**Министерство социальной политики**
**Калининградской области**

**Государственное бюджетное стационарное учреждение социального обслуживания**
**Калининградской области**
**«СОВЕТСКИЙ ПСИХОНЕВРОЛОГИЧЕСКИЙ ИНТЕРНАТ»**

Кутузова ул., 6 «А», Советск, 238750, тел. (40161) 3-69-00
Факс (840161) 3-69-00, e-mail: spni529@mail.ru; https:// spni529/ru
ОКПО 32760868, ОГРН 1023902005203, ИНН 3911001004, КПП 391101001

ПРИКАЗ

12.01. 2021 года № 17/5 о/д

**«Об утверждении перечня и границ контролируемых зон помещений, в которых осуществляется обработка персональных данных»**

В целях исключения неконтролируемого пребывания посторонних лиц при обработке персональных данных и в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», требованиями Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Приказом ФСТЭК России от 18 февраля 2013 года № 21, «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации»,утвержденными приказом Гостехкомиссии России от 30.08.2002 за № 282, рекомендациями ФСБ России «Методические рекомендации по обеспечению с помощью крипто средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ РФ 21.02.2008№ 149/54-144)

**П Р И К А З Ы В А Ю :**

1.Утвердить следующий перечень помещений, в которых ведется обработка персональных данных:

по адресу : 238750Калинингрвдская обл,г. Советск, ул. Кутузова ,6А

- кабинет директора и приемная каб. 1 ;
- кабинет аптеки каб. 2 ;
- кабинет специалиста по кадрам каб.3
- кабинет главного бухгалтера каб. 4 ;
- кабинет бухгалтерии каб.5 ;
- кабинет бухгалтерии каб. 6
- кабинет заместителя директора по медицинской части каб. 7 ;
- кабинет врача –терапевта каб.8 (отделение 1)
- кабинет врача –психиатра каб.9 (отделение 3)
- кабинет врача психиатра каб.10 ( отделение 10)
- кабинет заместителя директора каб.11(отделение 1)
- кабинет специалиста по социальной работе каб.12

1.Установить границы контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, средства защиты информации, предназначенные для обработки информации ограниченного пользования, по внешним ограждающим конструкциям помещений, согласно схемам представленным в Приложении к настоящему Приказу.

2 .Контроль за актуализацией и выполнением настоящего приказа возлагаю на заместителя директора –Яськова А.Ю..

Директор ГБСУСО КО
«Советский психоневрологический интернат» С.Н. Жирова

С приказом ознакомлен :

УТВЕРЖДАЮ
Директор
ГБСУСО КО «Советский
психоневрологический
интернат»
С.Н. Жтрова
от «12» декабря 2021 г.

**ПОЛОЖЕНИЕ**
**о порядке организации и проведения**
**работ по защите конфиденциальной информации**

Советск
2021г.

## 1. Общие положения

1.1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации.

1.2. Мероприятия по защите конфиденциальной информации являются составной частью управленческой и иной служебной деятельности и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.3. Информационные системы и ресурсы, являющиеся собственностью государства, подлежат обязательному учету и защите.

1.4. Режим защиты конфиденциальной информации устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством.

Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты конфиденциальной информации, сертифицируемых в установленном порядке .Обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для технической защиты конфиденциальной информации.

1.5.Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты конфиденциальной информации и величины ущерба, который может быть нанесен собственнику конфиденциальной информации при ее разглашении, утрате, уничтожении и искажении. Для сведений, составляющих служебную тайну не ниже требований, установленных данным документом и государственными стандартами Российской Федерации.

Системы и средства информатизации и связи, предназначенные для обработки(передачи) конфиденциальной информации должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

Проведение любых мероприятий и работ с конфиденциальной информацией, без принятия необходимых мер технической защиты информации не допускается.

1.6. Объектами защиты являются:

средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть (ЛВС), средства и системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации, содержащей конфиденциальную информацию -далее основные технические средства и системы (ОТСС);

технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается конфиденциальная информация - далее вспомогательные технические средства и системы (ВТСС);

помещения (служебные кабинеты, актовые, конференц-залы и т.п.),специально предназначенные для проведения конфиденциальных мероприятий –защищаемые помещения (ЗП).

1.7. Ответственность за выполнение требований настоящего Положения возлагается на руководителя, руководителей (начальников) подразделений (отделов), на начальника структурного подразделения защиты конфиденциальной информации, а также на специалистов, допущенных к обработке, передаче и хранению в технических средствах информации, содержащей конфиденциальную информацию.

1.8. Непосредственное руководство работами по защите конфиденциальной информации осуществляет ответственный за организацию обработки персональных данных в МАДОУ Детский сад №4.

## 2. Охраняемые сведения

2.1. Сведения, составляющие конфиденциальную информацию, определяются Перечнем сведений конфиденциального характера в соответствии с Указом Президента РФ от 6 марта 1997 года № 188.

Перечень сведений конфиденциального характера включает:

Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Сведения, составляющие тайну следствия и судопроизводства.

Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.).

Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна).

Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна).

Сведения, составляющие служебную тайну, определяются действующим в субъекте Российской Федерации "Перечнем сведений, составляющих служебную информацию ограниченного распространения".

Указанный перечень может включать следующие классы сведений ограниченного распространения:

сведения экономического характера;

сведения по финансовым вопросам;

сведения по науке и технике;

сведения по транспорту и связи;

сведения по вопросам внешней торговли и международных научно-технических связей;

сведения, связанные с обеспечением безопасности органов государственной власти субъекта РФ и органов местного самоуправления.

## 3. Технические каналы утечки конфиденциальной информации, несанкционированного доступа и специальных воздействий на нее.

3.1. Доступ к конфиденциальной информации, нарушение ее целостности и доступности возможно реализовать за счет:

– несанкционированного доступа к конфиденциальной информации при ее обработке в информационных системах и ресурсах;

– утечки конфиденциальной информации по техническим каналам.

3.2. Детальное описание возможных технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на ее содержится в Модели угроз безопасности информации.

## 4.Оценка возможностей технических разведок и других источников угроз безопасности конфиденциальной информации

4.1. Для добывания конфиденциальных сведений могут использоваться:

портативная возимая (носимая) аппаратура радио, акустической, визуально-оптической и телевизионной разведки, а также разведки побочных электромагнитных излучений и наводок (ПЭМИН);
автономная автоматическая аппаратура акустической и телевизионной разведки, а также разведки ПЭМИН;
компьютерная разведка, использующая различные способы и средства несанкционированного доступа к информации и специальных воздействий на нее.
Угроза компьютерной разведки объектам защиты возможна в случае подключения АС, обрабатывающим информацию ограниченного доступа к внешним, в первую очередь - глобальным сетям.
Портативная возимая аппаратура разведки может применяться из ближайших зданий и автомобилей на стоянках вблизи зданий.
Портативная носимая аппаратура имеет ограниченные возможности и может быть использована лишь для уточнения данных, или перехвата информации в непосредственной близости от защищаемых объектов.
Автономная автоматическая аппаратура радио, акустической, телевизионной, а также разведки ПЭМИН используется для длительного наблюдения за объектом защиты.
4.2. Несанкционированный доступ к информации и специальные воздействия на нее могут осуществляться при ее обработке на отдельных автоматизированных рабочих местах, в локальных вычислительных сетях, в распределенных телекоммуникационных системах.
4.3. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:
непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;
случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;
некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;
просмотра информации с экранов дисплеев и других средств ее отображения.
4.4. Оценка возможностей средств технической разведки осуществляется с использованием нормативных документов ФСТЭК России.
Наиболее опасной является аппаратура портативной (возимой и носимой)разведки электромагнитных излучений и аппаратура акустической речевой разведки, которая может применяться с прилегающей к зданиям администрации территорий, а также автономная автоматическая аппаратура акустической речевой разведки, скрытно устанавливаемая внутри помещений.
4.5. Оценка возможности НСД к информации в средствах вычислительной техники и автоматизированных системах осуществляется с использованием следующих руководящих документов ФСТЭК России:
Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;
Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;
Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по технической защите конфиденциальной информации.
НСД к информации и специальные воздействия на нее реально возможны, если не выполняются требования перечисленных выше документов, дифференцированные в зависимости от степени конфиденциальности обрабатываемой информации, уровня

полномочий пользователей по доступу к конфиденциальной информации и режимов обработки данных в автоматизированных системах.

## 5. Организационные и технические мероприятия по технической защите конфиденциальной информации

5.1. Разработка мер, и обеспечение защиты конфиденциальной информации осуществляются назначенными сотрудниками или отдельными специалистами, назначаемыми руководителем для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии ФСТЭК России и ФСБ России на право осуществления соответствующих работ.

5.2. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

5.3. Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

5.4. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителя, эксплуатирующего объекты информатизации.

5.5. Техническая защита информации в защищаемых помещениях.

К основным мероприятиям по технической защите конфиденциальной информации в ЗП относятся:

5.5.1. Определение перечня ЗП по результатам анализа циркулирующей в них конфиденциальной информации и условий ее обмена (обработки), в соответствии с нормативными документами ФСТЭК России.

5.5.2. Назначение сотрудников, ответственных за выполнение требований по технической защите конфиденциальной информации в ЗП, далее сотрудники, ответственные за безопасность информации.

5.5.3. Разработка частных инструкций по обеспечению безопасности информации в ЗП.

5.5.4. Обеспечение эффективного контроля за доступом в ЗП, а также в смежные помещения.

5.5.5. Инструктирование сотрудников, работающих в ЗП о правилах эксплуатации ПЭВМ, других технических средств обработки информации, средств связи с соблюдением требований по технической защите конфиденциальной информации.

5.5.6. Проведение в ЗП обязательных визуальных (непосредственно перед совещаниями) и инструментальных (перед ответственными совещаниями и периодически раз в квартал) проверок на наличие внедренных закладных устройств, в том числе осуществление контроля всех посторонних предметов ,подарков, сувениров и прочих предметов, оставляемых в ЗП.

5.5.7. Исключение неконтролируемого доступа к линиям связи, управления и сигнализации в ЗП, а также в смежных помещениях и в коридоре.

5.5.8. Оснащение телефонных аппаратов городской АТС, расположенных в ЗП, устройствами высокочастотной развязки подавления слабых сигналов, а также поддержание их в работоспособном состоянии. Для спаренных телефонов достаточно одного устройства на линию, выходящую за пределы ЗП.

5.5.9. Осуществление сотрудниками, ответственными за безопасность информации, контроля за проведением всех монтажных и ремонтных работ ввыделенных и смежных с ними помещениях, а также в коридорах.

5.5.10. Обеспечение требуемого уровня звукоизоляции входных дверей ЗП.

5.5.11. Обеспечение требуемого уровня звукоизоляции окон ЗП.

5.5.12. Демонтирование или заземление (с обеих сторон) лишних(незадействованных) в ЗП проводников и кабелей.

5.5.13. Отключение при проведении совещаний в ЗП всех неиспользуемых электро- и радиоприборов от сетей питания и трансляции.
5.5.14. Выполнение перед проведением совещаний следующих условий:
окна должны быть плотно закрыты и зашторены;
двери плотно прикрыты.
5.6. Защита информации, циркулирующей в ОТСС и наводящейся в ВТСС.
5.6.1. При эксплуатации ОТСС и ВТСС необходимо неукоснительное выполнение требований, определенных в предписании на эксплуатацию.
5.6.2. При невозможности обеспечения контролируемой зоны заданных размеров рекомендуется проведение следующих мероприятий:
Применение систем электромагнитного пространственного зашумления (СПЗ)в районе размещения защищаемого ОТСС.
Применение средств линейного электромагнитного зашумления (СЛЗ) линий электропитания, радиотрансляции, заземления, связи.
5.6.3. Техническая защита информации в средствах вычислительной техники(СВТ) и автоматизированных системах (АС) от несанкционированного доступа в соответствии с требованиями руководящих документов Гостехкомиссии России должна обеспечиваться путем:
проведения классификации СВТ и АС;
выполнения необходимых организационных мер защиты;
установки сертифицированных программных и аппаратно-технических средств защиты информации от НСД.
защита каналов связи, предназначенных для передачи конфиденциальной информации.
защиты информации от воздействия программ-закладок и компьютерных вирусов.
5.7. Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами Гостехкомиссии России.
Организация антивирусной защиты информации на объектах информатизации достигается путём:
установки и применения средств антивирусной защиты информации;
обновления баз данных средств антивирусной защиты информации;
действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.
5.7.1. Организация работ по антивирусной защите информации возлагается на руководителей структурных подразделений и должностных лиц, осуществляющих контроль за антивирусной защитой, а методическое руководство и контроль над эффективностью предусмотренных мер защиты информации на руководителя подразделения по защите конфиденциальной информации (ответственного) ОИВ.
5.7.2. Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:
обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации носителей информации,
информационных массивов, программных средств общего и специального назначения;
периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;
внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

восстановление работоспособности программных средств и информационныхмассивов в случае их повреждения программными вирусами.

5.7.3. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

5.7.4. Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

Входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения.

Входной антивирусный контроль всей информации, поступающей с электронной почтой;

Входной антивирусный контроль всей поступающей информации из сети Internet;

Выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а также передача информации посредством электронной почты;

Периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций и серверов;

Обязательная антивирусная проверка используемых в работе внешних носителей информации;

Постоянный антивирусный контроль на рабочих станциях и серверах с использованием резидентных антивирусных мониторов в автоматическом режиме;

Обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;

Внеплановая антивирусная проверка внешних носителей и жестких дисков рабочих станций и серверов на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;

Восстановление работоспособности программных и аппаратных средств, а также непосредственно информации в случае их повреждения компьютерными вирусами.

5.7.5.Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

5.7.6. При обнаружении на носителе информации или в полученных файлах программных вирусов пользователи докладывают об этом администратору безопасности или ответственному сотруднику, и принимают меры по восстановлению работоспособности программных средств и данных.

О факте обнаружения программных вирусов сообщается в орган, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

Перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов.

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на АРМ, поставить в известность подразделение информационно-технической службы органа власти по защите конфиденциальной информации и принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты.

При функционировании АРМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

Ликвидация последствий воздействия программных вирусов осуществляется подготовленными представителями подразделения информационно-технической службы органа власти по защите конфиденциальной информации.

5.7.7. Организация антивирусной защиты конфиденциальной информации должна быть направлена на предотвращение заражения рабочих станций, входящих в состав локальных компьютерных сетей, и серверов различного уровня и назначения вирусами.

1.8. Работа пользователей с неучтенными машинными носителями информации, оптическими и магнитными съемными носителями невозможна.

1.9. К работе с носителями информации со своих АРМ допускаются пользователи, ознакомившиеся под роспись с настоящей Инструкцией.

1.10. По фактам обнаружения подозрительных событий с несанкционированным подключением съемных носителей информации или несанкционированным перемещением данных на съемные носители администраторы безопасности информации инициируют служебное расследование.

## 2. Порядок использования носителей информации

2.1. В Организации допускается использование только учтенных носителей информации, которые являются собственностью и подвергаются регулярной ревизии и контролю.

2.2. Носители конфиденциальной информации предоставляются сотрудникам по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника производственной необходимости.

## 3. Порядок учета, хранения и обращения с носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации

3.1. Все находящиеся на хранении и в обращении носители с конфиденциальной информацией (персональными данными) в Организации подлежат учёту.

3.2. Каждый носитель с записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.3. Учет и выдачу носителей конфиденциальной информации (персональных данных) осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Факт выдачи носителя фиксируется в журнале учета носителей конфиденциальной информации.

3.4. Сотрудники организации получают учтенный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

3.5. Утилизация учтенных носителей информации возлагается на администраторов безопасности информации и/или на комиссию по информационной безопасности.

3.6. В рамках настоящей Инструкции вводится три типа утилизации носителя информации:

- **очистка:** тип утилизации, подразумевающий стирание данных с носителя информации с помощью штатных программных средств;

5.7.8. Необходимо постоянно осуществлять обновление вирусных баз. Частоту обновления установить в зависимости от используемых антивирусных средств и частоты выпуска обновления указанных баз.

5.7.9. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке, руководством по эксплуатации конкретного антивирусного программного продукта и инструкцией по антивирусной защите.

5.8. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах возлагается на системного администратора.

5.8.1. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

длина пароля должна быть не менее 8 символов;

пароль не должен включать в себя легко вычисляемые сочетания символов(имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения;

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5.8.2 Формирование личных паролей пользователей осуществляется централизованно. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

5.8.3. Полная плановая смена паролей пользователей должна проводиться регулярно.

5.8.4. Внеплановая смена личного пароля или удаление учетной информационной системы в случае прекращения его полномочий(увольнение, переход на другую работу и т.п.) должна производиться по представлению администратора безопасности уполномоченными сотрудника минемедленно после окончания последнего сеанса работы данного пользователя с системой.

5.8.5. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п.5.8.4настоящей Инструкции.

5.8.6 Хранение сотрудником (исполнителем) значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации иидентификатором TouchMemory).

5.8.7. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на администратора безопасности подразделения, периодический контроль – на специалиста по защите информации или ответственного сотрудника.

## 6. Обязанности и права должностных лиц

6.1. Руководство технической защитой конфиденциальной информации возлагается на Администратора безопасности.

6.2. Руководители подразделений организуют и обеспечивают техническую защиту информации, циркулирующую в технических средствах и помещениях подчиненных им подразделений.

6.3. Начальник структурного подразделения по технической защите конфиденциальной информации (ответственный сотрудник) осуществляет непосредственное руководство

разработкой мероприятий по технической защите конфиденциальной информации и ее контролю.

6.4. Владельцы и пользователи ОТСС обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

6.5. Руководители подразделений, владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием сведений, составляющих конфиденциальную или служебную тайну, в случае обнаружения утечки (или предпосылок к утечке) этих сведений. Предложения докладываются Администратору безопасности.

6.6. Администратор безопасности имеет право привлекать к проведению работ по технической защите конфиденциальной информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

## 7. Планирование работ по технической защите конфиденциальной информации и контролю.

7.1. В организации составляются годовые планы работ по технической защите конфиденциальной информации и контролю. Проекты планов разрабатываются ответственным сотрудником совместно с подразделениями, выполняющими работы с защищаемой информацией, рассматриваются постоянно действующей технической комиссией и утверждаются руководителем. Сроки разработки, представления и утверждения планов устанавливаются руководителем.

7.2. В годовые планы по технической защите конфиденциальной информации контролю включаются:

подготовка проектов распорядительных документов по вопросам организации технической защиты информации, инструкций, рекомендаций, памяток и других документов по обеспечению безопасности информации при использовании конкретных технических средств обработки и передачи информации, на автоматизированных рабочих местах, в ЗП;

аттестация вводимых в эксплуатацию ОТСС и ЗП, а также периодическая переаттестация находящихся в эксплуатации ОТСС и ЗП на соответствие требованиям по технической защите конфиденциальной информации;

проведение периодического контроля состояния технической защиты информации;

мероприятия по устранению нарушений и выявленных недостатков по результатам контроля;

мероприятия по совершенствованию технической защиты информации на объектах.

7.3. Контроль выполнения планов и отчетность по ним возлагается на ответственного сотрудника по технической защите конфиденциальной информации или Администратора безопасности.

## 8. Контроль состояния технической защиты конфиденциальной информации.

8.1. Основными задачами контроля состояния технической защиты конфиденциальной информации являются оценка уровня и эффективности, принятых мер защиты, своевременное выявление и предотвращение утечки по техническим каналам информации, составляющей конфиденциальную или служебную тайну, НСД к информации, преднамеренных программно-технических воздействий на информацию с целью ее уничтожения, искажения, блокирования, нарушения правового режима использования информации.

8.2. Контроль осуществляется:
ФСТЭК России;
Управлением Федеральной службы безопасности;
Ответственным сотрудником по технической защите конфиденциальной информации – непрерывно.
8.3. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты конфиденциальной информации, решений ФСТЭК России, наличия соответствующих документов по технической защите конфиденциальной информации, в инструментальной и визуальной проверке ОТСС и ЗП на наличие каналов утечки информации, на соответствие требованиям и нормам технической защиты информации.

## 9. Аттестация рабочих мест

9.1. Аттестации на соответствие требованиям по технической защите конфиденциальной информации в реальных условиях эксплуатации подлежат системы и средства информатизации и связи, предназначенные для обработки и передачи конфиденциальной информации, а также помещения, предназначенные для ведения конфиденциальных переговоров. Указанная аттестация проводится в соответствии с "Положением по аттестации объектов информатизации по требованиям безопасности информации", утвержденным Председателем Гостехкомиссии России 25 ноября 1994 г. Аттестация систем правительственной и иной закрытой шифрованием связи проводится в соответствии с нормативными документами ФАПСИ.
9.2. По результатам аттестации выдается "Аттестат соответствия", получение которого дает право использования аттестованных систем и средств для обработки и передачи информации, составляющей конфиденциальную или служебную тайну, и ведения конфиденциальных переговоров в аттестованных помещениях.
Переаттестация систем и средств информатизации, связи и помещений проводится по истечении срока действия "Аттестата соответствия", при изменении мер технической защиты информации, условий технической защиты или применяемых технологий обработки и передачи информации.

## 10. Взаимодействие с предприятиями, учреждениями и организациями

10.1. При проведении совместных работ с предприятиями, учреждениями и организациями должна быть обеспечена техническая защита информации, составляющей конфиденциальную или служебную тайну, независимо от места проведения работ.
10.2. В технических заданиях на выполнение совместных работ с использованием конфиденциальной информации, должны быть предусмотрены требования (или меры) по ее технической защите, которые должны выполняться каждой из сторон. Технические задания на выполнение совместных работ согласовываются с ответственными сотрудниками по технической защите конфиденциальной информации и взаимодействующих предприятий(учреждений, организаций).
10.3. Организация технической защиты информации возлагается на руководителей совместных работ, а ответственность за обеспечение технической защиты информации - на исполнителей работ (пользователей) при использовании ими технических средств для обработки и передачи информации, подлежащей защите.

«УТВЕРЖДАЮ»
Директор ГБСУСО КО
«Советский психоневрологический интернат»»

С.Н. Жирова
от «12» января 2021 г.

# ИНСТРУКЦИЯ
## о порядке учета, хранения, обращения и уничтожения съемных носителей, содержащих конфиденциальную информацию

### 1. Общие положения

1.1. Инструкция о порядке учета, хранения, обращения и уничтожения съемных носителей, содержащих конфиденциальную информацию в ГБСУСО КО «Советский психоневрологический интернат»» (далее – Инструкция, Организация) разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Указом Президента Российской Федерации от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера», иными нормативными правовыми актами РФ в области защиты персональных данных.

1.2. С Инструкцией знакомятся под подпись и выполняют её все лица, допущенные к обработке конфиденциальной информации, в том числе персональных данных «Приказом о допуске к обработке персональных данных».

1.3.Целью Инструкции является обеспечение режима конфиденциальности и предотвращения утечки информации, обрабатываемой в Организации.

1.4. Действие настоящей Инструкции распространяется на сотрудников Организации, в рамках выполнения своих должностных обязанностей, участвующих в обработке конфиденциальной информации (персональных данных).

1.5. Настоящей Инструкцией определяется три вида съемных носителей информации, подлежащих учету, в зависимости от механизмов и природы носителя:

– оптические носители информации (CDs, DVDs, BDs и пр.);

– магнитные носители информации (жесткие диски, магнитные карты, дискеты, ZIP, магнитные ленты и т.д.);

– электронные носители информации (Flash, карты памяти, память мобильных устройств и пр.).

1.6. Порядок учета различных видов съемных носителей приведен в п. 2.

1.7. Учет носителей информации осуществляется в специальном «Журнале учета носителей конфиденциальной информации» (Приложение № 1).

- **чистка:** тип утилизации, подразумевающий повышенную надежность уничтожения информации путем использования специальных программных или программно-аппаратных средств, позволяющий затруднить или не позволить восстановить информацию с носителя информации в лабораторных условиях с использованием специальных технических и программных средств;
- **уничтожение:** тип утилизации, подразумевающий физическое уничтожение носителя информации. Физическое уничтожение осуществляется только по Акту (Приложение 1.2) комиссией по ИБ.

Тип утилизации «очистка» может использоваться только для электронных и магнитных носителей информации, которые после утилизации будут повторно использоваться в АИС.

Тип утилизации «чистка» должен использоваться для электронных и магнитных носителей информации, которые после утилизации будут повторно использоваться за пределами ГИС. «Чистка» должна осуществляться средствами системы защиты от несанкционированного доступа.

Для оптических носителей должен использоваться тип утилизации «уничтожение», осуществляемый посредством измельчения или физического повреждения носителя с помощью специализированных шредеров и иным образом.

По результатам утилизации типа «чистка» и «уничтожение» составляется «Акт об утилизации» с указанием уникального идентификатора носителя, ФИО и должности администратора безопасности информации, даты, времени и типа утилизации.

4. **При использовании сотрудниками носителей конфиденциальной информации необходимо**:

4.1. Соблюдать требования настоящей Инструкции.

4.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

4.3. Ставить в известность администраторов о любых фактах нарушения требований настоящей Инструкции.

4.4. Бережно относится к носителям конфиденциальной информации.

4.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами.

4.6. Извещать администраторов о фактах утраты (кражи) носителей конфиденциальной информации.

5. **При использовании носителей конфиденциальной информации запрещено:**

5.1. Использовать носители конфиденциальной информации в личных целях.

5.2. Передавать носители конфиденциальной информации другим лицам (за исключением администраторов).

5.3. Хранить носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

5.4. Выносить носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

## 6. Ответственность

6.1. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником организации на неучтенных (личных) носителях информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администраторами заранее). Администратор оставляет за собой право блокировать или ограничивать использование носителей информации.

6.2. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей конфиденциальной информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется Руководителем организации.

6.3. По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Организации и действующему законодательству.

6.4. Информация, хранящаяся на носителях конфиденциальной информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

6.5. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на носителях осуществляется в порядке, установленном для документов для служебного пользования.

6.6. Вынос носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

6.7. В случае утраты или уничтожения носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета машинных носителей конфиденциальной информации (персональных данных).

6.8. Машинные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется Акт по прилагаемой форме.

6.9. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

6.10. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами организации.

Приложение 1:Журнал учета носителей конфиденциальной информации (образец листа).

Приложение 2: Форма Акта уничтожения машинного носителя

Приложение № 1
к Инструкции о порядке учета, хранения,
обращения и уничтожения съемных
носителей, содержащих
конфиденциальную информацию

**Журнал**
**учета носителей конфиденциальной информации**

| № п/п | Регистрационный номер | Дата учета | Тип/емкость носителя | Серийный номер | Отметка о постановке на учет (ФИО, подпись, дата) | Отметка о снятии с учета (ФИО, подпись, дата) | Отметка о получении носителя, ФИО, должность /реквизиты получателя | Отметка о сдаче носителя, ФИО, должность/ реквизиты | Сведения об уничтожении носителя /стирании информации |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

«УТВЕРЖДАЮ»
Директор
ГБСУСО КО «Советский психоневрологический интернат»
С.Н. Жирова
от «01» января 2021 г.

# ЖУРНАЛ
## учёта средств защиты информации в ГБССУСО КО «Советский психоневрологический интернат»

Начат «__» _____ 20__г.
Окончен «__» _____ 20__г.

18

| № п/п | Наименование СЗИ | Заводской номер/номер знака соответствия | Номер и дата сертификата | Срок действия сертификата | Продление сертификата | Место и дата установки |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Приложение № 2
к Инструкции о порядке учета,
хранения, обращения и уничтожения
съемных носителей, содержащих
конфиденциальную информацию

Форма Акта уничтожения съемного носителя

**АКТ № ___**
**уничтожения машинных носителей конфиденциальной информации**

_____ «___»_____201_г.
населенный пункт

Настоящий акт составлен в том, что комиссией в составе:
Члены комиссии:_____ _____
ФИО должность

_____ _____
ФИО должность

_____ _____
ФИО должность

проведено уничтожение съемных носителей:

| № | Уч. № носителя | Форма носителя | Способ уничтожения |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| | | | |
| | | | |
| | | | |

Члены комиссии:

_____ _____
ФИО должность

_____ _____
ФИО должность

_____ _____
ФИО должность

Приложение № 2
к приказу от «12» января № 1715 о/д
«Об определении порядка доступа
в служебные помещения
ГБСУСО КО «Советский психоневрологический интернат»»

**Правила организации режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения**

1.Настоящие правила устанавливают требования к организации режима обеспечения безопасности помещений ГБСУСО КО «Советский психоневрологический интернат»»

(далее – Организация), в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

2.Пропускной режим предусматривает:

- защиту от проникновения посторонних лиц в помещения Организации, которое обеспечивает само режим доступа.
- запрет на внос и вынос за пределы помещения материальных носителей конфиденциальной информации, в том числе персональных данных (далее – КИ);
- определение перечня должностных лиц, имеющих право доступа в помещения.

3.Внутриобъектовый режим предусматривает:

- назначение ответственного за помещение;
- помещения, в которых обрабатывается КИ с использованием средств автоматизации и без использования таких средств, должны иметь прочные двери, оборудованные механическими замками, а при необходимости, замками с контролем доступа;
- в нерабочее время помещения должны закрываться, а ключи сдаваться охране;
- выдачу ключей от помещения осуществляет по списку, утвержденному руководителем Организации;
- в случае ухода в рабочее время из помещения сотрудников, необходимо это помещение закрыть на ключ;
- уборка помещения должна производиться в присутствии лица, ответственного за это помещения.
- пребывание в помещениях посторонних лиц, не имеющих права доступа в эти помещения, разрешено только после согласования с руководителем Организации или его заместителем по направлению деятельности и в сопровождении лица, работающего в этом помещении.

- контроль за пребыванием в помещении посторонних лиц, не имеющих права доступа в эти помещения, осуществляет ответственный за это помещение.

4.Защита информационной системы и машинных носителей КИ от несанкционированного доступа, повреждения или хищения

4.1.В период эксплуатации информационных систем должны быть предусмотрены меры по исключению случаев несанкционированного доступа при проведении ремонтных, профилактических и других видов работ.

4.2.В случае необходимости проведения ремонтных работ средств вычислительной техники, входящих в состав информационной системы, с привлечением специализированных ремонтных организаций обеспечивается обязательное гарантированное уничтожение (стирание) КИ, записанной на материальном носителе под контролем лица, ответственного за организацию обработки КИ с составлением соответствующего акта.

4.3.Хранение съемных машинных носители КИ должно исключать возможность несанкционированного доступа к ним.

5.Работники Организации должны ознакомиться с настоящими Правилами под роспись.

Приложение № 17/5 к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «12» декабря 2021г № 171/5 ОД

# СОГЛАСИЕ
# НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____,
(ФИО)

паспорт _____ выдан _____,
(серия, номер) (когда и кем выдан)

адрес регистрации: _____,

даю свое согласие на обработку в _____
моих персональных данных, относящихся исключительно к перечисленным ниже категориям персональных данных: фамилия, имя, отчество; пол; дата рождения; тип документа, удостоверяющего личность; данные документа, удостоверяющего личность; гражданство.

Я даю согласие на использование персональных данных исключительно в целях

_____

_____

, а также на хранение данных об этих результатах на электронных носителях.

Настоящее согласие предоставляется мной на осуществление действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу третьим лицам для осуществления действий по обмену информацией, обезличивание, блокирование персональных данных, а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я проинформирован, что _____
гарантирует
обработку моих персональных данных в соответствии с действующим законодательством Российской Федерации как неавтоматизированным, так и автоматизированным способами.

Данное согласие действует до достижения целей обработки персональных данных или в течение срока хранения информации.

Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

"____" _____ 201__ г. _____

/_____/

Приложение № к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «[illegible]» [illegible] 2021 г. № 115

# Обязательство о неразглашении информации, содержащей персональные данные

Я, _____
(фамилия, имя, отчество полностью)

являясь работником ГБСУСО КО «Советский психоневрологический интернат»» в должности

_____

_____

(указать должность и наименование структурного подразделения) обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006
152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской

Федерации.

| _____ | _____ | _____ |
|---|---|---|
| дата | подпись | расшифровка |

Приложение № _____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «12» декабря 2020г № 175

# ПРОТОКОЛ N2

## заседания комиссии по защите информации

Дата и время проведения _____

Место проведения _____

Председатель комиссии _____ ФИО

Члены комиссии ФИО

_____ ФИО

_____ ФИО

_____

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих ГБСУСО КО «Советский психоневрологический интернат».

_____

Слушали:доложил(а) исходные данные об ИСПДн «Наименование».

_____

Выступил(а):предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Наименование».

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Наименование».

Слушали: _____

доложил(а) исходные данные об ИСПДн «Наименование».

_____

Выступил(а):предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Наименование».

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Наименование».

Председатель комиссии _____ ФИО

Члены комиссии ФИО

_____

ФИО

_____

ФИО

_____

Приложение № _____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «12» октября 2020г № 115 о/д

**АКТ**
**определения уровня защищенности ПДн при их обработке в ИСПДн «Наименование» и класса защищенности ИС «Наименование»**

Председатель комиссии ФИО

_____

Члены комиссии ФИО

_____

ФИО

_____

ФИО

_____

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

_Категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются специальные категории персональных данных;

— Категории субъектов: персональные данные субъектов персональньж данных, не являющихся сотрудниками оператора;

— Объем обрабатываемых персональных данных: менее 100 000;

— Тип актуальных угроз: для информационной системы актуальны угрозы 3-го типа;

_Уровень значимости информации: информация имеет низкий уровень значимости УЗ 3;

— Масштаб информационной системы: информационная система имеет объектовый масштаб.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а так же в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить третий уровень защищенности (УЗ 3) персональных данных и установить третий класс защищенности информационной системы (КЗ).

Результат оценки вреда:

Для информационной системы актуальны угрозы 3-го типа.

Уровень значимости информации определен степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации, руководствуясь следующей формулой:

УЗ = [(конфиденциальность, степень дерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации.

Комиссия утвердила следующее:

УЗ = [(конфиденциальность, низкая степень ущерба) (целостность, низкая степень ущерба) (доступность, низкая степень ущерба)] — таким образом, комиссия

Председатель комиссии _____ ФИО

Члены комиссии ФИО

установила низкий уровень значимости (УЗ 3) (возможны незначительные негативные последствия). _____

ФИО

_____ ФИО

_____

«__»_____20г.

Приложение № _____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «12» июня 2020г № 17/БОД

# АКТ
## об уничтожении персональных данных субъектов персональных данных

Комиссия в составе:

| Роль | ФИО | Должность |
|---|---|---|
| Председатель | | |
| Члены комиссии | | |
| | | |
| | | |

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные.

| № п/п | Сведения, содержащие персональные данные | Место хранения | Кол-во ед. хранения | Примечание |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

Указанные персональные данные уничтожены путем

_____

(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель комиссии:

_____ _____
подпись расшифровка

Члены комиссии:

_____ _____ _____
подпись расшифровка

_____ _____ _____
подпись расшифровка

Приложение к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «[illegible]» [illegible] 2021 г. № [illegible]

Перечень информационных систем персональных данных

| Наименование | Адрес расположения |
|---|---|
| | |
| | |

Приложение № _____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «12» декабря 2021г № 1115 ОД

**Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения**

## 1. Общие положения

1.1. Положение об организации режима обеспечения безопасности помещений ГБСУСО КО «Советский психоневрологический интернат»» (далее — Оператор), в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее — Положение) разработано в соответствии с Постановлением правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1 .2. Защита от проникновения посторонних лиц в помещения Оператора обеспечивается организацией порядка доступа, а также соответствующей инженернотехнической защитой помещений, а именно охранной сигнализацией и системой контроля и управления доступом.

## 2. Границы контролируемой зоны

2.1. Контролируемая зона — границы пространства (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

## 3. Порядок доступа в помещения

3.1. Перечень лиц, доступ которых в помещения находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых обязанностей) приведен в приложении 1 к настоящему приказу.

3.2. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 3.1 настоящего Положения разрешено в период рабочего времени в соответствии с утвержденным графиком работы Оператора, либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

3 . 3. Лица, не указанные в п. 3.1 настоящего Положения, допускаются в помещения в присутствии лиц, имеющих право пребывания в данных помещениях.

Приложение к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «12» [illegible] 2021 № 175 ОД

# ИНСТРУКЦИЯ

**ответственного за организацию обработки персональных данных**

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

— Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

— Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.112012 № 1 119;

— Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;

— Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

— Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Обязанности

Ответственный за организацию обработки персональных данных обязан:

— Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;

— Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;

— 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.

## 3. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

## 4. Права

Ответственный за организацию обработки персональных данных имеет право:

— Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;

— Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

Приложение № _____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «12 января 2021г № 1/15 о/д

**ПРАВИЛА**

**рассмотрения запросов субъектов персональных данных или их представителей**

1 . Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

_Подтверждение факта обработки персональных данных;

— Правовые основания и цели обработки персональных данных;

— Цели и применяемые оператором способы обработки персональных данных;

_ Наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Федеральный закон);

— Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

— Сроки обработки персональных данных, в том числе сроки их хранения;

— Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

2. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных

данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих правил, должен содержать обоснование направления повторного запроса.

7. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

8. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

— Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

— В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

— Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях, предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

_ Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение № _____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «12 июля» 2021г №115 ОД

**Правила**
**работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей**

Допуск для работы на автоматизированных рабочих местах (далее — АРМ) состоящих в составе информационной системы персональных данных (далее — ИСПДн{ осуществляется на основании утвержденного перечня лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей (далее — Пользователи ИСПДн).

Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей персональные данные (далее — ИПДн), разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

Вход пользователя в систему осуществляется по выдаваемому ему электронному идентификатору и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий

доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

— Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;

— Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

— Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;

— Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

— Выполнять требования инструкции по организации антивирусной защиты в полном объеме;

— Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

— Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;

— Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

Некорректного функционирования установленных на АРМ технических средств защиты;

— Непредусмотренных отводов кабелей и подключенных устройств.

Пользователю АРМ категорически запрещается:

— Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

— Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

— Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флэш-накопителях и т.п.);

— Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

— Оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители и распечатки, содержащие персональные данные;

— Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;

— Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.

Приложение № _____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»
От «12 сентября 2021г № 173/4д

# ИНСТРУКЦИЯ

**ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных**

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее — ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан :

— Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в испдн;

— Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.

— Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

— Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);

_ Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных,

обрабатываемых в ИСПДн;

_ Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;

_ Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;

_ Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;

— Обязан вести журнал учета средств защиты информации, используемых в испдн;

— Обязан присутствовать (участвовать) в работах по внесению изменении в аппаратно-программную конфигурацию АРМ;

— Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;

— Обязан проводить мероприятия по организации антивирусной защиты;

— Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;

_ Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

_Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

_Установить причины, по которым стал возможным НСД;

— Установить последствия, к которым привел НСД;

_Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

— Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к

защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;

_Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных,

3. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

_Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

— Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

— Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию испдн;

4. Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в испдн•,

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 1 к приказу ГБСУСО КО
«Советский психоневрологический интернат»

# ИНСТРУКЦИЯ
## по организации резервирования

### 1. Общие положения

Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция* определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных (далее - ИСПДН)

### 2. Резервируемое программное обеспечение и базы персональных данных

В ИСПДн резервированию подлежит:

— Общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее — АРМ), входящими в состав испдн)•,

— Прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);

— Базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);

— Программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

### 3.Порядок резервирования и хранения резервных копий

Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДН- машинных носителей информации, содержащих дистрибутивы Данного программного обеспечения.

Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора информационной безопасности в испдн.

Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервирование осуществляется ежемесячно.

Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации персональных данных.

К резервному носителю персональных данных должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

4 Порядок восстановления работоспособности ИСПДн

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы осуществляются администратором информационной безопасности в ИСПДН в соответствии С эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.

Учетная карточка резервного носителя персональных данных
№ _____

| Дата резервного копирования | Объект копирования | Кто производил копирование | Подпись |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

Приложение № _____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»

# ИНСТРУКЦИЯ

## по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее — ИСПДн), а также контроль за действиями пользователей при работе с паролями.

Личные пароли генерируются и распределяются централизованно Администратором информационной безопасности:

— Длина пароля должна быть не менее 8 символов;

— В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, 5, &, *, % и т.п.);

— Символы паролей должны вводиться в режиме латинской раскладки клавиатуры;

— Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

— При смене пароля новое значение должно отличаться от предыдущих;

— Пользователь не имеет права сообщать личный пароль другим лицам;

Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в 3 месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором информационной безопасности в ИСПДн немедленно после окончания последнего сеанса работы данного пользователя ИСПДн с системой на основании письменного указания непосредственного руководителя структурного подразделения.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности в ИСПДн.

В случае компрометации (утеря, передача другому лицу) личного пароля, Пользователь ИСПДн обязан незамедлительно сообщить об этом администратору информационной безопасности для принятия соответствующих мер.

Приложение № ____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»

# ИНСТРУКЦИЯ
## по организации антивирусной защиты

1. Общие требования

Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее испдн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководителя и работников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы.

К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка и настройка средств антивирусного контроля осуществляется администратором информационной безопасности в ИСПДн или специально назначенным лицом в соответствии с эксплуатационной документацией на антивирусных средств.

2. Применение средств антивирусного контроля

При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

Полному антивирусному контролю автоматизированные рабочие места (АРМ) должны подвергаться не реже одного раза в неделю.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в. месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения, администратором информационной безопасности в ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ.

При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник структурного подразделения самостоятельно или вместе с администратором информационной безопасности в ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

— Приостановить работу в ИСПДн;

— Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и администратора информационной безопасности в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

— Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

— Провести лечение или уничтожение зараженных файлов.

## 3. Ответственность

Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности в ИСПДн и всех работников, являющихся пользователями ИСПДн.

Приложение № к приказу ГБСУСО КО
«Советский психоневрологический интернат»

# ПОРЯДОК

## уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении инух законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при вступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется в свободной форме).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются,

После уничтожения материальных носителей ответственный за организацию подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт № (дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

Приложение № ____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»

# ПРАВИЛА
## осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в ГБСУСО КО «Психоневрологический интернат «Забота»» требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» (далее —» Правила), устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют порядок проведения процедур внутреннего контроля исполнения требований законодательства.

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных организовывается проведение периодических проверок.

Проверки осуществляются ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных.

Плановые проверки проводятся не чаще чем один раз в три месяца.

Внеплановые проверки проводятся по инициативе ответственного за организацию обработки персональных данных, либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

Основанием для проведения проверки служит издание приказа «О проведении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных»

При проведении проверки должны быть полностью, объективно и всесторонне установлены:

— соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора персональных данных;

— соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных,

— достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;

— отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных; _ порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных; _ порядок и условия применения средств защиты информации; _ соблюдение правил доступа к персональным данным;

— наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.

8. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных в ходе проверки имеют право:

— запрашивать у работников информацию, необходимую для реализации своих полномочий;

— требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

— принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

— вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

— вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. Ответственный за организацию обработки персональных данных в течение 3 (трех) рабочих дней направляет в адрес директора результаты проведения проверки в форме служебной записки.

Приложение № ____ к приказу ГБСУСО КО
«Советский психоневрологический интернат»

# ИНСТРУКЦИЯ
## по обращению с криптосредствами

**1. Общие положения**

Настоящая инструкция регламентирует порядок обращения с шифровальными средствами (средствами криптографической защиты информации, СКЗИ), предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, встраивания в прикладные системы, тестирования, передачи клиентам, а также порядок допуска к работам с шифровальными средствами.

Все сотрудники, допущенные к работе с СКЗИ, должны ознакомиться с данной инструкцией под подпись и строго выполнять требования настоящей инструкции в части, их касающейся, а также строго выполнять требования нормативных правовых актов Российской Федерации, относящихся к деятельности с СКЗИ, нормативных и методических документов лицензирующего органа.

Разработка и проведение мероприятий по обеспечению безопасности при работе с СКЗИ осуществляется ответственным за эксплуатацию СКЗИ.

Работы с СКЗИ должны проводиться с учетом Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

**2.Требования по размещению, оборудованию и охране помещений**

Размещение, оборудование, охрана и режим в помещениях, в которых проводятся работы с СКЗИ (далее — помещения), должны обеспечивать безопасность СКЗИ, сведение к минимуму возможности неконтролируемого доступа посторонних лиц. Доступ сотрудников в эти помещения должен быть ограничен в соответствии со служебной необходимостью и определяться перечнем лиц, допущенных в кабинеты,

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Для предотвращения просмотра извне окна помещений должны быть защищены (жалюзи, шторы и т.п.).

**3 Порядок обращения с СКЗИ Пользователи криптосредств обязаны:**

_ не разглашать информацию о ключевых документах; не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер; _ не допускать установки ключевых документов в другие ПЭВМ.

Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация (при наличии) к ним должны браться на поэкземплярный учет в журнале установленной формы (Приложение). Ведет журналы администратор информационной безопасности.

Единицей поэкземплярного учета СКЗИ является:

—для аппаратных и программно-аппаратных СКЗИ - конструктивно законченное техническое устройство;

—для программных СКЗИ — инсталлирующий СКЗИ носитель (дискета, компакт-диск (CD-ROM) и т.п.).

Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение.

В случае отсутствия у сотрудника индивидуального хранилища инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщйть об этом лицу, ответственному за обеспечение безопасности при обращении с СКЗИ.

Ответственным за эксплуатацию СКЗИ периодически должен проводиться контроль сохранности и работоспособности установленного СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программноаппаратных закладок и вирусов.

## 4.Ответственность за нарушение требований Инструкции

За нарушение требований настоящей Инструкции виновные лица несут дисциплинарную, либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.