Утверждаю:
Директор МБОУ «СОШ №16»
_____ В.Б.Каркин
Приказ №115-ОД от 14.09.2022г.

ПОЛОЖЕНИЕ

о порядке организации и проведения работ по защите конфиденциальной информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (конфиденциальная информация) в МБОУ «Средняя общеобразовательная школа №16»

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 Муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №16» (далее – Положение) 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 Муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №16» (далее МБОУ «СОШ №16»).

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. Сотрудники МБОУ «СОШ №16», 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)

1.5. Ознакомление сотрудников МБОУ «СОШ №16» с Положением и Перечнем, а также их инструктаж по работе с информацией конфиденциального характера, производится ответственным по защите персональных данных образовательного учреждения.

1.6. За общее состояние и организацию работ по технической защите информации ограниченного доступа в МБОУ «СОШ №16» 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 МБОУ «СОШ №16» по защите информации. Ответственность за выполнение мероприятий по защите информации ограниченного доступа в МБОУ «СОШ №16» 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 (СИРД), защищаемые помещения (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 МБОУ «СОШ №16»;
-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 МБОУ «СОШ №16» государственной политики по технической защите информации;
- подготовка предложений по совершенствованию правового, нормативнометодического и организационного обеспечения технической защиты информации в МБОУ «СОШ №16»;
- анализ состояния и прогнозирование источников угроз безопасности информации;
- учет информационных ресурсов, систем и средств формирования, передачи, хранения, обработки и распространения информации, подлежащих технической защите;
- контроль и анализ состояния технической защиты информации в МБОУ «СОШ №16»;
-развитие и совершенствование системы подготовки кадров в области технической защиты информации в МБОУ «СОШ №16».

4. Контроль состояния защиты информации в МБОУ «СОШ №16».

4.1. Контроль состояния защиты информации в МБОУ «СОШ №16» 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.

4.2. Основными задачами контроля являются:
- проверка организации выполнения мероприятий по защите информации в МБОУ «СОШ №16» 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 МБОУ «СОШ №16».

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

4.4. Периодический контроль за выполнением мероприятий по защите информации проводится руководителем образовательной организации, 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.

4.5. Контроль эффективности принятых мер защиты информации на объектах информатизации МБОУ «СОШ №16» с использованием технических средств осуществляется не реже одного раза в год руководителем образовательной организации.

5. Ответственность должностных лиц.

5.1. Ответственность за организацию работ по защите информации в МБОУ «СОШ №16» возлагается на должностное лицо, назначенное ответственным по защите информации.

5.2. Ответственность за планирование работ по защите информации, организацию контроля за эффективностью их выполнения, организацию разработки нормативно-методических документов по технической защите информации, разработку распорядительных документов по вопросам организации технической защиты информации, аттестацию объектов информатизации возлагается на директора МБОУ «СОШ №16».

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

5.4. 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.

5.5. Ответственность за своевременное ознакомление сотрудников с руководящими документами по организации защиты информации и порядку работу с информацией ограниченного доступа несет руководитель образовательной организации.

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