

Утверждено приказом по предприятию
№ 261 от «23» 06 2015г.

ПОЛОЖЕНИЕ
о защите персональных данных в
информационной системе
персональных данных ОАО «Калугаприбор»

1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

1.1. Термины и определения:

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

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор - 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.

Лица, допущенные к работе с персональными данными – должностные лица, допущенные к обработке персональных данных приказом по предприятию.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Источник угрозы безопасности персональных данных - объект или субъект, реализующий угрозы безопасности персональных данных путем воздействия на объекты среды обработки персональных данных.

Объект среды обработки персональных данных - материальный объект среды хранения, передачи, обработки, уничтожения и т.д. персональных данных.

Оценка риска нарушения безопасности персональных данных - систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения безопасности персональных данных, обрабатываемых ОАО «Калугаприбор».

Риск нарушения безопасности персональных данных¹- риск, связанный с угрозой безопасности персональных данных.

Угроза безопасности персональных данных - угроза нарушения свойств безопасности персональных данных - доступности, целостности или конфиденциальности персональных данных.

¹ Риски нарушения безопасности персональных данных заключаются в возможности утраты свойств безопасности персональных данных в результате реализации угроз безопасности персональных данных, вследствие чего субъекту персональных данных и (или) АО «Калугаприбор» может быть нанесен ущерб.

1.2.Сокращения:

ИСПДн — информационная система персональных данных.

НСД — несанкционированный доступ.

ПДн — персональные данные.

УБПДн – угроза безопасности персональных данных.

ОАСУ – отдел автоматизированных систем управления.

СНТС – специальная научно-техническая служба.

2.ОБЩИЕ ПОЛОЖЕНИЯ

2.1.Настоящее положение разработано в соответствии с требованиями Федерального закона «О персональных данных» от 27.07.2006г. № 152-ФЗ, Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. № 149-ФЗ, Приказом ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013г. № 21, Постановлением Правительства Российской Федерации от 1 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.2.Настоящее положение определяет модель угроз персональных данных, а также методы и способы защиты персональных данных работников ОАО «Калугаприбор» в информационной системе персональных данных (ИСПДн) ОАО «Калугаприбор».

2.3.Целью настоящего положения является обеспечение безопасности персональных данных (ПДн) работников ОАО «Калугаприбор» при их обработке в информационной системе персональных данных ОАО «Калугаприбор».

2.4.ОАО «Калугаприбор» является оператором персональных данных, обрабатывает персональные данные работников в информационной системе персональных данных с использованием средств автоматизации.

2.5.На ОАО «Калугаприбор» определен уровень защищенности информационной системы персональных данных в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Актом от 07.05.2015г., утвержденным генеральным директором предприятия, информационной системе персональных данных ОАО «Калугаприбор» присвоен 3 уровень защищенности.

2.6.С помощью информационной системы персональных данных ОАО «Калугаприбор» в автоматизированном режиме обрабатываются следующие персональные данные работников предприятия:

- фамилия, имя, отчество;
- паспортные данные или данные документа, удостоверяющего личность;
- адрес места жительства или места пребывания;
- дата рождения, место рождения;

- номер страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика (ИНН);
- дата приема, увольнения, перевода, стаж работы;
- размер заработной платы, должность, разряд, категория, специальность, график работы, сведения о зарплатном счете в банке;
- сведения о всех начислениях и удержаниях из заработной платы;
- сведения о родственниках, состоянии в браке;
- сведения о наградах, поощрениях, дисциплинарных взысканиях;
- данные об образовании, квалификации, о профессиональной переподготовке, повышении квалификации и аттестации;
- сведения о льготах, наличии инвалидности;
- сведения о воинском учете;
- номер страхового полиса;
- номер телефона (мобильный, домашний).

2.7. Персональные данные обрабатываются с помощью автоматизированных лицензионных программных средств, в том числе, таких как 1С: «Предприятие 8.3. Бухгалтерия 3.0.», «Интегрированная бухгалтерская система» (ИБС), программное обеспечение «Налогоплательщик», АСУ «Кадры», программное обеспечение АС «Клиент-Сбербанк», программное обеспечение «КалугаАстралОтчет», программное обеспечение АС ЕКК.

Персональные данные работников предприятия во вновь приобретаемых программных средствах, базах данных, должны обрабатываться исключительно в целях и на условиях, предусмотренных настоящим положением.

2.8. Целями обработки персональных данных работников в информационной системе персональных данных ОАО «Калугаприбор» являются:

- обеспечение соблюдения законов и иных нормативных правовых актов;
- содействие работникам в трудоустройстве, обучении и продвижении по службе;
- обеспечение личной безопасности работников;
- контроль количества и качества выполняемой работы и обеспечение сохранности имущества.

3.МОДЕЛЬ УГРОЗ

3.1.Выбор и реализация методов и способов защиты информации в информационной системе персональных данных определяются на основании модели угроз (угроз безопасности персональных данных) и зависит от уровня защищенности информационной системы, который определен в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.2.Модель угроз безопасности персональных данных в информационной системе персональных данных ОАО «Калугаприбор» разработана на основании следующих руководящих документов:

- Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013г. № 21;

- Постановление Правительства Российской Федерации от 1 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Гостехкомиссия России, 2001г (утв. приказом ГТК № 282 от 30.08.2002);

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008г.;

- Защита от несанкционированного доступа к информации. Термины и определения, Гостехкомиссия России, 1992г.

3.3.Модель угроз содержит актуальные угрозы безопасности персональных данных при их обработке в ИСПДн ОАО «Калугаприбор».

В качестве методики выбора актуальных для ОАО «Калугаприбор» угроз и составления модели угроз использованы рекомендации «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», разработанной ФСТЭК России.

3.4.Модель угроз содержит систематизированный перечень актуальных угроз безопасности ПДн при их обработке в ИСПДн ОАО «Калугаприбор», источников актуальных угроз безопасности ПДн, уровней реализации угроз безопасности ПДн, типов материальных объектов среды обработки ПДн (далее — актуальные угрозы безопасности ПДн).

Актуальная угроза безопасности ПДн — угроза безопасности ПДн, риск реализации которой не является допустимым для ОАО «Калугаприбор» по результатам проведения оценки рисков нарушения безопасности персональных данных, обрабатываемых в ИСПДн.

Модель угроз содержит единые исходные данные по актуальным для ОАО «Калугаприбор» угрозам безопасности ПДн, связанным с несанкционированным, в том числе случайным, доступом в ИСПДн с целью ознакомления, изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с целью уничтожения или блокирования ПДн.

В рамках модели угроз под доступом к ПДн понимаются ознакомление с ПДн, их обработка, в частности, копирование, модификация или уничтожение ПДн.

К несанкционированному доступу (НСД) к ПДн при их обработке в ИСПДн, в частности, относятся:

- доступ к ПДн или действия с ПДн, нарушающие установленные права и (или) правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн;
- несанкционированное воздействие на ресурсы ИСПДн, осуществляемое с использованием вредоносных программ (вредоносного кода).

3.5. Перечень основных источников угроз безопасности ПДн:

- компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе использование компьютерных вирусов и других типов вредоносных кодов и атак;
- поставщики программно-технических средств, расходных материалов, услуг и т.п.;
- подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования и его техническое обслуживание и ремонт;
- сотрудники ОАО «Калугаприбор», являющиеся легальными участниками процессов в ИСПДн и действующие вне рамок предоставленных полномочий;
- сотрудники ОАО «Калугаприбор», являющиеся легальными участниками процессов в ИСПДн и действующие в рамках предоставленных полномочий.

3.6. Уровни информационной инфраструктуры, на которых возможна реализация угроз безопасности ПДн:

- физический уровень;
- сетевой уровень;
- уровень сетевых приложений и сервисов;
- уровень операционных систем;
- уровень систем управления базами данных;
- уровень технологических приложений и сервисов.

3.7. Модель угроз безопасности ПДн (см. Таблицу № 1) содержит описание угроз безопасности ПДн, включающее:

- источник угрозы безопасности ПДн;
- уровень реализации угрозы безопасности ПДн;
- типы материальных объектов среды обработки ПДн (далее — типы объектов среды);
- содержание угрозы ПДн.

Таблица № 1
Модель угроз

№	Источник УБПДн	Уровень реализации УБПДн	Типы объектов среды	УБПДн
1	Поставщики программно-технических средств, расходных материалов, услуг и т.п. и подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования и его ремонт	Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
2				Нарушение целостности
3		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
4				Нарушение целостности
5		Уровень технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
6				Нарушение целостности
7	Компьютерные злоумышленники, осуществляющие целенаправленное деструктивное воздействие	Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы	Нарушение конфиденциальности
8				Нарушение целостности
9		Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)	Нарушение конфиденциальности
10				Нарушение целостности
11		Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
12				Нарушение целостности
13		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение доступности
14				Нарушение конфиденциальности
15				Нарушение целостности
16				Нарушение доступности
17	Сотрудники, действующие в рамках предоставленных полномочий	Физический уровень	Линии связи, аппаратные и технические средства, серверы, физические носители информации	Нарушение конфиденциальности
18				Нарушение целостности
19		Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы	Нарушение конфиденциальности
20				Нарушение целостности
21				Нарушение доступности
22		Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)	Нарушение конфиденциальности
23				Нарушение целостности

№	Источник УБПДн	Уровень реализации УБПДн	Типы объектов среды	УБПДн
24		Уровень операционных систем	Файлы данных с ПДн	Нарушение доступности
25				Нарушение конфиденциальности
26				Нарушение целостности
27				Нарушение доступности
28		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
29				Нарушение целостности
30				Нарушение доступности
31		Уровень технологических приложений и сервисов	Прикладные программы доступа и обработки Пдн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
32				Нарушение целостности
33				Нарушение доступности
34	Сотрудники, действующие вне рамок предоставленных полномочий	Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
35				Нарушение целостности
36				Нарушение доступности
37		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
38				Нарушение целостности
39		Уровень технологических приложений и сервисов	Прикладные программы доступа и обработки Пдн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
40				Нарушение целостности

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОАО «КАЛУГАПРИБОР»

4.1. Доступ к ПДн работников, обрабатываемых в информационной системе персональных данных ОАО «Калугаприбор» имеют только лица, допущенные к обработке ПДн приказом по предприятию.

4.2. Лица, допущенные к обработке ПДн приказом по предприятию, имеют право получать только те ПДн работников, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц.

5. МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОАО «КАЛУГАПРИБОР»

5.1. При обработке персональных данных в информационной системе ОАО «Калугаприбор» обеспечивается:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

5.2. ОАО «Калугаприбор» при обработке ПДн в ИСПДн использует следующие методы и способы защиты ПДн:

1) компьютеры, на которых осуществляется обработка ПДн оснащены антивирусным ПО;

2) осуществляется обнаружение вторжения, нарушающее или создающее предпосылки для нарушения установленных требований по обеспечению безопасности персональных данных;

3) осуществляется управление доступом – идентификация и проверка подлинности пользователя при входе в информационную систему по идентификатору (логину) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

4) осуществляется регистрация входа (выхода) пользователя в информационную систему (из системы), в параметрах регистрации указываются дата и время входа (выхода) пользователя в информационную систему (из системы), результат попытки входа (успешная или неуспешная);

5) осуществляется физическая охрана информационной системы (устройств и носителей информации), которая предусматривает контроль доступа

посторонних лиц, препятствия несанкционированному проникновению в информационную систему;

6) предусмотрено наличие средств восстановления информационной системы персональных данных путем ведения копий программных компонентов, их периодическое обновление и контроль работоспособности;

7) передача ПДн в Пенсионный фонд России, Фонд социального страхования России, Федеральную налоговую службу России, а также Сбербанк России осуществляется в информационной системе персональных данных ОАО «Калугаприбор» с использованием сертифицированных криптографических средств в зашифрованном виде;

5.3. Лица, допущенные к работе с персональными данными, обеспечивают конфиденциальность (защиту) персональных данных.

6. ПРАВА РАБОТНИКОВ НА ЗАЩИТУ СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. В целях обеспечения защиты своих персональных данных работники имеют право:

- получать полную информацию о своих персональных данных и обработке этих данных в информационной системе персональных данных;

- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных Федеральным законом;

- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона;

- требовать от руководителя предприятия или уполномоченных им лиц уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них изменениях или исключениях из них;

- обжаловать в суде любые неправомерные действия или бездействие руководителя предприятия или уполномоченных им лиц при обработке и защите персональных данных;

- вносить предложения по мерам защиты своих персональных данных, обработка которых осуществляется в информационной системе персональных данных.

6.2. Работник имеет право на получение информации, касающейся обработки его персональных данных в информационной системе, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных оператором;

- 2) правовые основания и цели обработки персональных данных;

- 3) цели и применяемые оператором способы обработки и защиты персональных данных в информационной системе;

- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным;

- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законом;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес рабочего места лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные законодательством РФ.

7. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГЛАМЕНТИРУЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Лица, допущенные к работе с персональными данными, за нарушение норм, регулирующих обработку и защиту персональных данных, а также за нарушение режима конфиденциальности несут ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. Обязательства по соблюдению конфиденциальности персональных данных остаются в силе и после окончания работы с ними.

8. ОРГАНИЗАЦИЯ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

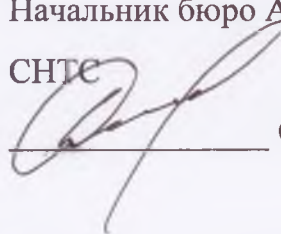
8.1. Организация обработки и защиты персональных данных в информационной системе предприятия возлагается на заместителя генерального директора по экономическим вопросам.

8.2. Техническую поддержку по обработке и защите персональных данных в информационной системе осуществляет ОАСУ.

8.3. Научно-методическое руководство обработкой и защитой персональных данных в информационной системе осуществляет СНТС.

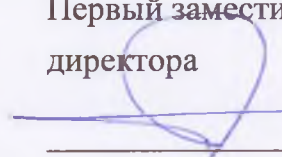
ПОДГОТОВЛЕНО

Начальник бюро АОИ
СНТС


_____ О.А. Дементьев

СОГЛАСОВАНО

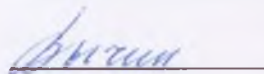
Первый заместитель генерального
директора


_____ С.В. Трусов

Заместитель генерального директора
по экономическим вопросам


_____ К.Х. Бестолов

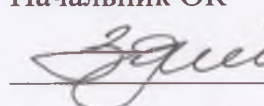
Главный бухгалтер


_____ О.Ю. Вычик

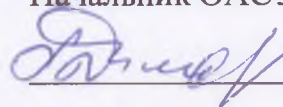
Начальник СНТС


_____ Л.Р. Кузнецов

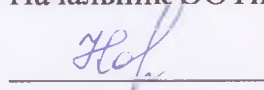
Начальник ОК


_____ А.И. Здонов

Начальник ОАСУ


_____ Т.Е. Дымовская

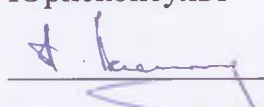
Начальник ООТиЗ


_____ А.С. Карева


Начальник ФО


_____ Н.Л. Волкова

Юрисконсульт


_____ А.А. Васильев

Начальник Первого отдела


_____ С.В. Бухтин