Управление по делам образования
города Челябинска
Муниципальное бюджетное
общеобразовательное учреждение
«Лицей № 11 г. Челябинска»
(МБОУ «Лицей № 11 г. Челябинска»)

УТВЕРЖДЕНО
приказом Муниципального бюджетного
общеобразовательного учреждения
«Лицей № 11 г. Челябинска»

от 15.12.2015 г. № 152

ПОЛОЖЕНИЕ
от 15.12.2015 г. № 139

о порядке организации и проведения работ
по защите персональных данных

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в Муниципальном бюджетном общеобразовательном учреждении «Лицей № 11 г. Челябинска» (далее - Учреждение).

1.2. Мероприятия по защите конфиденциальной информации являются составной частью управленческой и иной служебной деятельности и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.3. Режим защиты конфиденциальной информации устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством.

Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты конфиденциальной информации, сертифицируемых в установленном порядке. Обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для технической защиты конфиденциальной информации.

1.4. Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты конфиденциальной информации и величины ущерба, который может быть нанесен собственнику конфиденциальной информации при ее разглашении, утрате, уничтожении и искажении.

Системы и средства информатизации и связи, предназначенные для обработки (передачи) конфиденциальной информации должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

Проведение любых мероприятий и работ с конфиденциальной информацией, без принятия необходимых мер технической защиты информации не допускается.

1.5. Объектами защиты являются:

- средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть (ЛВС), средства и системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации, содержащей конфиденциальную информацию основные технические средства и системы - далее ОТСС;

- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается конфиденциальной информация - далее вспомогательные технические средства и системы (ВТСС);

1.6. Ответственность за выполнение требований настоящего Положения возлагается на руководителя Учреждения, а также на специалистов допущенных к обработке, передаче и хранению в технических средствах информации, содержащей конфиденциальную информацию.

2. ОХРАНЯЕМЫЕ СВЕДЕНИЯ

2.1. В организации разрабатывается Перечень сведений конфиденциального характера.

Перечень сведений конфиденциального характера включает:

- 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, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.).
- Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна).
- Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.
- Сведения, составляющие служебную тайну, определяются действующим в субъекте Российской Федерации "Перечнем сведений, составляющих служебную информацию ограниченного распространения".

Указанный перечень может включать следующие классы сведений ограниченного распространения:

- сведения экономического характера;
- сведения по финансовым вопросам;
- сведения по науке и технике;
- сведения по транспорту и связи;
- сведения по вопросам внешней торговли и международных научно-технических связей;

3. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И СПЕЦИАЛЬНЫХ ВОЗДЕЙСТВИЙ НА НЕЕ

3.1. Доступ к конфиденциальной информации, нарушение ее целостности и доступности возможно реализовать за счет:

- несанкционированного доступа к конфиденциальной информации при ее обработке в информационных системах и ресурсах;
- утечки конфиденциальной информации по техническим каналам.

3.2. Детальное описание возможных технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на нее содержится в Модели угроз безопасности информации.

4. ОЦЕНКА ВОЗМОЖНОСТЕЙ ТЕХНИЧЕСКИХ РАЗВЕДОК И ДРУГИХ ИСТОЧНИКОВ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

4.1. Для добывания конфиденциальных сведений могут использоваться:

- портативная возимая (носимая) аппаратура радио, акустической, визуально-оптической и телевизионной разведки, а также разведки побочных электромагнитных излучений и наводок (ПЭМИН);
- автономная автоматическая аппаратура акустической и телевизионной разведки, а также разведки ПЭМИН;
- компьютерная разведка, использующая различные способы и средства несанкционированного доступа к информации и специальных воздействий на нее.

Угроза компьютерной разведки объектам защиты возможна в случае подключения АС, обрабатывающим информацию ограниченного доступа к внешним, в первую очередь - глобальным сетям.

Портативная носимая аппаратура имеет ограниченные возможности и может быть использована лишь для уточнения данных, или перехвата информации в непосредственной близости от защищаемых объектов.

Автономная автоматическая аппаратура радио, акустической, телевизионной, а также разведки ПЭМИН используется для длительного наблюдения за объектом защиты.

4.2. Несанкционированный доступ к информации и специальные воздействия на нее могут осуществляться при ее обработке на отдельных автоматизированных рабочих местах, в локальных вычислительных сетях, в распределенных телекоммуникационных системах.

4.3. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:
- непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;
- случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;
- некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;
- просмотра информации с экранов дисплеев и других средств ее отображения.

4.4. Оценка возможностей средств технической разведки осуществляется с использованием нормативных документов ФСТЭК России.

Наиболее опасной является аппаратура портативной (возимой и носимой) разведки электромагнитных излучений и аппаратура акустической речевой разведки, которая может применяться с территорий прилегающей к зданию в котором располагается АС, а также автономная автоматическая аппаратура акустической речевой разведки, скрытно устанавливаемая внутри помещений.

4.5. Оценка возможности НСД к информации в средствах вычислительной техники и автоматизированных системах осуществляется с использованием следующих руководящих документов ФСТЭК России:

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по технической защите конфиденциальной информации.

НСД к информации и специальные воздействия на нее реально возможны, если не выполняются требования перечисленных выше документов, дифференцированные в зависимости от степени конфиденциальности обрабатываемой информации, уровня полномочий пользователей по доступу к конфиденциальной информации и режимов обработки данных в автоматизированных системах.

5. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

5.1. Разработка мер, и обеспечение защиты конфиденциальной информации осуществляются подразделением по защите информации (службой безопасности) или отдельными специалистами, назначаемыми руководителем организации для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии ФСТЭК России и ФСБ России на право осуществления соответствующих работ.

5.2. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

5.3. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителя организации, эксплуатирующей объекты информатизации.

5.4. Техническая защита информации в защищаемых помещениях (ЗП).

К основным мероприятиям по технической защите конфиденциальной информации в ЗП относятся:

5.4.1. Определение перечня ЗП по результатам анализа циркулирующей в них конфиденциальной информации и условий ее обмена (обработки), в соответствии с нормативными документами ФСТЭК России.

5.4.2. Назначение сотрудников, ответственных за выполнение требований по технической защите конфиденциальной информации в ЗП, далее сотрудники, ответственные за безопасность информации.

5.4.3. Разработка частных инструкций по обеспечению безопасности информации в ЗП.

5.4.4. Обеспечение эффективного контроля за доступом в ЗП, а также в смежные помещения.

5.4.5. Инструктирование сотрудников, работающих в ЗП о правилах эксплуатации ПЭВМ, других технических средств обработки информации, средств связи с соблюдением требований по технической защите конфиденциальной информации.

5.4.6. Исключение неконтролируемого доступа к линиям связи, управления и сигнализации в ЗП, а также в смежных помещениях и в коридоре.

5.4.7. Осуществление сотрудниками, ответственными за безопасность информации, контроля за проведением всех монтажных и ремонтных работ в выделенных и смежных с ними помещениях, а также в коридорах.

5.5. Защита информации, циркулирующей в ОТСС и наводящейся в ВТСС.

5.5.1. При эксплуатации ОТСС и ВТСС необходимо неукоснительное выполнение требований, определенных в предписании на эксплуатацию.

5.5.2. При невозможности обеспечения контролируемой зоны заданных размеров рекомендуется проведение следующих мероприятий:

Применение систем электромагнитного пространственного зашумления (СПЗ) в районе размещения защищаемого ОТСС.

Применение средств линейного электромагнитного зашумления (СЛЗ) линий электропитания, радиотрансляции, заземления, связи.

5.5.3. Техническая защита информации в средствах вычислительной техники (СВТ) и автоматизированных системах (АС) от несанкционированного доступа в соответствии с требованиями руководящих документов Гостехкомиссии России должна обеспечиваться путем:

- проведения классификации СВТ и АС;
- выполнения необходимых организационных мер защиты;
- установки сертифицированных программных и аппаратно-технических средств защиты информации от НСД.

- защита каналов связи, предназначенных для передачи конфиденциальной информации.
- защиты информации от воздействия программ-закладок и компьютерных вирусов.

5.6. Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами Гостехкомиссии России.

Организации антивирусной защиты информации на объектах информатизации достигается путём:
- установки и применения средств антивирусной защиты информации;
- обновления баз данных средств антивирусной защиты информации;
- действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

5.6.1. Организация работ по антивирусной защите информации возлагается на руководителей структурных подразделений и должностных лиц, осуществляющих контроль за антивирусной защитой, а методическое руководство и контроль над эффективностью предусмотренных мер защиты информации на руководителя подразделения по защите информации (ответственного).

5.6.2. Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:
- обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации носителей информации, информационных массивов, программных средств общего и специального назначения;
- периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;
- внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;
- восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

5.6.3. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

5.6.4. Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:
- Входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения.
- Входной антивирусный контроль всей информации поступающей с электронной почтой;
- Входной антивирусный контроль всей поступающей информации из сети Internet;
- Выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а так же передача информации посредством электронной почты;
- Периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций;
- Обязательная антивирусная проверка используемых в работе внешних носителей информации;
- Постоянный антивирусный контроль на рабочих станциях с использованием резидентных антивирусных мониторов в автоматическом режиме;
- Обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;

- Внеплановая антивирусная проверка внешних носителей и жестких дисков рабочих станций и серверов на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;
- Восстановление работоспособности программных и аппаратных средств, а так же непосредственно информации в случае их повреждения компьютерными вирусами.

5.6.5. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

5.6.6. При обнаружении на носителе информации или в полученных файлах программных вирусов пользователи докладывают об этом в подразделение по защите информации или ответственному сотруднику, и принимают меры по восстановлению работоспособности программных средств и данных.

Перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов.

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на АРМ, поставить в известность подразделение по защите конфиденциальной информации и принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты.

При функционировании АРМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

Ликвидация последствий воздействия программных вирусов осуществляется подготовленными представителями подразделения по защите информации.

5.6.7. Организация антивирусной защиты конфиденциальной информации должна быть направлена на предотвращение заражения рабочих станций, входящих в состав локальных компьютерных сетей, различного уровня и назначения вирусами.

5.6.8. Необходимо постоянно осуществлять обновление антивирусных баз. Частоту обновления установить в зависимости от используемых антивирусных средств и частоты выпуска обновления указанных баз.

5.6.9. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке, руководством по эксплуатации конкретного антивирусного программного продукта и инструкцией по антивирусной защите.

5.7. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах ведётся в соответствии с Инструкцией по организации парольной защиты.

6. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

6.1. Руководство технической защитой конфиденциальной информации возлагается на руководителя организации.

6.2. Начальник структурного подразделения по защите информации (ответственный сотрудник) осуществляет непосредственное руководство разработкой мероприятий по технической защите конфиденциальной информации.

6.3. Владельцы и пользователи ОТСС обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

6.4. Руководители подразделений, владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием сведений, составляющих конфиденциальную или служебную тайну, в случае обнаружения утечки (или предпосылок к утечке) этих сведений. Предложения докладываются руководителю подразделения по защите информации (ответственному сотруднику).

6.5. Руководитель организации имеет право привлекать к проведению работ по технической защите конфиденциальной информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

7. ПЛАНИРОВАНИЕ РАБОТ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И КОНТРОЛЮ

7.1. В организации составляются годовые планы работ по технической защите конфиденциальной информации и контролю. Проекты планов разрабатываются структурным подразделением по защите конфиденциальной информации или ответственным сотрудником. Сроки разработки, представления и утверждения планов устанавливаются руководителем организации.

7.2. В годовые планы по технической защите конфиденциальной информации и контролю включаются:

- подготовка проектов распорядительных документов по вопросам организации технической защиты информации, инструкций, рекомендаций, памяток и других документов по обеспечению безопасности информации при использовании конкретных технических средств обработки и передачи информации, на автоматизированных рабочих местах, в ЗП;
- аттестация вводимых в эксплуатацию ОТСС и ЗП, а также периодическая переаттестация находящихся в эксплуатации ОТСС и ЗП на соответствие требованиям по технической защите конфиденциальной информации;
- проведение периодического контроля состояния технической защиты информации;
- мероприятия по устранению нарушений и выявленных недостатков по результатам контроля;
- мероприятия по совершенствованию технической защиты информации в организации.

7.3. Контроль выполнения планов и отчетность по ним возлагается на структурное подразделение по защите информации или ответственного сотрудника.

8. КОНТРОЛЬ СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

8.1. Основными задачами контроля состояния технической защиты конфиденциальной информации являются оценка уровня и эффективности, принятых мер защиты, своевременное выявление и предотвращение утечки по техническим каналам информации, составляющей конфиденциальную или служебную тайну, НСД к информации, преднамеренных программно-технических воздействий на информацию с целью ее уничтожения, искажения, блокирования, нарушения правового режима использования информации.

8.2. Контроль осуществляется:

- ФСТЭК России;
- Управлением Федеральной службы безопасности;
- Роскомнадзор;
- Внутренней комиссией организации - не реже 1 раза в год;
- Структурным подразделением по защите информации или ответственным сотрудником и пользователем - непрерывно.

8.3. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты конфиденциальной информации, решений ФСТЭК России, наличия соответствующих документов по технической защите конфиденциальной информации, в инструментальной и визуальной проверке ОТСС и ЗП на наличие каналов утечки информации, на соответствие требованиям и нормам технической защиты информации.

9. АТТЕСТАЦИЯ РАБОЧИХ МЕСТ

9.1. Аттестации на соответствие требованиям по технической защите конфиденциальной информации в реальных условиях эксплуатации подлежат системы и средства информатизации и связи, предназначенные для обработки и передачи конфиденциальной информации, а также помещения, предназначенные для ведения конфиденциальных переговоров. Указанная аттестация проводится в соответствии с "Положением по аттестации объектов информатизации по требованиям безопасности информации", утвержденным Председателем Гостехкомиссии России 25 ноября 1994 г.

9.2. По результатам аттестации выдается "Аттестат соответствия", получение которого дает право использования аттестованных систем и средств для обработки и передачи информации, составляющей конфиденциальную или служебную тайну, и ведения конфиденциальных переговоров в аттестованных помещениях.

Переаттестация систем и средств информатизации, связи и помещений проводится по истечении срока действия "Аттестата соответствия", при изменении мер технической защиты информации, условий технической защиты или применяемых технологий обработки и передачи информации

СОГЛАСОВАНО
протокол заседания Совета
МБОУ «Лицей № 11 г. Челябинска»
от 15.09.2015 № 1