УТВЕРЖДЕНО
приказом директора
от 30.12 2022
№ 1083 -ОД

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите конфиденциальной информации в СПб ГБПОУ «ПКГХ»

1. Общие положения

1.1. Положение о порядке организации и проведения работ по защите конфиденциальной информации в СПб ГБПОУ «ПКГХ» (далее – Положение) определяет цели, задачи, содержание, порядок организации и проведения работ по защите конфиденциальной информации в СПб ГБПОУ «ПКГХ».

В соответствии с пунктом 1.16 приказа Государственной технической комиссии при Президенте Российской Федерации от 30.08.2012 № 282 под конфиденциальной информацией понимается информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Положение не распространяется на порядок организации и проведения работ по защите информации, содержащей сведения, составляющие государственную тайну.

1.2. Положение является документом, обязательным для выполнения всеми работниками СПб ГБПОУ «ПКГХ» при проведении работ, требующих технической защиты конфиденциальной информации, на проектируемых (реконструируемых) и действующих (находящихся в эксплуатации) объектах информатизации СПб ГБПОУ «ПКГХ».

Правовую основу Положения составляют Конституция Российской Федерации, Федеральные законы «О безопасности», «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О коммерческой тайне» и другие нормативные правовые акты Российской Федерации, определяющие права и ответственность граждан, общества и государства в области защиты информации.

Проведение мероприятий, связанных с возможным раскрытием охраняемых сведений, обсуждением, передачей, обработкой и хранением конфиденциальной информации, допускается только после определения и принятия, необходимых мер по их защите в соответствии с требованиями Положения и других нормативно-методических документов по защите информации.

На документах (в необходимых случаях и на их проектах), содержащих конфиденциальную информацию, проставляется пометка «Для служебного пользования».

Сотрудники (работники) СПб ГБПОУ «ПКГХ», принявшие решение об отнесении информации к категории ограниченного доступа, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений, предусмотренных пунктом 4.2 Положения.

Конфиденциальная информация не подлежит разглашению (распространению) без согласия сотрудника (работника) СПб ГБПОУ «ПКГХ», принявшего решение об отнесении информации к категории ограниченного доступа.

За разглашение конфиденциальной информации, а также нарушение порядка обращения с документами, содержащими такую информацию, сотрудник (работник) СПб ГБПОУ «ПКГХ» может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

В случае ликвидации СПб ГБПОУ «ПКГХ» решение о дальнейшем использовании конфиденциальной информации принимает ликвидационная комиссия.

2. Цели, задачи, содержание работ по защите конфиденциальной информации

2.1. Целями проведения работ по защите конфиденциальной информации является:

- предотвращение утечки информации по техническим каналам;
- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в системах информатизации СПб ГБПОУ «ПКГХ»;
- соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах обработки СПб ГБПОУ «ПКГХ»;
- сохранение возможности управления процессом обработки и пользования информацией.

2.2. В ходе проведения работ по защите конфиденциальной информации должны быть решены следующие задачи:

- предотвращение перехвата техническими средствами информации, передаваемой по каналам связи;
- предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований;
- исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;
- выявление возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- предотвращение перехвата техническими средствами речевой информации из помещений и объектов.

2.3. Основным содержанием работ по защите конфиденциальной информации является:

- применение криптографических и иных методов и средств защиты, а также проведение организационно-технических и режимных мероприятий;
- применение защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранирование зданий или отдельных помещений, установление контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами;
- применение специальных программно-технических средств защиты;
- применение специальных программных и аппаратных средств защиты (антивирусные процессоры, антивирусные программы), организация системы контроля безопасности программного обеспечения;
- проведение специальных проверок по выявлению возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- применение специальных средств защиты, проектных решений, обеспечивающих звукоизоляцию помещении, выявление специальных устройств подслушивания.

2.4. Информация, содержащая сведения, отнесенные к служебной тайне, должна обрабатываться с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств защиты, сертифицированных в установленном порядке.

2.5. Соответствие технического средства и его программного обеспечения требованиям защищенности подтверждается сертификатом, выдаваемым предприятием, имеющим лицензию на этот вид деятельности, по результатам сертификационных испытаний, или предписанием на эксплуатацию, оформляемым по результатам специальных исследований и специальных проверок технических средств и программного обеспечения.

2.6. Для оценки готовности систем и средств информатизации и связи к обработке (передаче) информации, содержащей сведения, отнесенные к служебной тайне, проводится аттестация указанных систем и средств в реальных условиях эксплуатации на предмет соответствия принимаемых методов, мер и средств защиты требуемому уровню безопасности информации.

3. Ответственность сотрудников (работников) СПб ГБПОУ «ПКГХ» за своевременность, качество формирования требований по защите информации и научно-технического уровня разработки системы защиты конфиденциальной информации

3.1. Ответственность за организацию и состояние защиты конфиденциальной информации на объектах СПб ГБПОУ «ПКГХ» возлагается на директора СПб ГБПОУ «ПКГХ». Непосредственное руководство работами по защите информации осуществляет специалист по защиты информации СПб ГБПОУ «ПКГХ». Сотрудники (работники) СПб ГБПОУ «ПКГХ», организующие работу с конфиденциальной информацией, несут персональную ответственность за соблюдение требований Положения.

3.2. Руководство разработкой и осуществлением мероприятий по обеспечению защиты конфиденциальной информации и проведения постоянного контроля за ее состоянием в СПб ГБПОУ «ПКГХ» проводит отдел информатизации образовательного и производственного процессов СПб ГБПОУ «ПКГХ». Для проведения работ непосредственно в СПб ГБПОУ «ПКГХ» приказом назначается штатный специалист по технической защите информации, который подчиняется начальнику отдела информатизации образовательного и производственного процессов СПб ГБПОУ «ПКГХ».

3.3. Отдел информатизации образовательного и производственного процессов СПб ГБПОУ «ПКГХ» осуществляет мероприятия по защите конфиденциальной информации, участвует в согласовании технических заданий на строительство (реконструкцию) объектов СПб ГБПОУ «ПКГХ», создание систем информатизации и связи, организует подготовку заключений о возможности проведения работ с соответствующей информацией и контроль эффективности выполняемых мероприятий по обеспечению защиты конфиденциальной информации в структурных подразделениях СПб ГБПОУ «ПКГХ».

3.4. При решении задач, связанных с защитой конфиденциальной информации, штатный специалист по защите информации взаимодействует с структурными подразделениями СПб ГБПОУ «ПКГХ» в пределах их компетенции.

3.5. Отдел информатизации образовательного и производственного процессов СПб ГБПОУ «ПКГХ» организует, руководит, координирует, осуществляет контроль и реализацию работ по информационной безопасности.

3.6. Отдел информатизации образовательного и производственного процессов СПб ГБПОУ «ПКГХ» решает следующие задачи:

- участие в разработке и создании защищенных телекоммуникационных и информационных сетей и систем СПб ГБПОУ «ПКГХ»;
- организация и реализация работ, связанных с разработкой и созданием систем защиты информации в уже существующих информационных и вычислительных сетях, а также в процессе их модернизации;
- организация и контроль использования криптографических средств для защиты документированной информации ограниченного доступа, а также порядка подтверждения с помощью электронной цифровой подписи юридической силы документов, хранимых, обрабатываемых и передаваемых в автоматизированных информационных и телекоммуникационных системах СПб ГБПОУ «ПКГХ»;

4. Порядок определения защищаемой информации

4.1. Согласно статье 5 Федерального закона «Об информации, информационных технологиях и защите информации» документированная информация, обрабатываемая в СПб

ГБПОУ «ПКГХ», в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен (информация ограниченного доступа).

4.2. Запрещено относить к информации ограниченного доступа:

- нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информацию о состоянии окружающей среды;
- информацию о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих служебную тайну);
- информацию, накапливаемую 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;
- иную информацию, недопустимость ограничения доступа к которой установлена действующим законодательством.

4.3. Отнесение информации к категории ограниченного доступа в СПб ГБПОУ «ПКГХ» осуществляется в соответствии с Перечнем сведений конфиденциального характера, подлежащих защите в СПб ГБПОУ «ПКГХ», утвержденным приказом СПб ГБПОУ «ПКГХ».

4.4. Необходимость проставления пометки «Для служебного пользования» на документах и изданиях, содержащих служебную конфиденциальную информацию, определяется должностным лицом СПб ГБПОУ «ПКГХ», подписывающим или утверждающим документ.

4.5. Правила работы с документами, имеющими пометку «Для служебного пользования» определяются приказом вице-губернатора Санкт-Петербурга – руководителя Канцелярии Губернатора Санкт-Петербурга от 08.09.1998 № 7-пв.

5. Порядок взаимодействия организаций, подразделений и специалистов, занятых в работах по защите конфиденциальной информации

5.1. Организация и проведение работ по защите конфиденциальной информации при ее обработке техническими средствами определяются Положением, действующими государственными стандартами и другими нормативно-методическими документами ФСТЭК России.

5.2. Работы по защите конфиденциальной информации могут осуществляться как подразделениями СПб ГБПОУ «ПКГХ», так и специализированными организациями, имеющими лицензии ФСТЭК России на соответствующий вид деятельности.

5.3. Контроль состояния защиты информации заключается в оценке:

- соблюдения требований действующих нормативно-методических документов по защите информации;
- работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;
- знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.

Разработчик:
Начальник отдела ИО и ПП С.В.Ваганов