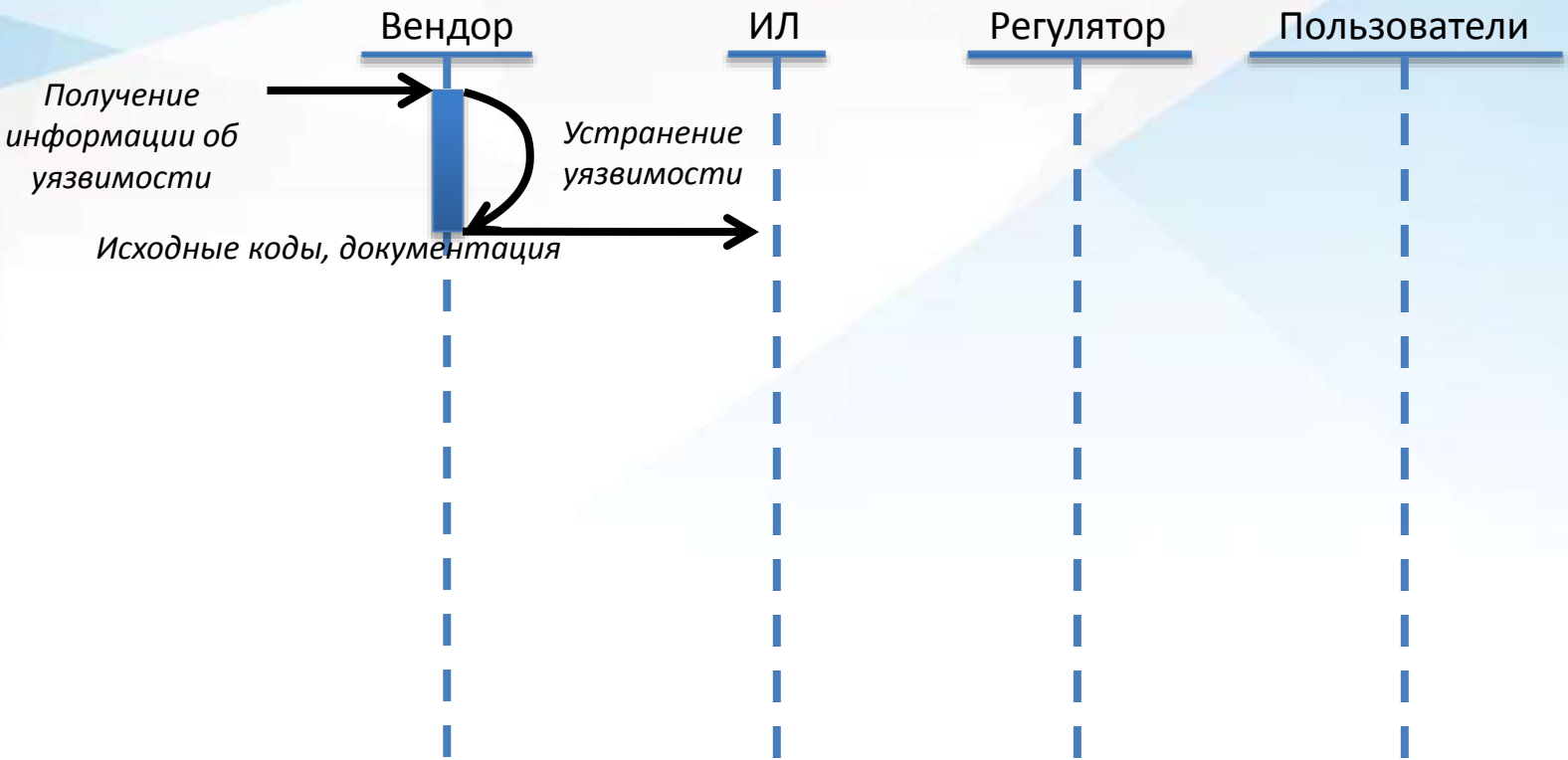
- Определены типы обновлений (включая обновления, направленные на устранение уязвимостей средств защиты информации), а также действия вендора (заявителя), испытательной лаборатории и конечных пользователей при применении данных обновлений.

- Все разработчики применяют данную методику.

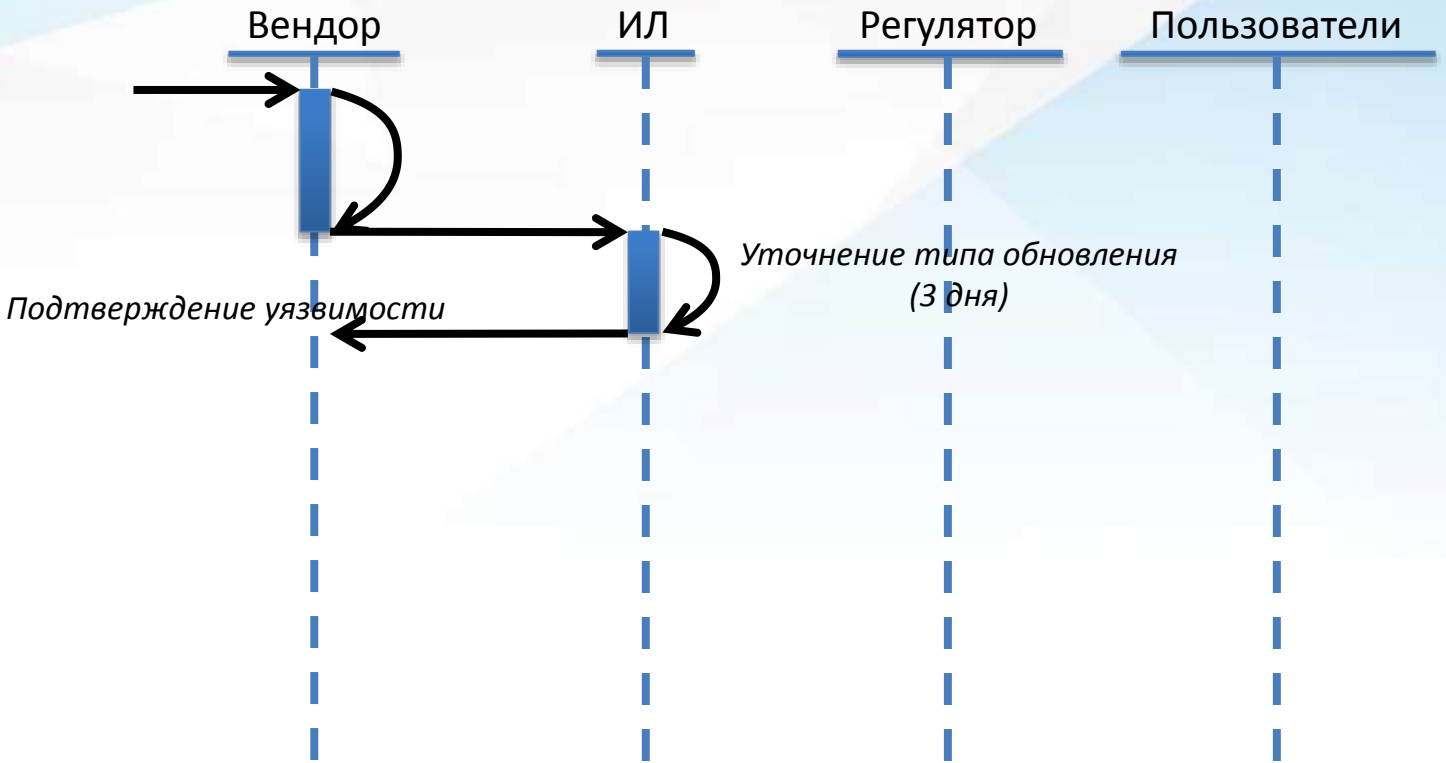
Обновление сертифицированных средств защиты информации



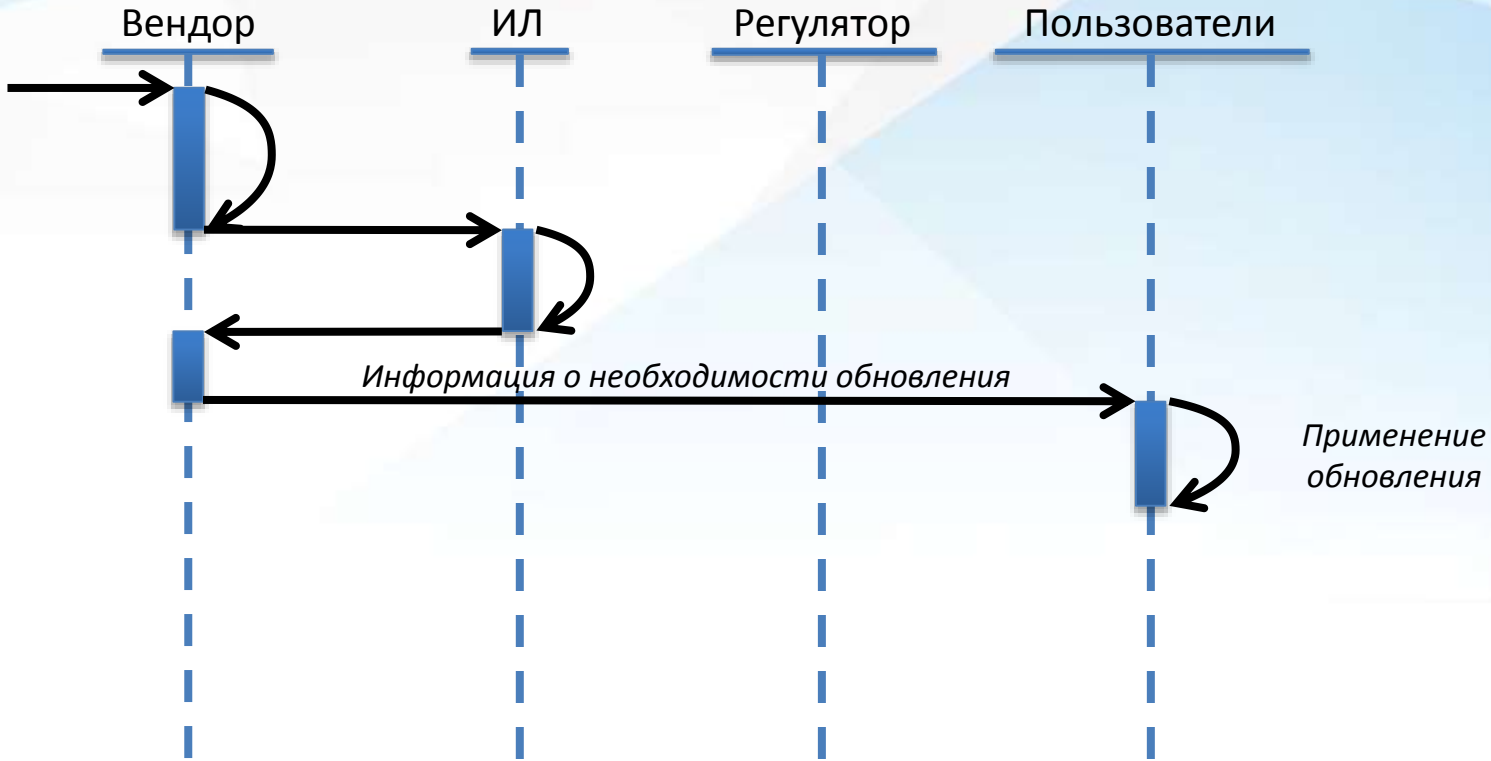
Обновление сертифицированных средств защиты информации



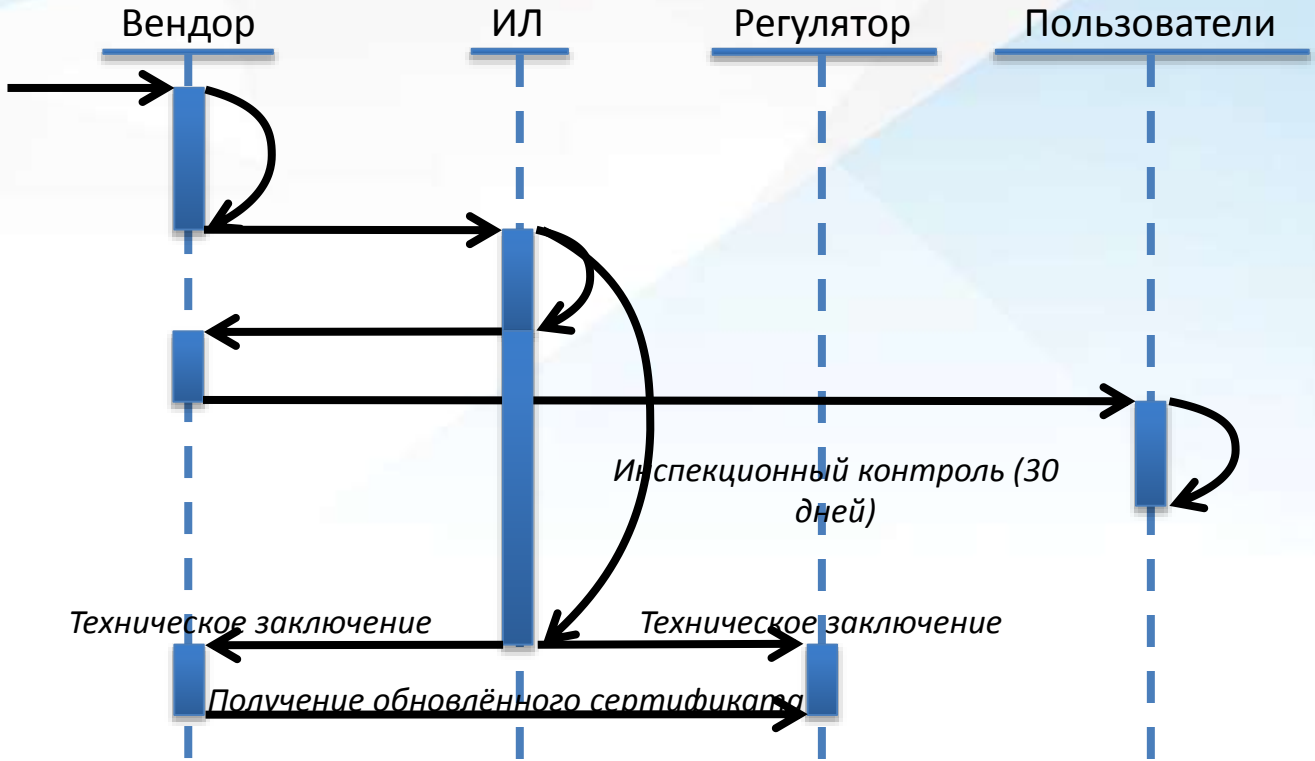
Обновление сертифицированных средств защиты информации



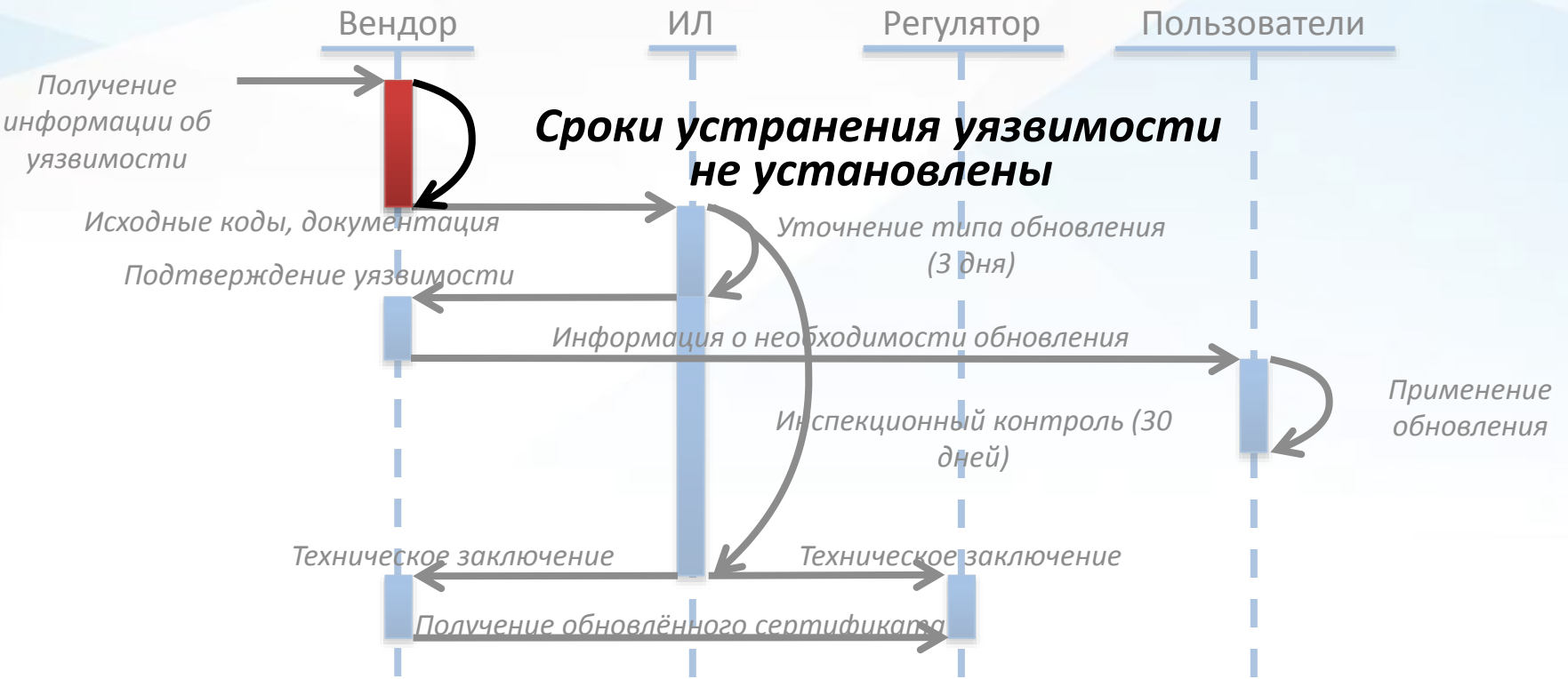
Обновление сертифицированных средств защиты информации



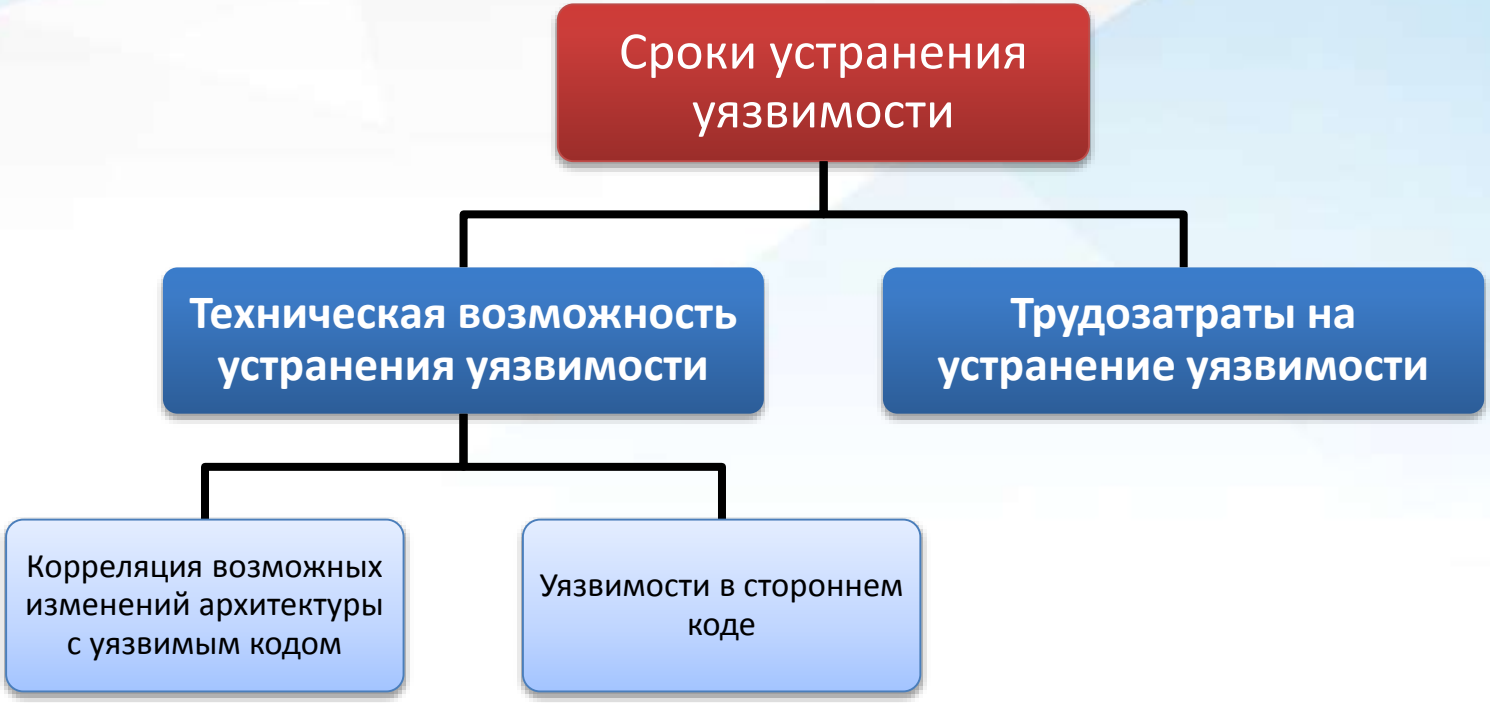
Обновление сертифицированных средств защиты информации



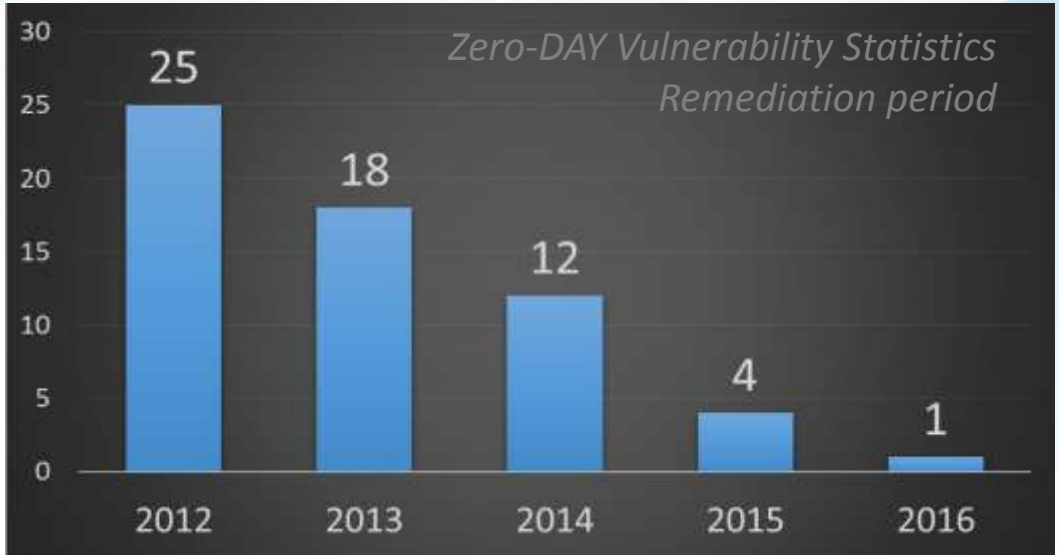
Обновление сертифицированных средств защиты информации



От чего зависят сроки устранения уязвимостей?



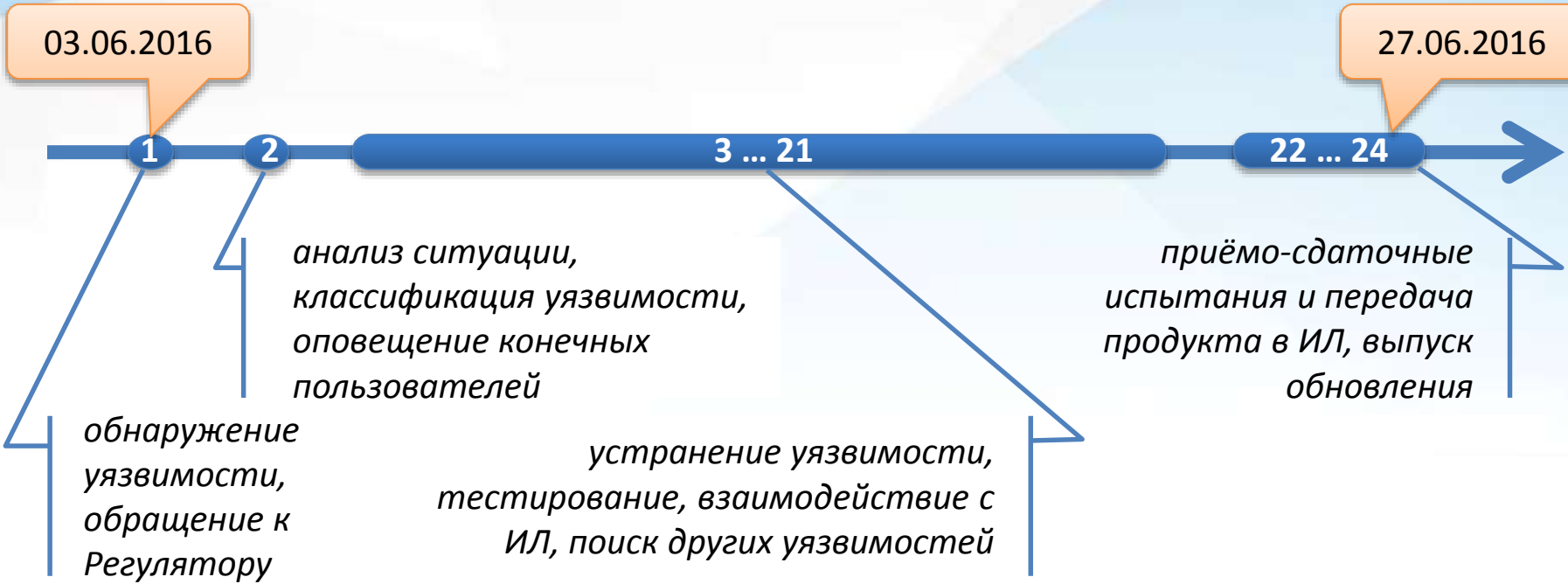
Сроки устранения уязвимостей ведущих мировых вендоров



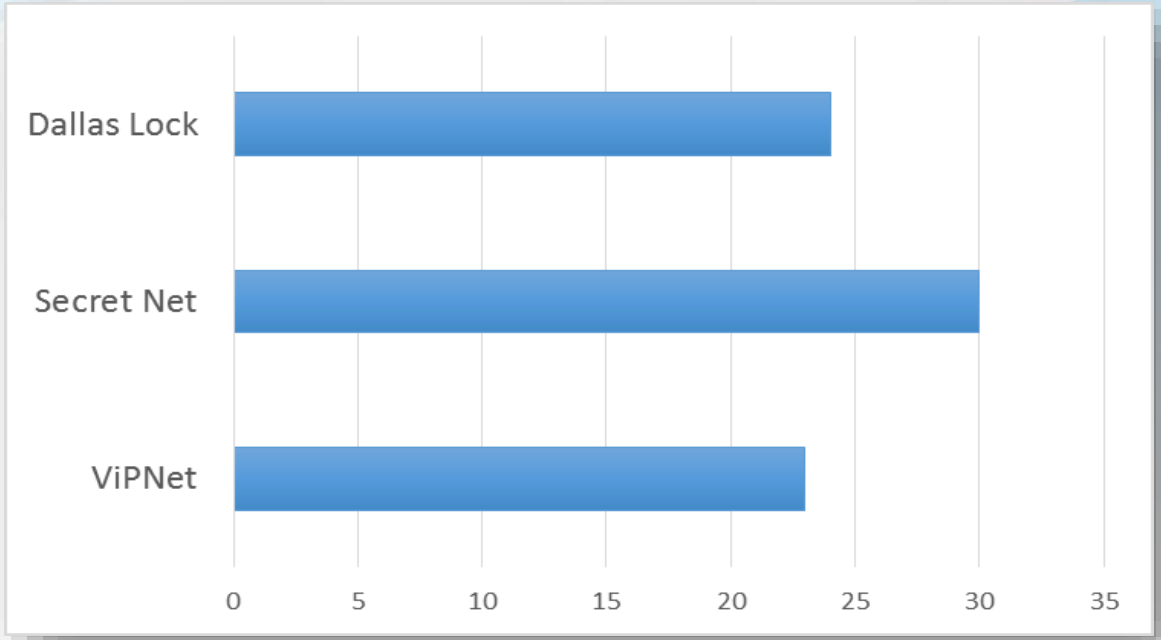
Статистика по средним срокам устранения уязвимостей (по закрытым уязвимостям)

Данные 0-DAY tracking project (www.zero-day.cz)

Практический кейс

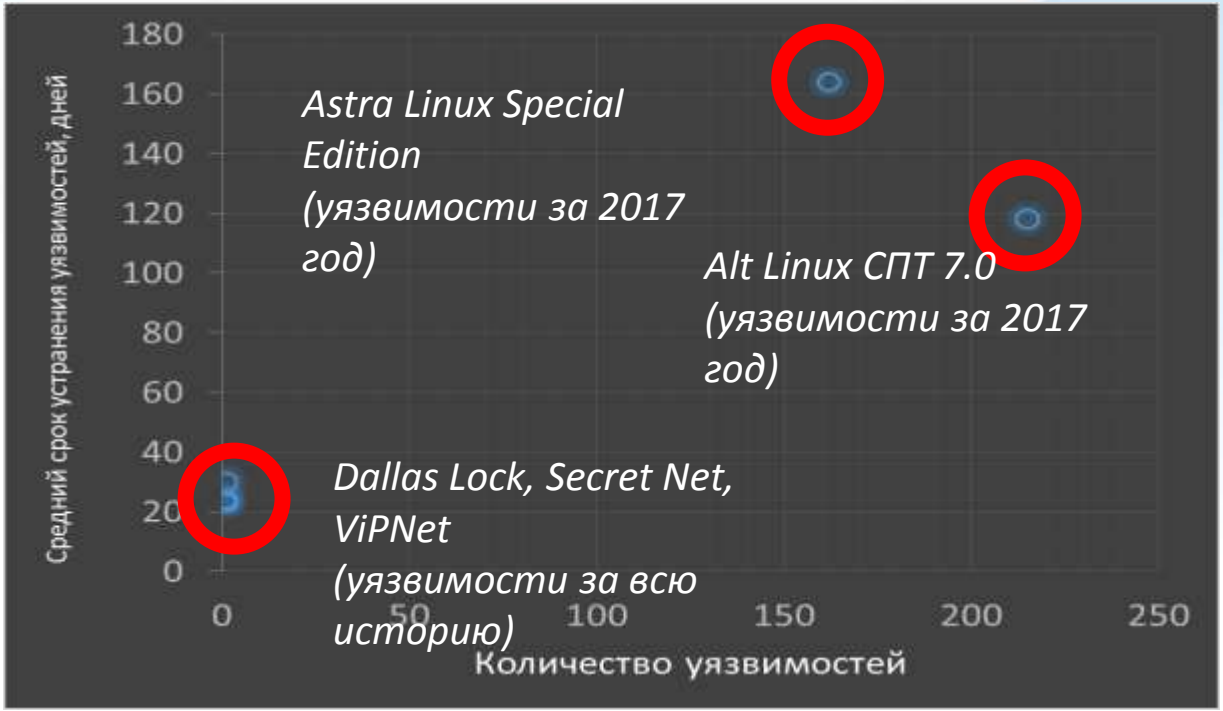


Сроки устранения уязвимостей российскими разработчиками

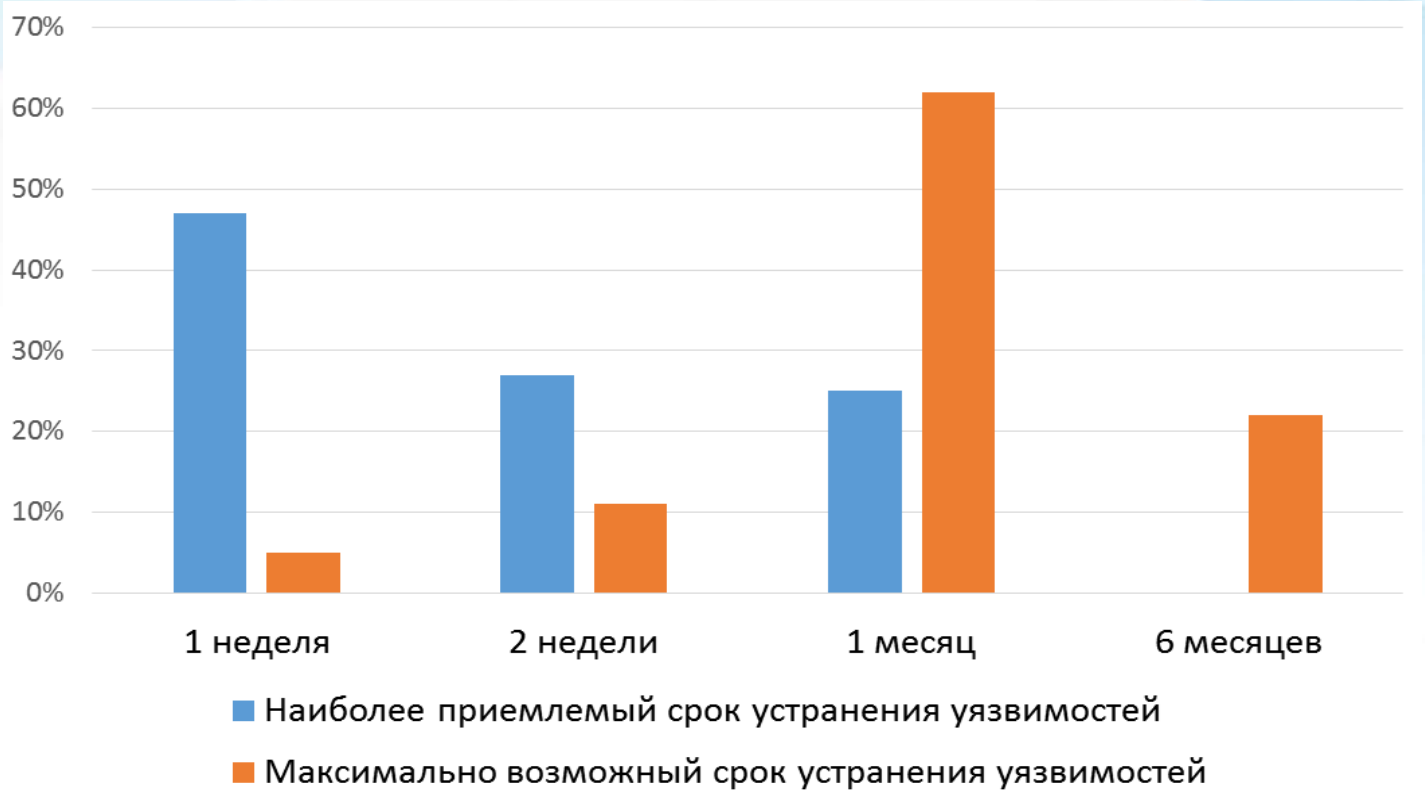


Российским разработчикам СЗИ требуется примерно 1 месяц для устранения уязвимости

Сроки устранения уязвимостей российскими разработчиками



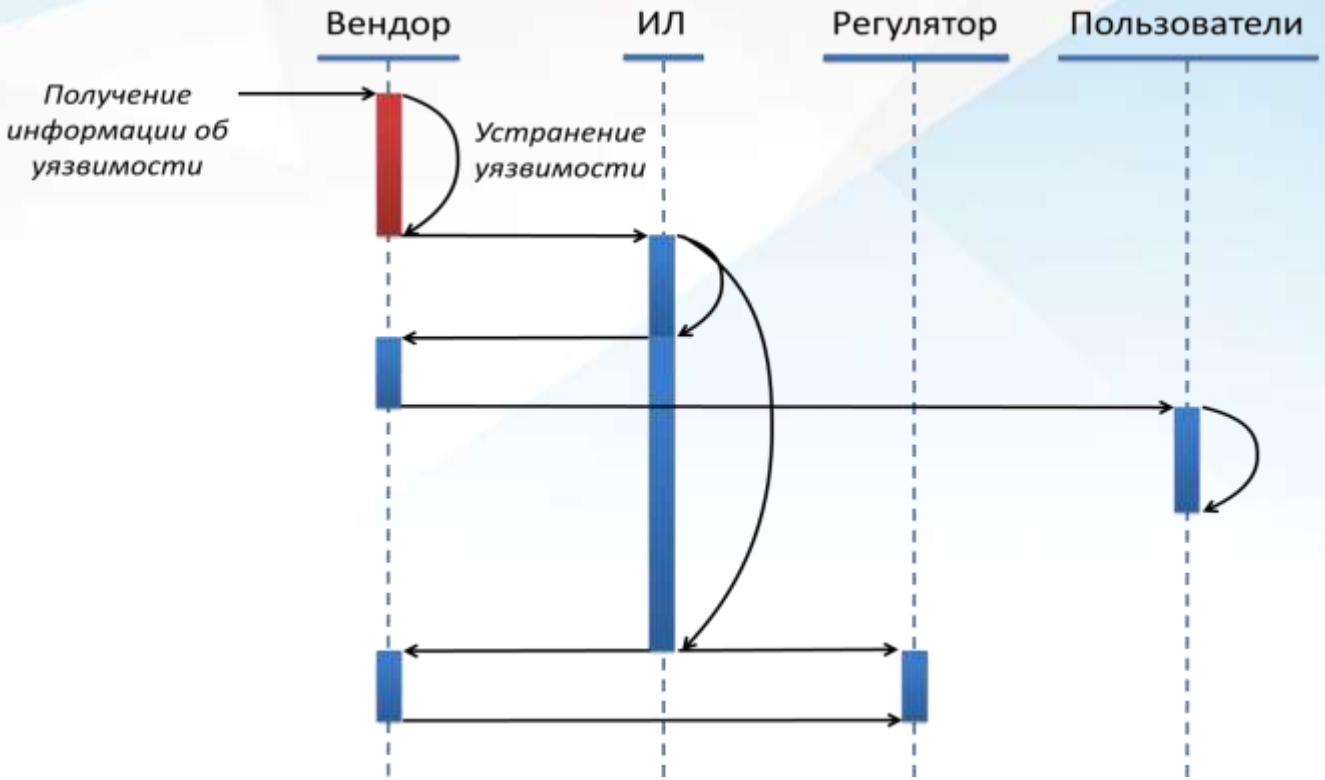
Результаты опроса партнёров и конечных пользователей ЦЗИ ГК «Конфидент»



Результаты опроса партнёров и конечных пользователей ЦЗИ ГК «Конфидент»

По мнению профессионального сообщества разработчики средств защиты информации должны устранять уязвимости в своих продуктах от 1 недели до 1 месяца

Минимизация вероятности возникновения уязвимостей в сертифицированных СЗИ



Минимизация вероятности возникновения уязвимостей в сертифицированных СЗИ

Работа с ВУЗами: бесплатное предоставление СЗИ и документации для обеспечения учебного процесса, сертификация специалистов по продуктам, методическая поддержка.

Оперативное оповещение пользователей через рассылку.

Проверка наличия обновлений в программном обеспечении.

Bug bounty (юридическое оформление для защиты прав вендора и исследователей, функциональность личного кабинета для получения версий ПО и отправки информации об уязвимостях). Уже более 100 исследователей зарегистрировались в программе.

Процесс безопасной разработки по ГОСТ Р 56939—2016, собственные методики и подходы к разработке безопасной архитектуры, использование автоматизированных проверок (статический и динамический анализ) кода.

Выводы

На безопасность ИС влияет не только количество уязвимостей, но и скорость их устранения.

Устранение уязвимостей в свободном ПО происходит значительно дольше, чем в проприетарном ПО.

Спасибо за внимание!