Обзор требований ГОСТ Р 57580.1-2017

Сергей Борисов
Диана Лейчук

Ведущие четвертого выпуска

Сергей Борисов

Заместитель руководителя по ИБ
обособленного подразделения УЦСБ
г. Краснодар
Работа в ИБ – 15 лет

Блог: https://sborisov.blogspot.com

Диана Лейчук

Руководитель направления аудитов
Аналитический центр УЦСБ
г. Екатеринбург
Работа в ИБ – 8 лет
CISM

План

- [ ] Обзор ГОСТ Р 57580.1-2017
- [ ] Рекомендации по выполнению первоочередных мероприятий
- [ ] Обсуждение сложных мероприятий
- [ ] Дорожная карта по реализации требований

ГОСТ Р 57580.1-2017

USSC

Основа для создания эффективной системы защиты информации

Набор лучших практик

- ✓ единая терминология
- ✓ каталог из 408 мер защиты информации
- ✓ обвязка, которая поможет определить объекты защиты, определить требуемый уровень защиты, выбрать меры защиты и способы их реализации
- ✓ методика, которая поможет оценить выбор и реализацию мер защиты в организации, итоговый уровень соответствия
- ✓ рекомендации по реализации отдельных мер*

Контуры безопасности и уровни защиты

Контур безопасности

Совокупность объектов информатизации, определяемая областью применения настоящего стандарта, используемых для реализации бизнес-процессов и (или) технологических процессов финансовой организации единой степени критичности (важности), для которой финансовой организацией применяется единая политика (режим) защиты информации (единый набор требований к обеспечению защиты информации)

Уровень защиты информации

Определенная совокупность мер защиты информации, входящих в состав системы защиты информации и системы организации и управления защитой информации, применяемых совместно в пределах контура безопасности для реализации политики (режима) защиты информации, соответствующей критичности (важности) защищаемой информации бизнес-процессов и (или) технологических процессов финансовой организации

Требования положений Банка России

683-П	Все кредитные финансовые организации	Реализация усиленного или стандартного уровня защиты Проведение оценки соответствия уровню защиты Обеспечить уровень соответствия не ниже третьего Обеспечить уровень соответствия не ниже четвертого	с 01.01.2021 с 01.01.2023
684-П	Некредитные финансовые организации	Реализация усиленного или стандартного уровня защиты Проведение оценки соответствия уровню защиты Обеспечить уровень соответствия не ниже третьего Обеспечить уровень соответствия не ниже четвертого	с 01.01.2021 с 01.01.2022 с 01.07.2023
672-П	Участники платежной системы Банка России	Реализация усиленного или стандартного уровня защиты Проведение оценки соответствия уровню защиты Обеспечить уровень соответствия не ниже четвертого	с 01.07.2021 с 06.04.2019
Приказ №321	Банки при подключении к ЕБС	Реализация стандартного уровня защиты	с 01.07.2021

Требования из НПА обеспечивать уровень защиты по ГОСТ 57580.1

USSC

	683-П	684-П	382-П (новый)	672-П	Приказ Минкомсвязи №321
Автоматизированные системы	+	+	+	+	+
Программное обеспечение	+	+	+	+	+
Средства вычислительной техники	+	+	+	+	+
Телекоммуникационное оборудования	+	+	+	+	+
.. Используемого и эксплуатируемого в целях осуществления	**Банковских операций**	**Финансовых операций**	**Переводов денежных средств**	**Переводов денежных средств**	**Идентификации с применением биометрии**

Пример меры защиты из ГОСТ Р 57580.1-2017

	Мера СЗИ	Уровень защиты информации		
		3	2	1
УЗП.21	Реализация правил управления правами логического доступа, обеспечивающих запрет совмещения одним субъектом логического доступа следующих функций: • эксплуатация и (или) контроль эксплуатации ресурса доступа, в том числе АС, одновременно с использованием по назначению ресурса доступа в рамках реализации бизнес-процесса финансовой организации; • создание и (или) модернизация ресурса доступа, в том числе АС. одновременно с использованием по назначению ресурса доступа в рамках реализации бизнес-процесса финансовой организации; • эксплуатация средств и систем защиты информации одновременно с контролем эксплуатации средств и систем защиты информации; • управление учетными записями субъектов логического доступа одновременно с управлением правами субъектов логического доступа	Н	О	Т

Меры:
Н – не применимы к уровню
О – организационные
Т – технические

Объекты и ресурсы доступа

USSC

Объект доступа

рекомендуется как минимум рассматривать:

- ✓ АРМ пользователей
- ✓ АРМ эксплуатационного персонала
- ✓ серверное оборудование
- ✓ сетевое оборудование
- ✓ СХД
- ✓ HSM
- ✓ устройства печати и копирования информации
- ✓ объекты в публичных местах (банкоматы, платежные терминалы)

Ресурс доступа

рекомендуется как минимум рассматривать:

- ✓ АС
- ✓ базы данных
- ✓ сетевые файловые ресурсы
- ✓ виртуальные машины с серверными компонентами
- ✓ виртуальные машины с АРМ пользователей
- ✓ сервисы электронной почты
- ✓ WEB-сервисы

Структурирование мер защиты информации

USSC

Процессы ЗИ \ Направления ЗИ	Выбор	Планирование	Реализация	Контроль	Совершенствование
Обеспечение защиты информации при управлении доступом	УЗП, РД, ФД, УИ	ПЗИ	РЗИ	КЗИ	СЗИ
Обеспечение защиты вычислительных сетей	СМЭ, ВСА, ЗВС, ЗБС	ПЗИ	РЗИ	КЗИ	СЗИ
Контроль целостности и защищенности информационной инфраструктуры	ЦЗИ	ПЗИ	РЗИ	КЗИ	СЗИ
Защита от вредоносного кода	ЗВК	ПЗИ	РЗИ	КЗИ	СЗИ
Предотвращение утечек информации	ПУИ	ПЗИ	РЗИ	КЗИ	СЗИ
Управление инцидентами защиты информации	МАС, РИ	ПЗИ	РЗИ	КЗИ	СЗИ
Защита среды виртуализации	ЗСВ	ПЗИ	РЗИ	КЗИ	СЗИ
Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств	ЗУД	ПЗИ	РЗИ	КЗИ	СЗИ
Защита на этапах жизненного цикла автоматизированных систем и приложений	ЖЦ				
(Рекомендуемые) Организационные меры, связанные с обработкой ПДн	Б				

Структурирование мер защиты информации

Процессы

Подпроцессы

Группы

Меры

Группа мер		Мера СЗИ	Уровень защиты информации		
			3	2	1
Регистрация событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации	ПУИ.33	Регистрация фактов стирания информации с МНИ	О	О	О

Выбор мер защиты из ГОСТ Р 57580.1-2017

1. Выбор базового состава мер

2. Адаптация выбранного состава мер с учетом модели угроз и структурно-функциональных характеристик

3. Исключение мер, не связанных с используемыми информационными технологиями

4. Дополнение мер требованиями, установленными другими НПА

5. Применение мер

Уровни соответствия ГОСТ 57580.2

Оценка процесса	Уровень соответствия
E = 0	Нулевой
0< E <=0,5	Первый
0,5< E <=0,7	Второй
0,7< E <=0,85	Третий
0,85< E <=0,9	Четвертый

План

- [x] Обзор ГОСТ Р 57580.1-2017
- [ ] Рекомендации по выполнению первоочередных мероприятий
- [ ] Обсуждение сложных мероприятий
- [ ] Дорожная карта по реализации требований

Модель угроз

Актуальная модель угроз
Охватывает контуры защиты

Соответствие между актуальными угрозами и мерами защиты из ГОСТ Р 57580.1-2017
Используется при выборе мер защиты или обосновании применения компенсирующих мер защиты

Необходимость сертифицированных СЗИ
Определение угроз, для нейтрализации которых необходимы сертифицированные СЗИ

Положение о применимости мер из ГОСТ Р 57580.1-2017

Перечень контуров безопасности
Требуемые для них уровни защиты

Выбор мер для указанных контуров
Обоснование выбора: наличие в базовом составе мер, адаптация, исключение, дополнение

Определение мер, техническая реализация которых невозможна / нецелесообразна
Обоснование невозможности или экономической нецелесообразности

Определение компенсирующих мер
Обоснование применения компенсирующей меры

Определение сертифицированных средств защиты
Зафиксировать меры, реализации которых требует применения сертифицированных средств защиты информации (когда это необходимо для нейтрализации актуальных угроз)

Реализация мер по направлению «Планирование процессов защиты информации»
(ПЗИ.1-ПЗИ.4)

Положение о применимости мер из ГОСТ Р 57580.1-2017

USSC

					Базовый состав мер защиты информации в завимости от уровня защиты			Уточнение	Исключение	Дополнение	Контуры ЗИ, для которых выбрана мера	Необходимость применения сертифицированных СЗИ	Сведения о невозможности технической реализации меры	Сведения об экономической нецелесообразности меры	
Процесс	Подпроцесс	Группа мер	Условное обозначение и номер меры	Содержание мер системы защиты информации	3	2	1	Необходима для нейтрализации угрозы	Не используемые технологии	Иные НПА	Контуры ЗИ, для которых выбрана данная мера				
Процесс 2. Обеспечение защиты вычислительных сетей	Подпроцесс "Сегментация и межсетевое экранирование вычислительных сетей"	Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.14	Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1. внутренних вычислительных сетей финансовой организации и сети Интернет	Н	Т	Т				ДБО, ЕБС, Процессинг карт				
Процесс 2. Обеспечение защиты вычислительных сетей	Подпроцесс "Сегментация и межсетевое экранирование вычислительных сетей"	Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.16	Межсетевое экранирование внутренних вычислительных сетей финансовой организации, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем. определенной 8 ГОСТ Р ИСО/МЭК 7498-1	Т	Т	Т				ДБО, ЕБС, Процессинг карт				
Процесс 2. Обеспечение защиты вычислительных сетей	Подпроцесс "Сегментация и межсетевое экранирование вычислительных сетей"	Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.17	Реализация и контроль информационного взаимодействия внутренних вычислительных сетей финансовой организации и сети Интернет в соответствии с установленными правилами и протоколами сетевого взаимодействия	Т	Т	Т				ДБО, ЕБС, Процессинг карт				
Процесс 2. Обеспечение защиты вычислительных сетей	и межсетевое экранирование вычислительных сетей"	вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.18	Сокрытие топологии внутренних вычислительных сетей финансовой организации	Т	Т	Т	**УБИ.104**			ДБО, ЕБС, Процессинг карт	**Да**			
Процесс 2. Обеспечение защиты вычислительных сетей	и межсетевое экранирование вычислительных сетей"	вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.19	Реализация сетевого взаимодействия внутренних вычислительных сетей финансовой организации и сети Интернет через ограниченное количество контролируемых точек доступа	Т	Т	Т				ДБО, ЕБС, Процессинг карт				
Процесс 2. Обеспечение защиты вычислительных сетей	Подпроцесс "Сегментация и межсетевое экранирование вычислительных сетей"	Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.20	Реализация почтового обмена с сетью Интернет через ограниченное количество контролируемых точек информационного взаимодействия, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (размещенного во внутренних сетях финансовой организации) почтовых серверов с безопасной репликацией почтовых сообщений между ними	Н	Т	Т	**УБИ.172**			ДБО, ЕБС, Процессинг карт	**Нет**			
Процесс 2. Обеспечение защиты вычислительных сетей	и межсетевое экранирование вычислительных сетей"	информации, связанных с операциями по изменению параметров защиты	СМЭ.21	Регистрация изменений параметров настроек средств и систем защиты информации. обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей финансовой организации	Т	Т	Т				ДБО, ЕБС, Процессинг карт				
Процесс 2. Обеспечение защиты вычислительных сетей	Подпроцесс "Выявление вторжений и сетевых атак"	Мониторинг и контроль содержимого сетевого трафика	ВСА.2	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между вычислительными сетями финансовой организации и сетью Интернет	Н	Т	Т				ДБО, ЕБС, Процессинг карт				
Процесс 2. Обеспечение защиты вычислительных сетей	Подпроцесс "Выявление вторжений и сетевых атак"	Мониторинг и контроль содержимого сетевого трафика	ВСА.4	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным логическим доступом к ресурсам доступа, размещенным в вычислительных сетях финансовой организации, подключенных к сети Интернет	Н	Т	Т				ДБО, ЕБС, Процессинг карт				

План реализации первой очереди мер защиты

USSC

По каждой мере защиты информации

Перечень контуров безопасности

Для которых необходима мера

Выбор способа реализации меры

Применением организационных или технических мер, встроенных или накладных СЗИ, конкретное средство

Ответственный за реализацию

Обоснование невозможности или экономической нецелесообразности

Срок реализации

Обоснование применения компенсирующей меры

Планируемый результат

Зафиксировать меры, реализации которых требует применения сертифицированных средств защиты информации (когда это необходимо для нейтрализации актуальных угроз)

План реализации первой очереди мер защиты

USSC

				Контуры ЗИ, для которых выбрана мера	Способ реализации мер защиты			Ответственный за реализацию	Планируемый результат	Срок реализации
3	Группа мер	Условное обозначение и номер меры	Содержание мер системы защиты информации	Контуры ЗИ, для которых выбрана данная мера	Технические меры защиты с использованием встроенных возможностей существующего ПО или оборудования	Дополнительные СЗИ	С применением организационных мер защиты			
100	Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.14	Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1. внутренних вычислительных сетей финансовой организации и сети Интернет	ДБО, ЕБС, Процессинг карт		FW L3		Иванов И.И.	Акт установки и настройки	01.06.2020
101	Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.16	Межсетевое экранирование внутренних вычислительных сетей финансовой организации, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем. определенной 8 ГОСТ Р ИСО/МЭК 7498-1	ДБО, ЕБС, Процессинг карт		FW L7		Иванов И.И.	Акт установки и настройки	01.07.2020
102	Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.17	Реализация и контроль информационного взаимодействия внутренних вычислительных сетей финансовой организации и сети Интернет в соответствии с установленными правилами и протоколами сетевого взаимодействия	ДБО, ЕБС, Процессинг карт		FW		Иванов И.И.	Акт установки и настройки	01.08.2020
103	Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.18	Сокрытие топологии внутренних вычислительных сетей финансовой организации	ДБО, ЕБС, Процессинг карт	Встроенные возможности АСО	FW		Иванов И.И.	Акт установки и настройки	01.09.2020
104	Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.19	Реализация сетевого взаимодействия внутренних вычислительных сетей финансовой организации и сети Интернет через ограниченное количество контролируемых точек доступа	ДБО, ЕБС, Процессинг карт	Встроенные возможности АСО	FW, VPN		Иванов И.И.	Акт установки и настройки	01.10.2020
105	Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет	СМЭ.20	Реализация почтового обмена с сетью Интернет через ограниченное количество контролируемых точек информационного взаимодействия, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (размещенного во внутренних сетях финансовой организации) почтовых серверов с безопасной репликацией почтовых сообщений между ними	ДБО, ЕБС, Процессинг карт	Встроенные возможности системы электронной почты	Mail GW		Петров П.П.	Акт установки и настройки	01.11.2020
106	Регистрация событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей	СМЭ.21	Регистрация изменений параметров настроек средств и систем защиты информации. обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей финансовой организации	ДБО, ЕБС, Процессинг карт	Встроенные возможности АСО	CMDB, система управления сетью		Иванов И.И.	Акт установки и настройки	01.12.2020
	Мониторинг и контроль содержимого сетевого		Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между вычислительными сетями финансовой организации и сетью Интернет	ДБО, ЕБС, Процессинг карт		IPS, FW			Акт установки и	

План

- [x] Обзор ГОСТ Р 57580.1
- [x] Рекомендации по выполнению первоочередных мероприятий
- [ ] Обсуждение сложных мероприятий
- [ ] Дорожная карта по реализации требований

П1. Обеспечение защиты информации при управлении доступом

Технические меры

- 2FA
- IDM и/или Система управления заявками на доступ к ресурсам и/или ЭДО
- SSO
- SIEM
- Система видеонаблюдения
- Система учета ИТ ресурсов и/или CMDB

встроенные возможности

- АС
- ОС
- СУБД
- Сетевого оборудования
- Файловых сервисов
- Систем виртуализации
- AD и/или LDAP
- BIOS и/или UEFI

Организационные меры

- Положение по управлению логическим доступом
- Распоряжение о назначении владельцев ресурсов
- Положение по управлению физическим доступом
- Учет ресурсов доступа

П2. Обеспечение защиты вычислительных сетей

USSC

Технические меры

- FW (L3 и L7)
- IPS
- VPN
- Mail GW
- AntiDDoS
- SIEM
- CMDB

встроенные возможности

- Сетевого оборудования
- Системы электронной почты
- Система управления сетью
- АС
- ОС
- СУБД
- Файловых сервисов

Организационные меры

- Положение по работе со съемными машинными носителями информации (контроль содержимого информации при ее переносе между сегментами контуров безопасности с использованием отчуждаемых носителей)

ПЗ. Контроль целостности и защищенности информационной инфраструктуры

Технические меры

- VM
- Pentest service
- Система управления обновлением ПО
- СЗИ от НСД и/или Endpoint protection
- AV
- SIEM

встроенные возможности

- АС
- ОС
- ППО
- Браузера
- СУБД
- Сетевого оборудования

Организационные меры

- Положение по управлению уязвимостями
- Порядок обновления программного обеспечения (ПО)
- Наличие эталонных копий ПО и возможности восстановления
- Перечень разрешенного для установки ПО

П4. Защита от вредоносного кода

Технические меры

- AV или Endpoint protection
- NGFW
- Web GW
- Mail GW
- SIEM

встроенные возможности

- ОС
- Браузера
- AD

Организационные меры

- Положение по антивирусной защите
- Порядок проведения предварительных проверок для устанавливаемого или изменяемого программного обеспечения
- Запрет неконтролируемого открытия самораспаковывающихся архивов и исполняемых файлов, полученных из сети Интернет

П5. Предотвращение утечек информации

Технические меры

- DLP
- Web GW
- Mail GW
- Endpoint Protection
- СЗИ от НСД
- Средство стирания информации
- SIEM

встроенные возможности

- системы электронной почты

Организационные меры

- Положение по работе со съемными машинными носителями информации (МНИ)
- Запрет обработки информации конфиденциального характера на объектах, подключенных к сети Интернет
- Регистрация фактов стирания информации с МНИ

П6. Управление инцидентами защиты информации

Технические меры

- SIEM
- VPN
- СЗИ от НСД
- NTP
- Система управления инцидентами

встроенные возможности

- АС
- ОС
- системы управления сетью
- системы мониторинга сервисов

Организационные меры

- Положение по управлению инцидентами информационной безопасности
- Формирование группы реагирования на инциденты защиты информации с перечнем ролей

П7. Защита среды виртуализации

Технические меры

- СЗИ среды виртуализации
- FW (L3 и L7)
- 2FA

встроенные возможности

- Среды виртуализации
- СХД
- Сетевого оборудования
- AD и/или LDAP

Организационные меры

- Положение по защите виртуальной инфраструктуры

П8. Защита информации при осуществлении удаленного логического доступа с мобильных устройств

Технические меры

- MDM
- 2FA
- VPN
- FW

встроенные возможности

- АС
- ОС
- СУБД
- Сетевого оборудования
- Файловых сервисов

Организационные меры

- Положение по организации удаленного доступа к ресурсам

ЗИ на этапах жизненного цикла АС

Технические меры

- Все СЗИ

встроенные возможности

- АС

Организационные меры

- Перечень защищаемой информации, планируемой к обработке в АС
- Состав и порядок применения организационных и технических мер защиты
- Запрет использования защищаемой информации в сегментах разработки и тестирования
- Регламент контроля применения мер защиты
- Сопровождение технических мер защиты в течение всего срока их использования (договоры на техническую поддержку)
- Положение по управлению уязвимостями / Порядок оперативного устранения обнаруженных уязвимостей

Сложно реализуемые технические меры

1. **Двухфакторная аутентификация**
   - ✓ П.1 РД.4 Идентификация и многофакторная аутентификация эксплуатационного персонала
   - ✓ П.1 РД.28 Регистрация персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации, реализующих многофакторную аутентификацию
   - ✓ П.1 УЗП.26 Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению техническими мерами, реализующими многофакторную аутентификацию
   - ✓ П.7 ЗСВ.9 Контроль и протоколирование доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных с реализацией двухфакторной аутентификации
   - ✓ П.8 ЗУД.5 Идентификация, двухфакторная аутентификация и авторизация субъектов доступа после установления защищенного сетевого взаимодействия, выполнения аутентификации, предусмотренной мерами ЗУД.2 и ЗУД.4

Сложно реализуемые технические меры

2. Системы управления учетными данными (IDM)

- ✓ УЗП.9 контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа
- ✓ УЗП.13 контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа
- ✓ УЗП.14 установление фактов неиспользования субъектами логического доступа, предоставленных им прав на осуществление логического доступа на протяжении установленного периода времени
- ✓ УЗП.17 реализация возможности определения состава предоставленных прав логического доступа для конкретного ресурса доступа
- ✓ УЗП.18 реализация возможности определения состава предоставленных прав логического доступа для конкретного субъекта логического доступа
- ✓ УЗП.19 и 20 определение состава ролей, реализация правил управления правами логического доступа, обеспечивающих запрет совмещения одним субъектом логического доступа определенных ролей

Сложно реализуемые технические меры

USSC

3. Межсетевое экранирование во внутренней сети (L3 и L7)

- ✓ сегменты контуров безопасности
- ✓ сегменты разработки и тестирования
- ✓ сегменты для банкоматов и платежных терминалов
- ✓ сегменты беспроводной сети
- ✓ сегменты системы виртуализации
- ✓ сегмент для проверки съёмных носителей
- ✓ сегмент мобильных устройств
- ✓ иные внутренние сегменты

4. Обнаружение вредоносного кода в межсетевом трафике

Статистика участия отдельных типов СЗИ в реализации мер

Межсетевой экран (FW)	35
Система управления событиями ИБ (SIEM)	32
Средства защиты от вредоносного кода (AV)	25
СЗИ среды виртуализации	20
Шлюз защиты электронной почты (Mail GW)	19
Система фильтрации web трафика (Web GW)	17
Система управления учетными записями (IDM)	17
Система двухфакторной аутентификации (2FA)	17
Межсетевой экран нового поколения (NGFW)	15
Система управления обновлением ПО	10
СЗИ от НСД	10
Система управления инцидентами (IRP)	8
IPS	6

Реализация организационных мер защиты

	Мера СЗИ	Уровень защиты информации		
		3	2	1
РД.26	Хранение копий аутентификационных данных эксплуатационного персонала на выделенных МНИ или на бумажных носителях	О	О	О
РД.27	Реализация защиты копий аутентификационных данных эксплуатационного персонала от несанкционированного доступа при их хранении на МНИ или бумажных носителях	О	О	О
ФД.6	Назначение для всех помещений распорядителя физического доступа	О	О	О
ФД.7	Предоставление права самостоятельного физического доступа по решению распорядителя физического доступа	О	О	О
РЗИ.10	Обеспечение возможности сопровождения технических мер защиты информации в течение всего срока их использования	Н	О	О
ЖЦ.8	Применение прикладного ПО, сертифицированного на соответствие требованиям по безопасности информации, 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	Н	О	О

Реализация организационных мер защиты

	Мера СЗИ	Уровень защиты информации		
		3	2	1
РИ.9	Выделение в составе ГРИЗИ следующих основных ролей: • руководитель ГРИЗИ, в основные функциональные обязанности которого входит обеспечение оперативного руководства реагированием на инциденты защиты информации: • оператор-диспетчер ГРИЗИ, в основные функциональные обязанности которого входит обеспечение сбора и регистрации информации об инцидентах защиты информации: • аналитик ГРИЗИ, в основные функциональные обязанности которого входит выполнение непосредственных действий по реагированию на инцидент защиты информации: • секретарь ГРИЗИ, в основные функциональные обязанности которого входит документирование результатов реагирования на инциденты защиты информации, формирование аналитических отчетов материалов	Н	О	О

План

- [x] Обзор ГОСТ Р 57580.1
- [x] Рекомендации по выполнению первоочередных мероприятий
- [x] Обсуждение сложных мероприятий
- [ ] Дорожная карта по реализации требований

Дорожная карта по реализации ГОСТ Р 57580.1-2017

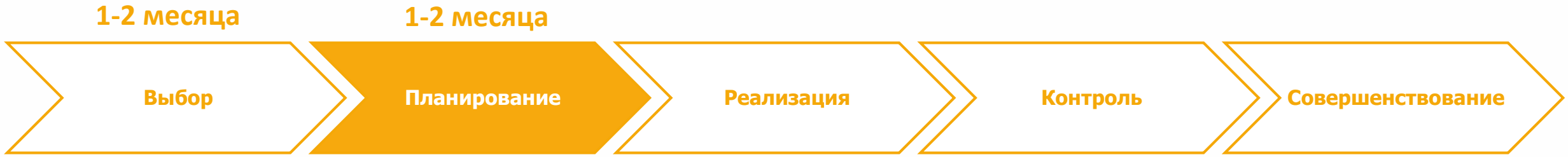
1-2 месяца

1. **Моделирование угроз**

2. **Положение о применимости мер из ГОСТ Р 57580.1-2017**

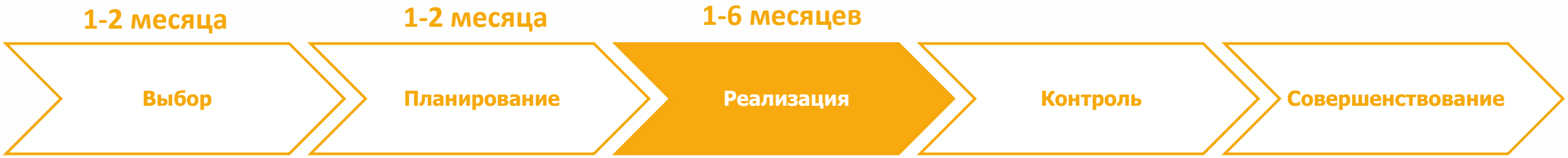
3. **Политика ИБ**

Дорожная карта по реализации ГОСТ Р 57580.1-2017



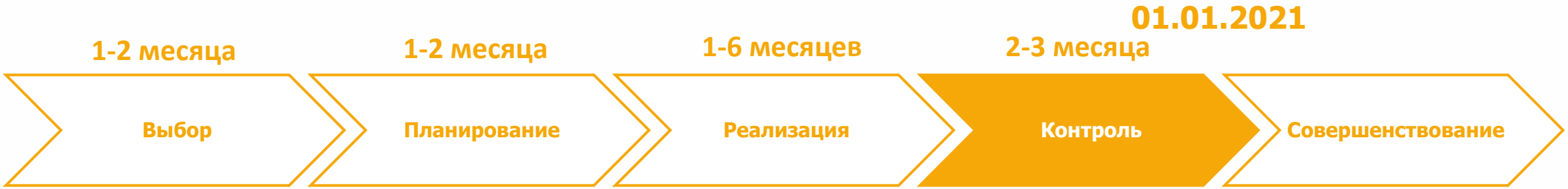
1. **Самооценка и GAP-анализ**
2. **Планы реализации первого этапа мер**

Дорожная карта по реализации ГОСТ Р 57580.1-2017



Реализация первого этапа мер

Дорожная карта по реализации ГОСТ Р 57580.1-2017



Провести оценку уровня соответствия

с привлечением лицензиатов
ФСТЭК России

Наши предложения для финансовых организаций

USSC

Оценка соответствия требованиям ГОСТ Р 57580

Тестирование на проникновение

Анализ уязвимостей по ОУД

Онлайн-сервис дистанционной оценки соответствия ГОСТ Р 57580

Комплексные аудиты

Предварительный аудит и приведение в соответствие с требованиями регуляторов

О компании

Опыт

Специалисты компании УЦСБ выполняют проекты в области информационной безопасности более 10 лет

Сертификации

Проектная команда - сотрудники с высшим профессиональным образованием по направлению подготовки 090100 «Информационная безопасность», имеющие сертификаты:

- Certified Information Systems Auditor (CISA);
- Certified Information Systems Security Professional (CISSP);
- Certified Information Security Manager (CISM);
- Cisco Certified Internetwork Expert (CCIE);
- Ethical Hacking and Penetration Testing (CEH);
- Computer Hacking Forensic Investigator (CHFI);
- Offensive Security Certified Professional (OSCP);
- Offensive Security Certified Expert (OSCE);

О компании

Уральский центр систем безопасности (УЦСБ) – компания-эксперт в области безопасного использования информационных технологий. С 2007 года компания непрерывно развивается, наращивает компетенции и выполняет все более сложные проекты.

Компетенции

Информационные технологии

Комплексы инженерно-технических средств охраны

Анализ защищенности

Сервисное обслуживание

Информационная безопасность

Информационные инфраструктуры

Безопасность промышленных систем автоматизации и управления

USSC.RU

620100, г. Екатеринбург, ул. Ткачей, д. 6

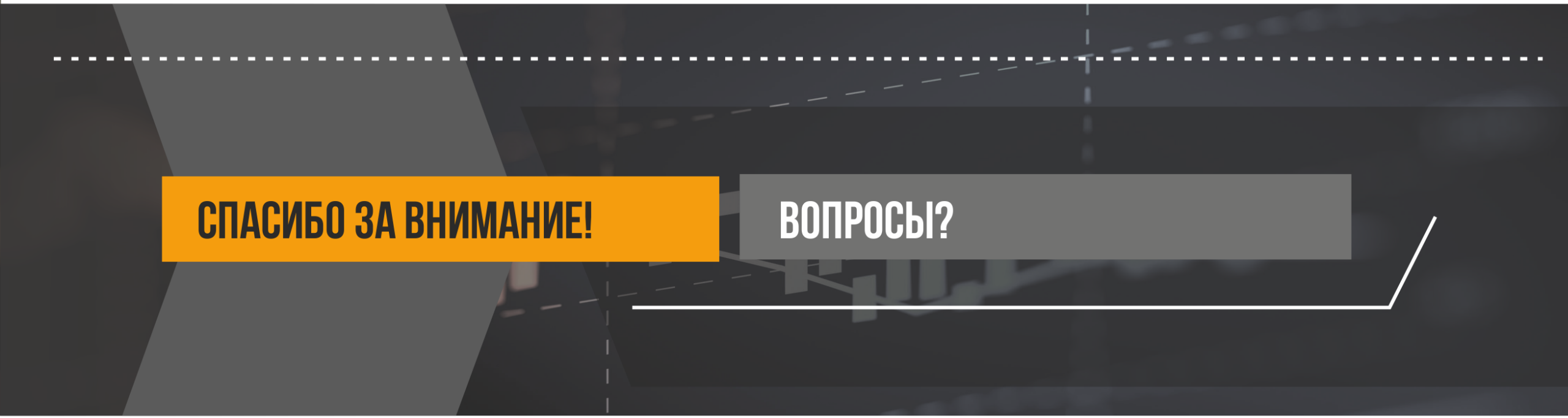
620100, г. Екатеринбург, ул. Ткачей, д. 23

Тел.: +7 (343) 379-98-34,

e-mail: info@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ

USSC



СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

НОВЫЙ СЕЗОН ВЕБИНАРОВ:

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Борисов Сергей

Обособленное подразделение в г. Краснодар

sborisov@ussc.ru

Лейчук Диана

Аналитический центр

dleichuk@ussc.ru