Федеральное государственное бюджетное образовательное учреждение высшего образования   
«Саратовский государственный технический университет имени Ю. А. Гагарина»

Кафедра прикладных информационных технологий

**Реферат по курсу**

**Безопасность информационных технологий и систем**

**«Оценка соответствия и аттестация информационных систем ПДн»**

Выполнил студент группы б1-ИФСТ-41,

Песчанов Арсений Андреевич

Проверил: Большаков Алексей Александрович

Саратов, 2024

Содержание

[Введение 3](#_Toc181556409)

[Актуальность 3](#_Toc181556410)

[Цель работы 3](#_Toc181556411)

[Основная часть 4](#_Toc181556412)

[Понятие персональных данных и их защита 4](#_Toc181556413)

[Законодательные основы (ФЗ-152 "О персональных данных") 4](#_Toc181556414)

[Основные принципы обработки ПДн 5](#_Toc181556415)

[Оценка соответствия информационных систем 6](#_Toc181556416)

[Аттестация информационных систем 8](#_Toc181556417)

[Преимущества оценки соответствия и аттестации 10](#_Toc181556418)

[Отличия оценки соответствия от аттестации 11](#_Toc181556419)

[Заключение 12](#_Toc181556420)

[Список литературы 13](#_Toc181556421)

# Введение

## Актуальность

Данная тема крайне важна в настоящее время, потому что:

* Она является ключевым элементом обеспечения безопасности ПДн в цифровой среде;
* Она позволяет организациям соответствовать законодательным требованиям и снизить риски нарушений конфиденциальности;
* Она повышает уровень доверия к организации и ее системам

## Цель работы

Продемонстрировать важность оценки соответствия и аттестации информационных систем, обрабатывающих персональные данные (ПДн), для обеспечения безопасности данных, соблюдения законодательства и повышения доверия к организации.

# Основная часть

## Понятие персональных данных и их защита

**Персональные данные** — это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Это могут быть:

* Имя, фамилия, отчество
* Дата рождения
* Адрес, телефон, email
* Паспортные данные
* Фотографии
* Финансовая информация
* Информация о здоровье
* Данные о политических взглядах

Здесь важно отметить, что даже косвенные данные, которые могут быть использованы для идентификации человека, также считаются персональными. Например, комбинация IP-адреса и времени доступа к сайту может быть использована для идентификации пользователя.

## Законодательные основы (ФЗ-152 "О персональных данных")

В России обработка персональных данных регулируется Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных". Этот закон устанавливает следующие основные принципы обработки ПДн:

* Законность обработки: Обработка ПДн допускается только при наличии законных оснований.
* Согласие субъекта данных: Обработка ПДн допускается только с согласия субъекта данных, кроме случаев, установленных законом.
* Цель обработки: ПДн могут обрабатываться только для определенных, явных и законных целей.
* Соответствие целям: Обработка ПДн должна соответствовать целям, для которых они были собраны.
* Точность: ПДн должны быть точными, полными и актуальными.
* Хранение: ПДн не должны храниться дольше, чем это необходимо для достижения целей обработки.
* Безопасность: ПДн должны быть защищены от несанкционированного доступа, изменения, разглашения и уничтожения.

## Основные принципы обработки ПДн

Помимо требований ФЗ-152, существуют некоторые общепринятые принципы обработки ПДн:

* Минимизация: Обработка должна охватывать только необходимые данные.
* Прозрачность: Субъект данных должен быть информирован о том, как его данные обрабатываются.
* Ответственность: Организация несет ответственность за соблюдение требований законодательства и безопасность ПДн.
* Контроль: Субъект данных имеет право контролировать обработку своих данных.

## Оценка соответствия информационных систем

**Оценка соответствия** - это систематический процесс, который определяет, насколько информационная система (ИС), обрабатывающая персональные данные, соответствует установленным требованиям безопасности ПДн. Проще говоря, это проверка системы на соответствие законодательным актам, стандартам безопасности и внутренним политикам организации.

Процесс оценки соответствия обычно включает в себя следующие этапы:

1. Планирование:
   1. Определение объекта оценки (конкретная ИС или часть системы).
   2. Выбор стандартов и требований, которые будут использоваться для оценки (например, ФЗ-152 "О персональных данных", ГОСТ Р ИСО/МЭК 27001, PCI DSS).
   3. Разработка плана работ с указанием сроков, ответственных лиц и ресурсов.
2. Сбор информации:
   1. Анализ документации (политики безопасности ПДн, процедуры обработки ПДн, техническая документация).
   2. Проверка технических средств (серверы, сети, ПО).
   3. Интервью с персоналом, ответственным за обработку ПДн.
   4. Проведение тестирования системы на уязвимости и соответствие требованиям безопасности.
   5. Анализ рисков, связанных с обработкой ПДн.
3. Анализ:
   1. Сравнение собранной информации с установленными требованиями.
   2. Выявление отклонений и рисков.
4. Составление отчета:
   1. Описание выявленных отклонений и рисков.
   2. Рекомендации по устранению отклонений и снижению рисков.

ИС, обрабатывающая ПДн, должна соблюдать требования ФЗ-152 "О персональных данных" и других применимых законодательных актов, также соблюдать международные и отраслевые стандарты (ISO/IEC 27001, ГОСТ Р ИСО/МЭК 27001, PCI DSS).

Для проведения оценки соответствия необходимо иметь следующую документацию:

* Политика безопасности ПДн: Документ, определяющий основные принципы и правила защиты ПДн в организации.
* Процедуры обработки ПДн: Описание процедур сбора, хранения, обработки и уничтожения ПДн.
* Техническая документация: Описание технических средств защиты (серверы, сети, ПО).
* Документация по управлению рисками: Описание процесса управления рисками, связанными с обработкой ПДн.
* Договоры с поставщиками услуг: Договоры с компаниями, предоставляющими услуги по обработке ПДн (например, хостинг-провайдеры, облачные сервисы).

Оценка соответствия может проводиться с использованием таких методов, как анализ документации, тестирование, интервью, анализ рисков.

## Аттестация информационных систем

**Аттестация информационных систем (ИС)** — это официальная процедура, направленная на подтверждение соответствия ИС установленным требованиям безопасности ПДн. Аттестация определяет готовность системы к обработке персональных данных и определяет уровень ее безопасности. Она включает проверку как технических, так и организационных мер для защиты данных.

**Цели аттестации:**

* Подтверждение соответствия: Установление того, что ИС соответствует законодательным требованиям и стандартам безопасности.
* Оценка безопасности: Определение эффективности реализованных мер защиты персональных данных.
* Анализ рисков: Выявление уязвимостей и слабых мест в информационной системе.
* Устранение недостатков: Предоставление рекомендаций для улучшения безопасности системы.
* Соблюдение законодательства: Обеспечение выполнения требований законодательства о защите персональных данных.

**Процедура аттестации**

1. Подготовка:
   1. Сбор необходимой документации и информации о системе, которую необходимо аттестовать.
   2. Изготовление заявки на аттестацию.
2. Подача заявки:
   1. Организация подает заявку на аттестацию в уполномоченный орган.
3. Производство аттестации:
   1. Выезд специалистов для проведения проверки системы.
   2. Оценка выполнения требований и норм законодательства, стандартов.
4. Составление отчета:
   1. Подготовка акта аттестации, содержащего заключение о соответствии/несоответствии ИС установленным требованиям.
5. Выдача сертификата:
   1. Если система соответствует требованиями, выдается сертификат о соответствии. Если нет — предоставляются рекомендации по исправлению выявленных недостатков.

Документация, необходимая для аттестации:

1. Заявка на аттестацию: Официальный документ, в котором содержится запрос на проведение аттестации.
2. Отчет об оценке: Содержит результаты тестирования и оценку соответствия ИС установленным требованиям.
3. Политики безопасности: Документация, подтверждающая меры и процедуры, используемые для защиты ПДн.
4. Анализ рисков: Документы, содержащие результаты анализа рисков, угроз безопасности и уязвимостей системы.

**Результат аттестации – сертификат соответствия**: официальный документ, подтверждающий, что ИС соответствует установленным требованиям безопасности.

## Преимущества оценки соответствия и аттестации

1. Снижение рисков утечки ПДн:
   1. Проактивная защита: Оценки соответствия и аттестация позволяют выявить уязвимости и слабые места в системах до того, как злоумышленники смогут их использовать.
   2. Устранение рисков: Выявленные проблемы и риски могут быть устранены, что снижает вероятность утечки персональных данных.
   3. Соответствие требованиям: Обеспечивает соответствие систем установленным стандартам безопасности, что уменьшает риск несанкционированного доступа к данным.
2. Увеличение доверия к системе:
   1. Подтверждение безопасности: Сертификат соответствия является доказательством того, что система отвечает требованиям безопасности и защищает персональные данные.
   2. Повышение доверия клиентов: Клиенты, партнеры и регуляторы чувствуют себя более уверенно, зная, что компания серьезно относится к защите их персональных данных.
   3. Создание позитивного имиджа: Демонстрирует ответственность и прозрачность в отношении к обработке ПДн.
3. Соответствие законодательным требованиям:
   1. Соблюдение закона: Оценка соответствия и аттестация гарантируют соблюдение требований законодательства о защите ПДн.
   2. Снижение рисков штрафов: Соответствие законодательству снижает риск наложения штрафов и других санкций.
4. Повышение имиджа организации:
   1. Доказательство безопасности: Сертификат о соответствии служит доказательством того, что компания принимает необходимые меры для защиты ПДн.
   2. Укрепление репутации: Положительно влияет на имидж и репутацию организации, повышая доверие к ней.
   3. Привлечение клиентов: Увеличивает конкурентоспособность организации и позволяет привлечь новых клиентов.

## Отличия оценки соответствия от аттестации

Оценка соответствия и аттестация - это два тесно связанных процесса, которые направлены на обеспечение безопасности информационных систем, обрабатывающих персональные данные. Однако между ними есть ключевые различия:

**Оценка соответствия:**

* Цель: Определить, насколько информационная система соответствует требованиям законодательства и стандартам безопасности ПДн.
* Проведение: Проводится организацией самостоятельно или с привлечением независимых экспертов.
* Результат: Определение соответствия или несоответствия системы установленным требованиям.
* Документация: Отчет с описанием выявленных отклонений и рекомендациями по их устранению.

**Аттестация:**

* Цель: Официальное подтверждение соответствия информационной системы установленным требованиям безопасности ПДн.
* Проведение: Проводится специально уполномоченным органом (например, Роскомнадзор в России).
* Результат: Выдача сертификата о соответствии (если система соответствует требованиям) или отказ в аттестации с рекомендациями по устранению недостатков.
* Документация: Акт аттестации и сертификат соответствия.

Аттестация - это более формальная процедура, чем оценка соответствия, и она часто требуется для систем, обрабатывающих критические данные или подпадающих под действие специальных законодательных требований.

Оценка соответствия может проводиться регулярно в качестве внутренней процедуры организации, чтобы обеспечить постоянное соответствие системы требованиям безопасности.

Из вышесказанного можно прийти к выводу, что оценка соответствия — это предварительная проверка системы, а аттестация — это официальное подтверждение ее безопасности.

# Заключение

Оценка соответствия и аттестация информационных систем, обрабатывающих персональные данные, играют критически важную роль в обеспечении безопасности данных и соблюдении законодательства. Эти процессы помогают выявлять и устранять риски, что способствует защищенности информации и повышению доверия со стороны клиентов.

# Список литературы

1. Consultant «Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция)» [Электронный ресурс] URL: https://www.consultant.ru/document/cons\_doc\_LAW\_61801/ (Дата обращения: 01.11.2024)
2. Электронный фонд правовых и нормативно-технических документов «ГОСТ Р 50739-95» [Электронный ресурс] URL: https://docs.cntd.ru/document/1200004675 (Дата обращения: 01.11.2024)
3. Электронный фонд правовых и нормативно-технических документов «ГОСТ Р ИСО/МЭК 27001-2021» [Электронный ресурс] URL: https://docs.cntd.ru/document/1200181890 (Дата обращения: 02.11.2024)
4. Wikipedia «Персональные данные» [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5\_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5 (Дата обращения: 02.11.2024)
5. Github «Основы информационной безопасности» [Электронный ресурс] // URL: https://github.com/itsecd/isb (дата обращения: 03.11.2024)
6. Consultant «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» [Электронный ресурс] // URL: <https://www.consultant.ru/document/cons_doc_LAW_121499/> (дата обращения: 03.11.2024)