Приложение № 1
Утверждено
приказом директора
ГБУ КЦСОН
Брасовского района
от 13.08.2018 г. № 38/1

Политика информационной безопасности информационных систем персональных данных ГБУ КЦСОН Брасовского района

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

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

Иные персональные данные – персональные данные не принадлежащие к специальным категориям персональных данных, не подпадающие под определение биометрических персональных данных, не являющимися общедоступными персональными данными и персональными данными сотрудников оператора.

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

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

Доступ к информации – возможность получения информации и ее использования.

Доступность информации - состояние информации, характеризуемое способностью информационной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

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

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 – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

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.

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.

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.

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

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.

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

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

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Событие информационной безопасности - идентифицированное возникновение состояния информационной системы, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

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

Средство защиты информации - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

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

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.

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.

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

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место;

ИСПДн – информационная система персональных данных;

НСД – несанкционированный доступ;

ОС – операционная система;

ПДн – персональные данные;

ПО – программное обеспечение;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных;

УБПДн – угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности информационных систем персональных данных ГБУ КЦСОН Брасовского района (далее – Политика) разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Политика регламентирует организацию защиты персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) Государственного бюджетного учреждения Брянской области «Комплексный центр социального обслуживания населения Брасовского района» (далее по тексту - ГБУ КЦСОН Брасовского района). В Политике определены структура и требования к построению системы защиты персональных данных (СЗПДн), порядок предоставления доступа к ИСПДн, требования к работникам по обеспечению безопасности ПДн, а также ответственность за нарушение требований по безопасности ПДн в ИСПДн ГБУ КЦСОН Брасовского района.

Требования настоящей Политики распространяются на всех работников ГБУ КЦСОН Брасовского района (штатных, временных, работающих по контракту и т.п.), а также всех третьих лиц, допущенных к ИСПДн ГБУ КЦСОН Брасовского района (подрядчики, аудиторы и т.п.).

Ответственным за контроль исполнения данной Политики, а также за её своевременное изменение и обновление является ответственный за организацию обработки персональных данных в ГБУ КЦСОН Брасовского района.

1 Общие положения

Безопасность персональных данных достигается путем принятия необходимых правовых, организационных и технических мер с целью исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иных неправомерных действий с персональными данными.

Мероприятия по защите персональных данных являются неотъемлемой частью деятельности ГБУ КЦСОН Брасовского района.

Целью проведения мероприятий по защите персональных данных является:

— обеспечение безопасности объектов защиты ГБУ КЦСОН Брасовского района от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных (УБПДн);

— выполнение требований по безопасности персональных данных при их обработке в ИСПДн, регламентируемых законодательством Российской Федерации в области защиты ПДн, а также государственными стандартами, руководящими и нормативно-методическими документами ФСТЭК и ФСБ России.

Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в ИСПДн информационные технологии.

2 Структура системы защиты персональных данных

Система защиты персональных данных – это не только совокупность организационных и технических мероприятий, но и объекты защиты, а также те ответственные лица, которые обеспечивают проведение мероприятий по обеспечению безопасности персональных данных.

Организация и функционирование вышеназванных составных элементов СЗПДн регламентируется правилами и нормами, установленными организационно-распорядительными документами ГБУ КЦСОН Брасовского района по вопросам обработки и защиты ПДн.

Принятие необходимых организационных и технических мер по обеспечению безопасности персональных данных обеспечивают:

— ответственный за организацию обработки персональных данных в ГБУ КЦСОН Брасовского района.

— ответственный за безопасность ИСПДн;

Указанные лица назначаются приказом директора ГБУ КЦСОН Брасовского района.

Обязанности и права ответственного за организацию обработки персональных данных в ГБУ КЦСОН Брасовского района и ответственного за безопасность ИСПДн и его заместителя определяются соответствующими инструкциями, утвержденными в ГБУ КЦСОН Брасовского района.

3 Требования к системе защиты персональных данных

Структура, состав и основные функции СЗПДн определяются исходя из установленного уровня защищенности ПДн в ИСПДн и перечня актуальных угроз безопасности ПДн при их обработке в ИСПДн. Соответственно разработка СЗПДн проводится на основе результатов обследования ИСПДн, акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных и частной модели угроз безопасности ПДн при их обработке в ИСПДн.

СЗПДн должна обеспечивать безопасность ПДн при обработке в ИСПДн согласно действующим нормативным документам ФСТЭК.

СЗПДн строится как иерархическая, многоуровневая система. Эффективность защиты достигается комплексным применением различных защитных механизмов, функционирующих в рамках единых принципов.

СЗПДн должна быть структурирована по функциональным подсистемам и при этом должны быть определены мероприятия по:

— защите ПДн от несанкционированного доступа (НСД);

— защите ПДн от утечки по техническим каналам.

Мероприятия по защите ПДн при их обработке в ИСПДн от НСД включают:

— управление доступом;

— регистрацию и учет;

— обеспечение целостности;

— антивирусную защиту;

— обнаружение вторжений;

— анализ защищенности;

— обеспечение безопасного межсетевого взаимодействия ИСПДн.

В соответствии с этим в СЗПДн выделяют следующие функциональные подсистемы:

1. Подсистема управления доступом.

Подсистема управления доступом должна проводить процедуру проверки подлинности пользователя, его авторизации, разграничивать доступ пользователей к ресурсам ИСПДн.

2. Подсистема регистрации и учета.

Подсистема регистрации и учета должна обеспечивать регистрацию действий пользователей при работе с ресурсами ИСПДн и учет событий информационной безопасности.

3. Подсистема обеспечения целостности

Подсистема обеспечения целостности должна обеспечивать контроль неизменности состояния рабочей среды пользователей при работе на АРМ, системных файлов ОС серверной части ИСПДн и СЗИ, используемых в СЗПДн, а также обеспечивать анализ защищенности системного и

прикладного программного обеспечения ИСПДн с помощью программных средств или программно-аппаратных средств анализа защищенности.

4. Подсистема антивирусной защиты.

Подсистема антивирусной защиты должна осуществлять защиту информационных ресурсов ИСПДн от внедрения вредоносного ПО. Подсистема антивирусной защиты должна минимизировать угрозы внедрения вредоносного ПО в СЗИ, операционную систему и общесистемное ПО, определенные Частной моделью угроз безопасности ПДн при их обработке в ИСПДн как актуальные.

5. Подсистема обнаружения вторжений.

Подсистема обнаружения вторжений должна своевременно обнаруживать и оповещать о несанкционированных воздействиях (атаках) на ИСПДн. Обнаружение вторжений обеспечивается путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений.

6. Подсистема анализа защищенности.

Подсистема анализа защищенности должна обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

7. Подсистема обеспечения безопасного межсетевого взаимодействия.

Подсистема обеспечения безопасного межсетевого взаимодействия должна обеспечивать безопасность ИСПДн при подключении к информационно-телекоммуникационной сети.

4 Доступ к информационным системам персональных данных

В ГБУ КЦСОН Брасовского района устанавливается разрешительная система доступа к обработке персональных данных в ИСПДн, а также к администрированию, техническому обслуживанию, сопровождению и другим работам с ИСПДн.

Доступ работников ГБУ КЦСОН Брасовского района к ИСПДн предоставляется на основании приказа ГБУ КЦСОН Брасовского района от _____ № _____ (Приложение № 4 к приказу «Список лиц, допущенных к обработке персональных данных в информационных системах персональных данных ГБУ КЦСОН Брасовского района и функции, выполняемые ими при работе в ИСПДн»).

Доступ к ИСПДн представителей сторонних организаций (третьих лиц), выполняющих работу по договору, предоставляется на основании приказа директора ГБУ КЦСОН Брасовского района, при условии наличия в договоре пункта о соблюдении конфиденциальности персональных данных или отдельного договора о конфиденциальности персональных данных. Приказом должны быть заданы: ИСПДн, к которой допущено лицо; виды работ, которые может производить допущенное лицо; срок действия допуска.

Лица, получившие допуск к ИСПДн, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, требованиями к защите персональных данных и организационно-распорядительными документами ГБУ КЦСОН Брасовского района по вопросам обработки и защиты ПДн.

Допуск к ИСПДн аннулируется, а доступ незамедлительно прекращается в случае изменения статуса допущенного лица (перевод на другую должность, увольнение, изменение должностных обязанностей и т.п.). За своевременное предоставление информации об изменении статуса допущенного лица ответственному за организацию обработки персональных данных в ГБУ КЦСОН Брасовского района и ответственному за безопасность ИСПДн отвечают сами допущенные лица, а также их непосредственные руководители.

За организацию разрешительной системы доступа к ИСПДн отвечает лицо, назначенное ответственным за организацию обработки персональных данных в ГБУ КЦСОН Брасовского района. Ответственный за безопасность ИСПДн обеспечивает реализацию и надлежащее функционирование разрешительной системы доступа к ИСПДн и составляет и обновляет необходимые для этого документы в соответствии с порядком, установленным Технологическим процессом обработки персональных данных в ИСПДн.

5 Требования к работникам по обеспечению защиты персональных данных

Все работники ГБУ КЦСОН Брасовского района, имеющие допуск к ИСПДн, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, настоящей Политикой и другими принятыми в ГБУ КЦСОН Брасовского района организационно-распорядительными документами по вопросам обработки и защиты ПДн.

Обязанности и права ответственного за организацию обработки персональных данных в ГБУ КЦСОН Брасовского района, ответственного за безопасность ИСПДн, пользователей ИСПДн определяются соответствующими инструкциями.

Все работники ГБУ КЦСОН Брасовского района, допущенные к ИСПДн, должны четко знать и неукоснительно выполнять установленные правила и обязанности по обеспечению безопасности ПДн при их обработке и соблюдению установленного режима конфиденциальности ПДн.

При вступлении в должность нового работника ответственный за организацию обработки персональных данных в ГБУ КЦСОН Брасовского района обязан организовать его ознакомление с необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Работники ГБУ КЦСОН Брасовского района должны быть проинформированы об угрозах безопасности ПДн и ответственности за нарушение требований безопасности ПДн. Работники обязаны информировать ответственного за организацию обработки персональных данных в ГБУ КЦСОН Брасовского района и ответственного за безопасность ИСПДн о ставших им известными фактах нарушения положений настоящей Политики и инцидентах информационной безопасности в незамедлительном порядке.

Ответственный за организацию обработки персональных данных в ГБУ КЦСОН Брасовского района инициирует и проводит служебные расследования по факту нарушений и инцидентов информационной безопасности в соответствии с установленной в ГБУ КЦСОН Брасовского района процедурой.

6 Ответственность работников за нарушение норм, регулирующих обработку и защиту персональных данных

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасности ПДн при их обработке и предусматривает ответственность за нарушение установленных правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-коммуникационных сетей, неправомерный доступ к охраняемой компьютерной информации, если эти действия привели к уничтожению, блокированию, модификации или копированию компьютерной информации (статьи 272, 273 и 274 УК РФ).

При нарушениях работниками ГБУ КЦСОН Брасовского района правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.