RTM GROUP

Практика проведения аудитов по ГОСТ 57580. Влияние применяемых систем SIEM и DLP на итоговую оценку. Рекомендации по оптимизации бюджетов

RTM TECHNOLOGIES — первая экспертная компания специализирующаяся на проведении нормативных и нормативно - технических экспертиз в области ИБ и ИТ.

rtmtech.ru

СОДЕРЖАНИЕ

ГОСТ 57580.1-2017

Когда появился?

ГОСТ Р 57580.1-2017 введен в действие **1 января 2018 года.**

Кем применяется?

- **кредитными организациями**;
- **некредитными финансовыми организациями**, (ч. 1 ст. 76.1 ФЗ от 10 июля 2002 года №86-ФЗ «О ЦБ РФ»);
- а также **субъектами национальной платежной системы**.

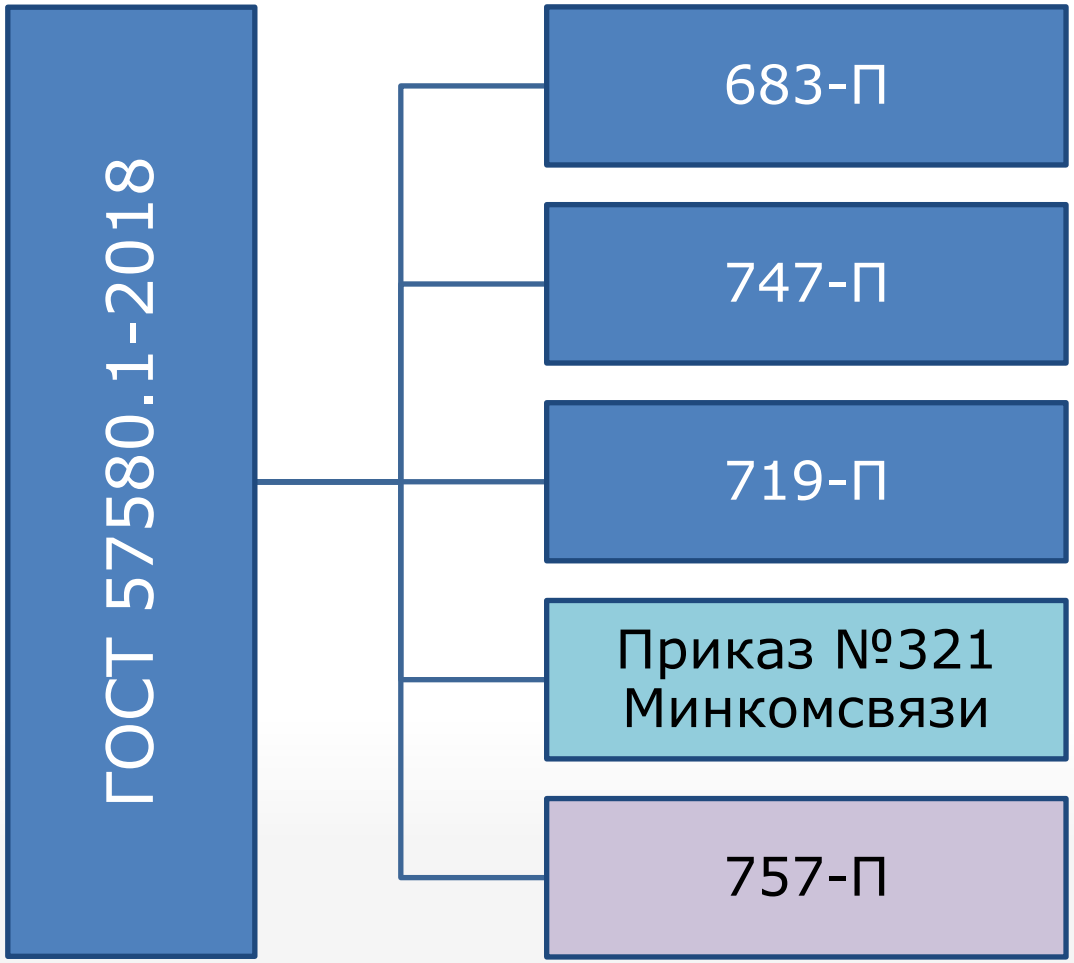
Для чего предназначен?

Стандарт определяет **уровни защиты информации** и **набор мер**, которые применяются для **реализации требований**, установленных нормативными актами ЦБ.

В стандарте определено три уровня защиты информации:

- **Уровень 3** – минимальный
- **Уровень 2** – стандартный
- **Уровень 1** – усиленный

Документы, требующие соответствия ГОСТ 57580:



Когда нужно соответствовать определенному уровню защиты?

Согласно 683-П:

Проведение оценки соответствия **не реже одного раза в два года**, с привлечением лицензиатов ФСТЭК (п.9).

С 1 января 2021	• Не ниже третьего • Числовая оценка < 0,70
С 1 января 2023	• Не ниже четвертого • Числовая оценка < 0,85

Когда нужно соответствовать определенному уровню защиты?

747-П

- Оценка соответствия не реже **одного раза в два года** (п.20)
- Уровень соответствия **не ниже четвертого** (п.20) с **1 января 2023 года** (> 0,85)
- **ССНП, СБП** должны применять меры защиты информации, реализующие **стандартный** уровень (уровень 2) защиты информации.

Приказ 321

- Оценка соответствия проводится **ежегодно** с привлечением **сторонних организаций**, имеющих лицензию ФСТЭК (п.9.2 Приложения 1).
- Должны использоваться информационные технологии и технические средства, соответствующие **стандартному** уровню защиты информации (п.5 Приложения 3).
- Необходимый уровень соответствия **не указан**.

Когда нужно соответствовать определенному уровню защиты?

Согласно 719-П:

Согласно п.2.4, п. 3.7, п. 4.5, п. 6.8 – необходимо обеспечить 4-ый уровень соответствия (0.85) со дня вступления положения в силу (01.01.2022 г).

Оценка соответствия защиты информации должна осуществляться **с привлечением сторонних организаций,** имеющих лицензию ФСТЭК (п.1.1).

Когда нужно соответствовать определенному уровню защиты?

Согласно 757-П:

Определение уровня защищенности - **ежегодно** (п.5.1.);

Оценка соответствия защиты информации **с привлечением лицензиата ФСТЭК** (п.1.5.1).

Для усиленного Уровня защиты	• Один раз в год
Для стандартного Уровня защиты	• Один раз в три года

Меры ГОСТ Р 57580.1-2017

- Большинство организационных мер защиты информации реализуются за счет введения организационно-распорядительной документации
- Технические меры защиты информации реализуются за счет технических решений применяемых в информационной инфраструктуре Организации

Соотношение мер для 2-го уровня защиты

Применяемые технические решения для выполнения мер ГОСТ 57580

Процесс 1 «Обеспечение защиты информации при управлении доступом»

- Технологии разграничения доступа реализуемые операционной системой (Active Directory, Парольная политика и т.д.);
- Технологии разграничения доступа реализуемые сторонними средствами (СЗИ от НСДи т.д.);
- Технологии регистрации событий в системах управления доступом;
- Системы управления физическим доступом (Физические замки, СКУД, Пожарная сигнализация и т.д.).

Процесс 2 «Обеспечение защиты вычислительных сетей»

- Межсетевые экраны;
- Криптошлюзы;
- IDS/IPS-системы;
- Антивирусы реализующие функции контроля отсутствия (выявления) аномальной сетевой активности;
- Функциональное оборудование беспроводного доступа.

Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»

- Сканеры уязвимостей;
- Средства доверенной загрузки ПО;
- Штатные средства аудита Windows.

Процесс 4 «Защита от вредоносного кода»

- Антивирусное программное обеспечение;
- Многовендорный подход при реализации системы антивирусной защиты.

Применяемые технические решения для выполнения мер ГОСТ 57580

Процесс 5 «Предотвращение утечек информации»

- DLP-системы, которые должны включать следующие функции:
- Средства доверенного уничтожения информации.

Процесс 6 «Управление инцидентами защиты информации»

- SIEM/ITSM-системы.

Процесс 7 «Защита среды виртуализации»

- Функциональные средства виртуализации.

Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»

- MDM-системы;
- Технологии защищенной связи переносных устройств;
- Использование антивирусов на переносных устройствах.

Влияние технических решений на итоговую оценку по ГОСТ 57580

Сокращение базового набора мер

— За счет грамотной разработки модели угроз

Применение компенсирующих мер

— За счет грамотной разработки модели угроз и документов верхнего уровня (положения, политики)

Выполнение организационных мер

— За счет прямого документирования базовых либо компенсирующих мер

Меры	Н	О	Т
Базовый состав	98	290	279
Адаптированный состав	250	200	217
После компенсации	250	250	167

Влияние ОРД и технических решений на итоговую оценку по ГОСТ 57580

До разработки ОРД/После разработки ОРД

Наименование процесса системы ЗИ, направления ЗИ	Выбор	Планирование (0.2)	Реализация (0.4)	Контроль (0.25)	Совершенствование (0.15)	Оценка процесса
Процесс 1 «Обеспечение ЗИ при управлении доступом»	0,64	0,40/1,00	0,60	0,64/1,00	0,00/1,00	0,56/0,74
Процесс 2 «Обеспечение защиты сетей»	0,66	0,40/1,00	0,67	0,60/1,00	0,00/1,00	0,58/0,76
Процесс 3 «Контроль целостности и защищенности»	0,65	0,00/1,00	0,64	0,58/1,00	0,00/1,00	0,53/0,75
Процесс 4 «Защита от ВВК»	0,94	1,00/1,00	0,80	0,68/1,00	0,00/1,00	0,82/0,93
Процесс 5 «Предотвращение утечек»	0,25	0,00/1,00	0,22	0,09/1,00	0,00/1,00	0,18/0,47
Процесс 6 «Управление инцидентами»	0,56	0,20/1,00	0,67	0,38/1,00	0,88/1,00	0,43/0,71
Процесс 7 «Защита среды виртуализации»	0,65	0,00/1,00	0,64	0,58/1,00	0,00/1,00	0,53/0,75
Процесс 8 «Защита мобильных (переносных) устройств»	0,00	0,00	0,00	0,00	0,00	Н
Применение организационных и технических мер ЗИ на этапах жизненного цикла АС						0,37/0,67
Количество нарушений ЗИ, выявленных в результате оценки соответствия ЗИ						3
Итоговая оценка соответствия ЗИ						0,49/0,71

Разработкой ОРД можно достичь только третий уровень соответствия.

Исходя из положений ГОСТ уровень соответствия оценивается за каждый из процессов.

Письмо ЦБ № 56-1-11/265 от 22.05.2020 г.

Практика применения систем SIEM и DLP. Обзор систем максимально соответствующих требованиям мер ГОСТ 57580

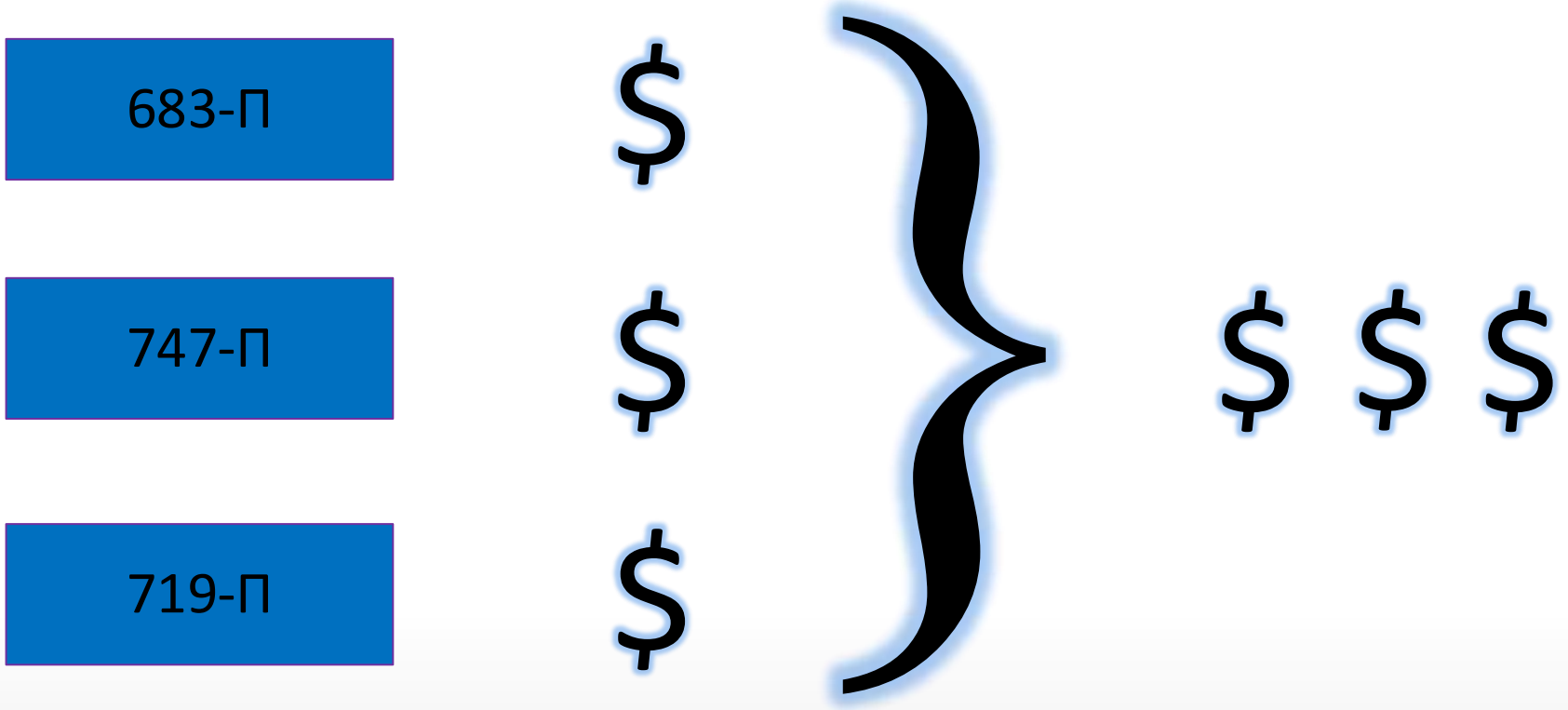
- **Процесс 5 «Предотвращение утечек информации»:**
- **DeviceLock DLP;**
- **Trend Micro DLP;**
- **Dallas Lock;**
- **…**
- **Symantec DLP;**
- **Forcepoint DLP;**
- **…**

- **Процесс 6 «Управление инцидентами защиты информации»:**
- **MaxPatrol SIEM;**
- **RUSIEM;**
- **…**
- **McAfee Enterprise Security Manager;**
- **IBM QRadar SIEM;**
- **…**

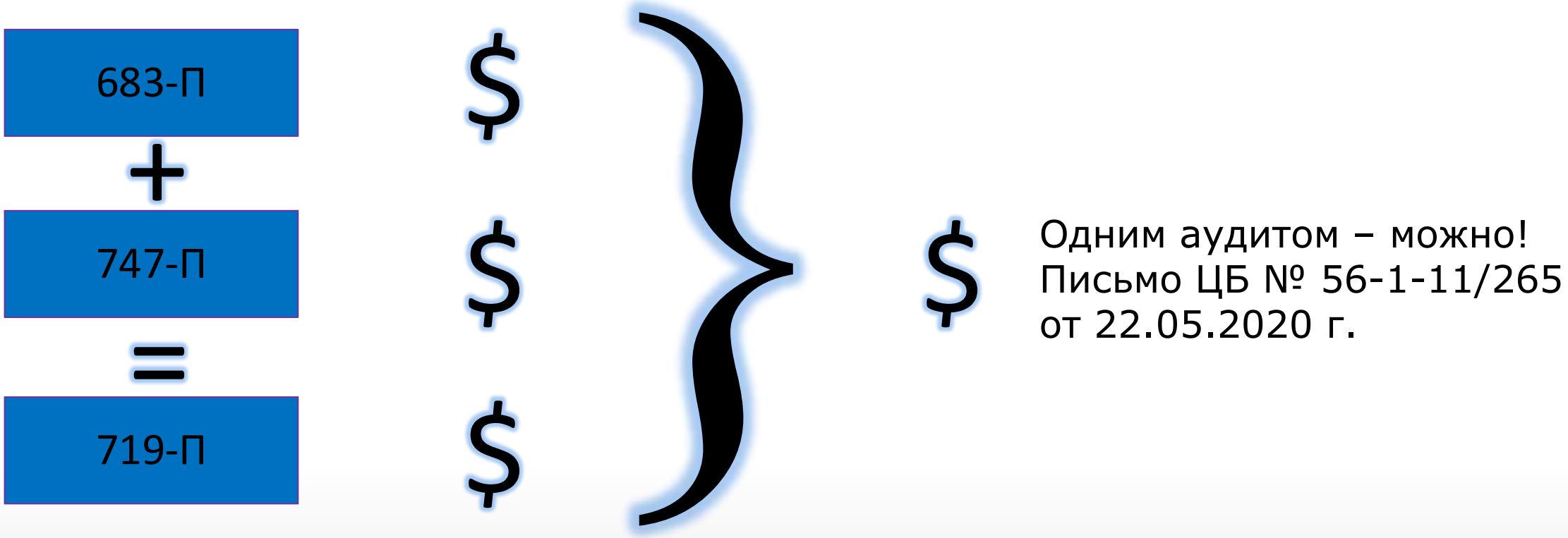
- Позволяют достичь 1

- Не позволяют достичь 1, но позволяют достичь 0,85

Рекомендации по оптимизации бюджета
Как выполнить все требования ЦБ и уменьшить на это затраты денежных средств



Рекомендации по оптимизации бюджета
Как выполнить все требования ЦБ и уменьшить на это затраты денежных средств



Одним аудитом – можно!
Письмо ЦБ № 56-1-11/265 от 22.05.2020 г.

Требования, реализуемые в виде отдельных работ

ОУД 4

ГОСТ Р 57580.1-2017 требует применение прикладного ПО АС, в отношении которого проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4 (мера ЖЦ.8).

Анализ уязвимостей проводится в соответствии с ГОСТ 15408-3-2013.

Пентест

Ежегодное тестирование на проникновение (пентест) (мера ЖЦ.20).

При модернизации элементов информационной инфраструктуры (мера ЖЦ.14).

Внедрение сертифицированных по требованиям безопасности не ниже:

4-го класса (для 1-го уровня защиты информации – усиленного) (мера РЗИ.11);

5-го класса (для 2-го уровня защиты информации – стандартного) (мера РЗИ.12);

6-го класса (для 3-го уровня защиты информации – минимального) (мера РЗИ.13).

А также применение СКЗИ, имеющих класс не ниже КС2 (для 1-го уровня защиты информации) (мера РЗИ.14).

ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Федор Музалевский

Кандидат физико-математических наук

Ведущий судебный эксперт

Директор технического департамента RTM Group

Кобец Дмитрий Андреевич

Эксперт в сфере информационной безопасности

Заместитель директора технического департамента RTM Group


+7 908 147 27 41


f.muzalevsky@rtmtech.ru


https://rtmtech.ru


GroupRTM


rtm.group


@GroupRtm


rtm.group.russia