НЕКОММЕРЧЕСКОЕ ПАРТНЕРСТВО
НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ
НЕГОСУДАРСТВЕННЫХ
ПЕНСИОННЫХ ФОНДОВ

leta
IT · COMPANY

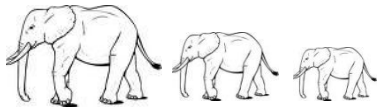
Обзор ситуации со стандартами НАПФ в свете изменения законодательства

Касина Светлана Алексеевна
Исполнительный директор «Национального НПФ» - члена Совета НП «НАПФ»

Бондаренко Александр
Технический директор ЗАО «ЛЕТА», CISA, CISSP

ЦЕЛЬ РАЗРАБОТКИ СТАНДАРТОВ

установка **общих принципов, требований и правил** по обработке и обеспечению безопасности персональных данных НПФ – членами НП «НАПФ»



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»

РЕЗУЛЬТАТЫ РАБОТЫ

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 т
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 нег
4.2-2010),
- «Рекомендации по формированию организационно-распорядительной документации для обеспечения обработки и защиты персо
- «Рекомендации по проведению аудита на соответствие требованиям к обработке и защите персональных данных в негосударстве

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

С уважением,

Люблин Ю.З.

Ссылка для скачивания - **http://napf.ru/14154**

СТАНДАРТЫ НАПФ

СТО НАПФ 4.1-2010 «Организация обработки и защиты ПДн в НПФ»

Р НАПФ 4.2-2010 «Рекомендации по обеспечению безопасности ПДн»

Р НАПФ 4.3-2010 «Рекомендации по формированию ОРД»

Р НАПФ 4.4-2010 «Проведение аудита на соответствие требованиям»

СТАНДАРТЫ НАПФ

Федеральный закон Российской Федерации от 25 июля 2011 г. N 261-ФЗ г. Москва "О внесении изменений в Федеральный закон "О персональных данных"

Ст.19 п.3 Правительство Российской Федерации <….> устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

СТАНДАРТЫ НАПФ

Федеральный закон Российской Федерации от 25 июля 2011 г. N 261-ФЗ г. Москва "О внесении изменений в Федеральный закон "О персональных данных"

Ст.19 п.4 Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются ФСТЭК и ФСБ.

СТАНДАРТЫ НАПФ

Федеральный закон Российской Федерации от 25 июля 2011 г. N 261-ФЗ г. Москва "О внесении изменений в Федеральный закон "О персональных данных"

Ст.19 п.6 Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

СТАНДАРТЫ НАПФ

Федеральный закон Российской Федерации от 25 июля 2011 г. N 261-ФЗ г. Москва "О внесении изменений в Федеральный закон "О персональных данных"«

Ст.19 п.7 7. Проекты решений, указанных в части 6 настоящей статьи, подлежат согласованию с ФСТЭК и ФСБ, в порядке, установленном Правительством Российской Федерации.

СТАНДАРТЫ НАПФ

Статья 18[1]. п.1 Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.
….

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

Предусмотрено в стандарте в виде иерархии ролей

СТАНДАРТЫ НАПФ

Статья 18[1]. п.1 Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.
….

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных..

Предусмотрено в виде РС по структуре и составу документации

СТАНДАРТЫ НАПФ

Статья 18[1]. п.1 Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.
….

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

Предусмотрено в виде РС с детальным описанием методов защиты

СТАНДАРТЫ НАПФ

Статья 18[1]. п.1 Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.
….

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону…

Предусмотрено в виде РС по порядку организации внутреннего аудита

СТАНДАРТЫ НАПФ

Статья 18[1]. п.1 Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.
….

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона

Предусмотрено в порядке составления модели угроз

СТАНДАРТЫ НАПФ

Статья 18[1]. п.1 Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.
….

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации

Предусмотрено как одна из мер по защите в части работы с персоналом

СТАНДАРТЫ НАПФ - ПЕРСПЕКТИВЫ

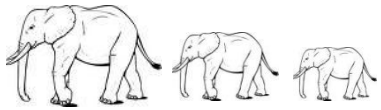
Небольшая корректировка для учета последних изменений

Выпуск новой редакции после выхода постановлений правительства и методических документов регуляторов

Согласование стандартов с ФСТЭК и ФСБ в соответствии с порядком, утвержденным Правительством

ЦЕЛЬ РАЗРАБОТКИ СТАНДАРТОВ

установка **общих принципов, требований и правил** по обработке и обеспечению безопасности персональных данных НПФ – членами НП «НАПФ»



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»

КОНТАКТНАЯ ИНФОРМАЦИЯ

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