СПРАВОЧНАЯ ИНФОРМАЦИЯ

Краткий справочник по нормативным актам

- **Федеральный закон от 29.07.2004 № 98-ФЗ** «О коммерческой тайне». Закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.
- **Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023)** «О персональных данных». Законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой операторами с использованием средств автоматизации или без использования таких средств. Целью закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
- **Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023)** «О безопасности критической информационной инфраструктуры Российской Федерации». Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.
- **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.
- **Положение Банка России № 719-П** 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».
- **Положение Банка России № 757-П** от 20 апреля 2021 г. «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».
- **Положение Банка России № 802** от 25 июля 2022 г. «О требованиях к защите информации в платежной системе Банка России».
- **ГОСТ Р 57580.1-2017** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер». ГОСТ БР по информационной безопасности. ГОСТ Р 57580.1, определяет базовый состав организационных и технических мер защиты информации.
- **ГОСТ Р 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.
- **ГОСТ Р ИСО/МЭК 27001-2021** «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Настоящий стандарт подготовлен с целью установления требований по созданию, внедрению, поддержке и постоянному улучшению системы менеджмента информационной безопасности. Решение о внедрении системы менеджмента информационной безопасности является стратегическим решением организации.

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»

1С совместимо! система программ 1С:ПРЕДПРИЯТИЕ

Модуль «Учет персональных данных», совместимый с системой программ «1С:Предприятие 8.3», предназначен 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. Ростов-на-Дону, ул. Береговая, 8, БЦ «Риверсайд-Дон», офис 808 — **+7 (863) 320-09-60**

г. Кемерово, пр-кт Октябрьский, 2 «Б», БЦ «Маяк-Плаза», офис 902/8 — **+7 (384) 221-56-41**

г. Новосибирск, ул. Инская, д. 69/1, «БЦ на Инской», офис 202 — **+7 (495) 221-21-41, доб. 2301**

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

Отрасль (по ОКВЭД)	187-ФЗ (КИИ)	152-ФЗ (ПДн)	Положения БР*	98-ФЗ	ИСО/МЭК 27001
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	+	+	–	+	+

* Положения Банка России (683-П, 719-П, 757-П, 802-П) включая ГОСТ Р 57580

КАЛЕНДАРНЫЙ ПЛАН

Шаг 2

	Вид работы	Периодичность	Самооценка	Требования к внешнему подрядчику
98-ФЗ	Исполнение нормативных требований по защите коммерческой тайны	—	Да	—
152-ФЗ	Исполнения требования по защите ПДн	1 раз в 3 года	Да	Лицензия ФСТЭК России
187-ФЗ	Исполнение нормативных требований по защите КИИ	1 раз в 5 лет	Да	Лицензия ФСТЭК России
Положения Банка России (683-П, 719-П, 757-П, 802-П)	Анализ исполнения требований положений Банка России	—	Да	Лицензия ФСТЭК России
	Проведение оценки соответствия защиты информации по ГОСТ Р 57580	1 раз в 2 года*	Нет	
	Тестирование на проникновение и анализ уязвимостей	1 раз в год**	Нет	
ГОСТ Р ИСО/МЭК 27001	Оценка исполнения требований к системе менеджмента (управления) информационной безопасности	—	Да	—

* Для 757-П 1 раз в год для усиленного уровня защиты и 1 раз в 3 года для стандартного уровня защиты

** Для 802-П тестирование на проникновение не требуется

ЭТАПЫ ПРОВЕДЕНИЯ АУДИТА

1 ПОДГОТОВИТЕЛЬНЫЙ ЭТАП

Определяются цели и задачи аудита, границы и глубина оценки, а также формируется команда, которая будет проводить аудит.

2 ОБСЛЕДОВАНИЕ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ

Аудиторы осуществляют сбор и систематизацию данных о том, как информация обрабатывается в рассматриваемых бизнес-процессах. Аудиторы проводят интервью с сотрудниками, участвующими в обработке информации, инвентаризацию технических и программных средств, используемых для генерации, хранения и передачи информации и осуществляют сбор данных о системе защиты информации, изучают документацию, а также проводят интервью с сотрудниками, ответственными за информационную безопасность.

3 АНАЛИЗ СОБРАННОЙ ИНФОРМАЦИИ

Аудиторы анализируют собранную информацию и оценивают эффективность системы защиты информации.

4 ПРОВЕРКА СООТВЕТСТВИЯ ЗАКОНОДАТЕЛЬСТВУ И СТАНДАРТАМ

Проводится проверка соответствия системы защиты информации законодательству и стандартам безопасности.

5 ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ И ВОЗМОЖНЫХ УГРОЗ БЕЗОПАСНОСТИ

Аудиторы выявляют уязвимости и возможные угрозы безопасности системы защиты информации, разрабатывают «Модель угроз и нарушителя».

6 ПОДГОТОВКА ОТЧЕТНЫХ ДОКУМЕНТОВ

По результатам аудита составляются отчетные документы, в которых указываются выявленные уязвимости и возможные угрозы безопасности, а также выдаются рекомендации по совершенствованию системы защиты информации.

ОТВЕТСТВЕННОСТЬ

98-ФЗ	**Штраф на юридическое лицо: от 100 000 руб. до 200 000 руб.** (административная ответственность) **Уголовная ответственность:** Штраф в размере до 1 500 000 руб. или в размере заработной платы или иного дохода осужденного за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо принудительными работами на срок до 5 лет, либо лишением свободы на тот же срок (при тяжких последствиях – принудительные работы на срок до 5 лет либо лишение свободы на срок до 7 лет).
152-ФЗ	**Штраф на юридические лицо: от 60 000 руб. до 18 000 000 руб.** (административная ответственность) **Уголовная ответственность:** Штраф в размере до 500 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 5 лет, либо лишением свободы на тот же срок.
187-ФЗ	**Штраф на юридическое лицо: от 50 000 руб. до 500 000 руб.** (административная ответственность) **Уголовная ответственность:** штраф до 1 000 000 руб. и/или ограничение/лишение свободы на срок до 8 лет (до 10 лет при тяжких последствиях).
Положения Банка России	В соответствии с Федеральным законом «О Центральном банке Российской Федерации (Банке России)» от 10.07.2002 № 86-ФЗ несоблюдение требований может привести к приостановке деятельности, замене руководства организации, штрафу до 0,1% от уставного капитала и т.д.

ПРЕДЛОЖЕНИЕ ПО АУДИТУ ОТ КОМПАНИИ ARINTEG

98-ФЗ	• Обследование компании на наличие информации, составляющей коммерческую тайну. • Разработка проектов документов, необходимых для ввода и поддержания режима коммерческой тайны.
152-ФЗ	• Сбор и анализ информации о процессах обработки персональных данных и их защите. • Разработка модели угроз и нарушителей. • Разработка ОРД, включая уведомление в РКН, и актуализация информации в РКН. • Разработка проектов согласий на обработку Пдн. • Предоставление рекомендаций по процессам обработки и защиты ПДн.
187-ФЗ	• Выявление критических процессов и подготовка перечня объектов КИИ, подлежащих категорированию, для предоставления в уполномоченный федеральный орган исполнительной власти (ФСТЭК России). • Категорирование объектов КИИ в соответствии с требованиями законодательства. • Формирование плана работ, включающего в себя организационные и технические меры по выполнению № 187-ФЗ и созданию системы безопасности значимых объектов КИИ. • Оценка мер защиты для значимых объектов КИИ на соответствие установленным требованиям. • Предоставление рекомендаций по построению системы безопасности значимых объектов КИИ и выполнения требований по обеспечению безопасности значимых объектов КИИ. • Разработка модели угроз и нарушителей.
Положения Банка России	• Оценка выполнения требований положений Банка России в соответствии с методическими рекомендациями Банка России от 02.11.2022 г. № 12-МР «По расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в целях составления отчетности об оценке выполнения требований к обеспечению защиты информации».
ГОСТ Р 57580	• Предварительная оценка соответствия требованиям ГОСТ Р 57580.1-2017 с предоставлением организационно-технических рекомендаций по улучшению соответствия требованиям ГОСТ Р 57580.1-2017. • Итоговая оценка соответствия по методике ГОСТ 57580.2-2018.
ГОСТ Р ИСО/МЭК 27001	• Оценка соответствия системы менеджмента (управления) информационной безопасностью требованиям ГОСТ Р ИСО/МЭК 27001. • Предоставление рекомендаций по приведению в соответствие СУИБ требованиям ГОСТ Р ИСО/МЭК 27001. • Подготовка проектов ОРД в области ИСО/МЭК 27001.