Приложение № 1

к приказу № 28-ОД

От 06.02.2024г

ПОЛИТИКА

информационной безопасности

краевого государственного бюджетного учреждения социального обслуживания

«Комплексный центр социального обслуживания населения «Краснотуранский»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Политика информационной безопасности (политики) КГБУ СО "КЦСОН "Краснотуранский" (учреждение) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Положении информационной безопасности.

Целью настоящей Политики является, обеспечение безопасности объектов защиты специалиста от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угрозу безопасности персональных данных. Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1. Область действия.

1.1. Настоящая Политика распространяется на все структурные подразделения Учреждения и обязательства для исполнения всеми его сотрудниками и должностными лицами (штатных, временных и т.п.) а также всех прочих лиц (подрядчики, аудиторы и т.п.). Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а так же в договорах и приказах.

1.2. Законодательной основой настоящей Политики являются, Конституция Российской Федерации, Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023) "О персональных данных", Гражданский и Уголовный кодексы Российской Федерации, Федеральные конституционные законы Российской Федерации, Указы и распоряжения Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации, другие нормативные документы действующего законодательства Российской Федерации.

Федерального агентства правительственной связи и информации при Президенте Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

2.Определения

2.1. 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.

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

2.3. Безопасность информации - деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию)

2.4. Информационная безопасность (ИБ) – технологическое обеспечение целостности, конфиденциальности и доступности

2.5 Информационная сфера (ИС) - совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

2. Подготовка знаний

3.1. Общетеоретическая подготовка специалистов по ИБ должна базироваться на следующих областях знаний:

-управление информационной безопасностью: методы организации адаптивной динамической системы со стохастическими характеристиками, адаптивное управление с использованием искусственного интеллекта.

-криптографическая защита: гомоморфная криптография, распределенные пост квантовые крипто алгоритмы, криптографическая защита в децентрализованных распределенных самоорганизующихся сетях, блокчейн.

-безопасность больших данных: принципы работы с большими данными, защищенные системы интеллектуального сбора и предобработки неструктурированных данных, анализ данных в облачных системах и на гетерогенном вычислительном кластере, применение гомоморфной криптографии для обработки больших и сверхбольших массивов данных, методы динамического
управления нагрузкой.

-киберустойчивость систем управления цифровым производством: методы обеспечения глобального доверия и киберустойчивости, методы глубокого обучения для обнаружения уязвимостей в программном обеспечении, анализа вредоносных программ, распознавания сетевых атак, обнаружения бот-сетей и кибермошенничества.

3.2. Что должен делать руководитель:

-Поставить цели по обеспечению ИБ для всего предприятия

- Обеспечить поддержку для службы ИБ и соответствующий приоритет задач, связанных с ИБ для всех структурных подразделений

- Обеспечить финансирование деятельности службы ИБ

- Установить ответственность за невыполнение требований ИБ

- Учредить комитет по ИБ или рискам ИБ

- Определить отчетность службы ИБ

- Контролировать деятельность службы ИБ

- Реализовывать ответственность тех, кто нарушил требования ИБ

3. Ответственность за ресурсы

4.1. В ИС Учреждения присутствуют следующие типы ресурсов:

- информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Учреждения;

-открыто распространяемая информация, необходимая для работы Учреждения, независимо от формы и вида её представления;

- информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

4.2. Для каждого ресурса должен быть назначен владелец, который отвечает за соответствующую классификацию информации и ресурсов, связанных со средствами обработки

информации, а также за назначение и периодическую проверку прав доступа и категорий, определённых политиками управления доступа.

5. Меры обеспечения информационной безопасности

5.1. Официальные материалы, подлежащие размещению на официальных информационных ресурсах Учреждения. Дополнительно допускается размещение в прочих официальных информационных ресурсах. Содержание официальных материалов должно удовлетворять требованиям нормативно-правовых актов Российской Федерации. Ответственность за соответствие содержания официальных материалов требованиям нормативно-правовых актов Российской Федерации возлагается на работника, уполномоченного и согласовавшего размещение таковых материалов. Размещение официальных материалов на официальных интернет порталах осуществляется Учреждением самостоятельно, за исключением случаев, предусмотренных прочими нормативными документами. Содержание официальных материалов должно быть общедоступно и содержать свободно распространяемую информацию. Размещение в официальных материалах информации (материалов) из сторонних источников (авторов) должно осуществляться с соблюдением требований нормативно-правовых актов в сфере защиты авторских прав и интеллектуальной собственности. В соответствии с нормативными правовыми актами публикация в официальных материалах информации ограниченного доступа и составляющих государственную тайну запрещена. Обладателем информации, публикуемой на официальных интернет порталах, является Учреждение, предоставляющее данные материалы.

5.2. Программное обеспечение, используемое для осуществления деятельности Учреждения, должно соответствовать условиям его лицензирования (независимо от того, является ли оно коммерческим или 11 свободно распространяемым) и использоваться строго в соответствии с лицензионным соглашением. Случаи хранения и/или использования программного обеспечения, не являющегося лицензионным, должны быть исключены. В случае, если нормативно-правовыми актами предъявляются особые требования к программному обеспечению (например, требование по сертификации такого программного обеспечения уполномоченными организациям и т.п.) необходимо обеспечить выполнение подобных требований. На каждое автоматизированное рабочее место должен быть установлен комплект программного обеспечения, необходимый и достаточный для выполнения на нем поставленных задач. Учреждение предоставляет работникам достаточное количество лицензий на использование программного обеспечения, необходимого для выполнения работником своих должностных обязанностей.

5.3. Все серверные помещения Учреждения должны отвечать требованиям нормативно-правовых актов в части оборудования устройствами сигнализации (например, пожарной, охранной и т.п.). Помещения, которые должны быть оборудованы дополнительными устройствами регистрации, контроля и поддержания заданных характеристик (например, система автоматического пожаротушения, контроля влажности, принудительной вентиляции, кондиционирования воздуха, защиты от статического электричества и т.п.), в соответствии с нормативно-правовыми актами или правилами эксплуатации оборудования, размещенного в таких помещениях, и требуемых для соблюдения гарантийных обязательств производителя, должны быть полностью укомплектованы подобными устройствами

5.4. В помещениях, в которых размещается имущество Учреждения, должна иметься возможность организации круглосуточной охраны. В помещениях, расположенных в зданиях, в которых возможно использование услуг служб централизованной охраны здания, охрана должна осуществляться силами таких служб. В помещениях, расположенных в зданиях без служб централизованной охраны, охрана должна осуществляться за счет привлечения специализированных организаций, предоставляющих услуги по круглосуточной охране.

5.5. Все помещения Учреждения должны быть оборудованы дверьми, закрываемыми на замок. Должен быть предусмотрен механизм установления личности осуществляющей санкционированное вскрытие помещений (например, проверка удостоверения личности, применение систем контроля и управления доступом, роспись за получения ключа от помещений на посту охраны и т.п.). Отдельные группы помещений, нахождение в которых посторонних лиц не требуется (например, серверные и архивные помещения), могут отделяться дополнительными дверьми, иными средствами ограничения доступа. Помещения, доступ в которые согласно нормативно-правовым актам должен быть ограничен, а также в которых хранится или обрабатывается информация ограниченного доступа, хранятся товарно-материальные ценности и иные подобные помещения, должны быть оборудованы механизмом ограничения доступа (автоматизированная система контроля доступа, устройства для опечатывания и т.п). Работники, имеющие право самостоятельного вскрытия таких помещений должны быть определены приказом, утверждаемым руководителем Учреждения. Двери в такие помещения должны быть оборудованы механизмом автоматического их закрытия. Работники не должны оставлять свои рабочие кабинеты без наблюдения. В случае, если помещение остается без наблюдения, помещение должно быть закрыто на замок.

5.6. Антивирусное программное обеспечение должно быть установлено и функционировать в штатном режиме на всех межсетевых экранах (в 19 программном исполнении), FTP-серверах, почтовых и прочих серверах Учреждения, автоматизированных рабочих местах отдельно стоящих и подключенных к локальным вычислительным сетям (в том числе к корпоративной сети Учреждения) и портативных компьютерах. Не допускается такое изменение настроек системы антивирусной защиты, в части оповещения о нахождении компьютерных вирусов или вредоносных программ, в результате которого уменьшается эффективность данной системы. Обновление баз системы антивирусной защиты должно производиться регулярно. Построение системы антивирусной защиты должно предусматривать возможность обновления ее антивирусных баз и компонентов производителем по мере их создания. В случае невозможности такого построения системы (например, отдельно стоящие автоматизированные рабочие места в удаленных подразделениях не подключенные к каким-либо сетям), обновление системы антивирусной защиты должно производиться с регулярностью, обеспечивающей ее эффективное функционирование. Запрещается отключение системы антивирусной защиты, за исключением случаев проведения тестирования программного обеспечения и иных тестов, проводимых уполномоченными работниками Учреждения.

6. Требования
к подтверждению уничтожения персональных данных

6.1. В случае если обработка персональных данных осуществляется без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

6.2. В случае если обработка персональных данных осуществляется с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных, соответствующий требованиям, содержащимся в пунктах 6. 3 и 6.4 настоящих Требований, и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

6.3. Акт об уничтожении персональных данных должен содержать:

а) наименование Учреждения или фамилию, имя, отчество (при наличии) (физического лица) и адрес ответственного лица;

б) наименование Учреждения или фамилию, имя, отчество (при наличии) (физического лица), адрес лица (лиц), осуществляющего (осуществляющих) обработку персональных данных субъекта (субъектов) персональных данных по поручению ответственного лица (если обработка была поручена такому (таким) лицу (лицам);

в) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

г) фамилию, имя, отчество (при наличии), должность лиц (лица), уничтоживших персональные данные субъекта персональных данных, а также их (его) подпись;

д) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

е) наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

ж) наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

з) способ уничтожения персональных данных;

и) причину уничтожения персональных данных;

к) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

6.4. Акт об уничтожении персональных данных в электронной форме, подписанный в соответствии с законодательством Российской Федерации, признается электронным документом, равнозначным акту об уничтожении персональных данных на бумажном носителе, подписанному собственноручной подписью лиц, указанных в подпункте "г" пункта 3 настоящих Требований.

6.5. Выгрузка из журнала должна содержать:

а) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

б) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

в) наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;

г) причину уничтожения персональных данных;

д) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

6.6. В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные пунктом 5 настоящих Требований, недостающие сведения вносятся в акт об уничтожении персональных данных.

6.7. В случае если обработка персональных данных осуществляется ответственным лицом одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных, соответствующий требованиям, установленным пунктами 3 и 4 настоящих Требований, и выгрузка из журнала, соответствующая требованиям, установленным пунктом 5 настоящих Требований.

6.8. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.