ДЕПАРТАМЕНТ СЕМЬИ, СОЦИАЛЬНОЙ И ДЕМОГРАФИЧЕСКОЙ ПОЛИТИКИ БРЯНСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ БРЯНСКОЙ ОБЛАСТИ
ОТДЕЛ СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ
БРАСОВСКОГО РАЙОНА

Приказ

28.06. 2023 года № 57

п. Локоть

Об утверждении Политики информационной безопасности информационных систем ГКУ «ОСЗН Брасовского района»

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», со статьями 6,16 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Политику информационной безопасности информационных систем ГКУ «ОСЗН Брасовского района».
2. Ознакомить сотрудников учреждения с положениями Политики информационной безопасности информационных систем ГКУ «ОСЗН Брасовского района», утвержденной настоящим приказом.
3. Хоченковой Т. А. обеспечить размещение Политики информационной безопасности информационных систем ГКУ «ОСЗН Брасовского района» на официальном сайте учреждения в информационно-телекоммуникационной сети «Интернет».
4. Сотрудникам учреждения руководствоваться в работе положениями Политики информационной безопасности информационных систем ГКУ «ОСЗН Брасовского района» по соблюдению принятого режима безопасности персональных данных в информационных системах персональных данных учреждения.

5. Местом хранения Политики информационной безопасности информационных систем ГКУ «ОСЗН Брасовского района» определить кабинет ответственного за организацию обработки персональных данных.

6. Приказ вступает в силу со дня его подписания.

7.Контроль за исполнением настоящего приказа возложить на ответственного за организацию обработки персональных данных-заместителя начальника отдела Иваникову В.Н.

Начальник А.В.Гуляева

С приказом ознакомлена:

«28» 06 2023года В.Н. Иваникова

«28» 06 2023 года Т.А.Хоченкова

Утверждена
приказом ГКУ «ОСЗН Брасовского района»
от 18.06 2023 года № 57

Политика
информационной безопасности информационных систем
ГКУ «ОСЗН Брасовского района»

1. Общие положения

1.1. Целью настоящей Политики является обеспечение безопасности объектов защиты персональных данных ГКУ «ОСЗН Брасовского района» (далее - учреждение) от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

1.2. Безопасность персональных данных достигается путём 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.

1.3. В учреждении обеспечивается осуществление своевременного обнаружения и реагирования на угрозы безопасности персональных данных, предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения персональных данных.

1.4. Требования настоящей Политики распространяются на всех специалистов учреждения (постоянных, временных), а также иных лиц (подрядчиков, исполнителей, аудиторов и т.п.).

2. Система защиты персональных данных

2.1. Система защиты персональных данных строится в учреждении на основании:

законодательства Российской Федерации в области защиты персональных данных, руководящих документов Федеральной службы по техническому и экспортному контролю России и Федеральной службы безопасности России;

организационно-распорядительных документов учреждения в сфере защиты персональных данных.

На основании указанных документов определяется необходимый уровень защищённости персональных данных каждой информационной системы учреждения.

2.2. На основании анализа актуальных угроз безопасности персональных данных, описанного в моделях угроз безопасности при их обработке в информационных системах учреждения и отчёте о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах учреждения, делается вывод о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности персональных данных.

2.3. Для каждой информационной системы должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке персональных данных, на всех элементах информационных систем:

персональные компьютеры пользователей;

система управления базами данных - СУБД;
граница локальной вычислительной сети;

каналы передачи в сети общего пользования и (или) международного обмена, если по ним передаются персональные данные.

2.4. В зависимости от уровня защищённости информационных систем и актуальных угроз система защиты персональных данных может включать в себя следующие технические средства:

антивирусные средства для персональных компьютеров пользователей;

средства межсетевого экранирования;

средства криптографической защиты информации при передаче защищаемой информации по каналам связи.

Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки персональных данных операционной системы, прикладным программным обеспечением и специальными комплексами, реализующими средства защиты.

Список функций защиты может включать в себя:

управление и разграничение доступа пользователей;

регистрацию и учёт действий с информацией;

обеспечение целостность данных;

осуществление обнаружения вторжений.

3. Требования к подсистемам системы защиты персональных данных

3.1. Система защиты персональных данных включает в себя следующие подсистемы:

управления доступом;

регистрации и учёта;

обеспечения целостности и доступности;

антивирусной защиты;

межсетевого экранирования;

анализа защищённости;

обнаружения вторжений;

криптографической защиты.

3.2. Подсистемы системы защиты персональных данных имеют различный функционал.

3.3. Подсистема управления доступом предназначена для реализации следующих функций:

идентификации и проверки подлинности субъектов доступа при входе в информационную систему;

идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

идентификации программ, томов, каталогов, файлов, записей, полей записей по именам.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки персональных данных (операционных систем, приложений и СУБД). Также может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю.

3.4. Подсистема регистрации и учёта предназначена для реализации следующих функций:

регистрации входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и её остановка;

регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема регистрации и учёта может быть реализована с помощью организационных мер защиты информации. Также может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по регистрации действий, осуществляемых в информационной системе.

3.5. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности персональных данных, программных и аппаратных средств информационных систем, а также средств защиты при случайной или намеренной модификации.

3.6. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты персональных компьютеров пользователей. Средства антивирусной защиты предназначены для реализации следующих функций:

резидентный антивирусный мониторинг;

антивирусное сканирование;

скрипт-блокирование;

централизованную /удалённую установку/ деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчётов и статистической информации по работе продукта;

автоматизированное обновление антивирусных баз;

ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путём внедрения специального антивирусного программного обеспечения на все элементы информационных систем.

3.7. Подсистема межсетевого экранирования должна обеспечивать безопасность информационной системы персональных данных при подключении к информационно-телекоммуникационной сети.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе локальной вычислительной сети классом не ниже 4.

3.8. Подсистема анализа защищённости должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационных систем, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

3.9. Подсистема обнаружения вторжений должна обеспечивать выявление сетевых атак на элементы информационных систем, подключённые к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

3.10. Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации при её передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется путём внедрения криптографических программно-аппаратных комплексов.

4. Категории пользователей информационных систем учреждения

4.1.Пользователем информационных систем учреждения является лицо, участвующее в функционировании информационной системы учреждения или использующее результаты её функционирования.

4.2.Для определения требований к пользователям информационных систем, степени ответственности, уровня защищённости, должностным обязанностям сотрудников, ответственных за обеспечение безопасности персональных данных выделяются следующие категории пользователей

информационных систем учреждения, участвующих в обработке и хранении персональных данных:

1) администратор информационной безопасности учреждения;

2) пользователь информационной системы учреждения.

4.3. Категории пользователей определяются для каждой информационной системы учреждения.

5. Администратор информационной безопасности учреждения

5.1. Администратором информационной безопасности учреждения является специалист учреждения, который выполняет функции настройки, внедрения и сопровождения, функционирование системы защиты персональных данных информационной системы учреждения.

5.2. Администратор информационной безопасности учреждения обеспечивает функционирование подсистемы управления доступом информационных систем учреждения и уполномочен осуществлять предоставление и разграничение доступа пользователей к элементам информационных систем, хранящим персональные данные.

5.3. Администратор информационной безопасности учреждения обладает следующим уровнем доступа:

обладает полной информацией об информационной системе учреждения;

обладает полной информацией о системном и прикладном программном обеспечении информационной системы учреждения;

обладает полной информацией о технических средствах и конфигурации информационной системы учреждения;

имеет доступ ко всем техническим средствам обработки информации и данным информационной системы учреждения;

имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационной системы учреждения;

не имеет прав доступа к конфигурированию технических средств сети, за исключением контрольных (инспекционных).

5.4. Администратор информационной безопасности учреждения уполномочен:

реализовывать политики безопасности в части настройки средств криптографической защиты информации, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь информационной системы получает возможность работать с элементами информационной системы;

осуществлять аудит средств защиты;

устанавливать доверительные отношения своей защищённой сети с сетями других учреждений.

6. Пользователь информационных систем учреждения

6.1. Пользователем информационной системы учреждения является специалист учреждения, участвующий в процессе эксплуатации информационной системы учреждения и осуществляющий обработку персональных данных.

6.2. Пользователь информационной системы учреждения обладает следующим уровнем доступа:

обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;

располагает конфиденциальными данными, к которым имеет доступ.

7.Требования к пользователям информационных систем учреждения по обеспечению защиты персональных данных

7.1. Все пользователи информационных систем учреждения должны чётко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных.

7.2. При назначении на должность сотрудника учреждения он должен быть ознакомлен с настоящей Политикой и документами, регламентирующими требования по защите персональных данных в учреждении, а также обучен навыкам выполнения процедур, необходимых для санкционированного использования информационных систем учреждения.

7.3. Пользователи информационных систем учреждения, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированный доступ к ним, а так же исключить возможность их утери или использования третьими лицами.

Пользователи информационных систем учреждения несут персональную ответственность за сохранность идентификаторов.

7.4. Пользователи информационных систем учреждения должны следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей (если не используются технические средства аутентификации).

7.5. Пользователи информационных систем учреждения должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица; должны знать требования по безопасности персональных

данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

7.6. Пользователям информационных систем учреждения запрещается: устанавливать постороннее программное обеспечение;

подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию;

разглашать защищаемую информацию третьим лицам.

7.7. При работе с персональными данными пользователи информационных систем Отдела обязаны обеспечить отсутствие возможности просмотра персональных данных третьими лицами с мониторов персональных компьютеров или терминалов.

При завершении работы в информационной системе пользователи информационных систем Отдела обязаны защитить персональный компьютер или терминал с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

7.8 Пользователи информационных систем учреждения должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение.

7.9. Пользователи информационных систем учреждения обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационных систем, которые могут повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководителю подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

8. Ответственность

8.1. Пользователи информационных систем учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность осуществляющий обработку персональных данных.

ДЕПАРТАМЕНТ СЕМЬИ, СОЦИАЛЬНОЙ И ДЕМОГРАФИЧЕСКОЙ ПОЛИТИКИ БРЯНСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ БРЯНСКОЙ ОБЛАСТИ
ОТДЕЛ СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ
БРАСОВСКОГО РАЙОНА

Приказ

5 марта 2024 года № 23

рп. Локоть

О внесении изменения в приказ
от 28 июня 2023 года № 57
«Об утверждении Политики
информационной безопасности
информационных систем
ГКУ «ОСЗН Брасовского района»

В связи с кадровыми изменениями

ПРИКАЗЫВАЮ:

1. Внести в приказ ГКУ «ОСЗН Брасовского района» от 28 июня 2023 года № 57 «Об утверждении Политики информационной безопасности информационных систем ГКУ «ОСЗН Брасовского района» следующее изменение:

пункт 7 приказа изложить в следующей редакции:

«7. Контроль за исполнением настоящего приказа возложить на ответственного за организацию обработки персональных данных».

2. Контроль за исполнением приказа оставляю за собой.

Начальник отдела А.В.Гуляева