

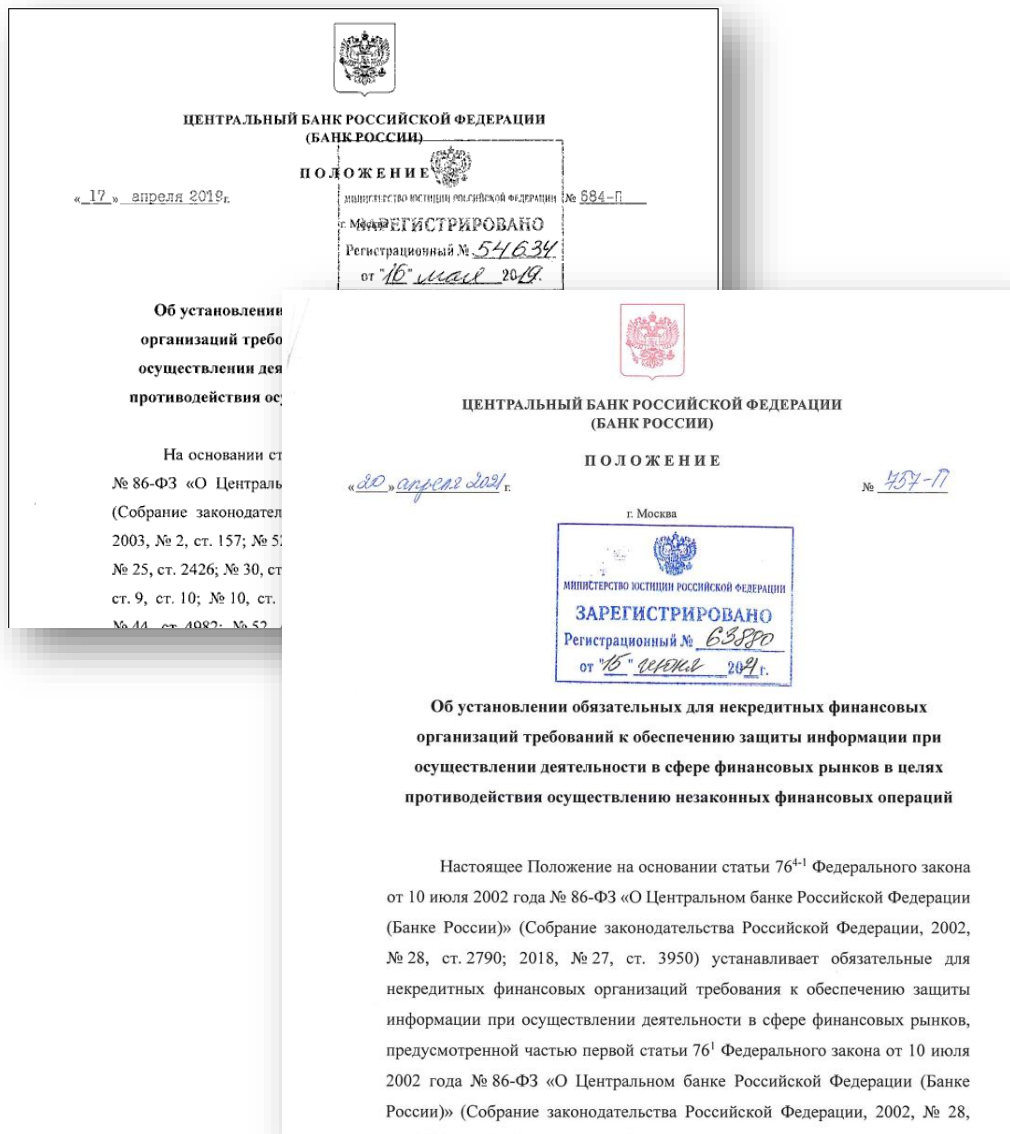
ПРАКТИЧЕСКИЕ ВОПРОСЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ПОЛОЖЕНИЯ № 757-П

ПОДГОТОВЛЕНО: Демидов С.В.
Директор департамента операционных рисков,
информационной безопасности и непрерывности
бизнеса

СТРУКТУРА ГРУППЫ «МОСКОВСКАЯ БИРЖА»



О КАКИХ ТРЕБОВАНИЯХ ИДЕТ РЕЧЬ?



- 17.04.2019 Утверждено положение Банка России №684-П;
- Часть норм Положения вступили в силу со дня опубликования, часть норм имеют отложенный срок;
- с 31.12.2019 по 1.7.2020 действовало Письмо Банка России о неприменении мер административного воздействия за нарушение п.9-11 684-П;
- 20.04.2021 Утверждено положение Банка России №757-П, взамен Положения №684-П;
- 27.04.2021 Разослано Письмо Банка России и неприменение мер административного воздействия до 31.12.2021 за нарушение Положения №684-П (?);

КЛЮЧЕВЫЕ РАЗЛИЧИЯ В 757-П?

- По сравнению с действующим 684-П происходит постепенный рост НФО подпадающих под регулирование;
- Для обеспечения целостности электронных сообщений можно использовать криптографию ГОСТ, RSA или выделенные каналы связи;
- Изменены сроки вступления в силу отложенных норм:
 - 1.07.2022 – нормативный акт должны соблюдать компании, которые соответствуют минимальному уровню защиты
 - Компании, соблюдающие усиленный и стандартный уровни, должны соответствовать:
 - с 01.01.2022 – не ниже 3го уровня соответствия;
 - с 01.07.2023 – не ниже 4го уровня соответствия;
 - 1.01.2024 – вступают отдельные требования к операторам выпускающим ЦФА;

ОСНОВНЫЕ ШАГИ

1. Определение уровня защиты и **Определение объектов на которые распространяются требования;**
2. Выполнение требований к СКЗИ (п.1.3), включая ПКЗ-2005 (**данный шаг касается всех и не является отложенной нормой**); также целесообразно проверить п.1.2, поскольку он **дает право Банку России провести проверку соблюдение норм. актов, указанных в данном пункте (ФЗ «об ЭЦП», ФЗ «о перс данных»);**
3. Выполнение требований ГОСТ 57580, в соответствии с определенным уровнем защиты (**теперь и для тех кто соблюдает минимальный уровень**);
4. Оценка соответствия ПО ОУД4 по ГОСТ 15480;
5. Реализация пунктов 1.9 – 1.10:
 - 1.9 - Целостность электронных сообщений;
 - 1.10 – Правила обработки информации (требования идентификации клиентов и сотрудников, требования к аутентификации, контроль целостности электронных сообщений, подпись сообщений);
 - 1.11 – 1.12 – Логирование, хранение информации;
 - 1.13 (**в том числе те кто соблюдает минимальный уровень защиты**) – Информирование клиентов;
 - 1.14 – 1.15 (**в том числе те кто соблюдает минимальный уровень защиты**) – Регистрация инцидентов ИБ и информирование Банка России;
6. Проведение оценки соблюдения уровня соответствия в соответствии ГОСТ 57580.2-2018;

Важно определить область применения ГОСТ 57580!

а) процесс 1 "Обеспечение защиты информации при управлении доступом":

- управление учетными записями и правами субъектов логического доступа;
- идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;
- защита информации при осуществлении физического доступа;
- идентификация, классификация и учет ресурсов и объектов доступа;

б) процесс 2 "Обеспечение защиты вычислительных сетей":

- сегментация и межсетевое экранирование вычислительных сетей;
- выявление сетевых вторжений и атак;
- защита информации, передаваемой по вычислительным сетям;
- защита беспроводных сетей;

в) процесс 3 "Контроль целостности и защищенности информационной инфраструктуры";

г) процесс 4 "Защита от вредоносного кода";

д) процесс 5 "Предотвращение утечек информации";

е) процесс 6 "Управление инцидентами защиты информации":

- мониторинг и анализ событий защиты информации;
- обнаружение инцидентов защиты информации и реагирование на них;

ж) процесс 7 "Защита среды виртуализации";

и) процесс 8 "Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств".

ТРЕБОВАНИЯ К ПО

1.8. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить использование для осуществления финансовых операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых некредитными финансовыми организациями своим клиентам для совершения действий в целях осуществления финансовых операций, а также программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), **прошедших сертификацию в системе сертификации** Федеральной службы по техническому и экспортному контролю (далее - сертификация) или **оценку соответствия по требованиям к оценочному уровню доверия (далее - ОУД) не ниже, чем ОУД 4**, в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности", утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года N 1340-ст "Об утверждении национального стандарта" (М., ФГУП "Стандартинформ", 2014) (далее - ГОСТ Р ИСО/МЭК 15408-3-2013) (далее - оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений).

...

По решению некредитной финансовой организации оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений проводится *самостоятельно или с привлечением проверяющей организации*.

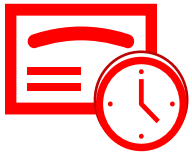


ВВ: поскольку de jure заявки клиентов участников торгов – это заявки участников торгов, можно сделать вывод, что данные требования касаются всего ПО с помощью которого выставляются заявки

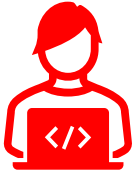
ПОЧЕМУ НЕ РАБОТАЕТ СЕРТИФИКАЦИЯ ФСТЭК?



Малое число сертификационных лабораторий;



Долгий срок проведения сертификации (около 6-12 месяцев на 1 продукт);

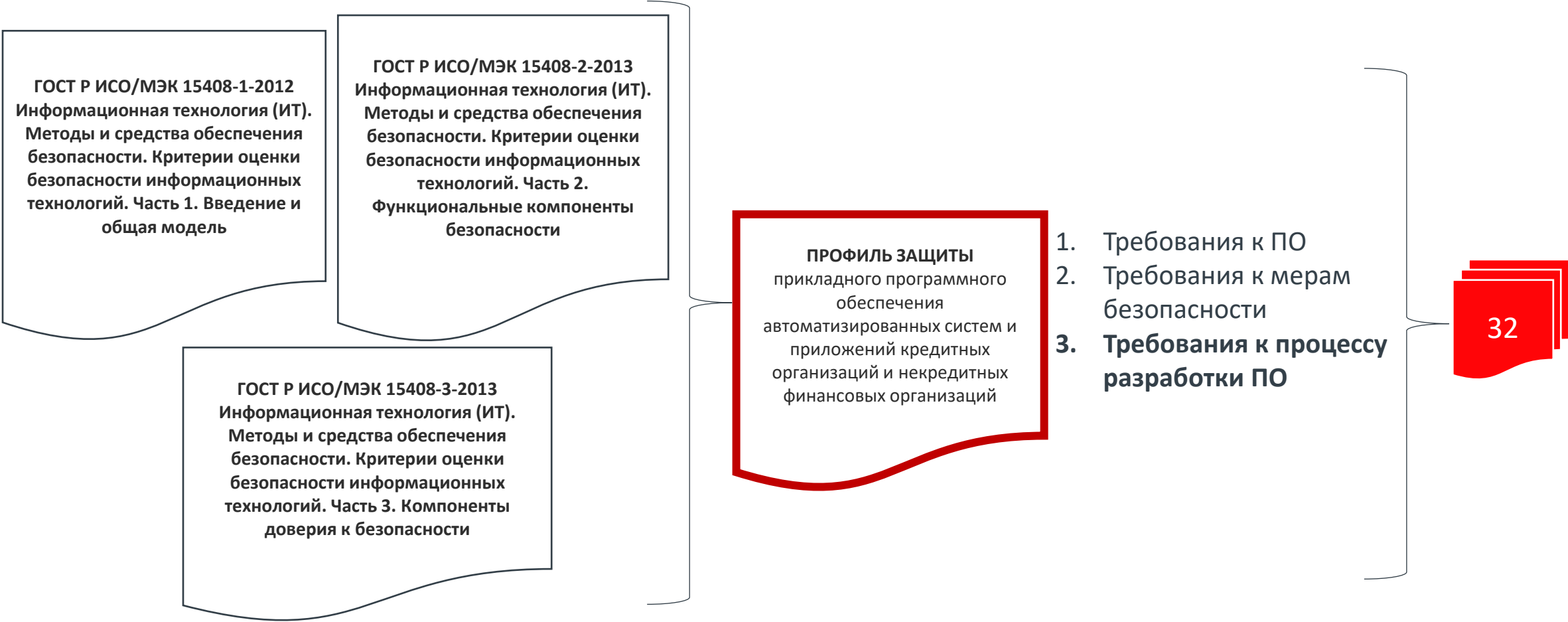


Любое изменение в ПО фактически **обнуляет** статус сертификации;



Продуктовые циклы участников торгов более динамичны.

КАК РАБОТАЕТ ГОСТ15408?



Совместимым объектом оценки для настоящего ПЗ является прикладное программное обеспечение автоматизированных систем и приложений финансовых организаций, предназначенное для функционирования на средствах вычислительной техники общего назначения (автоматизированные рабочие места, серверы), а также на мобильных устройствах (ноутбуки, смартфоны, планшеты, телефоны и иные).

СПИСОК ДОКУМЕНТОВ (ВСЕГО 32)

1. Описание архитектуры безопасности:

- Введение ЗБ,
- Справку ЗБ,
- Справку ОО,
- Аннотацию ОО,
- Описание ОО;

2. Проект ОО;

3. Описание архитектуры безопасности;

4. Полная функциональная спецификация;

5. Полное отображение представления реализации ФБО;

6. Описание реализация ОО;

7. Описание базовых модулей проекта;

8. Документацию по безопасности разработки;

9. Документацию по анализу скрытых каналов;

10. Документация выбранных опции инструментальных средств разработки (производства);

11. Результаты анализа покрытия тестами;

12. Результаты анализа глубины тестирования;

13. Тестовая документация;

14. Описание набора ресурсов, эквивалентных использованным им при функциональном тестировании ФБО;

12. Документацию по анализу скрытых каналов;

13. Документацию анализа уязвимостей разработчиком;

14. Выполнить динамический анализ кода ОО с целью выявления уязвимостей;

15. Материалы анализа влияния обновлений на безопасность ОО;

16. Определенные разработчиком сроки поддержки;

17. Полностью определенные инструментальные средства разработки;

18. Определение проблемы безопасности;

19. Определение целей безопасности;

20. Указание процедуры устранения недостатков, предназначенные для заявителей (разработчиков, производителей) ОО;

21. Руководство по устранению недостатков, предназначенное для пользователей ОО;

22. Документацию УК (Управление конфигурацией);

23. Список элементов конфигурации для ОО;

24. Процедуры поставки ОО или его частей потребителю;

25. Документацию по определению жизненного цикла.

26. Краткую спецификацию ОО;

27. Утверждения о соответствии;

28. Обоснование утверждений о соответствии;

29. Изложение «Требований безопасности»:

- описание ФТБ,
- описание ТДБ,
- все выполненные над требованиями безопасности операции;

30. Обоснование «Требований безопасности»:

- прослеживание каждого ФТБ к целям безопасности для ОО;

31. Определение расширенных компонентов;

32. Руководство пользователя по эксплуатации.

КАК РАБОТАЕТ ГОСТ15408? ЕСТЬ ЛИ СПАСЕНИЕ?

3.5 Изложение соответствия

При разработке ЗБ и (или) других ПЗ на основе настоящего ПЗ устанавливаются следующие типы соответствия: **«строгое соответствие»** – все требования настоящего ПЗ должны быть полностью удовлетворены в ЗБ, хотя при этом ЗБ может быть более широким, чем ПЗ.

Допустимой является реализация отдельных предположений, ФТБ, не влияющих на конечный уровень доверия, компенсационными и/или организационно-технологическими мерами при обязательном наличии достаточного обоснования, учитывающего технические ограничения и особенности компонент инфраструктуры и применяемых информационных технологий, а также риск-ориентированный подход организации при проведении оценки рисков нарушения информационной безопасности и особенности моделирования угроз и нарушителей.