МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по обеспечению информационной безопасности в образовательной организации основного общего образования

1. Общие положения

1.1. Методические рекомендации по обеспечению информационной безопасности (далее-методические рекомендации) разработаны в соответствии с ФЗ-152 от 27.07.2006г. «О персональных данных», ФЗ-149 от 27.07.2006г. «Об информации, информационных технологиях и о защите информации», ФЗ-273 от 29.12.2012г. «Об образовании в Российской Федерации».

1.2. Методические рекомендации предназначены для руководящих и педагогических работников образовательных организаций основного общего образования.

1.3. Методические рекомендации определяют необходимый перечень требований по обеспечению безопасности информации в образовательных организациях основного общего образования.

1.4. Методические рекомендации разработаны для использования образовательными организациями основного общего образования при работе с персональными данными учащихся, их родителей или законных представителей, педагогического состава и иных работников образовательной организации с целью защиты персональных данных и недопущения утечки информации, содержащей сведения персональных данных.

2. Основные понятия

2.1. Информация - сведения (сообщения, данные) независимо от формы их представления;

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

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

2.4. Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

2.5. Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

2.6. Доступ к информации - возможность получения информации и ее использования;

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

2.8. Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

2.9. Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

2.10. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.11. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Персональные данные: понятие, сущность, обработка.

3.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) согласно ФЗ-152 «О персональных данных» от 27.07.2006г. Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайны.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Образовательные учреждения попадают под это понятие и являются операторами персональных данных.

Под обработкой персональных данных понимается любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

При обработке персональных данных оператор обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. К персональным данным в образовательной организации основного общего образования относятся:

- Фамилия имя отчество (далее по тексту - Ф.И.О.) сотрудников организации;
- Ф.И.О. учащихся;
- Ф.И.О. родителей или законных представителей учащихся;

- Сведения, содержащиеся в основном документе, удостоверяющем личность субъекта;
- Информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- Сведения, содержащиеся в документах воинского учета для военнообязанных и лиц, подлежащих призыву на военную службу;
- Сведения об образовании, квалификации или наличии специальных знаний или подготовки;
- Сведения, содержащиеся в свидетельстве о постановке на учёт физического лица в налоговом органе на территории Российской Федерации;
- Сведения о семейном положении;
- Информация медицинского характера, в случаях, предусмотренных Законодательством;
- Сведения о заработной плате работников, родителей учащихся;
- Сведения о социальных льготах;
- Сведения о наличии судимостей.

3.3. Хранение сведений, содержащих персональные данные:
- на бумажных носителях;
- электронные базы данных: жесткий диск компьютера/сервера, flash-носители, оптические диски, облачные сервисы.

3.4. Для обеспечения безопасности персональных данных руководителю образовательной организации основного общего образования необходимо проанализировать, приняты ли следующие меры:
- Правовые меры (соблюдение Федеральных Законов, Указов и иных правовых актов, регламентирующих правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений и устанавливающих ответственность за нарушения этих правил);
- Организационные меры (меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, ОРД);
- Технические меры (применение технических или программных средств защиты информации).

3.5. Информационная безопасность проверяется надзорными органами:

- Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);
- Федеральной службой безопасности Российской Федерации (ФСБ РФ);
- Федеральной службой по техническому и экспортному контролю (ФСТЭК).

3.6. Действия по формированию и достижению необходимого уровня информационной безопасности включают в себя определение объекта защиты информации, описание процесса обеспечения информационной безопасности и определение конкретных мероприятий по защите персональных данных.

Полномочия руководителей образовательных организаций основного общего образования в области обеспечения информационной безопасности должны включать в себя:

- планирование и проведение мероприятий информационной безопасности;
- назначение ответственных за обеспечение информационной безопасности;
- обучение и повышение квалификации работников образовательной организации основного общего образования в сфере информационной безопасности;
- мониторинг и анализ принятых мер по обеспечению информационной безопасности;
- реагирование на инциденты, связанные с нарушением информационной безопасности.

4. Характеристика локальных нормативных документов по обеспечению безопасности информации образовательной организации

4.1. План мероприятий по обеспечению защиты персональных данных представляет собой сводную таблицу с обязательным указанием сведений в виде мероприятий по обеспечению защиты персональных данных в образовательной организации основного общего образования, срока исполнения, исполнителя.

4.2. Положение об обработке персональных данных должно содержать определение порядка обработки персональных данных, обеспечение защиты прав и свобод человека и гражданина при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайны. Положение об обработке персональных данных должно устанавливать ответственность должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Также обязательным является определение состава персональных данных, определение порядка предоставления доступа к персональным данным. Положением определяется и порядок обработки персональных данных, определяются права и обязанности субъектов персональных данных и оператора, а также порядок организации защиты персональных данных.

Согласно Законодательству Российской Федерации, Положение об обработки персональных данных должно в обязательном порядке размещаться на официальном сайте общеобразовательной организации.

4.3. План внутренних проверок состояния защиты персональных данных представляет собой сводную таблицу с указанием сведений в виде мероприятий по защите персональных данных, периодичности проведения и исполнителя таких мероприятий в образовательной организации основного общего образования.

4.4. Приказом «Об организации работ по обеспечению безопасности персональных данных» назначаются:

- ответственный за обеспечение безопасности персональных данных;
- ответственный по выполнению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- администратор информационной безопасности.

4.5. В образовательной организации основного общего образования должна быть создана комиссия по определению уровня защищённости персональных данных при их обработке в информационных системах персональных данных (распространённое сокращение - ИСПДн).

Данная комиссия назначается приказом «О назначении комиссии по определению уровня защищённости персональных данных при их обработке в информационных системах персональных данных» и должна состоять из председателя комиссии и не менее двух членов комиссии.

4.6. Приказ «Об утверждении мест хранения материальных носителей персональных данных» утверждает помещения с указанием номера или наименования помещений в качестве мест для хранения материальных носителей персональных данных. Приказ также должен определять ответственного за сохранность материальных носителей персональных данных, возлагая ответственность на работника образовательной организации основного общего образования с указанием его должности и Ф.И.О.

4.7. Обеспечение безопасности персональных данных предполагает наличие журнала учёта машинных носителей информации.

Журнал предполагает составление сводной таблицы с занесением следующих сведений:

- регистрационного (учётного) номера или маркировки носителя (жесткие диски аттестованных машин, флеш-носители, если используются для передачи персональных данных);
- типа носителей и его ёмкость;
- даты поступления в организацию;
- расписки в получении (с указанием Ф.И.О., подписи, даты);
- расписки в обратном приеме (с указанием Ф.И.О., подписи, даты);
- места хранения;
- даты и номера акта об уничтожении.

4.8. Перечень персональных данных фиксируется в виде сводной таблицы с указанием наименования персональных данных и способа их обработки и утверждается приказом образовательной организации основного общего образования. Включает в себя сведения, составляющие персональные данные работников образовательной организации основного общего образования; сведения, составляющие персональные данные учащихся образовательной

организации; сведения, составляющие персональные данные родителей и законных представителей учащихся.

4.9. Перечень информационных систем персональных данных утверждается приказом руководителя и предполагает наличие таких критериев, как наименование информационной системы персональных данных, наименование и адрес объекта, указание ответственного лица и способа обработки данных.

4.10. Список лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей. В списке должна указываться должность, Ф.И.О. и информационная система.

4.11. Журнал проверок юридического лица, проводимых органами государственного контроля (надзора), органами муниципального контроля.

В журнале указывается дата начала и окончания проверки, общее время проведения проверки, наименование органа государственного контроля (надзора), наименование органа муниципального контроля, дата и номер распоряжения или приказа о проведении проверки, цель, задачи и предмет проверки, определяется вид проверки (плановая или внеплановая): для плановой проверки даётся ссылка на ежегодный план проведения проверок, для внеплановой – дата и номер решения прокурора о согласовании проведения проверки, дата и номер акта, составленного по результатам проверки, дата его вручения представителю юридического лица, фиксируются выявленные нарушения обязательных требований (указываются содержание выявленного нарушения со ссылкой на положение нормативного правового акта, которым установлено нарушенное требование, допустившее его лицо), дата, номер и содержание выданного предписания об устранении выявленных нарушений.

В журнале обязательно указываются Ф.И.О. и должность должностного лица, проводящего проверку, Ф.И.О., должность экспертов, представителей экспертных организаций, привлеченных к проведению проверки. Конечной графой является графа с подписью должностного лица, проводившего проверку.

4.12. Журнал учёта ключей от сейфов и помещений - сводная таблица с занесением сведений: номер или маркировка сейфа, помещения, дата и время выдачи ключа, расписка о выдаче (Ф.И.О., подпись), расписка о получении (Ф.И.О., подпись), дата и время обратного приема ключа, расписка об

обратном получении (Ф.И.О., подпись), расписка о возвращении (Ф.И.О., подпись).

4.13. Журнал учёта обращения граждан - составление сводной таблицы с занесением сведений: дата обращения, Ф.И.О. посетителя, вид обращения и его краткое содержание, какое принято, решение, кто принимал (Ф.И.О., должность).

4.14. Журнал учёта средств защиты информации, эксплуатационной и технической документации к ним. Журнал представляет собой таблицу с занесением сведений: наименование средства защиты, эксплуатационной и технической документации к ним, регистрационные номера средств защиты, эксплуатационной и технической документации к ним, отметка о подключении (установке) средств защиты: Ф.И.О. пользователя производившего подключение (установку), дата подключения (установки) и подписи лиц, произведших подключение (установку), отметка об изъятии средств защиты из эксплуатации: дата изъятия, Ф.И.О. пользователя, производившего изъятие.

4.15. Приказ «Об утверждении границ контролируемой зоны». С целью организации работ по защите информации в образовательной организации основного школьного образования в соответствии с требованиями руководящих документов ФСТЭК Российской Федерации и Федерального Закона Российской Федерации от 27 июня 2006года №153-ФЗ «О персональных данных» утверждаются границы контролируемой зоны, в рамках которой контролируется нахождение посторонних лиц на территории образовательной организации основного общего образования.

4.16. Инструкция по физической охране, контролю доступа в помещения определяет основные требования к организации внутриобъектового режима в специализированных помещениях, в которых производится обработка и хранение информации ограниченного доступа, порядок организации и производства ремонтно-строительных работ в здании, порядок организации охраны и доступа в специализированные помещения, а также уборки в специализированных помещениях.

4.17. Инструкция обслуживающего персонала информационных систем персональных данных определяет порядок работы и доступа обслуживающего

персонала к ресурсам информационных систем персональных данных и устанавливает ответственность обслуживающего персонала.

4.18. Инструкция по работе ответственного лица за организацию обработки персональных данных определяет основные обязанности, права и ответственность ответственного лица за организацию обработки персональных данных в образовательной организации основного общего образования.

4.19. Инструкция ответственного за обеспечение безопасности персональных данных определяет основные обязанности и права ответственного лица за обеспечение безопасности персональных данных, а также определяет действия при обнаружении попыток несанкционированного доступа и устанавливает ответственность.

4.20. Инструкция администратора безопасности информационных систем персональных данных определяет порядок обеспечения безопасности информации при проведении работ администратором безопасности в информационных системах персональных данных, требования к администратору безопасности, определяет порядок доступа к ресурсам и порядок работы с ресурсами информационных систем персональных данных, определяет действия при обнаружении попыток несанкционированного доступа и устанавливает ответственность администратора безопасности.

4.21. Инструкция по разграничению доступа пользователей к средствам защиты и информационным ресурсам определяет порядок организации работ по разграничению доступа пользователей к средствам защиты и информационным ресурсам, обрабатываемым в информационных системах персональных данных и регламентирует обеспечение сохранности информации.

4.22. Инструкция по учёту машинных носителей и регистрации их выдачи содержит регламентирование порядка учета, хранения и регистрации выдачи машинных носителей персональных данных, а также определяет ответственность за соблюдение требований учёта.

4.23. Инструкция пользователя информационной системы персональных данных должна определять порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем

персональных данных, порядок работы пользователя с ресурсами информационной системы персональных данных, порядок организации парольной защиты.

4.24. Инструкция о порядке работы с персональными данными разрабатывается в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными. Определяет порядок работы со сведениями, содержащими персональные данные, а также устанавливает ответственность за разглашение персональных данных.

4.25. Инструкция по организации антивирусной защиты определяет требования к организации защиты информационной системы персональных данных от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения; устанавливает ответственность администратора безопасности информационной системы персональных данных и других должностных лиц, настраивающих и сопровождающих средства антивирусной защиты, за выполнение требований.

4.26. Инструкция по организации парольной защиты представляет собой регламентирование процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных, регламентирование контроля над действиями пользователей и обслуживающего персонала системы при работе с паролями.

4.27. Инструкция по учету лиц, допущенных к работе с персональными данными, определяет порядок учёта лиц, допущенных к работе с персональными данными в информационных системах образовательной организации основного общего образования, а также предполагает составление журнала учёта лиц, допущенных к работе с персональными данными в информационных системах.

4.28. Регламент резервного копирования данных, методика резервного копирования, методика восстановления данных представляет собой определение порядка резервирования данных для последующего восстановления работоспособности информационной системы персональных данных при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными

бедствиями и т.д.), порядка восстановления информации в случае возникновения такой необходимости. Регламент нацелен на упорядочение работы должностных лиц, связанной с резервным копированием и восстановлением информации.

4.29. Журнал учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных оформляется в виде сводной таблицы с занесением таких сведений как: должность и Ф.И.О. сотрудника, сведения о допуске к персональным данным (наименование информационной системы персональных данных, дата утверждения «Перечня лиц…», дата и подпись допускаемого лица), указание сотрудника, проводившего инструктаж, подпись инструктируемого лица, сведения о прекращении допуска к персональным данным (дата утверждения «Перечня лиц…» или дата приказа об увольнении, номер приказа об увольнении, дата и подпись лица об ознакомлении с документом, прекращающим допуск к персональным данным).

4.30. Журнал учёта паролей пользователей информационной системы персональных данных оформляется в виде сводной таблицы с занесением сведений: даты установки пароля, Ф.И.О. пользователя, номера конверта с паролем, причины изменения, подписи пользователя.