



НАУФОР

Jet

25/03/2021

ТРЕБОВАНИЯ БАНКА РОССИИ В ОБЛАСТИ ИБ ДЛЯ **НФО**

**Павел
Новожилов**

Руководитель группы консалтинга
по информационной
безопасности

**Бакин
Александр**

Старший консультант
по информационной
безопасности



Павел Новожилов

**Руководитель группы консалтинга
по информационной безопасности**

Обладает сертификатом по проведению аудитов по требованиям СТО БР ИББС-1.0, BS ISO/IEC 27001:2013 Information security management systems Lead Auditor.

Основным направлением деятельности сейчас является приведение организаций к соответствию нормативным требованиям ИБ (ПДн, КИИ, документы Банка России и др.)

Имеет большой опыт работы выполнения проектов, включая проекты по ИБ высокой сложности в финансовой сфере.

Является полномочным представителем компании Инфосистемы Джет в подкомитете 1 «Безопасность финансовых (банковских) операций» ТК122.



Бакин Александр

**Старший консультант
по информационной безопасности**

Обладает сертификатом CIPP/E (Certified Information Privacy Professional/Europe).

Основным направлением деятельности сейчас является выполнение проектов по оценке соответствия прикладного ПО требованиям ОУД4.

Также имеет опыт выполнения сложных комплексных проектов по реализации нормативных требований в области информационной безопасности.

СОДЕРЖАНИЕ



ЧАСТЬ 1

1 | Обзор нормативных документов по информационной безопасности

2 | Положение 684-П

3 | ГОСТ 57580.1-2017
ГОСТ 57580.2-2018

ЧАСТЬ 2

4 | ОУД4 — проведение оценки соответствия прикладного программного обеспечения

5 | Вопросы-ответы

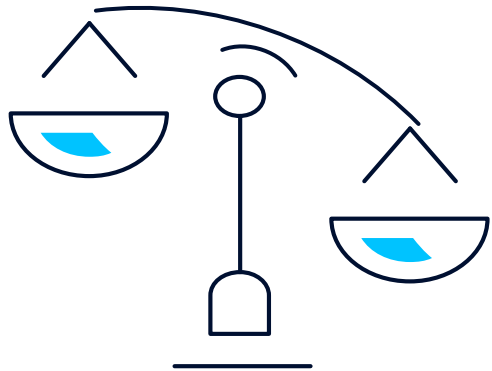


КРАТКИЙ ОБЗОР НОРМАТИВНЫХ ТРЕБОВАНИЙ ПО ИБ ДЛЯ НФО

КЛЮЧЕВЫЕ ТРЕБОВАНИЯ ПО ИБ



ШТРАФНЫЕ САНКЦИИ ЗА НЕВЫПОЛНЕНИЕ ТРЕБОВАНИЙ БАНКА РОССИИ



- **Требование об устранении** выявленных нарушений
- **Денежный штраф** в размере до 1 процента размера оплаченного уставного капитала, но не более 1 процента минимального размера уставного капитала
- **Запрет на осуществление финансовых операций**, предусмотренных выданной лицензией на срок до 1 года
- **Запрет на открытие филиалов** на срок до 1 года
- **Отзыв лицензии** на осуществление финансовых операций (неоднократные нарушения требований Банка России в течение 1 года)



ПОЛОЖЕНИЕ 684-П

НА ЧТО РАСПРОСТРАНЯЕТСЯ ПОЛОЖЕНИЕ 684-П?



Информация, содержащая в документах при осуществлении финансовых операций работниками и (или) клиентами



Информация об осуществлённых финансовых операциях



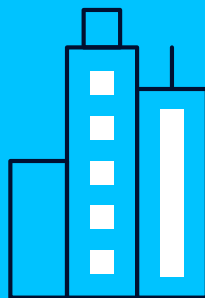
Информация, необходимая для авторизации клиентов



Ключевая информация СКЗИ



КТО ДОЛЖЕН ВЫПОЛНЯТЬ ПОЛОЖЕНИЕ 684-П?



- Центральный контрагент
- Центральный депозитарий
- Депозитарии
- Клиринговые организации
- Организаторы торговли
- Страховые организации
- Негосударственные пенсионные фонды

- **Брокеры**
- Дилеры
- Регистраторы
- **Управляющие компании**
- Бюро кредитных историй
- Кредитные рейтинговые агентства
- Другие в соответствии с статьей 76.1 Федерального закона №86-ФЗ «О Центральном банке РФ»

СТРУКТУРА ДОКУМЕНТА ПОЛОЖЕНИЯ 684-П



Требования к СКЗИ



**Требования
к уровням защиты**



**Требования к оценке
соответствия**



**Технологические
меры защиты**

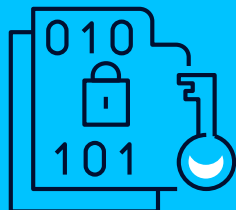


**Требования к управлению
инцидентами ИБ**



Оценка соответствия
прикладного ПО требованиям
по безопасности

ТРЕБОВАНИЕ К СКЗИ



Выполнение требований,
установленных в документах ФСБ
(ПКЗ-20056 Приказ №378»)



Выполнение требований,
установленных в эксплуатационной
документации СКЗИ

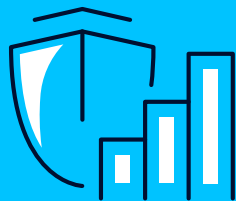


Выполнение требований,
установленных ФЗ-63
«Об электронной подписи»



Если применяются СКЗИ российского
производства, то такие СКЗИ должны
быть сертифицированы ФСБ

ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИТЫ (1/2)



Текущая редакция
Положения 684-П

1 Усиленный уровень защиты

Центральный контрагент,
Центральный депозитарий

2 Стандартный уровень защиты

- Брокеры, которые заключили сделки в объеме 100 000 миллионов или брокерское обслуживание более 100 000 лиц*
- Дилеры заключили за свой счет на торгах в объеме 200 000 миллионов*
- Управляющие компании в объеме 20 000 миллионов или брокерское обслуживание более 2 000 лиц, с которыми заключены договоры доверительного управления*
- др.

3 Минимальный уровень защиты

Данный уровень не применим к НФО

ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИТЫ (2/2)



1

Усиленный уровень защиты ▼

Регистраторы финансовых осуществляли оказание услуг более чем 2 миллионам лиц

Планируемые изменения
в Положении 684-П (в финальной
редакции могут быть изменения)

2

Стандартный уровень защиты ►

3

Минимальный уровень защиты ►

ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИТЫ (2/2)



1 Усиленный уровень защиты

2 Стандартный уровень защиты

Брокеры, дилеры, управляющие, определившие хотя бы по одному из показателей деятельности из перечисленных ниже*:

Название показателя	Параметр
Объем сделок купли-продажи ценных бумаг за счет клиентов	Более 100 000 млн. руб
Количество клиентов по договорам на брокерское обслуживание	Более 100 000 лиц
Объем сделок купли-продажи ценных бумаг, заключенных за свой счет на организованных торгах	Более 200 000 млн. рублей
Объем сделок купли-продажи ценных бумаг, заключенных при осуществлении деятельности по управлению ценными бумагами	Более 200 000 млн. рублей
Количество клиентов по договорам доверительного управления	Более 2000 лиц

3 Минимальный уровень защиты

Планируемые изменения в Положении 684-П (в финальной редакции могут быть изменения)

ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИТЫ (2/2)



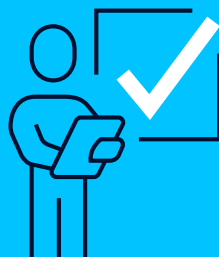
1 Усиленный уровень защиты ▼

Планируемые изменения
в Положении 684-П (в финальной
редакции могут быть изменения)

2 Стандартный уровень защиты ►

3 Минимальный уровень защиты ▼

- Брокеры, дилеры и управляющие компании, которые не реализуют второй уровень защиты
- Управляющие компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов



ТЕРМИНОЛОГИЯ:

Оценка соответствия – проверка соблюдения установленных мер защиты, в рамках которой выполняются:

- анализ документации
- проверка конфигураций средств защиты
- проведение интервью с работниками организации

По результатам оценки соответствия определяются требования, которые выполняются в неполном объеме или в целом не выполняются.

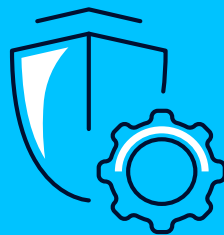
С 1 января 2022 года необходимо выполнять следующие требования к оценке соответствия (для второго уровня защиты):

- Оценка соответствия должна проводиться сторонней компанией, имеющей лицензию ФСТЭК на проведение работ и услуг по технической защите конфиденциальной информации, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации
- Оценка соответствия проводится **не реже одного раза в три года**

ТЕХНОЛОГИЧЕСКИЕ МЕРЫ ЗАЩИТЫ (1/3)



Данный блок требований относится для организаций, реализующих второй уровень защиты



Технологические процессы

- Подключение клиента к личному кабинету
- Формирование электронных сообщений при осуществлении финансовых операций клиентом
- Формирование электронных сообщений при осуществлении финансовых операций работником
- Другие

Технологические участки

Идентификация, аутентификация и авторизация своих клиентов при совершении финансовых операций

Идентификация, аутентификация и авторизация своих клиентов

При формировании (подготовке), передаче и приеме электронных сообщений

Учет результатов осуществления финансовых операций

Удостоверение права клиентов распоряжаться денежными средствами, ценными бумагами

Хранение электронных сообщений и информации об осуществленных операциях

Осуществление финансовых операций

ТЕХНОЛОГИЧЕСКИЕ МЕРЫ ЗАЩИТЫ (2/3)

СТАНДАРТНЫЙ УРОВЕНЬ ЗАЩИТЫ



Идентификация, аутентификация и авторизация своих клиентов при совершении финансовых операций



- Если используется ЕБС, то необходимо выполнять требования Приказа ФСТЭК №21, Приказа ФСБ №378
- Если используется ЕСИА, то необходимо выполнять требования Приказа Министерства цифрового развития, связи и массовых коммуникаций № 210

При формировании (подготовке), передаче и приеме электронных сообщений



- Двойной контроль
- Структурный контроль электронных сообщений
- Защита защищаемой информации при ее передаче
- Контроль дублирования электронных сообщений
- проверку правильности заполнения полей электронного сообщения и прав владельца электронной подписи (входной контроль)

Удостоверение права клиентов распоряжаться денежными средствами, ценными бумагами

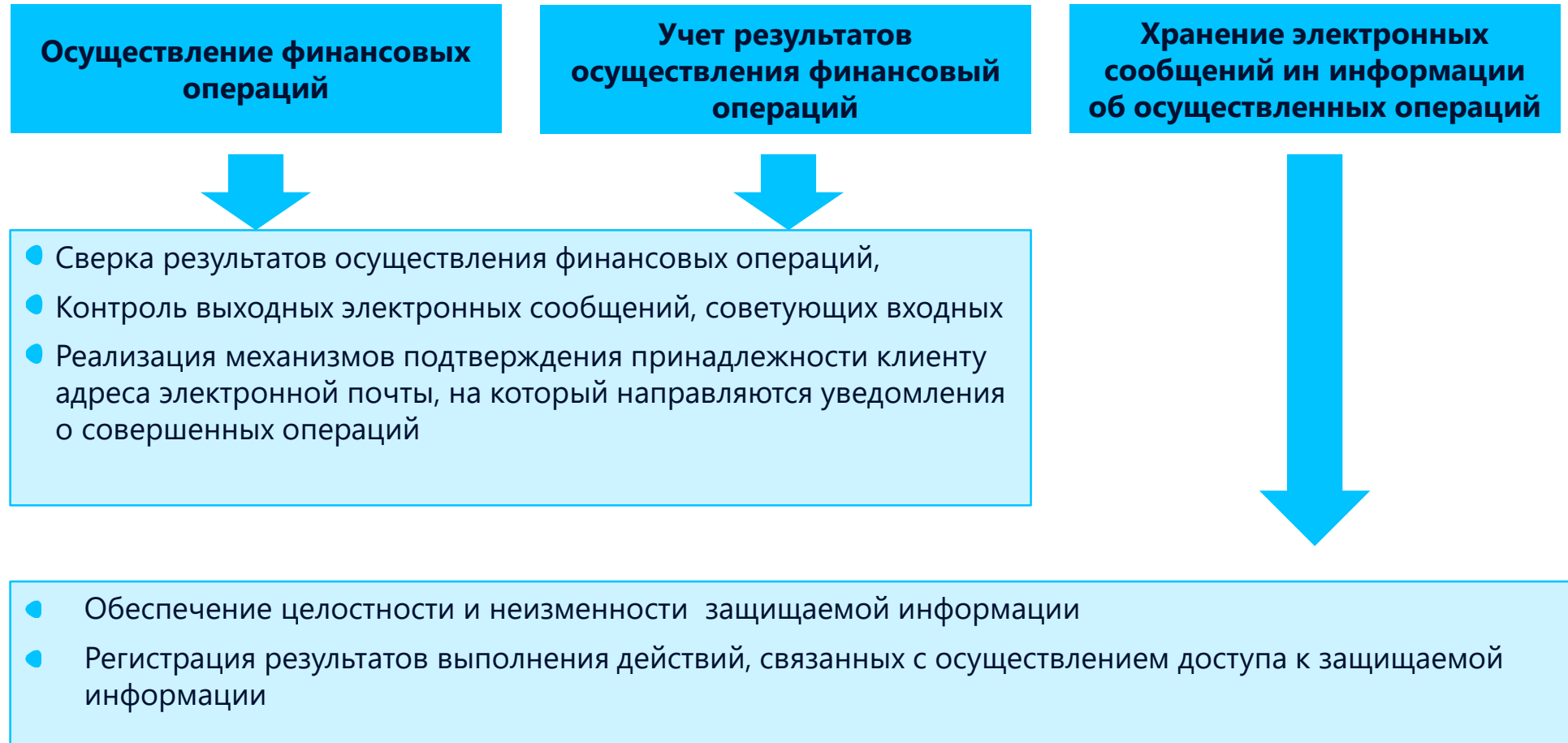


- Подписание электронных сообщений клиента
- Получение от клиента подтверждения совершенной финансовой операции

- Обеспечение целостности и неизменности защищаемой информации
- Регистрация результатов выполнения действий, связанных с осуществлением доступа к защищаемой информации

ТЕХНОЛОГИЧЕСКИЕ МЕРЫ ЗАЩИТЫ (3/3)

СТАНДАРТНЫЙ УРОВЕНЬ ЗАЩИТЫ



ТРЕБОВАНИЯ К УПРАВЛЕНИЮ ИНЦИДЕНТАМИ ИБ



- Регистрация выявленных инцидентов ИБ, в том числе операций без согласия клиента
- Предоставление информации о выявленных инцидентах ИБ в подразделение организации, ответственное за управление рисками
- Направление информации об инцидентах ИБ в ФинЦЕРТ, в том числе информации о планируемых мероприятиях, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах в сети «Интернет», в отношении инцидентов ИБ
- Обеспечение целостности и доступности информации об инцидентах ИБ в течение не менее чем пяти лет с момента обнаружения (для организаций, реализующих **второй уровень защиты**)

РЕЗЮМЕ ПО ПОЛОЖЕНИЮ 684-П



Планируются изменения документа Положения 684-П, в том числе которые касаются **брокерских и управляющих компаний**



С 1 января 2022 года для организаций, реализующий второй уровень защиты, необходимо проводить внешнюю оценку соответствия **не реже одного раза в три года**



Для второго уровня защиты должно проводиться ежегодное тестирование на проникновение



Каждый год необходимо пересматривать уровень защиты



ГОСТ 57580.1-2017, ГОСТ 57580.2-2018

ОТЛИЧИЕ МЕЖДУ ПЕРВОЙ И ВТОРОЙ ЧАСТЬЮ ГОСТ



ГОСТ 57580.1-2017

- Набор организационных и технических мер защиты

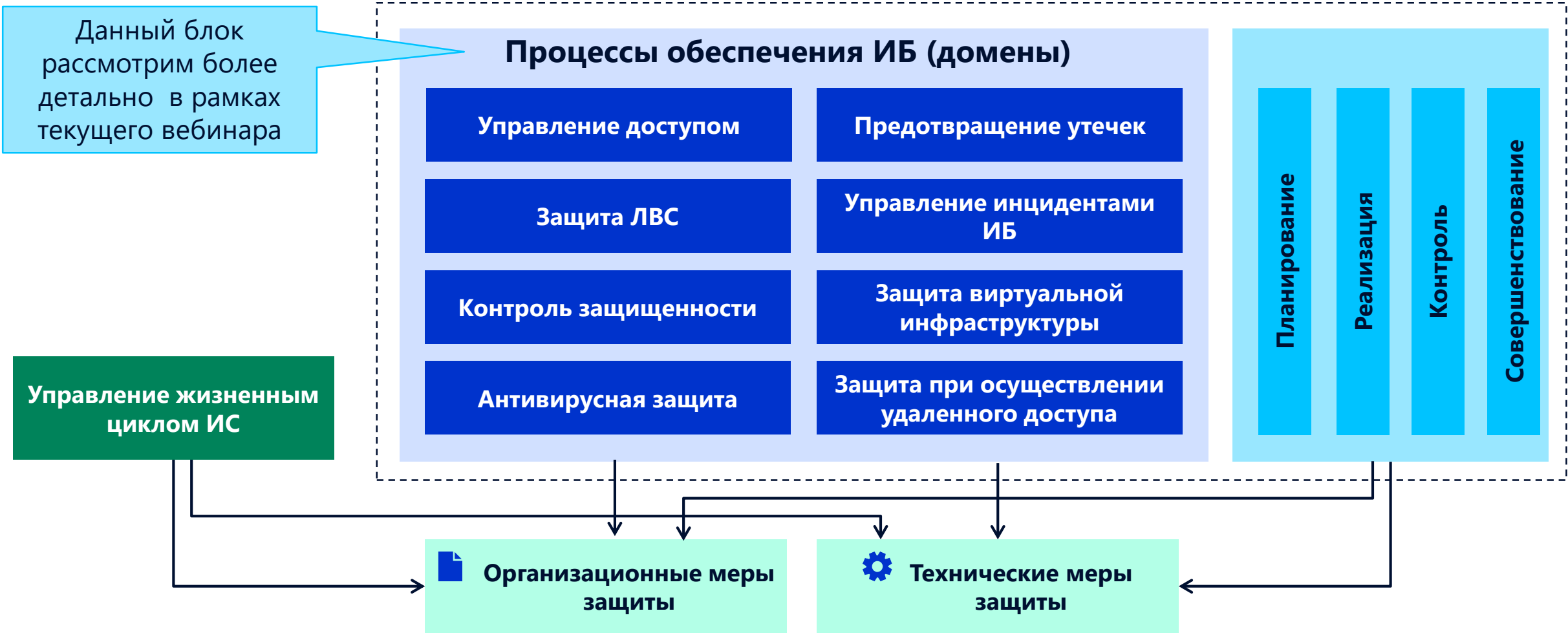
ГОСТ 57580.2-2018

- Методика расчета организационных и технических мер защиты
- Требования к оформлению отчетной документации

СТРУКТУРА ГОСТ 57580.1-2017



Данный блок рассмотрим более детально в рамках текущего вебинара



УПРАВЛЕНИЕ ДОСТУПОМ



**Второй
уровень защиты**

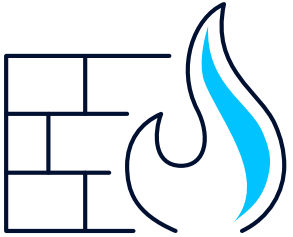
83
меры
защиты

**Третий
уровень защиты**

61
мера
защиты

- ⚙️ Наличие двухфакторной аутентификации для администраторов, подразделения ИБ
- ⚙️ Документирование правил предоставления физического доступа
- ⚙️ Учет объектов доступа
- 📄 Документально определенный порядок управления доступом
- 📄 Документирование требований по парольной политике
- ⚙️ Регистрация действия пользователей, администраторов
- 📄 Учет объектов доступа
- ⚙️ Применение мер по физической безопасности

ЗАЩИТА ЛВС



**Второй
уровень защиты**

35
мер
защиты

- ⚙ системы IPS\IDS
- ⚙ Сегментирование ЛВС
- ⚙ Защита от DDoS-атак

**Третий
уровень защиты**

13
мер
защиты

- ⚙ Межсетевое экранирование
- ⚙ Использование СКЗИ для шифрования защищаемой информации
- ⚙ Защита от SPAM

КОНТРОЛЬ ЗАЩИЩЕННОСТИ



**Второй
уровень защиты**

29
мер
защиты

- ⚙️ Наличие системы анализа защищенности (инструментальный сканер анализа защищенности, Compliance check)
- ⚙️ Установка обновлений безопасности
- ⚙️ Контроль установленного ПО на АРМ и серверах техническими мерами
- 📄 Документирование процесса управления уязвимостями

**Третий
уровень защиты**

14
мер
защиты

- 📄 Организационные меры по проверки на наличие уязвимостей
- 📄 Контроль установленного ПО на АРМ и серверах организационными мерами

АНТИВИРУСНАЯ ЗАЩИТА



**Второй
уровень защиты**

27
мер
защиты

**Третий
уровень защиты**

21
мера
защиты

- ⚙ Использование модуля антивирусной защиты на уровне межсетевого экранирования. При этом производитель должен отличаться от производителей антивирусных на АРМ и серверов
- ⚙ Установка антивирусных средств защиты на АРМ пользователей, в ОС на серверах, на уровне гипервизора системы виртуализации
- ⚙ Использование различных производителей антивирусных средств защиты на уровне АРМ, серверов
- ⚙ Возможность использования компенсирующих мер защиты

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК



**Второй
уровень защиты**

28
мер
защиты

- ⚙️ Внедрение DLP-системы
- ⚙️ Контроль использования съемных носителей
- ⚙️ Безопасность почтовой системы (при использовании для обработки защищаемой информации)
- ⚙️ Контроль подключения к сети Интернет

**Минимальный
уровень защиты**

6
мер
защиты

- 📄 Учет схемных носителей
- 📄 Маркировка съемных носителей
- 📄 ⚙️ Уничтожение защищаемой информации

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ



**Второй
уровень защиты**

38
мер
защиты

- ⚙ Использование SIEM-системы или подключение к сторонней организации, которая будет выполнять мониторинг
- 📄 Определение группы реагирования на инциденты ИБ

**Третий
уровень защиты**

24
меры
защиты

- ⚙ Мониторинг данных регистрации о событиях защиты информации
- 📄 Регламентация процесса управления инцидентами ИБ

ЗАЩИТА СРЕДЫ ВИРТУАЛИЗАЦИИ



**Стандартный
уровень защиты**

30
мер
защиты

- 📄 ⚙️ Наличие требований к VDI-инфраструктуре (при наличии)
- 📄 ⚙️ Защита среды контейнеризации
- 📄 ⚙️ Меры защиты применимы в целом из других доменов

**Третий
уровень защиты**

15
мер
защиты

- ⚙️ Регистрация действий администраторов
- 📄 Определение документальных требований к защите виртуализации

ЗАЩИТА УДАЛЕННОГО ДОСТУПА



**Второй
уровень защиты**

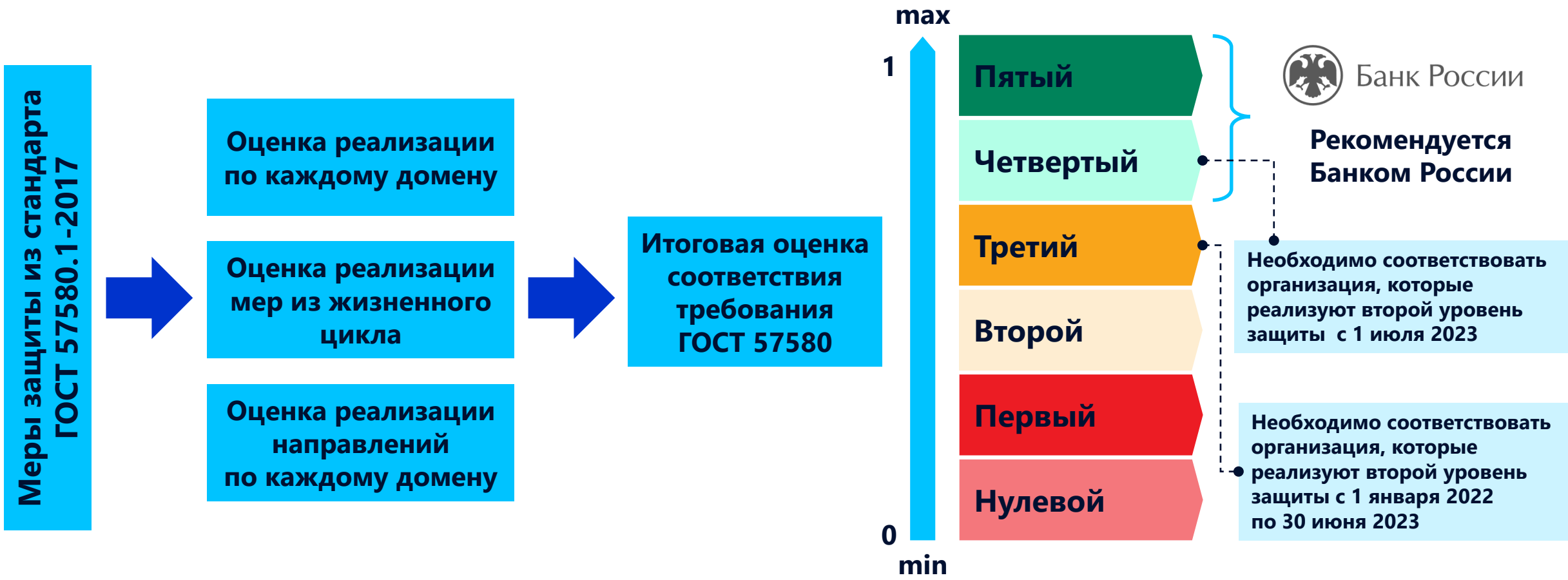
12
мер
защиты

**Третий
уровень защиты**

6
мер
защиты

- ⚙ Шифрование данных на корпоративных мобильных устройствах (за пределами организации)
- ⚙ Использование MDM системы для корпоративных мобильных устройств
- 📄 Регламентация удаленного доступа
- ⚙ Использование двухфакторной аутентификации для доступа к ЛВС

ОПРЕДЕЛЕНИЕ ИТОГОВОГО УРОВНЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ГОСТ 57580



РЕЗЮМЕ ПО ГОСТ 57580



ГОСТ 57580.1-2017 – «краеугольный камень» нормативных Банка России в области ИБ



По результатам оценки соответствия оформляются протоколы и листы наблюдений по установленной форме. Протоколы по результатам оценки соответствия подписываются работники, входящей в рабочую группу аудитов, и работника проверяемой организации



Необходим достаточно большой набор средств защиты (для усиленного и стандартного уровня защиты)



Остается не так много времени до реализации необходимых организационных и технических мер защиты для соответствия рекомендуемого четвертому уровню

СПРАВОЧНЫЙ МАТЕРИАЛ КЛЮЧЕВЫХ МЕР ЗАЩИТЫ



Второй уровень защиты		Третий уровень защиты	
Организационные меры защиты	Технические меры защиты	Организационные меры защиты	Технические меры защиты
Документированный порядок доступа, в том числе удаленного доступа	Двухфакторная аутентификация администраторов	Документированный порядок доступа, в том числе удаленного доступа	Двухфакторная аутентификация для удаленного доступа
Документированный порядок по физической безопасности	Межсетевые экраны	Документально определенные требования к парольной политике	Межсетевой экран
Настройка параметров регистрации событий пользователей, администраторов	Система IPS\IDS	Настройка параметров регистрации событий пользователей, администраторов	Антивирусные средства защиты разных производителей на АРМ и серверах
Документально определенные требования к парольной политике	Инструментальный сканер анализа защищенности, включая автоматизированную проверку параметров безопасности в инфраструктуре	Документальный порядок по управлению инцидентами ИБ	СКЗИ
Документальный порядок по управлению инцидентами ИБ	DLP-система	Учет, маркировка съемных носителей	Защита от SPAM

СПРАВОЧНЫЙ МАТЕРИАЛ КЛЮЧЕВЫХ МЕР ЗАЩИТЫ

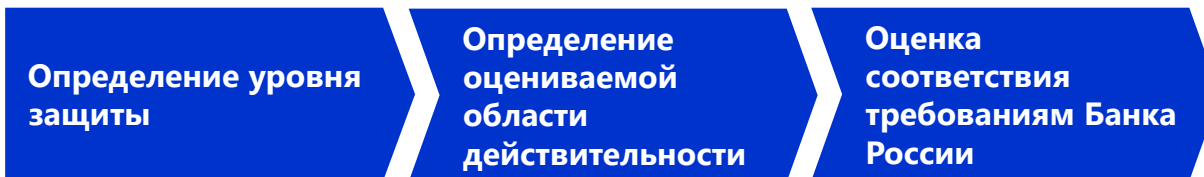


Второй уровень защиты		Третий уровень защиты	
Организационные меры защиты	Технические меры защиты	Организационные меры защиты	Технические меры защиты
Создание группы реагирования на инциденты ИБ	Шифрование данных на корпоративных ноутбуках	Документальный порядок по уничтожению защищаемой информации	
Учет, маркировка съемных носителей	Антивирусные средства защиты разных производителей на АРМ и серверах	Повышение осведомленности в области ИБ	
Документальный порядок по уничтожению защищаемой информации	СКЗИ	Разработка планов по совершенствованию системы ИБ	
Повышение осведомленности в области ИБ	SIEM-система	Назначение ответственного специалиста за ИБ	
Разработка планов по совершенствованию системы ИБ	MDM-система (при использовании корпоративных мобильных устройств)		
Назначение ответственного специалиста за ИБ	Защита от DDoS-атак		

С ЧЕГО СТОИТ НАЧАТЬ?

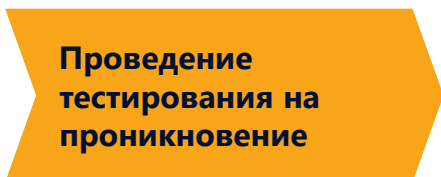
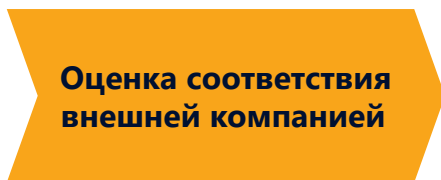


1 Подготовительный этап



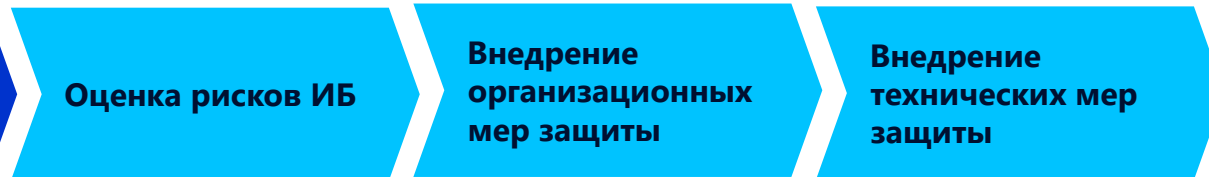
— Положение 684-П
— ГОСТ 57580.1-2017,
ГОСТ 57580.2-2018

3 Подтверждение реализации необходимых требований



Третий этап для брокерских организаций и управляющих компаний, реализующих стандартный уровень защиты

2 Внедрение организационных и технических мер защиты



— Актуализация необходимой документации по требованиям
— Разработка компенсирующих мер защиты
— Внедрение процессов по разработанным документам

ПОЛОЖЕНИЕ 684-П



Требования к СКЗИ



**Требования
к уровням защиты**



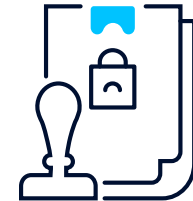
**Требования к оценке
соответствия**



**Технологические
меры защиты**



**Требования к управлению
инцидентами ИБ**



Оценка соответствия
прикладного ПО требованиям
по безопасности



ОЦЕНКА СООТВЕТСТВИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ (ОУД 4)

ОБЗОР СУЩЕСТВУЮЩИХ И ПЕРСПЕКТИВНЫХ РЕГУЛЯТОРНЫХ ТРЕБОВАНИЙ ДЛЯ НФО



684-П

НФО, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить использование для осуществления финансовых операций **прикладного ПО АС и приложений**, распространяемых некредитной финансовой организацией своим клиентам для совершения действий в целях осуществления финансовых операций, а также ПО, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в АС и приложениях с использованием информационно-телекоммуникационной сети «Интернет», сертифицированных в системе сертификации ФСТЭК на соответствие требованиям по безопасности информации, в том числе на наличие уязвимостей или недеklarированных возможностей, или **в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4**, предусмотренного пунктом 7.6 ГОСТ Р ИСО/МЭК 15408-3-2013

ГОСТ Р 57580.1-2017

ЖЦ.8: **Применение прикладного ПО АС**, сертифицированного на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недеklarированных возможностей, в соответствии с законодательством РФ или **в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4** в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3

Проект положения,
отменяющего
684-П

НФО, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить использование для осуществления финансовых операций **прикладного ПО АС и приложений**, распространяемых некредитной финансовой организацией своим клиентам для совершения действий в целях осуществления финансовых операций, а также ПО, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в АС и приложениях с использованием информационно-телекоммуникационной сети «Интернет», **прошедших** сертификацию в системе сертификации ФСТЭК или **оценку соответствия по требованиям к оценочному уровню доверия** не ниже чем ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3- 2013

ЧТО ТАКОЕ ОУД?



**Функциональные
требования
безопасности**



**Требования
доверия
к безопасности**

могут выдвигаться
на основе профиля защиты

могут составлять ОУД
или ОУД с усилениями (ОУД+)

Последовательность действий в соответствии с фреймворком:

- I. Разработать документацию
- II. Обеспечить практическое применение документов
- III. В ходе тестов подтвердить, что установленные на уровне документации и политик требования выполняются

ТРЕБОВАНИЯ ДОВЕРИЯ ПРОФИЛЯ ЗАЩИТЫ ЦБ РФ



Класс доверия	Семейство доверия	ОУД4	ОУД4+ ПЗ ЦБ	Наименование компонента доверия
Разработка	ADV_ARC	1	1	Описание архитектуры безопасности
	ADV_FSP	4	4	Полная функциональная спецификация
	ADV_IMP	1	2	Представления реализации ФБО
	ADV_IMP_EXT		3	Реализация ОО
	ADV_TDS	3	3	Базовый модульный проект
Руководства	AGD_OPE	1	1	Руководство пользователя по эксплуатации
	AGD_PRE	1	1	Подготовительные процедуры
Поддержка жизненного цикла	ALC_CMC	4	4	Поддержка генерации, процедуры приемки и автоматизация
	ALC_CMS	4	4	Охват УК отслеживания проблем
	ALC_DEL	1	1	Процедуры поставки
	ALC_DVS	1	1	Идентификация мер безопасности
	ALC_FLR		2	Процедуры сообщений о недостатках
	ALC_FPU_EXT		1	Процедуры обновления программного обеспечения
	ALC_LCD	1	1	Определенная заявителем модель жизненного цикла
	ALC_LCD_EXT		3	Определенные разработчиком сроки поддержки
	ALC_TAT	1	2	Полностью определенные инструментальные средства разработки
Оценка задания по безопасности	ASE_CCL	1	1	Утверждения о соответствии
	ASE_ECD	1	1	Определение расширенных компонентов
	ASE_INT	1	1	Введение ЗБ
	ASE_OBJ	2	2	Цели безопасности
	ASE_REQ	2	2	Производные требования безопасности
	ASE_SPD	1	1	Определение проблемы безопасности
	ASE_TSS	1	1	Краткая спецификация объекта оценки
Тестирование	ATE_COV	2	2	Анализ покрытия
	ATE_DPT	2	3	Тестирование: модули обеспечения безопасности
	ATE_FUN	1	1	Функциональное тестирование
	ATE_IND	2	2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_VAN	3	5	Анализ уязвимостей
	AVA_CCA_EXT		1	Анализ скрытых каналов
Обновление ОО	AMA_SIA_EXT		3	Анализ влияния обновлений на безопасность ОО

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

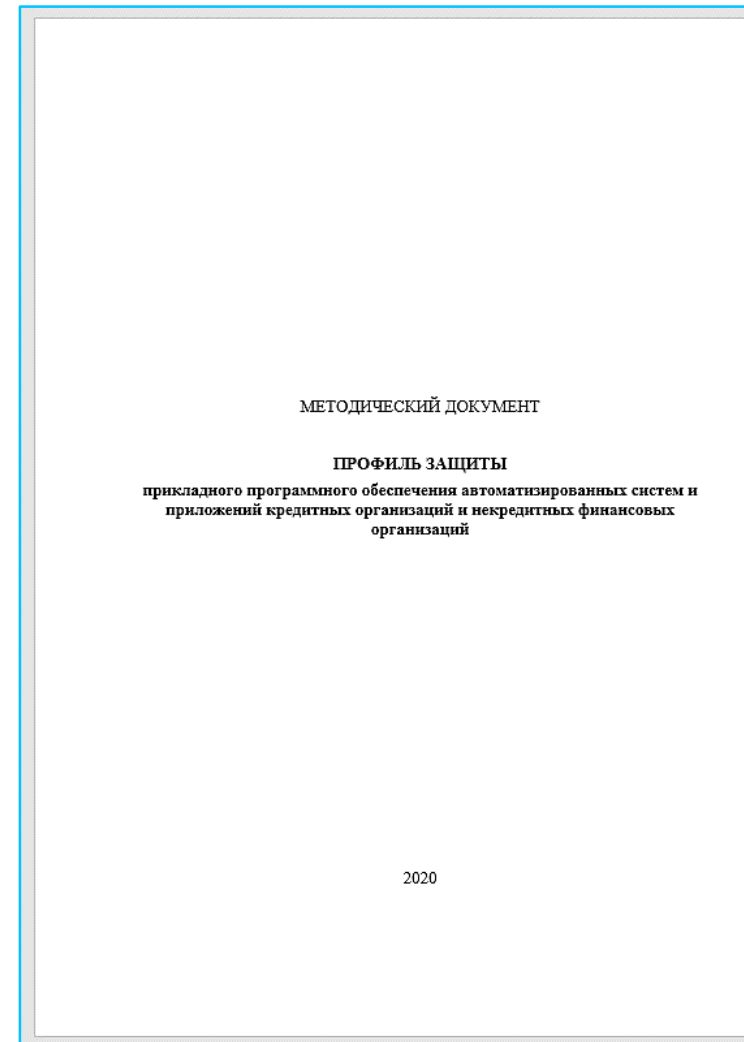
ПРОФИЛЬ ЗАЩИТЫ
прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций

2020

ТРЕБОВАНИЯ ДОВЕРИЯ ПРОФИЛЯ ЗАЩИТЫ ЦБ РФ



Класс доверия	Семейство доверия	ОУД4	ОУД4+ ПЗ ЦБ	Наименование компонента доверия
Разработка	ADV_ARC	1	1	Описание архитектуры безопасности
	ADV_FSP	4	4	Полная функциональная спецификация
	ADV_IMP	1	2	Представления реализации ФБО
	ADV_IMP_EXT		3	Реализация ОО
	ADV_TDS	3	3	Базовый модульный проект
Руководства	AGD_OPE	1	1	Руководство пользователя по эксплуатации
	AGD_PRE	1	1	Подготовительные процедуры
Поддержка жизненного цикла	ALC_CMC	4	4	Поддержка генерации, процедуры приемки и автоматизация
	ALC_CMS	4	4	Охват УК отслеживания проблем
	ALC_DEL	1	1	Процедуры поставки
	ALC_DVS	1	1	Идентификация мер безопасности
	ALC_FLR		2	Процедуры сообщений о недостатках
	ALC_FPU_EXT		1	Процедуры обновления программного обеспечения
	ALC_LCD	1	1	Определенная заявителем модель жизненного цикла
	ALC_LCD_EXT		3	Определенные разработчиком сроки поддержки
	ALC_TAT	1	2	Полностью определенные инструментальные средства разработки
Оценка задания по безопасности	ASE_CCL	1	1	Утверждения о соответствии
	ASE_ECD	1	1	Определение расширенных компонентов
	ASE_INT	1	1	Введение ЗБ
	ASE_OBJ	2	2	Цели безопасности
	ASE_REQ	2	2	Производные требования безопасности
	ASE_SPD	1	1	Определение проблемы безопасности
	ASE_TSS	1	1	Краткая спецификация объекта оценки
Тестирование	ATE_COV	2	2	Анализ покрытия
	ATE_DPT	2	3	Тестирование: модули обеспечения безопасности
	ATE_FUN	1	1	Функциональное тестирование
	ATE_IND	2	2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_VAN	3	5	Анализ уязвимостей
	AVA_CCA_EXT		1	Анализ скрытых каналов
Обновление ОО	AMA_SIA_EXT		3	Анализ влияния обновлений на безопасность ОО



ТРЕБОВАНИЯ ДОВЕРИЯ ПРОФИЛЯ ЗАЩИТЫ ЦБ РФ



Класс доверия	Семейство доверия	ОУД4	ОУД4+ ПЗ ЦБ	Наименование компонента доверия
Разработка	ADV_ARC	1	1	Описание архитектуры безопасности
	ADV_FSP	4	4	Полная функциональная спецификация
	ADV_IMP	1	2	Представления реализации ФБО
	ADV_IMP_EXT		3	Реализация ОО
	ADV_TDS	3	3	Базовый модульный проект
Руководства	AGD_OPE	1	1	Руководство пользователя по эксплуатации
	AGD_PRE	1	1	Подготовительные процедуры
Поддержка жизненного цикла	ALC_CMC	4	4	Поддержка генерации, процедуры приемки и автоматизация
	ALC_CMS	4	4	Охват УК отслеживания проблем
	ALC_DEL	1	1	Процедуры поставки
	ALC_DVS	1	1	Идентификация мер безопасности
	ALC_FLR		2	Процедуры сообщений о недостатках
	ALC_FPU_EXT		1	Процедуры обновления программного обеспечения
	ALC_LCD	1	1	Определенная заявителем модель жизненного цикла
	ALC_LCD_EXT		3	Определенные разработчиком сроки поддержки
Оценка задания по безопасности	ALC_TAT	1	2	Полностью определенные инструментальные средства разработки
	ASE_CCL	1	1	Утверждения о соответствии
	ASE_ECD	1	1	Определение расширенных компонентов
	ASE_INT	1	1	Введение ЗБ
	ASE_OBJ	2	2	Цели безопасности
	ASE_REQ	2	2	Производные требования безопасности
	ASE_SPD	1	1	Определение проблемы безопасности
Тестирование	ASE_TSS	1	1	Краткая спецификация объекта оценки
	ATE_COV	2	2	Анализ покрытия
	ATE_DPT	2	3	Тестирование: модули обеспечения безопасности
	ATE_FUN	1	1	Функциональное тестирование
	ATE_IND	2	2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_VAN	3	5	Анализ уязвимостей
	AVA_CCA_EXT		1	Анализ скрытых каналов
Обновление ОО	AMA_SIA_EXT		3	Анализ влияния обновлений на безопасность ОО



ОПРЕДЕЛЕНИЕ ОБЛАСТИ ОЦЕНКИ СООТВЕТСТВИЯ



ПО распространяемое некредитной финансовой организацией своим клиентам для совершения действий в целях осуществления финансовых операций, а также ПО, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложения с использованием Интернет



ПО распространяется клиентам организации (физическим или юридическим лицам)

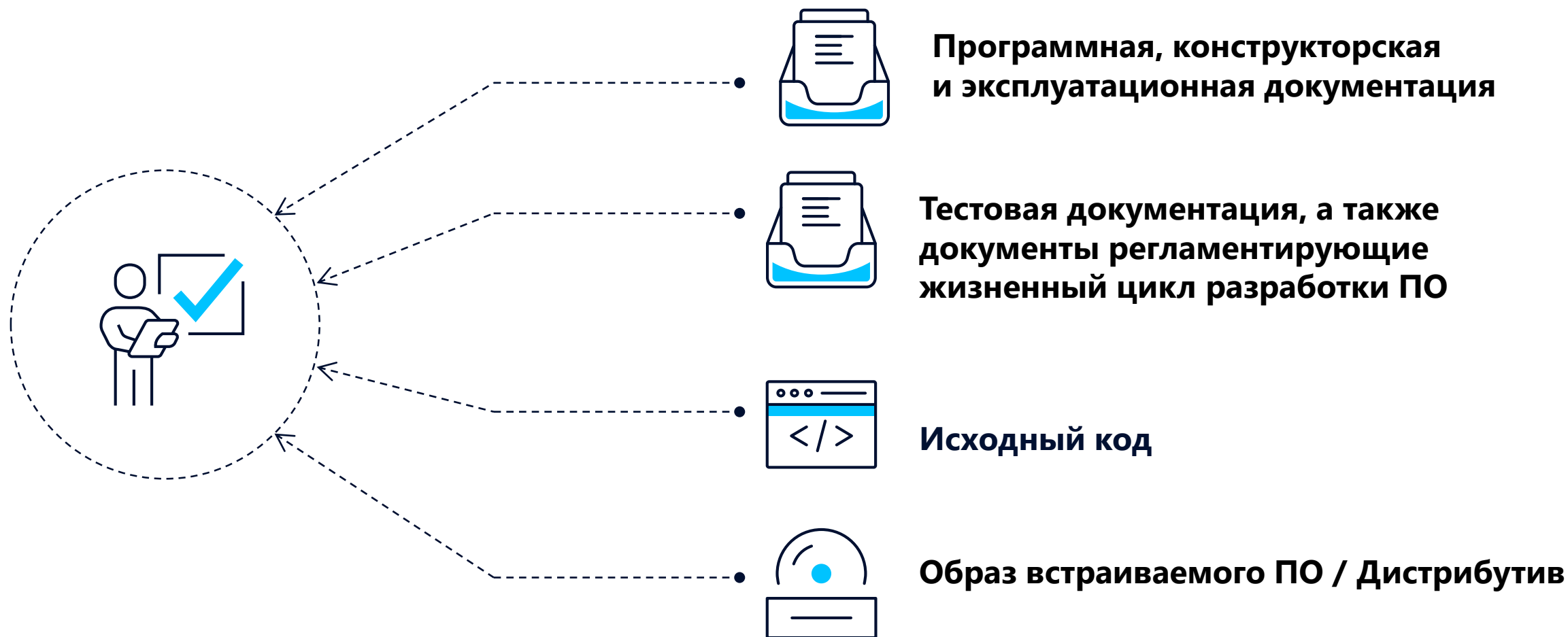


ПО доступно через Интернет неограниченному кругу лиц (а не закрыто VPN или иными ограничителями)

ПРОБЛЕМАТИКА



ИСХОДНЫЕ ДАННЫЕ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ



НЕОБХОДИМАЯ ДОКУМЕНТАЦИЯ ДЛЯ АНАЛИЗА УЯЗВИМОСТЕЙ



Функциональная спецификация

Описание функций безопасности и интерфейсов, реализующих функциональные возможности безопасности ПО, возможных сообщений об ошибках или при вызове каждого интерфейса функций безопасности



Базовый модульный проект

Описание ПО на уровне подсистем, модулей, подсистем и модулей реализующих функциональные возможности безопасности ПО, их взаимодействия



Описание архитектуры безопасности

Обоснования безопасности процесса инициализации объекта оценки, обеспечения собственной защиты объекта оценки от НСД, невозможности обхода функций безопасности объекта оценки



Эксплуатационная документация

- Инструкция администратора, содержащая описание действий по установке, настройке и действий по реализации функций безопасности среды функционирования
- Инструкция пользователя

ДОПОЛНИТЕЛЬНАЯ ДОКУМЕНТАЦИЯ ДЛЯ ПРОВЕДЕНИЯ ОЦЕНКИ СООТВЕТСТВИЯ



Задание по безопасности

Излагаются потребности в безопасности



Документация на средства, применяемые для разработки

Описание средств, применяемых для разработки, с детализацией использованных опций таких средств



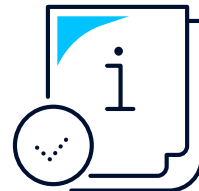
Документация по управлению конфигурацией

Порядок управления изменения ПО и документации, описание методов уникальной идентификации элементов конфигурации и их идентификаторов



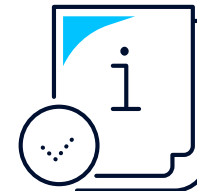
Тестовая документация

Тестовая спецификация, покрывающая все функциональные возможности ПО, а также протоколы тестирования



Документация анализа скрытых каналов

Документ, в котором идентифицированы скрытые каналы и содержится оценка их пропускной способности



Документация по безопасной разработке

Описание всех физических, процедурных, организационных и других мер безопасности, применяемых в среде разработки, направленные на снижение вероятности возникновения уязвимостей и иных недостатков, а также применяемых для защиты конфиденциальности и целостности проектной документации и реализации ПО

ПОДГОТОВКА К ОЦЕНКЕ СООТВЕТСТВИЯ



1 Подготовка проектной
и процедурной документации

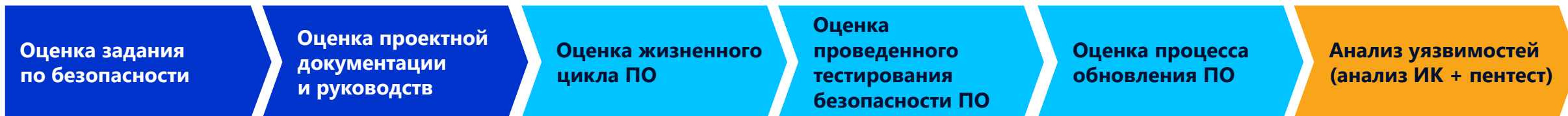


2 Подготовка
исследовательского стенда



3 Проведение предварительного
анализа уязвимостей (опционально)

ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ



СРЕДНЯЯ ДЛИТЕЛЬНОСТЬ ПРОЕКТА

~ 5 МЕСЯЦЕВ*

* - без учета разработки документации

ПО РЕЗУЛЬТАТАМ ПРОЕКТА ЗАКАЗЧИК ПОЛУЧАЕТ:

- Внедрение упрощенного SDLC
- Выполнение регуляторных требований
- Повышение защищенности ПО

ПРОВЕДЕНИЕ АНАЛИЗА УЯЗВИМОСТИ



1 Подготовительный этап

Анализ предоставленной документации

Подготовка/верификация исследовательского стенда

- I. Формирование представления о структуре, режимах функционирования, параметрах, функциональных возможностях

2 Проведение анализа уязвимостей

Идентификация потенциальных уязвимостей

- I. Анализ архитектуры
- II. Исследование общедоступных источников
- III. Фокусированный поиск в предоставленной документации

Анализ исходного кода на уязвимости

- I. Автоматическое сканирование приложения инструментальными средствами
- II. Экспертная проверка исходного код
- III. Регресс тестирование по результатам устранения разработчиком выявленных уязвимостей

Проведение тестирования на проникновение

- I. Разработка тестов проникновения
- II. Разработка детализированной тестовой документации
- III. Тестирование проникновения

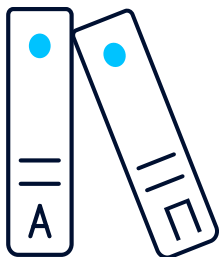
3 Оформление результатов

Разработка документации по результатам анализа уязвимостей

СРЕДНЯЯ ДЛИТЕЛЬНОСТЬ ПРОЕКТА

~ 3 МЕСЯЦА*

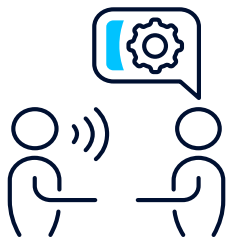
* - без учета разработки документации



Регуляторные требования по ОУД
делятся на актуальные (АУ)
и перспективные
(оценка соответствия)



Профиль защиты ЦБ –
методический документ



Для подготовки документации,
необходимой для оценки, необходима
коммуникация с разработчиками



Требования уже действуют, остается
не так много времени до окончания
отсрочки ЦБ по применению штрафных
санкций за их невыполнение

КОМПЕТЕНЦИИ ИНФОСИСТЕМЫ ДЖЕТ (ДЛЯ ТРЕТЬЕГО УРОВНЯ ЗАЩИТЫ)

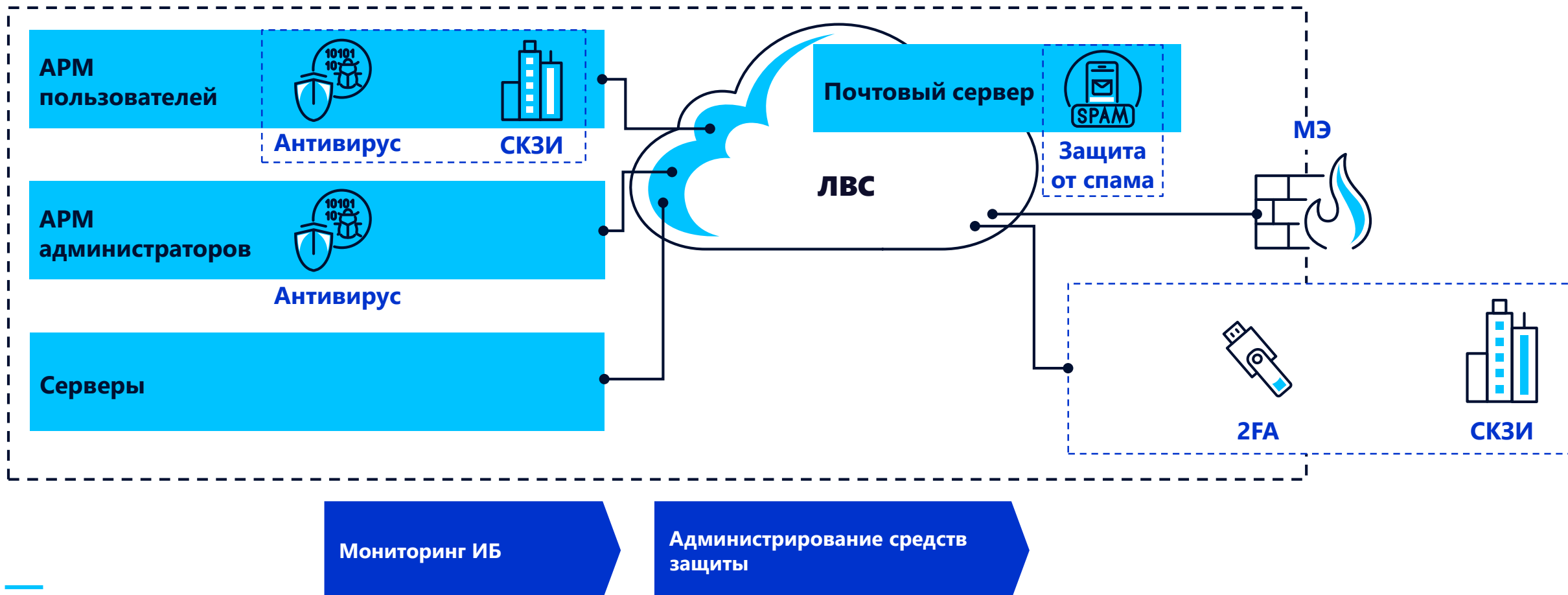


Оценка соответствия
требованиям Положения
684-П, ГОСТ 57580.1-2017

Разработка организационно-
распорядительных
документов

Разработка
компенсирующих мер

Внедрение
технических средств



КОМПЕТЕНЦИИ ИНФОСИСТЕМЫ ДЖЕТ (ДЛЯ ВТОРОГО УРОВНЯ ЗАЩИТЫ)



Оценка соответствия
требованиям Положения
684-П, ГОСТ 57580.1-2017

Оценка соответствия
прикладного ПО требованиям
безопасности

Разработка организационно-
распорядительных
документов

Разработка
компенсирующих мер

Внедрение
технических средств





НАУФОР

Jet

25/03/2021

СПАСИБО ЗА ВНИМАНИЕ!

По всем вопросам вы можете обращаться
к **Штыркину Валентину**,
Директору по развитию бизнеса
ve.shtyrkin@jet.su | +7 (925) 985 77 67