Приложение 4

УТВЕРЖДАЮ
директор СОГБУ
«Шаталовский детский дом»
_____ Т. А. Соколова
«__4__» ____11____ 2017г.

ПРАВИЛА
осуществления внутреннего контроля выполнения требований по защите персональных данных в СОГБУ «Шаталовский детский дом»

Правила осуществления внутреннего контроля выполнения требований по защите персональных данных (далее - Правила) в СОГБУ «Шаталовский детский дом» (далее - Учреждение) определяют порядок организации и осуществления внутреннего контроля выполнения требований по защите персональных данных в структурных подразделениях Учреждения.

Требования правил обязательны для исполнения всеми должностными лицами Учреждения, осуществляющими контроль состояния защиты персональных данных.

1. Общие положения

Контроль выполнения требований по защите персональных данных в структурных подразделениях Учреждения осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных в Учреждении. Для участия в проведении контроля решением ответственного за организацию обработки персональных данных могут также привлекаться другие специалисты подразделений Учреждения (по согласованию с их руководителями структурных подразделений Учреждения). В таких случаях контроль носит комплексный характер.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов Учреждения или нарушения требований по защите персональных данных.

Сроки проведения контрольных проверок доводятся руководителям проверяемых подразделений не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых подразделений.

Периодичность и сроки проведения плановых проверок подразделений Учреждения устанавливаются графиком проверок на календарный год. План утверждает директор Учреждения. Сроки проведения плановых проверок доводятся руководителям проверяемых подразделений не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Для участия в проведении проверки ответственным за организацию обработки персональных данных заблаговременно назначаются соответствующие компетентные специалисты (далее – проверяющие лица). В случае проведения проверки комиссией также назначается ее председатель.

Председатель комиссии (старший по проверке) подготавливает в адрес руководителя проверяемого подразделения распоряжение о проверке за подписью ответственного за организацию обработки персональных данных в Учреждении и перечень вопросов проверки (при необходимости). Председатель комиссии (старший по проверке) распределяет обязанности по проверке конкретных участков работы между проверяющими лицами.

Проверяющие лица инструктируются непосредственным начальником об особенностях работы в конкретном подразделении Учреждения. За 3 – 4 дня до начала проверки они должны изучить материалы предыдущих проверок данного подразделения, уточнить наличие в нем защищаемых ресурсов, сил и средств защиты персональных данных, а также особенности их функционирования.

3. Порядок проведения проверки

По прибытию в подразделение для проведения проверки председатель комиссии (старший по проверке) прибывает к руководителю проверяемого подразделения Учреждения, представляется ему и представляет других прибывших на проверку лиц. При этом согласовываются конкретные вопросы по объему, содержанию, срокам проверки, а также каких должностных лиц подразделения необходимо привлечь к проверке и какие объекты следует посетить. Допуск лиц, прибывших на проверку, к конкретным информационным ресурсам, охраняемым сведениям и техническим средствам производится руководителем подразделения на основании распоряжения о проверке. Подобный допуск должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать.

Руководителем подразделения принимаются необходимые меры для обеспечения работы комиссии по проверке и определяется должностное лицо подразделения, ответственное за обеспечение работы комиссии.

В ходе осуществления контроля выполнения требований по защите персональных данных в подразделении Учреждения проверке подлежат следующие показатели:

1. В части общей организации работ по защите персональных данных:

соответствие информации, указанной в уведомлении об обработке персональных данных, реальному положению дел;

наличие нормативных документов по защите персональных данных;

знание нормативных документов сотрудниками, имеющими доступ к персональным данным;

полнота и правильность выполнения требований нормативных документов

сотрудниками, имеющими доступ к персональным данным;

наличие лиц, назначенных ответственными за организацию обработки персональных данных в подразделении, уровень их профессиональной подготовки и способность выполнить возложенные обязанности;

наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объема персональных данных и сроков обработки целям обработки персональных данных;

соответствие схемы контролируемой зоны, перечня мест хранения материальных носителей, перечня лиц, допущенных к обработке персональных данных фактическому состоянию.

2. В части защиты персональных данных в информационных системах персональных данных (ИСПДн):

соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных (СПД);

контроль целостности пломб на аппаратных средствах, с которыми осуществляется штатное функционирование средств криптографической защиты информации;

соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах ЭВТ;

соблюдение требований, предъявляемых к паролям на информационные ресурсы;

соблюдение требований и правил антивирусной защиты ПЭВМ и программ;

контроль журналов учета носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учета носителей);

тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3. В части защиты информационных ресурсов и помещений:

правильность отнесения обрабатываемой информации к персональным данным;

правильность классификации информационной системы;

закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о подразделениях Учреждения, должностных инструкциях сотрудников и трудовых договорах;

порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

состояние конфиденциального делопроизводства, соблюдение установленного

порядка подготовки, учета, использования, хранения и уничтожения документов, содержащих персональные данные;

выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т. п.).

В ходе работы проверяющие лица должны принимать меры по устранению на месте отмечаемых нарушений и недостатков. Для этого с должностными лицами подразделения, ответственными за конкретные участки работы, где отмечались недостатки, одновременно должны проводиться разъяснения требований руководящих документов и оказываться практическая помощь в правильной постановке работы.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

актом - при проведении проверки комиссией;
служебной запиской - при проведении проверки назначенными специалистами.

Акт (служебная записка) составляется в двух экземплярах, как правило, на месте в подразделении, подписывается председателем и членами комиссии (старшим по проверке), докладывается под роспись руководителю подразделения и представляется на утверждение (на доклад) ответственному за организацию обработки персональных данных в Учреждении. Один экземпляр документа высылается в подразделение.

В случае несогласия с выводами комиссии (проверяющих лиц) руководитель подразделения может выразить в письменном виде свое особое мнение (прилагается к акту или служебной записке).

Результаты проверок подразделений периодически обобщаются ответственным за организацию обработки персональных данных в Учреждении и доводятся до руководителей подразделений.