Банк России

ОТ СЕРТИФИКАЦИИ И ОЦЕНКИ СООТВЕТСТВИЯ ПО ОУД-4 ДО БЕЗОПАСНОЙ РАЗРАБОТКИ ПО

СТАРОДУБОВ КОНСТАНТИН

ДЕПАРТАМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
БАНК РОССИИ

2024 г.

Банк России

Требование о проведении оценки соответствия по ОУД4

Выполнение требований ПО по ОУД4

П. 4.1 Положения Банка России от 17.04.2019 № 683-П - Об информационной безопасности для кредитных финансовых организаций

П. 1.8 Положения Банка России от 20.04.2021 № 757-П - Об информационной безопасности для некредитных финансовых организаций

П. 1.2 Положения Банка России от 17.08.2023 № 821-П - Об информационной безопасности в денежных переводах

П. 3.1 Положения Банка России от 17.10.2022 № 808-П - Об информационной безопасности в сфере финансовых рынков

Требования распространяются на:

ППО АС и **приложений**, распространяемых клиентам для совершения действий, непосредственно связанных с осуществлением переводов денежных средств, осуществления банковских и финансовых операций

ПО, обрабатывающего защищаемую информацию на участках, используемых для приема электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием сети "Интернет"

Банк России

Выполнение требований о проведении оценки соответствия по ОУД4

ТРЕБОВАНИЯ К ППО И ПРИЛОЖЕНИЯМ

Сертификация ФСТЭК России

Оценка соответствия ОУД4 в соответствии с ГОСТ Р ИСО/МЭК 15408-3-2013

В целях разработки и внедрения безопасных программных продуктов при сохранении гарантированного и достаточного уровня защищенности ППО АС и приложений, используемых при осуществлении финансовых (в т. ч. банковских) операций, Банк России рекомендует использовать раздел 7.4. Методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций»*

* Информационное письмо от 02.02.2022 № ИН-017-56/5

БЕЗОПАСНАЯ РАЗРАБОТКА

Методический документ «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций» (далее – ПЗ) с включенным разделом по безопасной разработке **одобрен ПК №1 ТК №122** и **опубликован на официальном сайте Банка России.**

От ОУД к безопасной разработке

ЦЕЛИ

1. Быстрая разработка в условиях изменяющихся требований;
2. Повысить защищенность разрабатываемого ППО, снизить количество уязвимостей;
3. Сделать обеспечение ИБ неотъемлемой частью процесса разработки.

ОБЪЕКТЫ ПРИМЕНЕНИЯ

Жизненный цикл разработки, тестирования и сопровождения, включая контроли по безопасности.

ПОДХОД

Переход от требований ОУД (ТДБ, п. 7.2 ПЗ) к требованиям по организации процесса безопасной разработки при выборе конкретных требований по ИБ с учетом реальных рисков, специфики разработки и функционирования продукта.

Банк России Условия и критерии перехода от ОУД к безопасной разработке

ППО/приложения не относятся к категории критичных информационных систем (КИИ).

Инфраструктура разработки и тестирования, среды постоянной эксплуатации (в том числе СОИБ) соответствуют требованиям ГОСТ Р 57580.1-2017.

Наличие собственной разработки с соответствующей компетенцией, постоянное обучение по ИБ разработчиков, сотрудников ИБ.

Наличие необходимых автоматизированных инструментов для создания сред и настройки жизненного цикла.

Наличие документированного процесса разработки, тестирования и эксплуатации с описанными контролями и проверками по обеспечению ИБ и документированного процесса управления версиями и изменениями ППО/приложений.

Инфраструктурные системы (платформы) и решения по обеспечению ИБ документированы в достаточном виде.

Банк России Условия и критерии перехода от ОУД к безопасной разработке

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД ПРИМЕНЕНИЯ КОНТРОЛЕЙ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ И ТЕСТИРОВАНИИ ППО/ПРИЛОЖЕНИЙ

Определение актуальных требований ИБ и мер защиты связанных с атаками слабостей (CWE), составление связанных с CWE уязвимостей (CVE) и уязвимых конфигураций (CPE).

Анализ рисков нарушения информационной безопасности и определение векторов и актуальных атак (CAPEC).

Проведение контролей ИБ при переносах между средами (контроль корректности требований ИБ, авто-тесты, статический анализ, динамический анализ, пентесты).

Мониторинг инцидентов, при внесении изменений в ППО/приложение - анализ необходимости проведения полного цикла контролей.

Внедрение решений и мер по минимизации рисков ИБ.

Условия и критерии перехода от ОУД к безопасной разработке

РОЛИ В КОМАНДЕ

Аналитик ИБ/Офицер ИБ

Обычно роль выполняет сотрудник подразделения информационной безопасности и защиты информации, являющийся специалистом по ИБ прикладного программного обеспечения и приложений.

Security Champion

Роль для специалиста с высокой осведомленностью в вопросах ИБ и имеющего компетенции в области безопасности прикладного программного обеспечения и принципов безопасной разработки.

- Разработчику необходимо обеспечить подготовку и повышение компетенций сотрудников.
- Разработчику необходимо осуществлять периодический пересмотр состава ролей и их обязанностей.

Ожидаемый эффект от внедрения модели безопасной разработки

Коллегиальное принятие решений в отношении операционных рисков с привлечением всех заинтересованных сторон – участников процесса внедрения ППО/приложений.

Уменьшение стоимости и скорости исправления уязвимостей благодаря нахождению их на более ранних этапах разработки.

Повышение качества и безопасности быстрой разработки за счет глубокого анализа работы продукта и обучения разработчиков принципам безопасности.

Непрерывный мониторинг защищенности ППО/приложений, своевременность исправления уязвимостей и управление обновлениями.

О планах

Разработка МР по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры организаций финансового рынка.
Описание подходов по проведению тестирования на проникновение, по классификации и устранению уязвимостей ИБ.

Синхронизация ПЗ с новой редакции ГОСТ Р 56939-2024 «Разработка безопасного программного обеспечения. Общие требования» и новыми стандартам в серии.

Дополнение и уточнение отдельных контролей безопасности.

Постоянное улучшение и обратная связь.

Банк России

СПАСИБО ЗА ВНИМАНИЕ!