Принято:	Утверждено:
Решением Общего собрания Работников ГБОУ школы №565 Кировского района Санкт-Петербурга Протокол №003 от 29 августа 2019г.	**Приказом директора ГБОУ школы №565 Кировского района Санкт-Петербурга №524 от 29 августа 2019г. Директор _____Чалапко Е.В.**

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите конфиденциальной информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (конфиденциальная информация) в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга

1. Общие положения

1.1. Настоящее Положение о порядке организации и проведения работ по защите конфиденциальной информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (конфиденциальная информация) в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга разработано в соответствии с Федеральным Законом от 27.07.2006 г № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 г. № 282, и другими нормативно-методическими документами по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита от несанкционированных действий - деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

Защита информации от утечки - деятельность по предотвращению неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к защищаемой информации и получения защищаемой информации.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями действующего законодательства.

Любая информация ограниченного доступа, вне зависимости от форм хранения, подлежит дифференцированной защите, в том числе:

-речевая информация;

-информация, циркулирующая в средствах связи и вычислительной техники;

-информация, передаваемая по каналам связи, локальным или глобальным вычислительным сетям;

-информация на бумажной, магнитной или другой основе;

-информационные массивы и базы данных, которые должны защищаться в соответствии с законодательством Российской Федерации.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Категорирование защищаемой информации (объекта защиты) - установление градаций важности защиты защищаемой информации (объекта защиты).

Конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Охраняемые сведения - сведения, составляющие государственную, служебную, коммерческую или личную тайну, на распространение которых накладываются ограничения в установленном порядке.

Пользователь информации - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Правило доступа к информации (правило доступа) - совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, осуществляющий владение, пользование и распоряжение указанными объектами.

Целостность информации - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

1.2. Настоящее положение определяет порядок организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (далее именуется – информация ограниченного доступа), в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга.

1.3 Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее собственника.

1.4 При определении конфиденциальности документов, в том числе в электронной форме, необходимо руководствоваться Перечнем сведений конфиденциального характера в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга.

1.5 Сотрудники Государственного бюджетного общеобразовательного учреждения школа № 565 Кировского района Санкт-Петербурга, которые в силу служебной необходимости должны иметь доступ к информации конфиденциального характера, обязаны ознакомиться с настоящим Положением и подписать обязательство о неразглашении информации конфиденциального характера (приложение 1)

1.6 Ознакомление сотрудников Государственного бюджетного общеобразовательного учреждения школа № 565 Кировского района Санкт-Петербурга с Положением и Перечнем, а также их инструктаж по работе с информацией конфиденциального характера, производится их непосредственными руководителями.

Подписанное сотрудником Государственного бюджетного общеобразовательного учреждения школа № 565 Кировского района Санкт-Петербурга обязательство о неразглашении информации конфиденциального характера (далее – Обязательство) хранится в его личном деле.

1.7 Порядок обращения со служебной информацией ограниченного доступа должен осуществляться в соответствии с требованиями Положения о порядке обращения со

служебной информацией ограниченного распространения Государственного бюджетного общеобразовательного учреждения школа № 565 Кировского района Санкт-Петербурга.

1.8 За общее состояние и организацию работ по технической защите информации ограниченного доступа в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга возложена на ответственного за организацию обработки персональных данных.

При выполнении работ, определенных настоящим Положением, следует учитывать организационные меры, обусловленные необходимостью проведения технического обслуживания, устранения неисправностей, обновления программного обеспечения и других мероприятий, проводимых в Государственного общеобразовательного учреждения школе № 565 Кировского района Санкт-Петербурга по защите информации.

Ответственность за выполнение мероприятий по защите информации ограниченного доступа в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга возложена на директора.

2. Информация, подлежащая защите, и потенциальные угрозы информационной безопасности объектов защиты

2.1. Защите подлежит информация ограниченного доступа (речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде носителей на бумажной, магнитной, магнитно-оптической и другой основе).

Объектами защиты при этом являются:

Автоматизированные системы (АС)

Средства изготовления и размножения документов далее СИРД)

Защищаемые помещения (далее – ЗП).

2.2 В качестве угроз информационной безопасности объектов защиты необходимо рассматривать:

- использование разведками иностранных государств технических средств для получения информации ограниченного доступа, перехват информации, обсуждаемой в защищаемых помещениях и циркулирующей в основных технических средствах и системах, а также воздействие на информационные ресурсы автоматизированных систем с целью разрушения, искажения и блокировки информации;

- использование криминальными структурами технических средств для получения информации, представляющей ценность в интересах планирования криминальных акций;

-преднамеренные действия нарушителей и злоумышленников, незаконным путем приникших на объекты посредством контактного несанкционированного доступа к

элементам автоматизированных систем, к носителям информации, к вводимой и выводимой информации, к программному обеспечению, а также подключения к линиям связи;

-непреднамеренные действия персонала, приводящие к утечке, искажению, разрушению информации, подлежащей защите, в том числе ошибки эксплуатации технических и программных средств автоматизированных систем.

2.3. Понятие и состав конфиденциальной информации.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию (публикации, сообщения в средствах массовой информации, выступления на конференциях и выставках, интервью и т.п.), а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) и другими нормативно-правовыми актами.

Информация ограниченного доступа включает в себя:

-информацию, составляющую государственную тайну (секретную), защита которой осуществляется в соответствии с законодательством Российской Федерации о государственной тайне;

-конфиденциальную информацию.

К сведениям конфиденциального характера относятся:

-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;

-служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

-сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами.

Состав сведений, относящихся к служебной тайне, регламентируется специальным перечнем, который утверждается руководителем учреждения.

Носители информации, составляющей служебную тайну, могут иметь гриф ограничения доступа "Для служебного пользования".

Информация ограниченного доступа, не содержащая сведений, отнесенных к государственной тайне, должна иметь гриф конфиденциальности.

При организации защиты конфиденциальных сведений необходимо четко регламентировать:

-перечень сведений конфиденциального характера специалиста по информатизации, осуществляющего техническое обслуживание информационного ресурса Государственного бюджетного общеобразовательного учреждения школа № 565 Кировского района Санкт-Петербурга;

-процедуру допуска сотрудников к сведениям, составляющим служебную, коммерческую или другую тайну;

-обязанности исполнителей, допущенных к сведениям, которые составляют служебную, коммерческую или другую тайну;

-правила обращения (делопроизводство, учет, хранение, размножение и т.д.) с документами;

-правила доступа (передачи) к информации иных лиц;

-ответственность за разглашение сведений, оставляющих служебную, коммерческую или другую тайну.

3. Цели и задачи технической защиты информации ограниченного доступа

3.1. Целями технической защиты информации ограниченного доступа являются:

- исключение утечки информации ограниченного доступа с помощью технических средств разведки;

- предотвращение несанкционированного доступа (далее – НСД) к информации ограниченного доступа, ее разрушения, искажения, уничтожения, блокировки и несанкционированного копирования в системах и средствах информатизации;

-обеспечение условий быстрого, полного и всестороннего расследования случаев утечки информации;

- устранение негативных последствий и условий в случае несанкционированной утечки или утраты информации.

3.2. Задачами технической защиты информации ограниченного доступа являются:

- реализация в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга государственной политики по технической защите информации;

- подготовка предложений по совершенствованию правового, нормативно-методического и организационного обеспечения технической защиты информации в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга;

- анализ состояния и прогнозирование источников угроз безопасности информации;

- разработка целевых программ по технической защите информации в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга;

- учет информационных ресурсов, систем и средств формирования, передачи, хранения, обработки и распространения информации, подлежащих технической защите;

- контроль и анализ состояния технической защиты информации в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга;

-развитие и совершенствование системы подготовки кадров в области технической защиты информации в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга.

4. Порядок аттестации, ввода в эксплуатацию объектов информатизации и взаимодействия Государственного бюджетного общеобразовательного учреждения школа № 565 Кировского района Санкт-Петербурга и специализированных сторонних организаций при эксплуатации объектов информатизации и системы защиты информации

4.1. В Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга документально оформляется перечень объектов информатизации (АС, СИРД, ЗП..), а также лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации.

4.2. Все объекты информатизации (далее – ОИ), предназначенные для обработки (хранения, циркуляции) информации ограниченного доступа, должны быть аттестованы на соответствие установленным нормам и требованиям по защите информации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации.

4.3. Аттестационные испытания проводятся аттестационной комиссией предприятий (организаций), имеющих лицензию Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации (организации-лицензиаты ФСТЭК России).

Для проведения испытаний аттестационной комиссии подготавливаются и представляются:

-технический паспорт на объект информатизации;

-акт классификации объекта информатизации по требованиям защиты информации;

-состав технических и программных средств, входящих в автоматизированную систему (или технических средств, расположенных в защищаемом помещении);

-план контролируемой зоны;

-перечень защищаемых в АС ресурсов (или конфиденциальность обсуждаемых в защищаемых помещениях вопросов);

- организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам АС (обсуждаемым вопросам);

-инструкции пользователям и администратору безопасности информации;

-инструкции по эксплуатации средств защиты информации;

-сертификаты соответствия требованиям по безопасности информации на используемые средства защиты информации.

В результате аттестационных испытаний оформляется «Аттестат соответствия», которым подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативных документов по защите конфиденциальной информации, утвержденных Федеральной службой по техническому и экспортному контролю Российской Федерации и другими органами государственного управления в пределах их компетенций.

На основании выданного специализированной организацией аттестата соответствия издается приказ о разрешении обработки информации ограниченного доступа на объекте информатизации и назначении лиц, ответственных за обеспечение защиты информации при его эксплуатации.

Методическое руководство, разработку требований к мерам защиты и контроль за эффективностью использования предусмотренных мер защиты информации ограниченного доступа обеспечивает Комитет по информатизации и связи Санкт-Петербурга.

Комитет по информатизации и связи Санкт-Петербурга осуществляет следующие основные функции:

- проводит государственную политику Санкт-Петербурга в сфере информатизации и связи, управления информационными и телекоммуникационными ресурсами Санкт-Петербурга, обеспечения информационной безопасности и защиты информации,

содержащей сведения государственной или служебной тайны, в исполнительных органах государственной власти Санкт-Петербурга, а также направляет деятельность исполнительных органов государственной власти Санкт-Петербурга в данной сфере;

- осуществляет методическое руководство и участвует в разработке (согласовании) конкретных требований по защите информации ограниченного доступа и разработке технического задания на аттестацию объекта информатизации;

- согласовывает степень участия персонала в обработке (обсуждении, передаче, хранении) защищаемой информации;

-определяет класс защищенности объектов информатизации;

- определяет перечень предполагаемых к использованию к использованию сертифицированных средств защиты информации;

-участвует в организации обучения должностных лиц, ответственных за эксплуатацию СЗИ, по направлению обеспечения безопасности информации.

Привлечение для организации работ по созданию системы защиты информации (далее – СЗИ) или ее отдельных компонентов сторонних специализированных организаций осуществляется в соответствии с порядком, устанавливаемым нормативными и организационно-распорядительными документами ФСТЭК России.

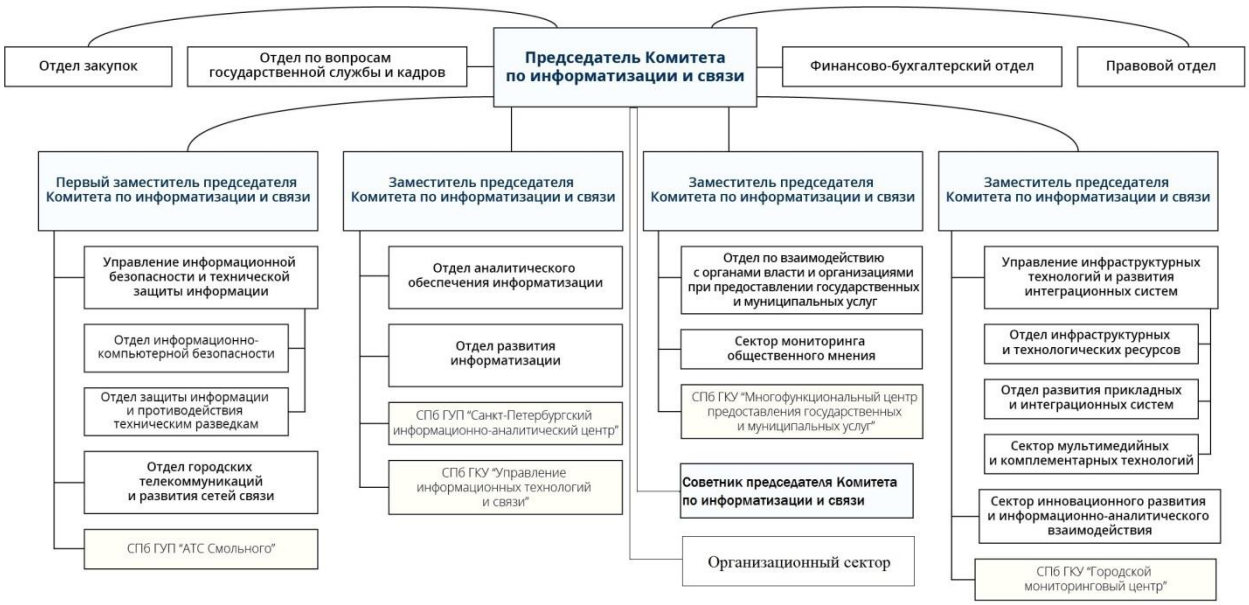
В случае привлечения для обеспечения безопасности информации сторонних специализированных организаций в соответствии с требованиями Федерального закона от 05.04.2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» рекомендуется выполнение следующих условий:

- наличие у организации лицензии на право проведения работ по технической защите конфиденциальной информации;

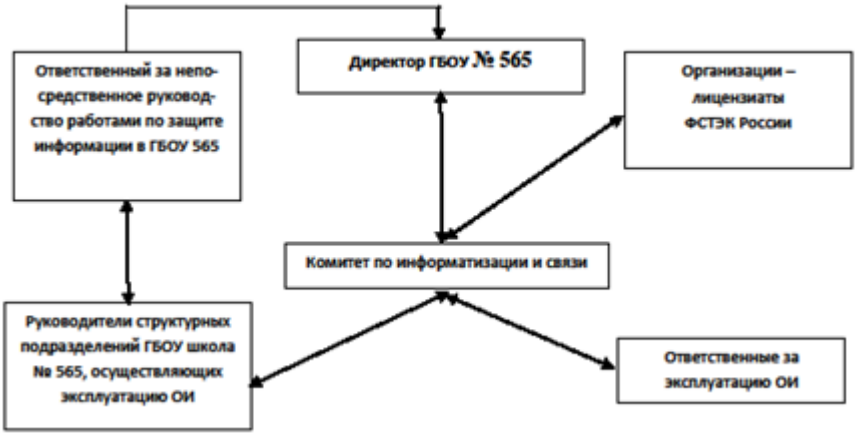
-проведение инструктажа исполнителей работ по вопросам информационной безопасности;

- другие условия, устанавливаемые соответствующими нормативными и организационно-распорядительными документами.

Структурная схема работы комитета по информатизации и связи.



Структурная схема взаимодействия Государственного бюджетного общеобразовательного учреждения школы № 565 Кировского района Санкт-Петербурга и специализированных сторонних организаций при аттестации, вводе в эксплуатацию и эксплуатацию ОИ и системы защиты информации.



5. Контроль состояния защиты информации в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга

5.1. Контроль состояния защиты информации в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга осуществляется в целях:

- предупреждения и пресечения возможности получения техническими средствами разведки охраняемых сведений об объектах информатизации органа;

-выявления и предотвращения утечки информации по техническим каналам;

- исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации;

-предотвращение специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

5.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

- проверка выполнения установленных норм и требований по защите информации;

- оценка достаточности и эффективности мероприятий по защите информации;

-проверка выполнения требований по защите автоматизированных систем от несанкционированного доступа;

-проверка выполнения требований по антивирусной защите автоматизированных рабочих мест;

-проверка знаний должностных лиц по вопросам защиты информации и их соответствия необходимому уровню подготовки для конкретного рабочего места;

-оперативное принятие мер по пресечению нарушений требований (норм) защиты информации на объектах информатизации Государственного бюджетного общеобразовательного учреждения школе № 565 Кировского района Санкт-Петербурга.

5.3. Повседневный контроль за выполнением мероприятий по защите информации осуществляет специалист, ответственный за эксплуатацию объекта информатизации.

5.4. Периодический контроль за выполнением мероприятий по защите информации проводится руководителями структурных подразделений, где эксплуатируется объект информатизации, совместно с администратором АС и специалистом, ответственным за эксплуатацию объекта информатизации не реже одного раза в три месяца.

В ходе контроля проверяется:

-соблюдение организационно-режимных требований;

-выполнение требований по защите автоматизированных систем от несанкционированного доступа;

-выполнение требований по антивирусной защите автоматизированных систем.

5.5. Контроль эффективности принятых мер защиты информации на объектах информатизации Государственного бюджетного общеобразовательного учреждения школа № 565 Кировского района Санкт-Петербурга с использованием технических

средств осуществляется не реже одного раза в год директором Государственного бюджетного общеобразовательного учреждения школе № 565 Кировского района Санкт-Петербурга.

6. Ответственность должностных лиц

6.1. Ответственность за организацию работ по защите информации в Государственном бюджетном общеобразовательном учреждении школе № 565 Кировского района Санкт-Петербурга возлагается на должностное лицо, назначенное ответственным за непосредственное руководство работами по защите информации.

6.2. Ответственность за планирование работ по защите информации, организацию контроля за эффективностью их выполнения, организацию разработки нормативно-методических документов по технической защите информации, разработку (совместно со структурными подразделениями, эксплуатирующими ОИ) распорядительных документов по вопросам организации технической защиты информации, аттестацию объектов информатизации возлагается на директора Государственного бюджетного общеобразовательного учреждения школе № 565 Кировского района Санкт-Петербурга.

6.3. Ответственность за выполнение установленных мероприятий по технической защите информации на введенных в эксплуатацию объектах информатизации, возлагается на руководителя структурного подразделения, эксплуатирующего объект информатизации и ответственного за эксплуатацию объекта информатизации.

6.4. Ответственность за формирование политики антивирусной защиты, организацию своевременной инсталляции средств антивирусной защиты информации и обновление баз данных вирусных описаний на АС возлагается на администратора безопасности.

6.5. Ответственность за своевременное ознакомление сотрудников с руководящими документами по организации защиты информации и порядку работу с информацией ограниченного доступа несут их непосредственные руководители.

6.6. Должностные лица, допустившие разглашение информации ограниченного доступа, несут ответственность в соответствии с действующим законодательством Российской Федерации.