ГОСТ Р 57580.1-2017. ОТВЕТЫ НА ВОПРОСЫ ПО ОЦЕНКЕ СООТВЕТСТВИЯ И РЕАЛИЗАЦИИ.

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

Ксения Засецкая
Старший консультант
АО «ДиалогНаука»

Москва, 10 ноября 2020

ДиалогНаука

План вебинара

В рамках вебинара будут даны ответы на вопросы по следующим направлениям:

- ✓ Порядок проведения оценки соответствия
- ✓ Сроки выполнения требований
- ✓ Ответственность за невыполнение
- ✓ Реализация конкретных мер

Положение Банка России 683-П

Обеспечение с 01.01.2021 реализации требований ГОСТ Р 57580.1-2017:

- ✓ системно значимые КО - усиленный уровень (уровень 1) защиты информации по ГОСТ Р 57580.1-2017;
- ✓ остальные КО - стандартный уровень (уровень 2) защиты информации ГОСТ Р 57580.1-2017.

Требования к технологии обработки защищаемой информации

- ✓ на технологическом участке формирования (подготовки), передачи и приема электронных сообщений;
- ✓ на технологическом участке удостоверения прав клиентов распоряжаться денежными средствами;
- ✓ на технологическом участке осуществления банковской операции, учета результатов ее осуществления

Привлечение лицензиата!

Положение Банка России 683-П

- Сертификация прикладного ПО АС и приложений, распространяемых кредитной организацией клиентам для совершения действий в целях осуществления банковских операций, а также ПО, обрабатывающего защищаемую информацию на участках, используемых для приема электронных сообщений
- Требования к защите электронных сообщений на различных технологических участках обработки:
  - идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций;
  - формирование (подготовка), передача и прием электронных сообщений;
  - удостоверение права клиентов распоряжаться денежными средствами;
  - осуществление банковской операции, учет результатов ее осуществления;
  - хранение электронных сообщений и информации об осуществленных банковских операциях

Положение Банка России 672-П

Часть требований – с 01.07.2021

ПС БР

Участники ССНП

Участники СБП

ОПКЦ

Документирование

Защита электронных сообщений

Применение СКЗИ

Положение Банка России 684-П

Усиленный уровень защиты

- ✓ Центральные контрагенты, центральный депозитарий

Стандартный уровень

- ✓ специализированные депозитарии инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов;
- ✓ клиринговые организации;
- ✓ организаторы торговли;
- ✓ страховые организации (…);
- ✓ НПФ, осуществляющие деятельность по обязательному пенсионному страхованию;
- ✓ НПФ и иные организации ...

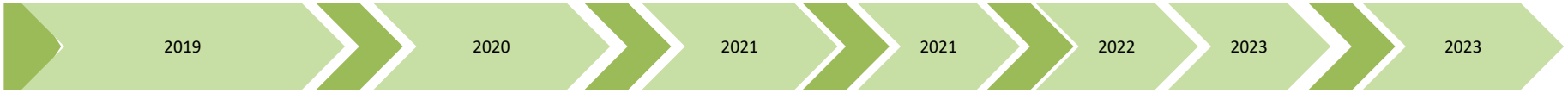
Для остальных реализовывать 3 уровень (минимальный) не надо!

Положение Банка России 719-П (новое)

- ✓ оператор по переводу денежных средств (ОПДС);
- ✓ банковский платежный агент (субагент) (БПА);
- ✓ оператор услуг информационного обмена (ОУИО);
- ✓ поставщик платежного приложения (ППП);
- ✓ оператор платежной системы (ОПС);
- ✓ оператор услуг платежной инфраструктуры (ОУПИ)

Требования вступают в силу с 1 января 2022 года, кроме требований к использованию СКЗИ (вступают в силу в 2024 году и 2031 году)

Сроки



06.04.2019
Вступил в силу 672-П

26.05.2019
Вступили в силу 684-П, 683-П

01.01.2020
Необходимость сертификации прикладного ПО АС

01.01.2021
1. Необходимость выполнения требований ГОСТ Р 57580.1-2017
2. Уровень не ниже 3 для КО
3. Проведение тестирований на проникновение
4. Проведение оценки соответствия

01.07.2021
Дополнительные требования 672-П

01.01.2022
Необходимость обеспечения не ниже 3 уровня соответствия для НФО
ГОСТ Р 57580.1-2017
Вступает в силу 719-П

01.01.2023
Необходимость обеспечения не ниже 4 уровня соответствия ГОСТ Р 57580.1-2017 для КО

01.07.2023
Необходимость обеспечения не ниже 4 уровня соответствия ГОСТ Р 57580.1-2017 для НФО

Требования Положения Банка России 683-П

Системно значимые кредитные организации, кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитные организации, значимые на рынке платежных услуг

→ **усиленный уровень защиты информации**

оценка соответствия

→ Не реже одного раза в 2 года

уровень соответствия не ниже третьего

→ **с 1 января 2021 года**

Требования Положения Банка России 672-П

Участники ССНП
Участники СБП

→ **стандартный уровень защиты информации**

оценка соответствия →

Не реже одного раза в 2 года

уровень соответствия не ниже четвертого →

с 1 января 2023 года

Требования для НФО, реализующие усиленный и стандартный уровни защиты информации

Требование	Ссылка	Период.
Проведение тестирования на проникновение	п.5.4 684-П ЖЦ.20 ГОСТ 57580	ежегодно
Сертификация прикладного ПО АС	п.9 684-П	разово (а также в случаях предусмотренных выданным сертификатом)
Подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить их составление уполномоченным на это лицом	п.10 684-П	постоянно
Регламентация, реализация, контроль (мониторинг) технологии безопасной обработки защищаемой информации	п.11 684-П	постоянно
Регистрация событий информационной безопасности	п.12 684-П	постоянно
Внедрение процесса управления инцидентами информационной безопасности	пп.13-15 684-П	постоянно
Пересмотр применимого уровня защиты	п.5.1 684-П	ежегодно не позднее 1 рабочего дня года
Оценка выполнения требований ГОСТ Р 57580.1	п.6 684-П	ежегодно (для 1 уровня) раз в 3 года (для 2 уровня)

Вопросы по методике

- ✓ Отличаются ли подходы в оценке крупных и мелких/средних банков?
- ✓ Как оценить выполнение требований ИБ к процессам, которые в банке не применяются?
  Правильно ли я понимаю, что в ходе аудита, если, к примеру, отсутствует беспроводная связь, по всему разделу ставится оценка «не применимо»?
- ✓ Каков исчерпывающий перечень свидетельств аудита? Каков срок хранения результатов оценки соответствия?
- ✓ По требованиям ЦБ, Банк должны провести оценку по 672-П и 683-П. Может ли Банк провести общую оценку ИБ по ГОСТ Р 57580.1-2017, а не как предлагают сейчас по каждому положению отдельно?
- ✓ Как требования данных правил коррелирует с уже существующими правилами и ограничениями?
- ✓ Будет ли ЦБ более мягче и лояльнее в рамках своих проверок по ГОСТ относиться к организациям в связи с пандемией? Есть ли официальная информация от ЦБ на этот счет? Будут ли проверки проходить дистанционно?

Методика. Формулы

Требования к системе защиты информации

$$\mathrm{Е}_{\mathrm{ПЗИ}_i} = \frac{\sum_{j=1}^{N} E_{\mathrm{МЗИ}_j}}{N}$$

$$E_i = \frac{\mathrm{Е}_{\mathrm{ПЗИ}_i} + (0{,}2 * \mathrm{Е}_{\mathrm{П}_i} + 0{,}4 * \mathrm{Е}_{\mathrm{Р}_i} + 0{,}25 * \mathrm{Е}_{\mathrm{К}_i} + 0{,}15 * \mathrm{Е}_{\mathrm{С}_i})}{2}$$

Если в область оценки соответствия входят несколько контуров безопасности разного уровня

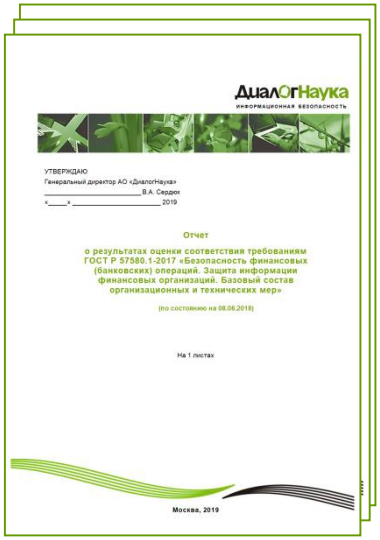
$$E_i = k_1 E_{1i} + k_2 E_{2i} + k_3 E_{3i}$$

Наличие контура заданного уровня			Корректирующий коэффициент		
3	2	1	E_{3i}	E_{2i}	E_{1i}
+	+	+	0,1	0,3	0,6
	+	+		0,3	0,7
+		+	0,2		0,8
+	+		0,4	0,6	

Требования к отчетным документам

Отчет о результатах оценки соответствия требованиям ГОСТ

- ✓ сведения о проверяющей организации
- ✓ сведения о руководителе и членах проверяющей группы
- ✓ сведения о проверяемой организации
- ✓ сведения о заказчике оценки соответствия ЗИ
- ✓ цель оценки соответствия ЗИ
- ✓ сроки проведения оценки соответствия ЗИ
- ✓ область оценки соответствия ЗИ
- ✓ перечень неоцениваемых областей оценки соответствия ЗИ (процессов системы ЗИ, подпроцессов системы ЗИ, направлений ЗИ, мер ЗИ) с обоснованием их исключения из области оценки соответствия ЗИ
- ✓ обоснование применения компенсирующих мер ЗИ при невозможности реализации отдельных выбранных мер ЗИ
- ✓ краткое изложение процесса оценки соответствия ЗИ, включая элемент неопределенности и (или) проблемы, которые могут отразиться на надежности заключения по результатам оценки соответствия ЗИ
- ✓ числовое значение итоговой оценки соответствия ЗИ, характеризующей соответствие ЗИ проверяемой организации установленным требованиям на дату завершения оценки соответствия ЗИ
- ✓ подтверждение, что цель оценки соответствия ЗИ достигнута в области оценки соответствия ЗИ
- ✓ неразрешенные разногласия между проверяющей группой и проверяемой организацией
- ✓ перечень и сведения о представителях проверяемой организации, которые сопровождали проверяющую группу при проведении оценки соответствия ЗИ
- ✓ сведения о конфиденциальном характере содержания отчета по результатам оценки соответствия ЗИ
- ✓ **опись документов (копий документов) на бумажных носителях**, прилагаемых к отчету по результатам оценки соответствия ЗИ, с указанием общего количества томов приложений, количества и наименований документов, а также количества листов в каждом из них
- ✓ **опись машинных носителей информации, прилагаемых к отчету** по результатам оценки соответствия ЗИ, с указанием их реквизитов (наименование, тип, учетный номер и т.п.) и содержащихся на них файлов данных, а также результатов вычисления по каждому из них хэш-функции, реализованной в соответствии с ГОСТ Р 34.11-2012



Отчетные документы

- ✓ Можно ли использовать иную форму, так как собирать 600+ подписей с представителей финансовой организации является трудоемким процессом, в первую очередь для самой финансовой организации?

- ✓ В методике оценки соответствия не указано, как надо поступать в случае, если финансовая организация использует меры, отличные от мер, определенных ГОСТ Р 57580.1 (например, компенсирующие меры в соответствии с п.6.4 ГОСТ Р 57580.1):
  - *Применение компенсирующих мер защиты информации должно быть направлено на обработку операционного риска, связанного с реализацией тех же угроз безопасности информации, на нейтрализацию которых направлены меры из базового состава мер защиты информации настоящего стандарта, не применяемые финансовой организацией в связи с невозможностью технической реализации и (или) экономической целесообразностью.*
  - Правильно ли мы понимаем, что в таком случае базовая мера из ГОСТ Р 57580.1 должна быть помечена как «Н», а компенсирующие меры просто должны быть указаны в соответствующем разделе отчета, при этом они не учитываются при расчете итоговой оценки соответствия по данному процессу (подпроцессу)?

Ответы на санкционные вопросы

- ✓ Федеральный закон от 27.06.2011 N 161-ФЗ «О национальной платежной системе»

Статья 34. Действия и меры принуждения, применяемые Банком России в случае нарушения поднадзорной организацией требований настоящего Федерального закона или принятых в соответствии с ним нормативных актов Банка России
Последствия – **приостановление деятельности по переводу денежных средств**

- ✓ КоАП РФ. ч. 6 Ст. 13.12. Нарушение правил защиты информации

Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных частями 1, 2 и 5 настоящей статьи, -
влечет наложение **административного штрафа** на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - **от одной тысячи до двух тысяч рублей**; на юридических лиц - **от десяти тысяч до пятнадцати тысяч рублей**

- ✓ КоАП РФ. ч. 9 Ст. 19.5

Невыполнение в установленный срок законного предписания Банка России - влечет наложение **административного штрафа** на должностных лиц в размере **от двадцати тысяч до тридцати тысяч рублей**; на юридических лиц - **от пятисот тысяч до семисот тысяч рублей**

Выбор мер

- При разработке модели угроз безопасности информации какой необходимо воспользоваться методикой для определения актуальных угроз?

- Подходы к выборности мер:
  - выставить оценку «1» при наличии хотя бы одного свидетельства реализации меры ЗИ в отношении одного ресурса или объекта доступа, входящего в границы области оценивания;
  - выставить оценку «0» при наличии хотя бы одного свидетельства не реализации меры ЗИ в отношении ресурсов или объектов доступа, входящих в границы области оценивания»

Ответы на вопросы по реализации

- ✓ Какие есть варианты технической реализации требования ЗВК.20, без проведения «ручной» проверки устанавливаемого/изменяемого ПО? Как исполнять ЗВК.20 при обновлении Windows и ПО обновляемого онлайн (*Выполнение предварительных проверок на отсутствие вредоносного кода устанавливаемого или изменяемого ПО, а также выполнение проверки после установки и/или изменения ПО)?

- ✓ В ГОСТ есть термин «средства защиты информации» (КЗИ.9, КЗИ.10), к данным средствам относятся только антивирусы, МСЭ или любое ПО с функцией разграничения логического доступа (ActiveDirectory, ПО от вендоров, самописное ПО)?

- ✓ СМЭ.6 - 1. О каком тестировании идет речь? 2. Есть ли ограничения по межсегментному взаимодействию (тестирование и разработка) (Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры, используемой только на этапе создания и/или модернизации АС, в том числе тестирования ПО и СВТ)

Ответы на вопросы по реализации

- ✓ Какие есть варианты технической реализации требования ЗВК.20, без проведения «ручной» проверки устанавливаемого/изменяемого ПО? Как исполнять ЗВК.20 при обновлении Windows и ПО обновляемого онлайн (*Выполнение предварительных проверок на отсутствие вредоносного кода устанавливаемого или изменяемого ПО, а также выполнение проверки после установки и/или изменения ПО)?

- ✓ В ГОСТ есть термин «средства защиты информации» (КЗИ.9, КЗИ.10), к данным средствам относятся только антивирусы, МСЭ или любое ПО с функцией разграничения логического доступа (ActiveDirectory, ПО от вендоров, самописное ПО)?

- ✓ СМЭ.6 - 1. О каком тестировании идет речь? 2. Есть ли ограничения по межсегментному взаимодействию (тестирование и разработка) (Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры, используемой только на этапе создания и/или модернизации АС, в том числе тестирования ПО и СВТ)

Ответы на вопросы по реализации

- ✓ Какие есть варианты технической реализации требования ЗВК.20, без проведения «ручной» проверки устанавливаемого/изменяемого ПО? Как исполнять ЗВК.20 при обновлении Windows и ПО обновляемого онлайн (*Выполнение предварительных проверок на отсутствие вредоносного кода устанавливаемого или изменяемого ПО, а также выполнение проверки после установки и/или изменения ПО)?

- ✓ В ГОСТ есть термин «средства защиты информации» (КЗИ.9, КЗИ.10), к данным средствам относятся только антивирусы, МСЭ или любое ПО с функцией разграничения логического доступа (ActiveDirectory, ПО от вендоров, самописное ПО)?

- ✓ СМЭ.6 - 1. О каком тестировании идет речь? 2. Есть ли ограничения по межсегментному взаимодействию (тестирование и разработка) (Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры, используемой только на этапе создания и/или модернизации АС, в том числе тестирования ПО и СВТ)

Ответы на вопросы по реализации

- ✓ Как возможно выполнить меру ПУИ.11 и ПУИ.17, без использования DLP-системы?
  - ✓ *ПУИ.11 Контентный анализ информации, передаваемой в сеть Интернет с использованием информационной инфраструктуры финансовой организации*
  - ✓ *ПУИ.17 Контентный анализ информации, копируемой на переносные (отчуждаемые) носители информации*
- ✓ Реализация контроля использования технологий мобильного кода средствами АВЗ
  - ✓ *ЗВК.24 Регистрация неконтролируемого использования технологии мобильного кода Примечание: В том числе Java, JavaScript, ActiveX, VBScript и иные аналогичные технологии*
- ✓ Обязательно ли использование сертифицированных средств защиты?
- ✓ Как возможно реализовать ЗСВ.7
  - ✓ *Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине с одного АРМ пользователя или эксплуатационного персонала*

Ответы на вопросы по реализации

- ✓ Как возможно выполнить меру ПУИ.11 и ПУИ.17, без использования DLP-системы?
  - ✓ *ПУИ.11 Контентный анализ информации, передаваемой в сеть Интернет с использованием информационной инфраструктуры финансовой организации*
  - ✓ *ПУИ.17 Контентный анализ информации, копируемой на переносные (отчуждаемые) носители информации*
- ✓ Реализация контроля использования технологий мобильного кода средствами АВЗ
  - ✓ *ЗВК.24 Регистрация неконтролируемого использования технологии мобильного кода Примечание: В том числе Java, JavaScript, ActiveX, VBScript и иные аналогичные технологии*
- ✓ Обязательно ли использование сертифицированных средств защиты?
- ✓ Как возможно реализовать ЗСВ.7
  - ✓ *Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине с одного АРМ пользователя или эксплуатационного персонала*

Ответы на вопросы по реализации

- ✓ Как возможно выполнить меру ПУИ.11 и ПУИ.17, без использования DLP-системы?
  - ✓ *ПУИ.11 Контентный анализ информации, передаваемой в сеть Интернет с использованием информационной инфраструктуры финансовой организации*
  - ✓ *ПУИ.17 Контентный анализ информации, копируемой на переносные (отчуждаемые) носители информации*
- ✓ Реализация контроля использования технологий мобильного кода средствами АВЗ
  - ✓ *ЗВК.24 Регистрация неконтролируемого использования технологии мобильного кода Примечание: В том числе Java, JavaScript, ActiveX, VBScript и иные аналогичные технологии*
- ✓ Обязательно ли использование сертифицированных средств защиты?
- ✓ Как возможно реализовать ЗСВ.7
  - ✓ *Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине с одного АРМ пользователя или эксплуатационного персонала*

Ответы на вопросы по реализации

- ✓ Как возможно выполнить меру ПУИ.11 и ПУИ.17, без использования DLP-системы?
  - ✓ *ПУИ.11 Контентный анализ информации, передаваемой в сеть Интернет с использованием информационной инфраструктуры финансовой организации*
  - ✓ *ПУИ.17 Контентный анализ информации, копируемой на переносные (отчуждаемые) носители информации*
- ✓ Реализация контроля использования технологий мобильного кода средствами АВЗ
  - ✓ *ЗВК.24 Регистрация неконтролируемого использования технологии мобильного кода Примечание: В том числе Java, JavaScript, ActiveX, VBScript и иные аналогичные технологии*
- ✓ Обязательно ли использование сертифицированных средств защиты?
- ✓ Как возможно реализовать ЗСВ.7
  - ✓ *Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине с одного АРМ пользователя или эксплуатационного персонала*

Вопросы по жизненному циклу

- ✓ В ГОСТ 57580.2, пункт 7.8 для процессов даны объединяющие формулы, а для ЖЦ нет. Вопрос: как считать совокупную оценку для нескольких контуров в части ЖЦ?

- ✓ Здравствуйте! Подскажите, как на практике можно реализовать выполнение требования ЖЦ.4 ГОСТ 57580.1?
  - ✓ *Реализация управления версиями (сборками) и изменениями создаваемого (модернизируемого), в том числе тестируемого, прикладного ПО АС, осуществляемого для цели:*
    - *контроля реализации функций защиты информации в определенной версии (сборке) прикладного ПО;*
    - *принятия мер, препятствующих несанкционированному внесению изменений в версии (сборки) прикладного ПО*

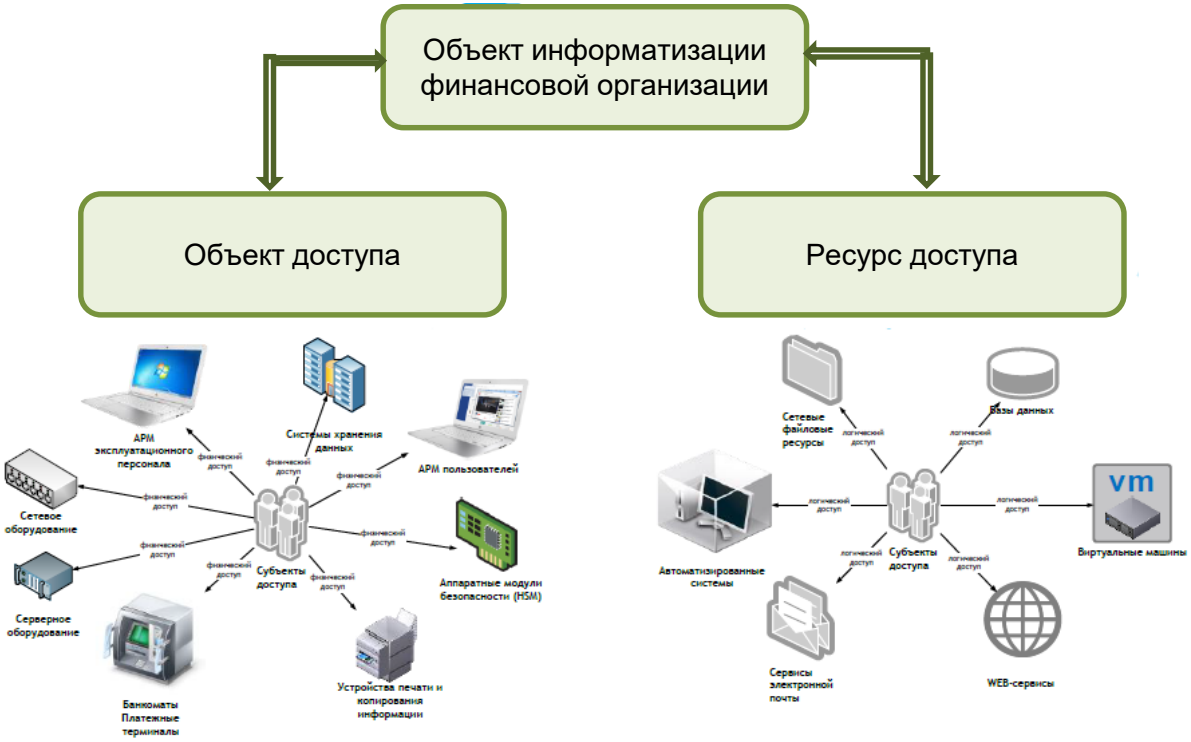
Вопросы по жизненному циклу

- ✓ В ГОСТ 57580.2, пункт 7.8 для процессов даны объединяющие формулы, а для ЖЦ нет. Вопрос: как считать совокупную оценку для нескольких контуров в части ЖЦ?

- ✓ Здравствуйте! Подскажите, как на практике можно реализовать выполнение требования ЖЦ.4 ГОСТ 57580.1?
  - ✓ *Реализация управления версиями (сборками) и изменениями создаваемого (модернизируемого), в том числе тестируемого, прикладного ПО АС, осуществляемого для цели:*
    - *контроля реализации функций защиты информации в определенной версии (сборке) прикладного ПО;*
    - *принятия мер, препятствующих несанкционированному внесению изменений в версии (сборки) прикладного ПО*

Вопросы по контурам

- ✓ Как правильно определять контуры безопасности?



- ✓ Как оценивать контур СБП ?

Финансовая составляющая

- ✓ Порядок цен на услугу по оценке соответствия по ГОСТ Р 57580.1-2018?

- ✓ Каким образом обосновываются меры компенсационного характера? Экономическая целесообразность - по какой методике считать?

Спасибо за внимание!

Вопросы?

АО «ДиалогНаука»

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

E-mail:

svintsitskii@DialogNauka.ru

K.Zasetskaya@DialogNauka.ru

http://www.DialogNauka.ru