Государственное бюджетное дошкольное образовательное учреждение
детский сад № 27 комбинированного вида
Красногвардейского района Санкт-Петербурга

Принято
Общим собранием трудового
коллектива ГБДОУ детский сад
№ 27
Красногвардейского района СПб
Протокол № 1 от 07.02. 2019

Утверждаю :
Заведующий ГБДОУ
детский сад № 27
_____Е.Е.Мелешкина
« 07 » 02.2019г.
Приказ № 10/1-о
От 07.02.2019г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 6635680065ADB8A64357E0855B692FE1
Владелец: Мелешкина Елена Евгеньевна
Действителен: с 14.07.2021 до 14.10.2022

ПОЛОЖЕНИЕ

о порядке организации и проведения работ по защите конфиденциальной информации в Государственном бюджетном дошкольном образовательном учреждении детский сад № 27 комбинированного вида Красногвардейского района Санкт-Петербурга

Санкт-Петербург
2019г.

Оглавление

1. Термины, определения и сокращения

АС	**Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
ЗП	**Защищаемые помещения** - помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.)
КЗ	**Контролируемая зона** - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств
НСД	**Несанкционированный доступ** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых СВТ или АС
СЗИ	**Система защиты информации** - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации
СТР-К	**Специальные требования и рекомендации по защите конфиденциальной информации** – нормативно-методический документ. Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282
ТЗИ	**Техническая защита информации** - защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

2. Общие положения

2.1. Настоящее «Положение о порядке организации и проведения работ по защите конфиденциальной информации» (далее Положение) определяет содержание, порядок организации и проведения работ по технической защите конфиденциальной информации на объектах информатизации Государственного бюджетного дошкольного образовательного учреждения детский сад № 27 комбинированного вида Красногвардейского района Санкт-Петербурга (далее Организация).

2.2. Положение является документом, обязательным для выполнения всеми должностными лицами Организации при проведении работ, требующих технической защиты конфиденциальной информации, на проектируемых (реконструируемых) и действующих (находящихся в эксплуатации) объектах информатизации Организации.

2.3. К конфиденциальной информации в Положении относится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну:

– персональные данные (доступ к персональным данным должен быть ограничен в соответствии с ФЗ «О персональных данных» - № 152-ФЗ от 27.07.2006 г.);

– коммерческая тайна (доступ к информации, составляющей коммерческую тайну, может быть ограничен обладателем информации в соответствии с ФЗ «О коммерческой тайне» - № 98-ФЗ от 29.07.2004 г.);

– служебная информация ограниченного распространения – информация, касающаяся деятельности Организации, ограничение на распространение которой вызвано служебной необходимостью (доступ к служебной информации ограничивается в соответствии с «Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», утвержденным постановлением Правительства Российской Федерации от 3 ноября 1994 года N 1233 (документы с пометкой «Для служебного пользования»).

2.4. Совокупность средств и систем обработки информации вместе с помещениями (зданиями, сооружениями), в которых они установлены, образуют **объект информатизации**.

2.5. Речевая информация подлежит защите на объектах информатизации предназначенных для ведения конфиденциальных переговоров – в защищаемых помещениях.

2.6. На объектах информатизации, использующих для обработки информации технические средства (средства вычислительной техники, средства и системы связи и передачи данных, тиражирования документов) защите подлежит информация, обрабатываемая техническими средствами, информация, зафиксированная на съемных носителях и на бумажной основе,

а при необходимости и информация, представленная в виде информативных электрических сигналов и физических полей.

2.7. Правовую основу Положения составляют Конституция Российской Федерации, Федеральные законы «О безопасности», «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Специальные требования и рекомендации по технической защите конфиденциальной информации» (далее – СТР-К), утвержденные приказом ФСТЭК России от 30.08.2002 № 282, другие нормативные акты Российской Федерации, определяющие права и ответственность граждан, Организации и государства в сфере защиты информации ограниченного доступа (Постановления 781, 687).

2.8. Работы по защите информации на объектах информатизации являются составной частью деятельности Организации и осуществляются во взаимосвязи с работами по другим направлениям обеспечения безопасности. Проведение мероприятий, связанных с возможной утечкой (или раскрытием) сведений конфиденциального характера, при обсуждении, передаче, обработке и хранении конфиденциальной информации на объектах информатизации допускается только после определения и принятия необходимых мер по их защите в соответствии с требованиями настоящего Положения и других нормативных методических документов по защите информации.

2.9. Ответственность за организацию и состояние защиты конфиденциальной информации на объектах информатизации возлагается на Заведующего ОУ.

2.10. Непосредственное руководство работами по защите конфиденциальной информации осуществляет заместитель заведующего Организации, курирующий вопросы защиты информации.

2.11. Проведение единой политики и методическое руководство при проведении работ по защите информации, а также контроль за эффективностью предусмотренных мер защиты информации на объектах информатизации Организации возложено на заместитель заведующего

2.12. Ответственность за реализацию мероприятий по защите информации возлагается на руководителей подразделений Организации, в которых осуществляется работа с конфиденциальной информацией.

2.13. Должностные лица, организующие работу с конфиденциальной информацией на объектах информатизации, несут персональную ответственность за соблюдение требований настоящего Положения.

2.14. Объектами информатизации Организации, на которых необходимо проведение работ по технической защите информации, являются: автоматизированные системы (далее – АС), локальные вычислительные сети, средства и системы связи и передачи информации, используемые для обработки, хранения и передачи конфиденциальной информации, а также помещения, предназначенные для проведения конфиденциальных мероприятий – защищаемые помещения.

2.15. Средства защиты информации, используемые на объектах информатизации Организации, в установленном порядке проходят процедуру оценки соответствия.

2.16. На объектах информатизации, предназначенных для обработки конфиденциальной информации, необходимо проведение работ по технической защите информации (далее – ТЗИ) в соответствии нормативными методическими документами ФСТЭК России.

2.17. Должностные лица, принявшие решение об отнесении информации к разряду конфиденциальной, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений, предусмотренных настоящим Положением.

2.18. За разглашение конфиденциальной информации, а также за нарушение установленного порядка обращения с ней на объектах информатизации, работники Организации могут быть привлечены к ответственности, предусмотренной законодательством Российской Федерации.

3. Порядок определения защищаемой информации

3.1. Отнесение сведений к конфиденциальной информации осуществляется на основании «Перечня сведений конфиденциального характера Государственного бюджетного дошкольного образовательного учреждения детский сад № 27 комбинированного вида Красногвардейского района Санкт-Петербурга ».

3.2. На основании пункта 4 статьи 8 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ не может быть ограничен доступ к следующей информации:

- нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информации о состоянии окружающей среды;
- информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

3.3. На основании статьи 5 Федерального закона «О коммерческой тайне» от 29 июля 2004 года N 98-ФЗ режим коммерческой тайны не может быть установлен в отношении следующих сведений:

- содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах;

- содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- о загрязнении окружающей среды, состоянии противопожарной безопасности и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
- о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;
- о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица.

4. Порядок привлечения подразделений Организации и специализированных сторонних организаций к разработке и эксплуатации объектов информатизации и систем защиты информации

4.1. Проведение единой политики по защите конфиденциальной информации, циркулирующей на объектах информатизации Организации, а также осуществление контроля эффективности принимаемых мер по ее защите осуществляет заместителя заведующего.

На заместителя заведующего возложены следующие основные задачи:

– разработка и осуществление в пределах своей компетенции мероприятий по защите информации ограниченного доступа в Обществе;

– проведение периодического контроля эффективности мероприятий по защите информации на объектах информатизации Организации;

– оказание методической помощи структурным подразделениям Организации по вопросам защиты информации.

При проведении работ по защите информации на объектах информатизации Организации оператор взаимодействует со структурными подразделениями Организации, а также с территориальными органами ФСТЭК России и ФСБ России.

4.2. Для проведения работ по технической защите конфиденциальной информации на объектах информатизации Организации могут привлекаться специализированные организации, имеющие лицензии ФСТЭК России на соответствующий вид деятельности.

Перечень работ, для которых необходимо привлечение указанных организаций-лицензиатов ФСТЭК России, определяется заместителем директора, согласовывается с руководителями подразделений, в чьих интересах проводятся работы по ТЗИ. Указанный перечень работ до заключения договора должен быть утвержден директором Организации.

4.3. С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения несанкционированного доступа к ней и предотвращения специальных программно-технических воздействий, вызывающих нарушение конфиденциальности, целостности и (или) доступности информации, должен проводиться периодический (не реже одного раза в год) контроль состояния защиты конфиденциальной информации на объектах информатизации Организации. Контроль осуществляется специалистами управления защиты информации по поручению заместителя директора и заключается в оценке:

- соблюдения требований нормативно-методических документов по защите информации, а также эксплуатационной документации;
- работоспособности и эффективности применяемых средств защиты информации;
- знаний и выполнения персоналом своих функциональных обязанностей в области ТЗИ.

5. Порядок взаимодействия подразделений Организации при проведении работ по разработке и эксплуатации объектов информатизации и средств защиты информации

5.1. Разработка и внедрение системы защиты информации (далее – СЗИ) на объекте информатизации должны проводиться во взаимодействии организации - разработчика СЗИ с Начальником управления защиты информации. Специалисты управления защиты информации должны участвовать в разработке конкретных требований по ТЗИ, обосновании необходимости создания СЗИ, согласовании технических и программных средств защиты информации, организации работ по выявлению возможных каналов утечки информации или воздействий на нее и предупреждению утечки и нарушения целостности защищаемой информации, а также в аттестации объектов информатизации.

5.2. Проекты организационно-распорядительной документации, разработанные на объект информатизации, должны быть согласованы с начальником управления защиты информации.

5.3. Подразделением Организации, в интересах которого создается объект информатизации, во взаимодействии с сотрудниками управления защиты информации осуществляется опытная эксплуатация и приемо-сдаточные испытания СЗИ.

5.4. В случае выявления нарушений предусмотренных мер защиты информации в ходе эксплуатации объекта информатизации оператор должен

сообщить о них заместителя заведующего, разработать мероприятия по их устранению и проконтролировать их выполнение.

5.5. Руководитель подразделения, на объекте информатизации которого выявлены нарушения по ТЗИ, должен немедленно принять меры по их устранению, а в случае невозможности их устранения – приостановить обработку конфиденциальной информации на объекте информатизации и сообщить об этом заведующему.

6. Порядок разработки, ввода в действие и эксплуатацию объектов информатизации

6.1. Защита информации на объекте информатизации достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам, несанкционированного доступа к ней, программно-технических воздействий на защищаемую информацию с целью нарушения ее целостности (модификации, уничтожения) и доступности в процессе обработки, передачи и хранения информации, а также обеспечения работоспособности технических средств.

6.2. В соответствии с разделом 3 СТР-К создание СЗИ на объектах информатизации должно осуществляться по следующим стадиям:

- *предпроектная стадия;*
- *стадия проектирования;*
- *стадия ввода в действие.*

6.3. *На предпроектной стадии* проводится обследование объекта информатизации, разработка аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание.

6.3.1. В процессе обследования:

- устанавливается необходимость обработки (обсуждения) конфиденциальной информации на данном объекте информатизации;
- определяется перечень сведений конфиденциального характера, подлежащих защите;
- определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта;
- определяются условия расположения объектов информатизации относительно границ КЗ;
- определяются конфигурация и топология автоматизированных систем (далее АС) и систем связи в целом и их отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

- определяются технические средства и системы, предполагаемые к использованию в разрабатываемой АС и системах связи, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;
- определяются режимы обработки информации в АС в целом и в отдельных компонентах;
- проводится классификация АС с целью определения необходимого для нее класса защищенности;
- определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности;
- определяются мероприятия по обеспечению конфиденциальности информации на этапе проектирования объекта информатизации.

6.3.2. По результатам предпроектного обследования объекта информатизации должны быть разработаны:

- аналитическое обоснование необходимости создания СЗИ (требования к содержанию документа приведены в п. 3.12 СТР-К);

- техническое задание на разработку СЗИ (требования к содержанию документа приведены в п. 3.13 СТР-К).

Указанные документы должны быть подписаны организацией – разработчиком (в случае привлечения сторонней организации), согласованы с заместителем заведующего, и утверждены заведующим Организации.

6.3.3. При проведении классификации АС используется Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», (Гостехкомиссия России, 1992).

Для проведения классификации АС приказом заведующего Организации назначается комиссия, в состав которой должны входить сотрудники управления защиты информации.

Исходными данными для проведения классификации являются:

– перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

– перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;

– матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

– режим обработки данных в АС (коллективный или индивидуальный).

Результат классификации оформляется актом, который подписывается членами комиссии и утверждается заведующим Организации. Пересмотр класса защищенности АС производится в обязательном порядке, если произошло изменение хотя бы одного из критериев, на основании которых он был установлен.

6.3.4. Классификация информационных систем персональных данных (далее ИСПДн) проводится в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года N 55/86/20. При проведении классификации ИСПДн используется разработанная для этой системы частная модель угроз безопасности персональным данным.

Порядок создания комиссии и оформления акта классификации ИСПДн аналогичен пункту 5.2.1.

6.4. *На стадии проектирования* СЗИ объекта информатизации на основе предъявляемых требований и заданных Организацией (как заказчиком работ) ограничений на финансовые, материальные, трудовые и временные ресурсы разработчиком осуществляются:

- разработка раздела технического проекта на объект информатизации в части защиты информации;
- разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- закупка при необходимости сертифицированных технических, программных и программно-технических средств защиты информации и их установка;
- разработка эксплуатационной документации на объект информатизации и средства защиты информации;
- реализация разрешительной системы доступа персонала к обрабатываемой (обсуждаемой) на объекте информатизации информации;
- выполнение инсталляции пакета прикладных программ в комплексе с программными средствами защиты информации.

6.4.1. При проектировании СЗИ Организация должна:

- обеспечить охрану и физическую защиту помещений объекта информатизации, исключающих НСД к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;
- разработать и утвердить организационно-распорядительную документацию по защите информации (приказы, инструкции);
- определить подразделения и лиц, ответственных за эксплуатацию средств защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации.

6.4.2. При необходимости, по распоряжению заведующего, могут быть проведены работы по поиску электронных устройств съема информации (закладочных устройств), возможно внедренных на объектах

информатизации. Для этих работ привлекаются организации, имеющие соответствующие лицензии ФСБ России.

6.4.3. На стадии проектирования и создания СЗИ объекта информатизации также должны быть оформлены Технический проект и эксплуатационная документация СЗИ, оформленные в соответствии с требованиями п. 3.18 СТР-К.

6.5. *На стадии ввода в действие* СЗИ объекта информатизации должны быть оформлены:

- акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний;
- протоколы аттестационных испытаний и заключение по их результатам;
- аттестат соответствия объекта информатизации требованиям безопасности информации.

6.6. Эксплуатация объекта информатизации осуществляется в соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией.

7. Ответственность должностных лиц за своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗИ

7.1. При проведении работ с информацией конфиденциального характера должностные лица Организации несут ответственность за качество разработки и реализации требований по ТЗИ. В частности:

- *заместитель заведующего* несет ответственность за научно-технический уровень разработки и функционирование СЗИ на объектах информатизации Организации;

- *руководители подразделений* отвечают за выполнение комплекса организационно-технических мероприятий при осуществлении обработки конфиденциальной информации на закрепленных объектах информатизации;

- *сотрудники подразделений Организации* отвечают за выполнение на своих рабочих местах требований организационно-распорядительных документов (приказов, распоряжений, указаний, инструкций) Организации по порядку обращения (обработки) с конфиденциальной информацией в процессе эксплуатации объектов информатизации и средств защиты информации.

7.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.