Вебинар по Информационной безопасности

для образовательных организаций

Терехова Маргарита

Специалист Астрал. Безопасность

t.me/margoshater

tmv@astral.ru

АО «Калуга Астрал»

15 лет

на рынке информационной безопасности

100%

успешное прохождение проверок контролирующими органами

80+

лицензий и сертификатов на осуществление деятельности

70+

компаний-вендоров в нашем brand-листе

32 000+

реализованных проектов

ТОП-30

CNews и Tadviser. Крупнейшие компании России в сфере ИБ

ТОП-3

Magic People IT Channel Awards 2020. В номинации «Антикризисная команда»

Направления «Астрал. Безопасность»

1. Защита персональных данных
2. Защита конфиденциальной информации
3. Защита государственной тайны
4. Защита коммерческой тайны
5. Защита объектов КИИ
6. Поставка средств защиты информации
7. Проведение пентестов
8. Импортозамещение
9. Аудит информационной безопасности
10. Разработка информационных систем
11. Внедрение системы видеонаблюдения
12. Обучение в области информационной безопасности
13. Организация защищенного удаленного рабочего места
14. Подключение к корпоративному центру мониторинга ГосСОПКА
15. Аттестация государственных информационных систем (ГИС)

Будьте в курсе последних новостей

is.astral.ru

vk.com/is.astral

t.me/is_astral

План вебинара:

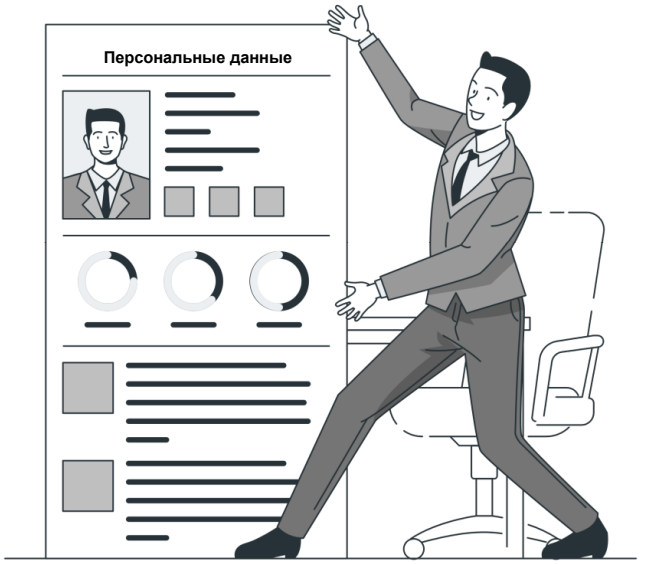
1. Информационная безопасность
2. информационные системы
3. Аттестация или Оценка эффективности?
4. Импортозамещение

Основные понятия

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.

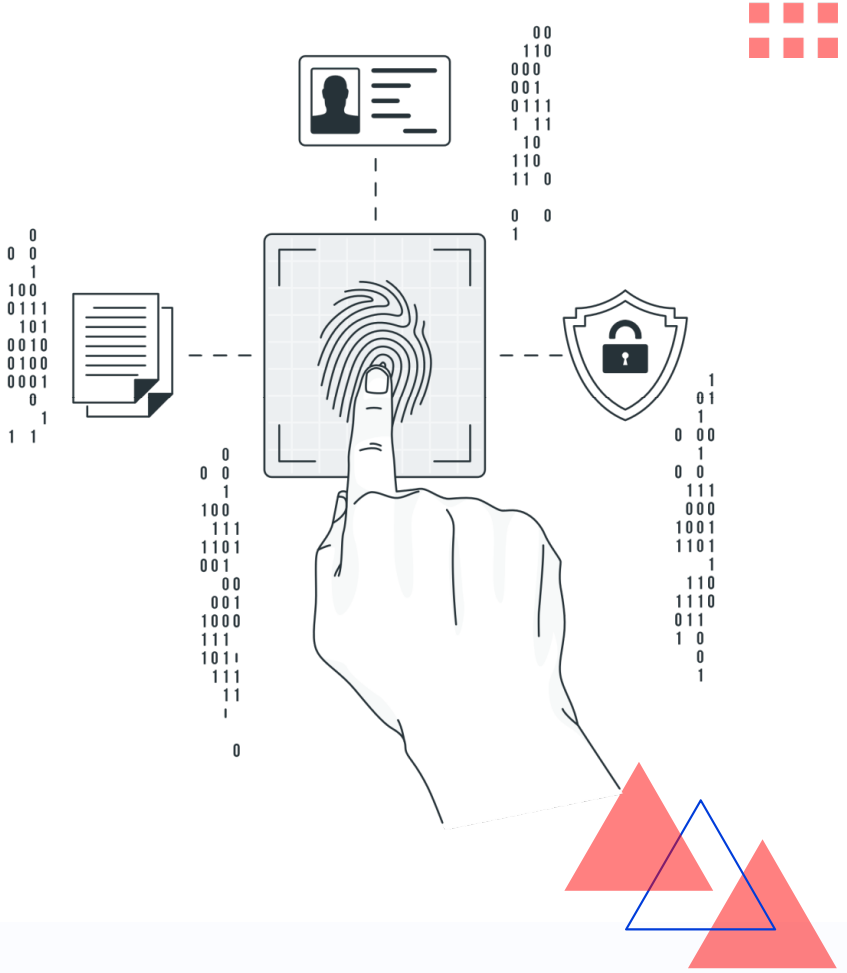
От 27.07.2006 N 152-ФЗ «О персональных данных»

Персональные данные — это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. Главное условие — по этим данным должно быть возможно однозначно определить, к какому конкретно человеку она относится.



От 27.07.2006 N 152-ФЗ «О персональных данных»

оператор персональных данных — это государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.



Основные понятия

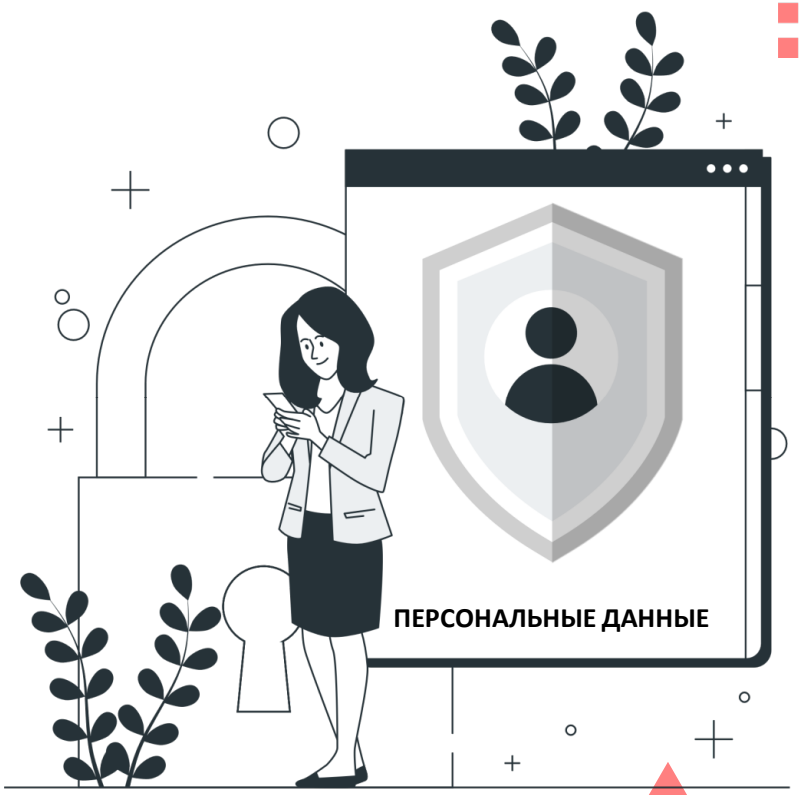
Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств (согласно ФЗ-152).

Нормативные документы регламентирующие обработку и защиту ПДн.

1	**Приказ ФСТЭК №21**	Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных
2	**ПРИКАЗ ФСТЭК от 11 февраля 2013 г. N 17**	Об утверждении требований о защите информации, не составляющих гос. тайну, содержащейся в государственных информационных
3	**Приказ ФСБ России от 10 июля 2014 г. № 378**	Описывает состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах

Защита персональных данных.

Защита персональных данных — это комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определённому или определяемому на основании такой информации физическому лицу



Проверяющие органы:

1. **Роскомнадзор**
2. **ФСТЭК**
3. **ФСБ**

Меры по оценке соответствия.

Существует две формы проведения мероприятий по оценке соответствия системы защиты ПДн требованиям по защите информации:

Оценка эффективности реализованных в рамках системы защиты ПДн мер по обеспечению безопасности ПДн

Аттестация ИСПДн на соответствие требованиям по защите информации

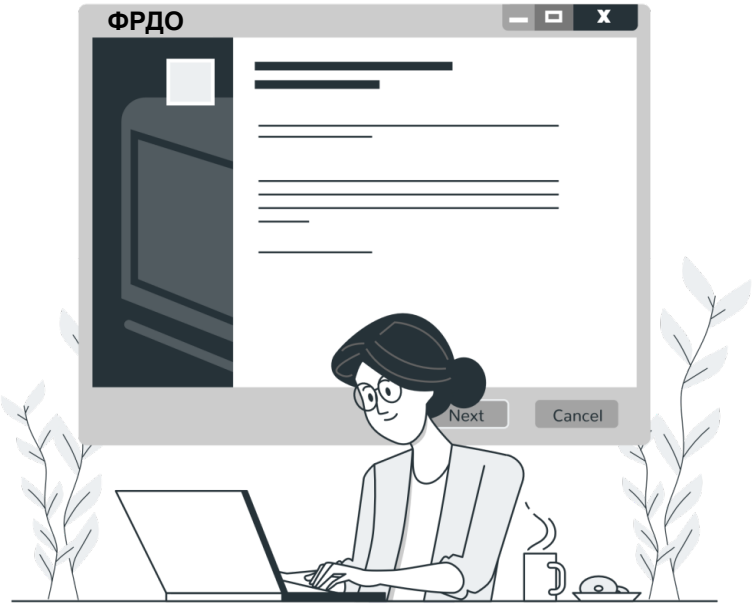
Талица №1. Отличия мер оценки соответствия системы защиты ПДн:

Критерии сопоставления	**Оценка эффективности** реализованных в рамках системы защиты ПДн мер по обеспечению безопасности ПДн	**Аттестация ИСПДн** на соответствие требованиям по защите информации
Разрабатываемые итоговые документы подтверждающие соответствие ИСПДн требованиям защиты информации (далее – Итоговые документы)	– «Протокол проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных»; – «Заключение по результатам оценки эффективности реализованных мер по обеспечению безопасности персональных данных».	– «Протокол проведения аттестационных испытаний информационной системы персональных данных»; – «Заключение по результатам аттестационных испытаний информационной системы персональных данных»; – «Аттестат соответствия информационной системы персональных данных требованиям по защите информации»
Срок действия итоговых документов при неизменности архитектуры ИСПДн	До 3 (трех) лет	В течение всего срока эксплуатации ИСПДн
Периодичность проведения периодического контроля уровня защиты ПДн, при их обработке в ИСПДн	Только при измении инфраструктуры ИСПДн	Не реже 1 (одного) раза в 2 (два) года
Предоставление Заказчиком протоколов контроля уровня защищенности ПДн, при их обработке в ИСПДн, во ФСТЭК России	Не требуется	Обязательное условие. В случае невыполнения, действие Итоговых документов приостанавливается

Федеральный реестр сведений о документах об образовании

ФРДО - информационная система «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» (ФИС ФРДО.

ФИС ФРДО - Постановление Правительства Российской Федерации от 26 августа 2013 г. № 729 «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении».



Цели создания Федерального реестра:

- ✓ Ликвидация оборота поддельных документов государственного образца об образовании
- ✓ Обеспечение ведомств и работодателей достоверной информацией о квалификации претендентов на трудоустройство
- ✓ Сокращение числа нарушений и коррупции в образовательных учреждениях
- ✓ Повышение качества образования за счёт обеспечения общественности достоверной информацией о выпускниках

Ключевые термины используемые при подключении к ФИС ФРДО:

- Канал защищённой сети (Сеть 11028)
- Электронная подпись (ЭП)
- Автоматизированное рабочее место (АРМ)
- Взаимодействие АРМ и ЭП
- Средства криптографической защиты информации (СКЗИ)
- Организационно - распорядительная документация (ОРД)

Этапы подключения к ФРДО

1. **Создать систему защиты:**
   - Сбор и анализ данных ✓
   - Установка СЗИ ✓
2. **Разработать Организационно-распорядительную документацию**
3. **Пройти Оценка эффективности**
4. **Получить электронно-цифровую подпись**
5. **Отправить запрос в ЦИТиС**

Импортозамещение

Установление запрета на госзакупки зарубежных промтоваров. Постановление № 616 от 30.04 2020 г.

Установление приоритета отечественных товаров перед импортными при осуществлении закупок с помощью конкурса, аукциона или других способов закупок. Постановление № 925 от 16.09.2016 г.

Увеличение доли государственного финансирования в грантах на создание отечественных аналогов комплектующих для различных отраслей промышленности. Постановление № 522 от 31.03.2022 г.

Установление приоритета российского ПО, входящего в специальный реестр, при госзакупках. Федеральный закон № 188-ФЗ от 29.06.2015 г.

Указ Президента РФ 250 от 1.05.2022 с 1 января 2025 г. организациям запрещается использовать СЗИ, странами происхождения которых являются иностранные государства.

Указ № 166 от 31.03.2022 г.. заказчики, осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ не могут приобретать иностранное ПО, в том числе в составе программно-аппаратных комплексов без согласования с федеральным органом исполнительной власти.

Наши контакты:

Головной офис в г. Калуга:

Кристина Чалышева
тел.: +7 (920) 092-92-25
+7 (4842) 788-999, доб. 7486
email: vkd@astralnalog.ru
сайт: www. is.astral.ru

Офис в г. Махачкала:

г. Махачкала,
ул. Магомедтагирова, д. 161 А
тел.: +7 (988) 298-88-99
email: info@astral-rd.ru
сайт: www.astral-rd.ru