

Общество с Ограниченной Ответственностью «Учет.Кадры.Безопасность»

Адрес юридический:

236023 г. Калининград, ул. Чекистов д. 28-а -13

Р/сч 40702810920100000133

к/сч 30101810100000000634

ОГРН 1093925037711

Адрес почтовый:

236029 г. Калининград, ул. Горького 5

В отделении №8626 Сбербанка России г. Калининграда

ИК 042748634

ИНН/КПП 3904609602/390601001



УТВЕРЖДАЮ

Генеральный директор

ООО «Учет.Кадры.Безопасность»

Ю.В. Зуев

«08» июня 2017 г.



Политика информационной безопасности

г. Калининград
2017 г.



Введение

Настоящая Политика информационной безопасности (далее – Политика) *общества с ограниченной ответственностью «Учет.Кадры.Безопасность»* (далее - ООО «УКБ»), разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных и является официальным документом.

Политика разработана в соответствии с требованиями:

- Федерального закона РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- постановления Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства РФ от 01 ноября 2012 года № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18 Февраля 2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В Политике определены требования к работникам, допущенных для работы в информационных систем персональных данных (далее – ИСПДн), степень ответственности данных работников, структура и необходимый уровень защищенности ИСПДн ООО «УКБ», статус и обязанности работников, ответственных за обеспечение безопасности персональных данных (далее – ПДн) в ИСПДн ООО «УКБ».

1. Общие положения

Целью настоящей Политики является: обеспечение безопасности объектов защиты ООО «УКБ» от всех видов угроз (внешних, внутренних, умышленных, непреднамеренных), минимизация ущерба от возможной реализации угроз безопасности персональных данных (далее - УБПДн).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей.

В ООО «УКБ» осуществляется своевременное обнаружение и реагирование на УБПДн и предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты ООО «УКБ» утвержден приказами генерального директора **«Об утверждении перечня информационных систем персональных данных, контролируемой зоны помещений», «Об утверждении организационно-распорядительной документации, определении мест хранения материальных носителей персональных данных».**

Состав ПДн подлежащих защите, утвержден приказом генерального директора **«Об утверждении списка лиц, имеющих доступ к персональным данным и перечня персональных данных, подлежащих защите».**

Политика информационной безопасности утверждена приказом генерального директора **«Об утверждении Политики информационной безопасности».**

Требования настоящей Политики распространяются на всех работников ООО «УКБ» (штатных, работающих по различным видам договоров, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

2. Система защиты персональных данных

Система защиты персональных данных (далее - СЗПДн), строится на основании:

- аналитических отчетов по результатам обследования информационных систем персональных данных (далее – Аналитический отчет);
- частных моделей угроз безопасности персональных данных при их обработке в информационной системе персональных данных;
- перечня персональных данных, подлежащих защите;
- актов определения уровня защищенности персональных данных, при их обработке в информационной системе персональных данных;
- приказов по ООО «УКБ»;
- организационно-распорядительной документации относящейся к системе защиты информации и персональных данных ООО «УКБ»;
- руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн ООО «УКБ».

На основании анализа актуальных угроз безопасности ПДн описанных в частных моделях угроз безопасности персональных данных, технических заданиях на разработку системы защиты информационной системы персональных данных делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

Выбранные необходимые мероприятия отражаются в **Плане мероприятий по обеспечению безопасности персональных данных.**

Для каждой ИСПДн в Аналитических отчетах составляется перечень используемых технических средств, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн, включающих в себя:

- перечень основных технических средств (далее – ОТСС);
- перечень вспомогательных технических средств, располагаемых совместно с ОТСС;
- перечень программного обеспечения, используемого в ИСПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства защиты информации (далее – ТСЗИ):

- антивирусные средства для рабочих мест пользователей и серверов;
- средства защиты информации от несанкционированного доступа;
- средства межсетевого экранирования;
- средства криптографической защиты информации, используемые при передаче защищаемой информации по открытым каналам связи.

Список используемых технических средств защиты отражается в *«Журнале учета средств защиты»*.

Список используемых технических средств защиты информации должен поддерживаться в актуальном состоянии. При изменении состава ТСЗИ соответствующие изменения должны быть внесены в *«Журнал учета средств защиты»*.

3. Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрацией и учетом;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- отсутствие недеklarированных возможностей;

- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от определенных уровней защищенности ИСПДн, определенного в акте определения уровня защищенности персональных данных, при их обработке в информационной системе персональных данных.

4. Пользователи ИСПДн

В ИСПДн ООО «УКБ» выделены следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратор информационной безопасности;
- пользователь.

Данные о пользователях, уровне их доступа и информированности отражены в приказах по ООО «УКБ» **«Об утверждении списка лиц, имеющих доступ к персональным данным и перечня персональных данных, подлежащих защите».**

4.1. Администратор информационной безопасности

Администратор информационной безопасности (далее – администратор ИБ), штатный работник ООО «УКБ», ответственный за функционирование СЗПДн, включая обслуживание и настройку клиентской и серверной составляющих.

Администратор ИБ назначается приказом генерального директора **«О назначении администратора информационной безопасности и утверждение инструкции администратора информационной безопасности».**

Администратор ИБ обладает следующим уровнем доступа и знаний:

- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.

Администратор ИБ уполномочен:

- реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор АРМ) получает возможность работать с элементами ИСПДн;

- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других учреждений;
- осуществлять внутренние проверки режима защиты персональных данных в информационных системах персональных данных и фиксировать в **«Журнале внутренних проверок режима защиты персональных данных в информационных системах персональных данных»**.

4.2. Пользователи (Оператор)

Пользователь - работник ООО «УКБ», осуществляющий обработку ПДн.

Пользователи назначаются приказом по ООО «УКБ» **«Об утверждении списка лиц, имеющих доступ к персональным данным и перечня персональных данных, подлежащих защите»**.

Пользователь имеет доступ к обработке ПДн, которая включает в себя: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми знаниями для работы с ПДн;
- имеет личный идентификатор (имя пользователя) и аутентификатор (пароль).

5. Требования к персоналу по обеспечению защиты ПДн

Все работники ООО «УКБ», являющиеся пользователями ИСПДн, должны четко знать, и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдать принятый режим безопасности ПДн, а также быть ознакомленными со сборником руководящих инструкций по информационной безопасности ООО «УКБ».

При вступлении в должность нового работника, ответственный за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных в ООО «УКБ» (далее – Ответственный за обработку ПДн) знакомит работника с необходимыми

документами, регламентирующими требования по защите ПДн, а также обучает его правилам работы с ПДн в ИСПДн.

Работники ООО «УКБ» под роспись знакомятся с должностными инструкциями, настоящей Политикой, принятыми процедурами работы с элементами ИСПДн и СЗПДн, а так же с Положением об обработке и защите персональных данных ООО «УКБ».

Работники ООО «УКБ», использующие технические средства аутентификации, в обязательном порядке обеспечивают сохранность идентификаторов (электронных ключей) и не допускают НСД к ним, возможность их утери, использования третьими лицами.

Работники ООО «УКБ» проинструктированы о необходимости следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники ООО «УКБ» ознакомлены с правилами обеспечения надлежащей защиты оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

Все работники, как пользователи, ознакомлены с требованиями по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

При работе с ПДн работники ООО «УКБ» ознакомлены с требованиями обеспечения отсутствия возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест (далее – АРМ) или терминалов.

При завершении работы с ПДн работники ознакомлены с правилами защиты АРМ с помощью блокировки (комбинация Ctrl-Alt-Del, далее Блокировка компьютера; комбинация Клавиша Windows+L).

Работники ООО «УКБ» проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Работники ООО «УКБ» ознакомлены с дисциплинарными взысканиями при нарушении требований безопасности ПДн в соответствии с действующим федеральным

законодательством Российской Федерации в области защиты информации и персональных данных.

Контроль за соблюдением режима безопасности ПДн возложен на Ответственного за обработку ПДн, в соответствии с приказом **«О создании комиссии по проведению обследования и определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных, разработке организационно-распорядительной документации».**

Работники ООО «УКБ» обязаны без промедления сообщать генеральному директору или Ответственному за обработку ПДн обо всех случаях работы ИСПДн, которые могут повлечь за собой угрозу безопасности ПДн.

Работникам ООО «УКБ» ЗАПРЕЩАЕТСЯ

- устанавливать постороннее программное обеспечение,
- подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.
- разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ООО «УКБ» третьим лицам.

6. Должностные обязанности пользователей (операторов)

ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих организационно-распорядительных документах:

- инструкция ответственного за организацию обработки персональных данных;
- инструкция ответственного за эксплуатацию объекта информатизации;
- инструкция по организации парольной защиты;
- инструкция по организации антивирусной защиты;
- инструкция пользователя информационных систем персональных данных;
- инструкция по организации режима доступа в помещения;

- инструкция о порядке организации учета хранения и выдачи машинных носителей персональных данных ИСПДн;
- инструкция о порядке планирования и проведения проверок информационной безопасности в информационных системах персональных данных;
- инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации ИСПДн;
- должностных инструкциях (регламентах) работников ООО «УКБ».

7. Ответственность работников ООО «УКБ» обрабатывающих ПДн в ИСПДн

ООО «УКБ», как Оператор, обязано назначить лицо, ответственное за организацию обработки персональных данных.

Лицо, ответственное за организацию обработки персональных данных в ООО «УКБ» получает указания непосредственно от генерального директора и подотчетно ему.

Лицо, ответственное за организацию обработки персональных данных в ООО «УКБ», **ОБЯЗАНО:**

- осуществлять внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников ООО «УКБ» положения: законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных (приказы, инструкции), требования к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, подлежит

возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных изложена в:

➤ Кодексе об административных правонарушениях Российской Федерации (КоАП РФ) – статьи **5.27, 5.39, 13.11-13.14, 19.4-19.7, 19.20, 20.25, 32.2;**

➤ Уголовном Кодексе Российской Федерации (УК РФ) – статьи **137, 140, 155, 183, 272, 273, 274, 292, 293;**

➤ Трудовом Кодексе Российской Федерации (ТК РФ) – статьи **81, 90, 195, 237, 391.**

Администратор ИБ несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

ОПРЕДЕЛЕНИЯ

При обработке персональных данных используются следующие определения:

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

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ к информации – получение возможности ознакомления с информацией, в том числе при помощи технических средств.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (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.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).