



О подготовке отраслевых стандартов и рекомендаций для НПФ по исполнению требований закона №152-ФЗ

Касина Светлана Алексеевна

Исполнительный директор «Национального НПФ» - члена
Совета НП «НАПФ»

Бондаренко Александр

Директор департамента консалтинга ЗАО «ЛЕТА», CISA, CISSP

Отсутствие необходимого количества **квалифицированных** кадров

Отсутствие четких **рекомендаций** и типовых примеров

Специфика обработки персональных данных, связанная с осуществляемой организацией деятельностью

Сложность реализации общих рекомендаций и требований ФСТЭК

Отсутствие единой позиции по различным **спорным вопросам**

Динамично меняющееся законодательство

установка **общих принципов, требований и правил** по обработке и обеспечению безопасности персональных данных НПФ – членами НП «НАПФ» в целях защиты прав вкладчиков, участников и застрахованных лиц

соответствие процессов обработки персональных данных в НПФ – членах НП «НАПФ» **требованиям** действующего **законодательства** Российской Федерации

определение **порядка контроля** за выполнением требований по обработке и защите персональных данных в НПФ – членах НП «НАПФ»

4 документа, составляющих пакет отраслевых стандартов и рекомендаций в области персональных данных

Уважаемые коллеги!

Сообщаю Вам, что Рабочая группа для разработки комплексного пакета документов, регулирующего порядок организации и обработки персональных данных в негосударственных пенсионных фондах, разработала и утвердила проекты следующих Стандартов НАПФ:

- «Организация обработки и защиты персональных данных в негосударственных пенсионных фондах» (СТО НАПФ 4.1-2010),
- «Рекомендации по обеспечению безопасности персональных данных в информационных системах персональных данных в негосударственных пенсионных фондах» (СТО НАПФ 4.2-2010),
- «Рекомендации по формированию организационно-распорядительной документации для обеспечения обработки и защиты персональных данных в негосударственных пенсионных фондах» (СТО НАПФ 4.3-2010),
- «Рекомендации по проведению аудита на соответствие требованиям к обработке и защите персональных данных в негосударственных пенсионных фондах» (СТО НАПФ 4.4-2010).

В данный момент стандарты направлены на рассмотрение в комитеты и комиссию НАПФ.

С уважением,

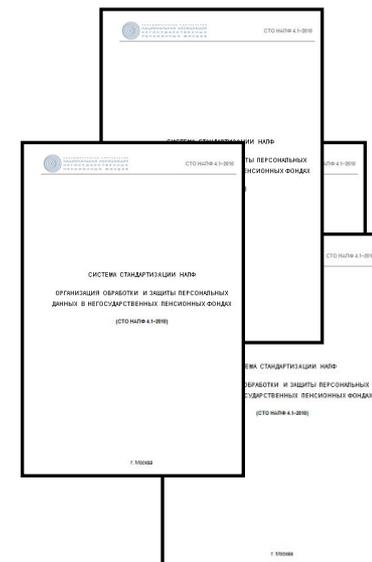
Люблин Ю.З.

Ссылка для скачивания - <http://napf.ru/14154>

Документы, содержащие практические, реализуемые примеры и рекомендации

Более понятные формулировки, описывающие подходы по обеспечению безопасности ПДн

Понятный набор критериев для проверки выполнения требований законодательства

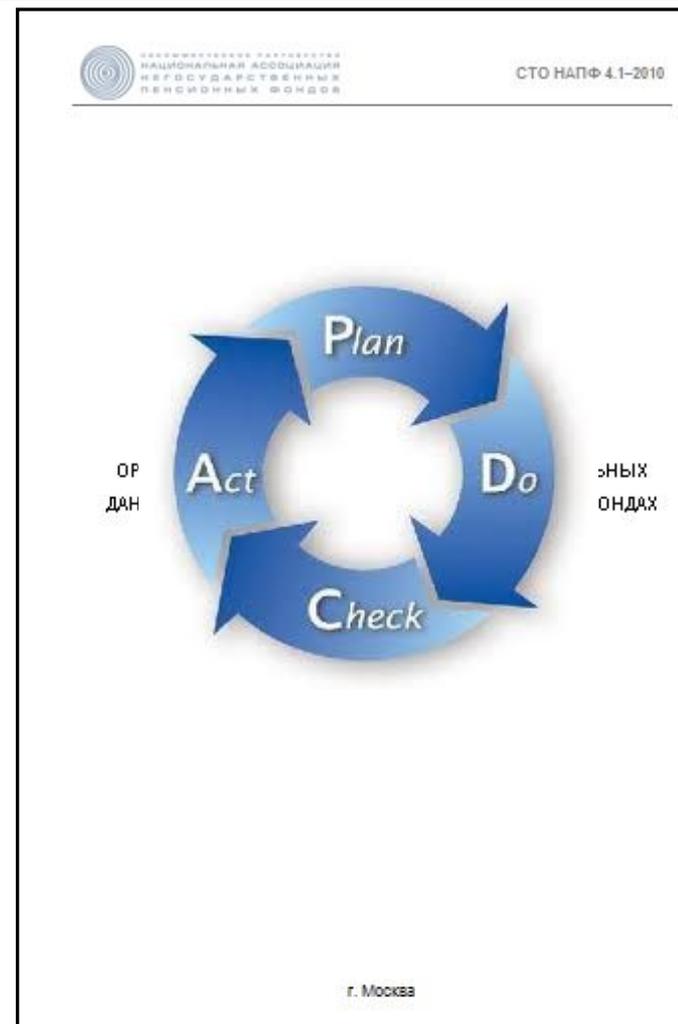


Организация обработки и защиты персональных данных в негосударственных пенсионных фондах

Планирование и подготовка к проведению мероприятий

Реализация требований по обработке и защите персональных данных

Контроль и корректировка мероприятий по обработке и защите персональных данных



Рекомендации по обеспечению безопасности персональных данных в информационных системах персональных данных в негосударственных информационных системах персональных данных



НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ НЕГОСУДАРСТВЕННЫХ ПЕНСИОННЫХ ФОНДОВ

Р НАПФ 4.2-2010

ИИ НАПФ

О БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМАХ ГОСУДАРСТВЕННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Москва

негос

Порядок персона

Методы персона

Методик

№ п/п	Описание угрозы	Последствия	Возможные меры защиты (ссылка на п. 6 настоящего стандарта)											
			6.2	6.3	6.4	6.5	6.6	6.7	6.8	6.9	6.10	6.11	6.12	6.13
Угрозы, связанные с действиями внешних нарушителей														
1.	Получение несанкционированного доступа к информации за счет воздействия на программное обеспечение (переполнение буфера и пр.) внедрения по сети вредоносного программного обеспечения	Нарушение К, Ц, Д ¹												
2.	Получение несанкционированного доступа к информации за счет подбора/перехвата пароля доступа	Нарушение К, Ц, Д												
3.	Получение несанкционированного доступа к информации за счет внедрения ложного доверенного объекта и перенаправление сетевого соединения (трафика)	Нарушение К, Ц, Д												
4.	Получение несанкционированного доступа к информации за счет физического проникновения в помещения, в которых расположены носители информации, средства обработки информации, средства коммуникации	Нарушение К, Ц, Д												
5.	Получение несанкционированного доступа к информации путем доступа к каналу связи и/или коммутационному оборудованию	Нарушение К, Ц, Д												

Рекомендации по организации аудита на соответствие требованиям к обработке и защите персональных данных в негосударственных пенсионных фондах



Р НАПФ 4.3-2010

Основн

Управл

Порядк

№ п/п	Описание критерия	Оценка критерия	Свидетельства аудита
1.7.	Проводится ли в пенсионном фонде периодический аудит на соответствие требованиям к обработке и защите персональных данных?		
1.8.	Проводится ли со стороны руководства пенсионного фонда периодический анализ мероприятий по обработке и защите персональных данных?		
1.9.	Выполняется ли корректировка мероприятий по обработке и защите персональных данных по результатам мониторинга и анализа со стороны руководства?		
2.	Критерии выполнения требований к обработке персональных данных		
2.1.	Определен ли состав/содержание персональных данных, обрабатываемых в пенсионном фонде?		
2.2.	Определены ли категории субъектов персональных данных, обработка которых осуществляется в пенсионном фонде?		
2.3.	Определены ли цели обработки персональных данных?		
2.4.	Определено ли правовое основание обработки персональных данных?		
2.5.	Определены ли сроки хранения персональных данных?		
2.6.	Определено ли, в каких случаях требуется письменное согласие		

ОРГАНИЗАЦИИ НАПФ
 АУДИТА НА СООТВЕТСТВИЕ
 И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ
 ПЕНСИОННЫХ ФОНДАХ
 4.3-2010)

ОСКВА

Рекомендации по формированию организационно-распорядительной документации для обеспечения обработки и защиты персональных данных



НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ НЕГОСУДАРСТВЕННЫХ ПЕНСИОННЫХ ФОНДОВ

Р. НАПФ 4.4-2010

Осно
рган

Реко

Образцы положении, перечней,

А К Т № _____

классификации информационной системы персональных данных
« _____ »

от « _____ » _____ 2010 г.

Комиссия в составе:

Председатель: _____

Члены комиссии: _____

рассмотрела следующие исходные данные информационной системы персональных данных « _____ »:

На основании и в соответствии с «Порядком проведения классификации информационных систем персональных данных» (утв. совместным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20) а также в результате анализа исходных данных и проведенного анализа и оценки угроз безопасности персональных данных с учетом особенностей данной информационной системы (результаты анализа закреплены в Модели угроз безопасности « _____ » от _____ № _____), комиссия

РЕШИЛА:

1. Отнести информационную систему персональных данных « _____ » к специальным информационным системам, для которых

АРТИЗАЦИИ НАПФ

РОВАНИЮ ОРГАНИЗАЦИОННО-МЕНТАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.4-2010)

оскба

№ п/п	Группа ПДн	Основание для обработки ПДн	Срок хранения, основание прекращения обработки ПДн
Обработка персональных данных работников пенсионного			
4.1	Общие сведения о работнике	Трудовые отношения между работником и Фондом (ст. 16 ТК РФ) Трудовой договор с работником Ст. 36, 24 ФЗ «О негосударственных пенсионных фондах»	
4.2	Финансовые сведения по работнику	Трудовые отношения между работником и Фондом (ст. 16 ТК РФ) Трудовой договор с работником	



Снижение стоимости и сроков работ за счет:

- использования типовых решений (особенно полезно для регионов) и документов
- отражения в стандарте специфики работы пенсионных фондов
- предварительного согласования позиции с регуляторами
- унификации выполняемых работ

Повышение общего уровня состояния ИБ в организациях НАПФ – еще один элемент качества оказываемых услуг

Возможность расширить стандарт, затронув вопросы обеспечения ИБ в целом.

Возможность включения новых изменений/требований в заложенную стандартом систему

Бондаренко Александр Валерьевич
Директор департамента консалтинга
Моб. тел.: +7 (495) 921-1410
e-mail: abondarenko@leta.ru

LETA IT-company
109129, Россия, Москва, ул. 8-я
Текстильщиков, д.11, стр. 2
Тел./факс: +7 (495) 921-1410

www.leta.ru