# СПРАВОЧНАЯ ИНФОРМАЦИЯ

**Краткий справочник по нормативным актам**

- **161-ФЗ** Федеральный закон «О национальной платежной системе» от 27.06.2011 N 161-ФЗ.
- **ГОСТ 57580.1- 2017** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер». ГОСТ БР по информационной безопасности. Определяет базовый состав организационных и технических мер защиты информации.
- **ГОСТ 57580.2-2018** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия». Устанавливает требования к методике и оформлению результатов оценки соответствия защиты информации финансовой организации при выборе и реализации организационных и технических мер в соответствии с требованиями ГОСТ 57580.1.
- **№ 719-П** положение Банка России от 4 июня 2020 г. «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».
- **№ 802-П** положение Банка России от 23 декабря 2020 г. «О требованиях к защите информации в платежной системе Банка России».
- **№ 321-П** положение Банка России от 29.08.2008 (ред. от 27.09.2017) «О порядке представления кредитными организациями в уполномоченный орган сведений, предусмотренных Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»».
- **№ 757-П** положение ЦБ РФ от 20.04.2021 «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».
- **№ 930** приказ Минцифры России «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации».
- **Указ Президента РФ №250 от 1 мая 2022 г.:** Что нужно делать организациям в связи с выходом Указа?
  - Установить определённую структуру ответственности за обеспечение ИБ.
  - Создать структурное подразделение, ответственное за обеспечение ИБ, либо возложить такие функции на существующее подразделение.
  - Выполнить другие мероприятия по ИБ.

## ARinteg ПРЕДОСТАВЛЯЕТ УСЛУГИ СОПРОВОЖДЕНИЯ ПРОЦЕССОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:


- экспертный анализ в области информационной безопасности;
- проведение периодических проверок процессов информационной безопасности с целью определения их эффективности и выработку рекомендаций по улучшению;
- поддержка в актуальном состоянии организационно-распорядительной документации;
- техническая поддержка в части эксплуатации средств защиты информации.

## ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «УЧЕТ ПЕРСОНАЛЬНЫХ ДАННЫХ»

Сертификат

1С совместимо! система программ 1С:ПРЕДПРИЯТИЕ

Дополнение к конфигурации «Учет персональных данных», разработанное компанией ARinteg для платформы 1С: ЗУП, предназначено для ведения документов необходимых при обработке персональных данных, в соответствии с требованиями Федерального закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ.

ISO

**Сертификат соответствия системы менеджмента качества стандарту ISO 9001:2015 (ГОСТ Р ISO 9001-2015)**


**г. Москва**, ул. Радио, 24к1 БЦ «Яуза-Тауэр», офис 107
**+7 (495) 221-21-41**

**г. Санкт-Петербург**, ул. Большая Конюшенная, 27, БЦ «Медведь», офис 528
**+7 (812) 407-34-71**

**г. Ростов-на-Дону**, ул. Береговая, 8, БЦ «Риверсайд-Дон», офис 808
**+7 (812) 407-34-71**

www.ARinteg.ru
vk.com/club211130645
t.me/ARinteg


ARinteg

ВАШ ГАРАНТ **ИНФОРМАЦИОННОЙ** БЕЗОПАСНОСТИ

Защищаем с 1996 года

# ЛЁГКИЙ СПОСОБ ПРОЙТИ АУДИТ

## ПОШАГОВАЯ ИНСТРУКЦИЯ

**Шаг 1**

| Вид деятельности организации (ОКВД) | 187-ФЗ (КИИ)[1] | 152-ФЗ (ПДн)[2] | 719-П | 747-П[3] | 683-П | 930[4] | 757-П |
|---|---|---|---|---|---|---|---|
| Связь | + | + | | | | | |
| Оборонная промышленность | + | + | | | | | |
| Здравоохранение | + | + | | | | | |
| Транспорт | + | + | | | | | |
| Атомная энергетика | + | + | | | | | |
| Энергетика | + | + | | | | | |
| Топливно энергетический комплекс | + | + | | | | | |
| Химическая промышленность | + | + | | | | | |
| Ракетно-космическая промышленность | + | + | | | | | |
| Банковская и финансовая сфера | + | + | + | + | + | + | + |
| Горнодобывающая промышленность | + | + | | | | | |
| Металлургическая промышленность | + | + | | | | | |
| Наука | + | + | | | | | |
| Прочие кредитные организации, имеющие действующую лицензию ЦБ РФ, не являющиеся банками и НКО | + | + | | | | + | |
| Любые организации, обрабатывающие персональные данные, не связанные с заключенными трудовыми договорами | | + | | | | | + |
| Организации, осуществляющие обработку ПДн, включая сбор и хранение параметров биометрических персональных данных для идентификации | | + | | | | | |

[1] Необходимо своевременно подавать сведения обо всех изменениях по объектам КИИ.

[2] С учетом изменений, внесенных 266-ФЗ от 14.07.2022 г.

[3] Также подаются сведения при изменении роли КО, по запросу ЦБ, по инициативе руководства организации.

[4] Приказ 930 Минцифры относится только к кредитным организациям, в которых есть подключение к ЕБС (Единой Биометрической Системе)

# КАЛЕНДАРНЫЙ ПЛАН

**Шаг 2**

| | Виды работы | Раз в год | Раз в 2 года | Самооценка | Требования к внешнему подрядчику |
|---|---|---|---|---|---|
| 187-ФЗ | Исполнение нормативных требований по защите КИИ | - | - | Да | - |
| 152-ФЗ | Исполнения требования по защите ПДн | - | - | Да | - |
| 719-П | Оценка исполнения требований Положения Банка России 719- П с применением ГОСТ Р 57580 | - | Да | Нет | Лицензия ФСТЭК России |
| | Тестирование на проникновение и анализ уязвимостей | Да | | | |
| 930 | Оценка исполнения требований Приказа Минсвязи России 930 с применением ГОСТ Р 57580 | Да | - | Нет | Лицензия ФСТЭК России |
| 802-П | Оценка исполнения требований Положения Банка России 802- П с применением ГОСТ Р 57580 | - | Да | Нет | Лицензия ФСТЭК России |
| 683-П | Оценка исполнения требований Положения Банка России 683- П с применением ГОСТ Р 57580 | | Да | Нет | Лицензия ФСТЭК России |
| | Тестирование на проникновение и анализ уязвимостей | Да | - | Нет | |
| 757-П (тип 1) | Тестирование на проникновение и анализ уязвимостей | Да | - | Нет | Лицензия ФСТЭК России |
| | Оценка исполнения требований Положения Банка России 757- П с применением ГОСТ Р 57580 | Нет | Да | Нет | |
| 757-П (тип 2) | Тестирование на проникновение и анализ уязвимостей | Да | - | Нет | Лицензия ФСТЭК России |
| | Оценка исполнения требований Положения Банка России 757- П с применением ГОСТ Р 57580 | Нет | Да | Нет | |

# ОТВЕТСТВЕННОСТЬ

| | |
|---|---|
| 152-ФЗ | **Штраф.** Взыскивается за каждый случай.<br>Например, в организации штат 100 работников, обработка их персональных данных осуществляется без «Согласия на обработку ПДн». При проверке Роскомнадзор может применить санкции по невыполнению ст. 9 ФЗ-152 по каждому случаю.<br>Итог – 75 000 руб. (штраф) * 100 (штат организации) = 7 500 000 руб. |
| 187-ФЗ | **Штраф** на должностное лицо - от 10 000 до 50 000 руб. (административная ответственность) |
| | **Штраф** на юридическое лицо - от 50 000 до 500 000 руб. (административная ответственность) |
| | Уголовная ответственность: лишение свободы на срок до 10 лет, принудительные работы на срок до 5 лет, штраф до 1000000 рублей, запрет на занятия определенной деятельностью на срок до 5 лет. |
| 719-П | Возможно получение предписания регулятора |
| 802-П | Возможно получение предписания регулятора, при нарушении - отключение от ПС БР |
| 683-П | Возможно получение предписания регулятора |
| 757-П | Возможно получение предписания регулятора |

# ИСПОЛНЕНИЕ НОРМАТИВНЫХ ТРЕБОВАНИЙ ПО ЗАЩИТЕ КИИ

| Срок | Действия |
|---|---|
| По уже имеющимся ОКИИ | |
| До 1 сентября 2019 года | Утвердить перечень ОКИИ, подлежащих категорированию |
| До 13 сентября 2019 года | Подать перечень ОКИИ во ФСТЭК в печатном и электронном виде |
| До 1 сентября 2020 года (в течение года со дня утверждения субъектом КИИ перечня ОКИИ) | Провести категорирование ОКИИ |
| До 15 октября 2020 года | Подать сведения во ФСТЭК, если категорирование проведено 1 сентября 2020 года |
| По вновь создаваемым ОКИИ | |
| В течение 10 рабочих дней после утверждения требований к создаваемому ОКИИ (акты) | • Сведения об ОКИИ<br>• Сведения о субъекте КИИ<br>• Сведения о взаимодействии ОКИИ и сетей электросвязи<br>• Категорию значимости |
| В течение 10 рабочих дней после ввода в эксплуатацию ОКИИ | • Сведения о лице, эксплуатирующем ОКИИ<br>• Сведения о программных и программно-аппаратных средствах, используемых на ОКИИ<br>• Сведения об угрозах безопасности информации и о категориях нарушителей в отношении ОКИИ<br>• Возможные последствия в случае возникновения компьютерных инцидентов на ОКИИ<br>• Организационные и технические меры, применяемые для обеспечения безопасности ОКИИ |
| - Не реже чем один раз в 5 лет<br>- При изменении показателей критериев значимости ОКИИ или их значений | Пересмотр установленных категорий значимости |

# ПРЕДЛОЖЕНИЕ ПО АУДИТУ ОТ КОМПАНИИ ARinteg

**Шаг 3**

| | |
|---|---|
| 152-ФЗ | • Сбор и анализ информации о процессах обработки персональных данных ИСПДн. (Информационная система персональных данных).<br>• Разработка модели угроз и модели нарушителя.<br>• Разработка ОРД, включая заявку в РКН и актуализация информации в РКН.<br>• Проектирование системы защиты ПДн. Документирование системы защиты ПДн.<br>• Предоставление рекомендаций по процессам обработки и защиты ПДн. |
| 187-ФЗ | • Подготовка перечня объектов КИИ, подлежащих категорированию, для представления в уполномоченный федеральный орган исполнительной власти (ФСТЭК России).<br>• Категорирование объектов КИИ в соответствии с требованиями законодательства.<br>• Формирование плана работ, включающего в себя организационные и технические меры по выполнению 187-ФЗ и созданию системы безопасности значимых объектов КИИ.<br>• Создание систем безопасности значимых объектов КИИ и выполнение требований по обеспечению безопасности значимых объектов КИИ. |
| 719-П | • Проведение аудита соответствия состояния обеспечения информационной безопасности банка.<br>• По результатам проведения аудита соответствия - подготовка отчета о соответствии состояния обеспечения информационной безопасности организации.<br>• Проведение анализа расхождений состояния обеспечения информационной безопасности банка с требованиями Положения № 719-П. По результатам проведенного анализа расхождений (в случае наличия расхождений) разработка (доработка) комплекса организационно-распорядительной и нормативной документации для приведения организации в соответствие требованиям Положения № 719-П.<br>• По результатам проведения аудита соответствия - подготовка отчетных документов, с учетом всех дополнительных указаний ЦБ России. |
| 802-П | Предаудит, выработка рекомендаций по улучшению соответствия требованиям ГОСТ Р 57580.1-2017, аудит по методике ГОСТ 57580.2-2018 сегмента ПС БР (платежной системы Банка России). |
| 683-П | Предаудит, выработка организационно- технических рекомендаций по улучшению соответствия требованиям ГОСТ Р 57580.1-2017, аудит по методике ГОСТ 57580.2-2018 информационной инфраструктуры кредитной организации. |
| 757-П | Предаудит, выработка организационно- технических рекомендаций по улучшению соответствия требованиям ГОСТ Р 57580.1-2017, аудит по методике ГОСТ 57580.2-2018 информационной инфраструктуры некредитной финансовой организации. |