SAFE-DOC.COM

Онлайн-сервис подготовки документов

Подготовка к проверке регуляторов: основные этапы и типовые нарушения

partners@safe-doc.com
8(3852)200-460, доб.1113

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Подготовка к проверке Роскомнадзора

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) – регулятор в сфере защиты персональных данных (ПДн).

Задачи: защита прав субъектов персональных данных;
контроль и надзор за соответствием обработки персональных данных требованиям законодательства.

Предмет государственного контроля (надзора):
- документы, характер информации в которых предполагает или допускает включение в них ПДн
- информационные системы ПДн (ИСПДн)
- деятельность по обработке ПДн

Полномочия:
- проверяет сведения, указанные организацией в Уведомлении;
- может требовать от оператора уничтожения недостоверных или полученных незаконным путем ПДн;
- может ограничивать доступ к информации, обрабатываемой с нарушением законодательства;
- вправе обращаться в суд с исковыми заявлениями в защиту прав субъектов ПДн и представлять их в суде;
- наделен полномочиями по привлечению к административной ответственности лиц, виновных в нарушении настоящего Федерального закона;
- обязан рассматривать жалобы и обращения по вопросам, связанным с обработкой ПДн, а также принимать по ним решения в пределах своих полномочий.

http://rkn.gov.ru - официальный сайт Роскомнадзора

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Виды проводимых проверок

Вид проверки	Плановая	Внеплановая	Мониторинг
Форма проверки	Выездная (до 20 дней с возможностью продления на срок от 15 часов до 20 дней): в организацию приезжают представители Роскомнадзора и проводят проверку на предмет соответствия требованиям 152-ФЗ		Мероприятия систематического наблюдения: удаленный контроль за выполнением требований законодательства операторами ПДн
	Документарная (до 20 дней): Роскомнадзор запрашивает список документов, копии которых необходимо предоставить в территориальный орган Роскомнадзора	-	

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Плановые проверки Роскомнадзора

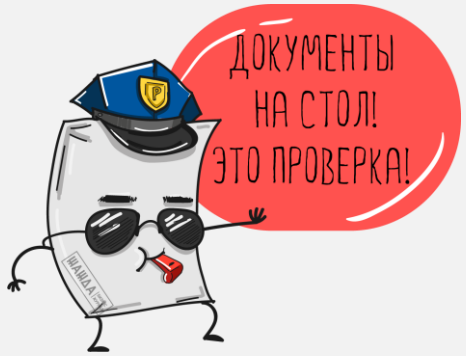
- проводятся раз в 3 года (в соответствии с 294-ФЗ)
- проводятся как в отношении Операторов включенных в Реестр, так и не включенных в Реестр, но осуществляющих обработку ПДн
- о плановых проверках Роскомнадзор предупреждает заранее (не позднее, чем за 3 рабочих дня).

Чтобы узнать, стоит ли ожидать плановой проверки в вашем учреждении, зайдите на сайт Управления Роскомнадзора вашего региона и в разделе «Планирование, отчеты о деятельности» найдите «План проведения плановых проверок»

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Внеплановые проверки Роскомнадзора



- чаще всего проводятся
а) на основании выявленных нарушений в действиях Оператора
б) в случае поступления жалобы на действия оператора
в) по результатам мероприятий систематического наблюдения

- о внеплановых проверках Роскомнадзор предупреждает не менее чем за 24 часа до начала проверки

- в случае причинения вреда жизни и здоровью граждан Оператор не предупреждается о начале внеплановой проверки

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Порядок подготовки к проверке Роскомнадзора

1.Подать уведомление о намерении осуществлять обработку ПДн/информационное письмо о внесении изменений в Роскомнадзор

2.Назначить лиц, ответственных за организацию обработки и за обеспечение безопасности ПДн

3. Провести внутренний аудит в целях анализа процессов обработки ПДн в учреждении

3. Разработать и утвердить необходимую документацию по защите ПДн

4. Ознакомить всех сотрудников, осуществляющих обработку ПДН и имеющих доступ к обрабатываемым в учреждении ПДн, под роспись с локальными актами по защите ПДн

5.Определить места нахождения баз данных ПДн граждан РФ

6. Завести и поддерживать в актуально состоянии журналы

7. Вести план внутренних проверок режима обработки и защиты ПДн

8. Обратить внимание на особенности разработки согласий для категорий субъектов, чьи ПДн обрабатываются

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Перечень наиболее часто встречающихся замечаний от Роскомнадзора

нарушение	рекомендации
Отсутствие у Оператора места (мест) хранения ПДн (материальных носителей), перечня лиц, осуществляющих обработку ПДн, либо имеющих к ним доступ	обеспечьте раздельное хранение документов, содержащих ПДн разных физических лиц; обеспечьте контролируемый доступ в помещения, в которых обрабатываются ПДн. В конце рабочего дня документы с ПДн должны быть убраны в запираемые шкафы, сейфы.
Невыполнение требований по обучению и ознакомлению сотрудников с порядком обработки, хранения ПДн и ответственностью за нарушение требований законодательства при обработке ПДн	соберите все необходимые подписи сотрудников, которые работают с ПДн. Они должны ознакомиться под роспись с Политикой, Положением, инструкциями, подписать обязательство о соблюдении конфиденциальности, согласие на обработку их ПДн
Неопубликование Оператором документа, определяющего Политику в отношении обработки ПДн	выкладывайте Политику в отношении обработки на сайт на видное место, в т.ч. если используется сбор ПДН через онлайн-формы.
Отсутствие уведомления об обработке ПДн / представление в уполномоченный орган уведомления об обработке ПДн, содержащего неполные или недостоверные сведения / непредставление сведений об изменении информации	вовремя актуализируйте уведомление об обработке ПДн, отправляйте информационное письмо в Роскомнадзор
Отсутствие условий соблюдения конфиденциальности ПДн в договорах с третьими лицами, а также требований к защите обрабатываемых ПДн	в договоре должно быть прописано, с какой целью передаются ПДн другой организации, какие действия она будет совершать с ними, обязанность организации обеспечивать конфиденциальность и безопасность полученных ПДн (ч.3. ст.6 152-ФЗ)

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Общие рекомендации от экспертов

1. Не выкидывайте ранее разработанные документы по защите ПДн
2. Ведите все журналы и формы документов, необходимые для выполнения законодательства
3. Ведите план внутренних проверок режима обработки и защиты ПДн
4. Будьте готовы предъявить обезличенные копии документов, содержащих ПДн (копии личных дел, согласий, анкет и др.)
5. Будьте готовы начать работать с ПДн при представителях. Подготовьте документы по системе видеонаблюдения, если она ведется
6. Заблаговременно готовьтесь к проверке

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Подготовка к проверкам ФСБ России

Федеральная служба безопасности (ФСБ) – регулятор в сфере обеспечения информационной безопасности

Предмет государственного контроля(надзора):
- организационные меры защиты информации
- криптографические меры защиты информации
- разрешительная и эксплуатационная документация на средства криптографической защиты информации (СКЗИ)
- требования к персоналу, допущенному к работе с СКЗИ
- эксплуатация СКЗИ
- оценка соответствия применяемых СКЗИ

http://www.fsb.ru - официальный сайт ФСБ России

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Виды проверок ФСБ России

Плановая проверка

Проводится согласно «Плану проведения плановых проверок юридических лиц и индивидуальных предпринимателей», план проверок ФСБ на год публикуется на официальном сайте Генеральной прокуратуры РФ https://proverki.gov.ru.

Основания для проведения внеплановой проверки

- ✓ истечение срока исполнения Оператором ранее выданного предписания об устранении выявленных нарушений требований к обеспечению безопасности информации
- ✓ поступление обращений и заявлений граждан, юридических лиц, информации от органов госвласти, ОМСУ, из СМИ о фактах возникновения угрозы причинения вреда жизни, здоровью граждан, безопасности государства
- ✓ распоряжение начальника органа безопасности о проведении проверки, изданное в соответствии с поручениями Президента/Правительства РФ

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Подготовка к проверкам ФСБ России: требования по технической защите информации

Проверяемые требования	Предоставляемые документы
Организационные меры защиты информации	Приказ о назначении ответственного пользователя СКЗИ Инструкция ответственного пользователя СКЗИ
Криптографические меры защиты информации	Модель угроз на каждую ИС Документы на поставку СКЗИ организации
Разрешительная и эксплуатационная документация на СКЗИ	Лицензия на СКЗИ Сертификаты соответствия на СКЗИ Формуляры на СКЗИ
Требования к персоналу, допущенному к работе с СКЗИ	Перечень сотрудников, допущенных к работе с СКЗИ Инструкция пользователей СКЗИ
Эксплуатация СКЗИ	Журнал поэкземплярного учета СКЗИ Лицевые счета пользователей СКЗИ Акты установки СКЗИ
Оценка соответствия применяемых СКЗИ	СКЗИ Дистрибутивы на СКЗИ

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Типовые нарушения при проверках ФСБ России

- ✓ Отсутствие необходимых журналов
- ✓ Журналы есть, но не ведутся
- ✓ Отсутствие, либо утеря эталонных дистрибутивов СКЗИ, документации, формуляров
- ✓ Некорректно разработанная модель угроз и действий нарушителя
- ✓ Использование СКЗИ более низкого класса, чем необходимо
- ✓ Недостаточные меры по физической защите носителей ключевой информации
- ✓ Недостаточные меры по физической защите помещений

Ст.19 ФЗ-152

8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Таким образом ФСБ и ФСТЭК могут проверять только организации, эксплуатирующие государственные информационные системы. Для остальных информационных систем контроль в законе не закреплен.

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Подготовка к проверкам ФСТЭК России

Федеральная служба по техническому и экспортному контролю (ФСТЭК) – регулятор в сфере обеспечения технической защиты информации

Предмет государственного контроля(надзора):

✓ соблюдение обязательных требований в области технической защиты информации, в том числе ПДн при их автоматизированной обработке в информационных системах (ГИС/ИСПДн)

✓ эксплуатационные документы и материалы аттестационных испытаний объектов информатизации

✓ техническая и иная документация по созданию системы защиты информации в государственных информационных системах

✓ планирующие и отчетные документы о деятельности по технической защите информации, в том числе материалы о результатах контроля эффективности принимаемых мер и СЗИ

http://www.fstec.ru - официальный сайт ФСТЭК России

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Подготовка к проверкам ФСТЭК России: требования по технической защите информации

Проверяемые требования	Предоставляемые документы
Соблюдение обязательных требований в области технической защиты информации, в том числе ПДн при их автоматизированной обработке в информационных системах (ГИС/ИСПДн)	Приказ о назначении ответственных за обеспечение безопасности информации Инструкция ответственного за обеспечение безопасности информации Модели угроз на каждую ИС Акты классификации ИС Сертифицированные СЗИ
Эксплуатационные документы и материалы аттестационных испытаний объектов информатизации	Сертификаты, формуляры на СЗИ Лицензии на СЗИ Аттестационная документация Технический паспорт ИС Журнал учета СЗИ
Техническая и иная документация по созданию системы защиты информации в ГИС	Техническое задание на создание системы защиты Регламент применения технических мер по защите информации
Требования к персоналу, допущенному к работе с СКЗИ	Договор/контракт на создание системы защиты информации Материалы о результатах контроля эффективности

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Типовые нарушения при проверках ФСТЭК России

- ✓ Отсутствие СЗИ
- ✓ Средства защиты есть, но не используются и/или некорректно настроены
- ✓ Использование несертифицированных СЗИ, либо с истекшим сроком действия сертификата соответствия
- ✓ Отсутствие, либо утеря эталонных дистрибутивов СЗИ, документации, формуляров
- ✓ Низкий уровень знаний ответственных за обеспечение безопасности информации в сфере информационной безопасности
- ✓ Не проводятся мероприятия, прописанные в утвержденной документации по защите информации
- ✓ Некорректно разработана модель угроз и модель нарушителя
- ✓ ГИС не аттестована
- ✓ Недостаточная физическая защита технических средств

SAFE-DOC.COM

Онлайн-сервис подготовки документов

Ответственность за нарушение требований по защите персональных данных

Административная : Роскомнадзор - ст. 5.39, **13.11**, 13.14 и 19.7; ФСБ, ФСТЭК - ст. 13.12, 13.13, 19.4, 19.5, 19.6, 19.20 КоАП РФ **до 75 тыс.руб.**

Уголовная: Роскомназдор - ст. 137, 140, 272; ФСБ, ФСТЭК - 171 УК РФ – **штраф до 300 тыс. руб. или принудительные работы либо лишение свободы**

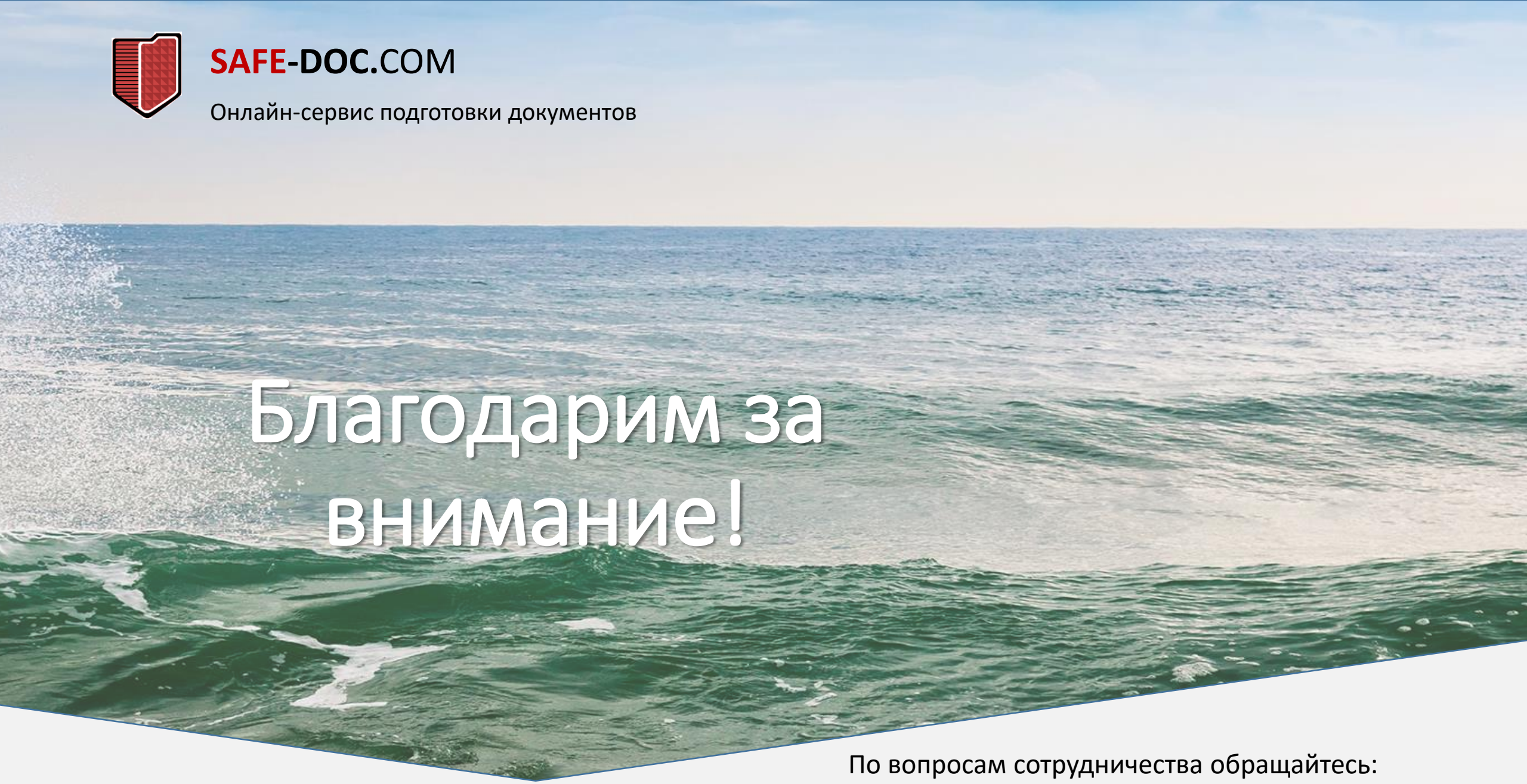
Дисциплинарная (пп. «в» п. 6 ст. 81 ТК РФ) – **увольнение или выговор**

Материальная (ст. 238 ТК РФ) – **компенсация понесенных убытков**

Гражданско-правовая – **компенсация убытков и морального вреда**

SAFE-DOC.COM

Онлайн-сервис подготовки документов



Благодарим за внимание!

По вопросам сотрудничества обращайтесь:

Тел.: 8(3852)**200-460, доб.1113**, e-mail: **partners@safe-doc.com**