



**Требования Банка России
по информационной безопасности
для некредитных финансовых
организаций.
Обзор 684-П**

**Сергей Борисов
Диана Лейчук**

№	Дата	Название
1	15.04	Требования Банка России по информационной безопасности некредитных финансовых организаций
2	22.04	Требования Банка России по информационной безопасности кредитных финансовых организаций
3	29.04	Анализ уязвимостей по требованиям к ОУД4
4	20.05	Обзор требований ГОСТ Р 57580.1-2017
5	17.06	Как проводится аудит по ГОСТ Р 57580?
6	15.07	Пентесты для финансовых организаций
7	19.08	Биометрия в финансовых организациях
8	16.09	Требования к средствам криптографической защиты информации в финансовых организациях
9		Онлайн-сервис оценки соответствия ГОСТ Р 57580.2-2018

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

- Устанавливает требования ИБ для некредитных финансовых организаций
- В случае неисполнения требований – предписание Банка России
- В случае не устранения нарушений, указанных в предписании, – предусмотренная законом ответственность

- организации, на которые распространяется 684-П
- системы, на которые распространяется 684-П
- основные требования 684-П
- дорожная карта по выполнению 684-П

Организации, на которые распространяется 684-П

	Усиленный уровень	Центральный контрагент	Центральный депозитарий
Специальные + общие требования	Стандартный уровень	Организаторы торговли	Репозитарии
		Клиринговые организации	Специализированные депозитарии ИФ, ПИФ, НПФ
		<i>Профессиональные участники рынка ценных бумаг (брокеры, дилеры, депозитарии, регистраторы, управляющие)*</i>	<i>Негосударственные пенсионные фонды*</i>
		<i>Страховые организации*</i>	
Общие требования	Нет обязанности реализовать уровень защиты	Актуарии	Управляющие компании ИФ, ПИФ, НПФ
		Микрофинансовые организации	Кредитные рейтинговые агентства
		Кредитные потребительские кооперативы	С/х кредитные потребительские кооперативы
		Акционерные инвестиционные фонды	Жилищные накопительные кооперативы
		Оператор инвестиционной платформы	Бюро кредитных историй
		Ломбарды	

Все системы, в которых обрабатывается следующая информация:



электронные сообщения



криптографические ключи



информация об осуществленных
финансовых операциях



информация, необходимая
для авторизации клиентов

1. Доведение до клиентов рекомендаций:

- по защите информации от воздействия вредоносного кода
- о возможных рисках несанкционированного доступа (НСД)
- о мерах по предотвращению НСД

Организация **самостоятельно** принимает решение о способе и периодичности доведения информации.

Варианты:

- приложение к договору
- рассылка на электронные адреса
- размещение на сайте организации
- периодическая sms-рассылка

Рекомендуется фиксировать факт ознакомления клиентов с рекомендациями

2. Требования к средствам криптографической защиты информации (СКЗИ):

- эксплуатация СКЗИ в соответствии с технической документацией
- применение СКЗИ, сертифицированных ФСБ России

Вебинар:

16.09	Требования к средствам криптографической защиты информации в финансовых организациях
-------	--

3. Определение организацией применимого к ней в течение календарного года уровня защиты информации, определенного в ГОСТ Р 57580.1-2017 (с 01.01.2021):

- решение должно быть задокументировано
- решение должно приниматься ежегодно

организации, которым не предписано реализовывать усиленный или стандартный уровень защиты информации, могут принять решение **об отсутствии необходимости** применения одного из уровней защиты

Специальные + общие требования	Усиленный уровень	Центральный контрагент	Центральный депозитарий
	Стандартный уровень	Организаторы торговли	Репозитарии
		Клиринговые организации	Специализированные депозитарии ИФ, ПИФ, НПФ
		<i>Профессиональные участники рынка ценных бумаг (брокеры, дилеры, депозитарии, регистраторы, управляющие)*</i>	<i>Негосударственные пенсионные фонды*</i>
Общие требования	Нет обязанности реализовать уровень защиты	<i>Страховые организации*</i>	
		Актуарии	Управляющие компании ИФ, ПИФ, НПФ
		Микрофинансовые организации	Кредитные рейтинговые агентства
		Кредитные потребительские кооперативы	С/х кредитные потребительские кооперативы
		Акционерные инвестиционные фонды	Жилищные накопительные кооперативы
		Оператор инвестиционной платформы	Бюро кредитных историй
		Ломбарды	

1. Сертифицированное прикладное ПО или ПО, в отношении которого проведен анализ уязвимостей к ОУД4:

- ПО, распространяемое клиентам для осуществления финансовых операций
- ПО, обрабатывающее защищаемую информации при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием сети Интернет

Сертификация – в системе сертификации ФСТЭК России

Анализ уязвимостей – самостоятельно или с привлечением организации-лицензиата ФСТЭК России

2. Тестирование на проникновение

Вебинары:

29.04	Анализ уязвимостей по требованиям к ОУД4
15.07	Пентесты для финансовых организаций

3. Подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить составление уполномоченным на это лицом

- усиленная квалифицированная электронная подпись
 - усиленная неквалифицированная электронная подпись
 - простая электронная подпись
- } условия их использования отражать в договорах с клиентами

4. Реализация технологии безопасной обработки защищаемой информации

5. Информирование Банка России об инцидентах защиты информации

СТО БР БФБО-1.5-2018

Основной канал:

- АСОИ ФинЦЕРТ (<https://lk.fincert.cbr.ru>)

Резервные каналы:

- электронная почта (fincert@cbr.ru);
- телефонный звонок в Банк России (+7 495 7 727 090)

6. Хранение электронных сообщений и информации об осуществленных финансовых операциях – не менее 5 лет

7. Оценка соответствия уровня защиты информации по ГОСТ Р 57580.2-2018 (с 01.01.2021):

- с привлечением лицензиатов
- не реже одного раза в год / три года
- хранение отчета по результатам оценки – не менее 5 лет

8. Уровень соответствия – не ниже третьего (01.01.2022 – 30.06.2023)

9. Уровень соответствия – не ниже четвертого (с 01.07.2023)

Вебинары:

20.05	Обзор требований ГОСТ Р 57580.1-2017
17.06	Как проводится аудит по ГОСТ Р 57580?



с 01.06.2019

Формирование и доведение до клиентов рекомендаций



с 01.01.2021 - ежегодно

Решение о применении к организации уровня защиты информации

Сертифицированное ПО /
анализ уязвимостей к ОУД 4

с 01.01.2020

Уровень соответствия ≥ 3
(по ГОСТ Р 57580.2-2018)

с 01.01.2022

с 01.06.2019

с 01.01.2021

с 01.07.2023

Формирование и доведение до
клиентов рекомендаций

Подписание электронных
сообщений

Технология безопасной обработки
защищаемой информации

Регистрация инцидентов ИБ и
информирование о них Банка России

Решение о применении
к организации уровня
защиты информации (ежегодно)

Тестирование на
проникновение

Оценка уровня соответствия
требованиям к уровню защиты,
реализованного по ГОСТ Р 57580.1
(не реже одного раза в год / три года)
с привлечением лицензиатов ФСТЭК России



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

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

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

НОВЫЙ СЕЗОН ВЕБИНАРОВ:

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ
ОРГАНИЗАЦИЙ

Лейчук Диана

Аналитический центр
dleichuk@ussc.ru

Борисов Сергей

Обособленное подразделение
в г. Краснодар
sborisov@ussc.ru