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, 27 апреля 2021

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 747-П

Часть требований – с 01.07.2021
Часть – с 01.01.2022 и с 01.07.2022

ПС БР

Участники ССНП

Участники СБП

ОПКЦ

ОУИО СБП

С 01.01.2023 – уровень соответствия не ниже 4!

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

- ✓ 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)

Положение Банка России 719-П

- ✓ Сертификация либо оценка соответствия по ОУД 4:
  - ✓ Прикладного ПО АС и приложений, распространяемых клиентам ОПДС для совершения действий, непосредственно связанных с осуществлением переводов денежных средств;
  - ✓ ПО, эксплуатируемого на участках, используемых для приема документов, связанных с осуществлением переводов денежных средств, составленных в электронном виде, к исполнению в АС и приложениях с использованием информационно-телекоммуникационной сети «Интернет»
- ✓ Сертификация прикладного ПО АС и приложений по уровням доверия для ОПДС

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

25.02.2021
Вступило в силу 747-П

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 747-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 747-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)

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	

Вопросы по методике

- ✓ В случае, если какая-то деятельность в маленьком банке не осуществляется (разработка ПО, предоставление клиентам доступа в интернет посредством беспроводных сетей), каким образом аудитор оценивает соответствие требованиям ГОСТ к ним?
- ✓ Как аудитор оценивает соответствие требованиям ГОСТ к процессам, которые в Банке не реализованы (например, разработка ПО, общедоступная сеть Wi-Fi)?
- ✓ Какие актуальные сроки по наличию результатов аудита в связи с пандемией?
- ✓ 1) требования к организации для проведения оценки соответствия банкам. 2) сколько по времени занимает процесс оценки для небольшого банка. 3) какие рекомендации даются по результатам
- ✓ Из каких соображений присвоены весовые коэффициенты в формулах 8-12? Почему в формуле 8 происходит деление на 2, а не на количество процессов? Если это среднее арифметическое.
- ✓ На какие основные вопросы следует обратить внимание при проведении самооценки?

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**

Контуры безопасности

- ✓ Как правильно определять контуры безопасности?

- ✓ Как оценивать контур СБП ?

Вопросы по контурам

- Относить ли к контурам безопасности:
  - 1. АРМ пользователей, имеющих доступ в АБС, но не осуществляющих банковские операций (юристы, ...)?
  - 2. серверы организации (WSUS, АВЗ, DNS, NTP, DC), которые не используются для предоставления финансовых услуг?

- Требуется ли в контуре отдельная инфраструктура: почтовик, релеи, DNS, NTP, гипервизоры и т.д.

- Необходимо ли выполнять сбор свидетельств со всех рабочих мест, входящих в контур?

Ответы на вопросы по реализации

- ✓ Возможно ли совмещение норм ГОСТ и требований импортозамещения ПО ?
- ✓ Применение к экосистемам.
- ✓ Кто назначается распорядителем логического доступа (владельцем ресурса доступа) и распорядителем физического доступа?
- ✓ Что является эталонной копией ПО АС, ПО средств и систем ЗИ, системного ПО?
- ✓ Примеры выполнения мер ГОСТ
- ✓ Как применять ПЭП для подписания электронных сообщений в связи с грядущими изменениями в 684-П?

Ответы на вопросы по реализации

- ✓ Реализация мер РД.26, как реализовать хранение копий аутентификационных данных на МНИ и отказаться от бумажных носителей? Возможно использование менеджеров паролей?
- ✓ Какие продукты рекомендуются для закрытия требований?
- ✓ Какие мероприятия необходимо предпринять для выполнения требования РД.30 "Авторизация логического доступа к ресурсам доступа, в том числе АС"?

Ответы на вопросы по реализации

- ✓ ЗВК.18 и ЗВК.19 подразумевает автономный АРМ для предварительной проверки или нет? Как трактовать данные требования

ЗВК.18 Входной контроль всех устройств и переносных (отчуждаемых) носителей информации (включая мобильные компьютеры и флеш-накопители) перед их использованием в вычислительных сетях финансовой организации

ЗВК.19 Входной контроль устройств и переносных носителей информации перед их использованием в вычислительных сетях финансовой организации, в выделенном сегменте вычислительной сети, с исключением возможности информационного взаимодействия указанного сегмента и иных сегментов вычислительных сетей финансовой организации (кроме управляющего информационного взаимодействия по установленным правилам и протоколам)

- ✓ Что именно подразумевается и как можно выполнить требование ГОСТ 57580 ЗВК.24?

ЗВК.24 Регистрация неконтролируемого использования технологии мобильного кода Примечание: В том числе Java, JavaScript, ActiveX, VBScript и иные аналогичные технологии

Ответы на вопросы по реализации

- ✓ Вопрос применения сертифицированных СКЗИ/СЗИ (прошедших процедуру оценки) по ГОСТ57580.1 ложится на организацию с учетом её моделей угроз и нарушителя?

- ✓ Обязательство в использовании исключительно сертифицированных СЗИ в компании

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

- ✓ 7 процесс: можно ли выполнить все меры штатными средствами гипервизоров? Или необходимо докупать СЗИ?

Вопросы по защите удаленного доступа

- ✓ Что в рамках ГОСТ понимается под мобильным / переносным устройством в рамках секции 7.9
- ✓ Что имеется в виду под MDM
- ✓ ЗУД 5. Как реализовать?

Идентификация, двухфакторная аутентификация и авторизация субъектов доступа после установления защищенного сетевого взаимодействия, выполнения аутентификации, предусмотренной мерами ЗУД.2 и ЗУД.4

- ✓ По возможности раскрыть основные принципы достижения соответствия по п.7.9. Какие конкретно рекомендуется применять инструменты (ПО) для этого.

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