Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа № 28 имени П.В. Рыженко» города Калуги

Принято

Педагогическим советом
протокол № 1
от «30» августа 2021г.

Утверждаю

Директор _____ Е.В. Христофорова
Приказ № 145-ОД от 01.09.2021г.

ПОЛОЖЕНИЕ
О КОМИССИИ ПО ОПРЕДЕЛЕНИЮ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящее Положение о комиссии по определению уровня защищенности персональных данных (далее – Положение) разработано на основании:

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящее Положение определяет функции, состав и порядок работы Комиссии по определению уровня защищенности персональных данных школы (далее – Комиссия).

1.3. Комиссия формируется из числа штатных сотрудников школы, участвующих в процессе обработки персональных данных.

1.4. В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.

1.5. Состав Комиссии утверждается приказом директора школы.

1.6. Комиссия в своей деятельности руководствуется действующим законодательством Российской Федерации, уставом и локальными нормативными актами школы.

2. Типы угроз безопасности ПДн в ИСПДн

2.1. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

2.2. Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

2.3. Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

2.4. Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

2.5. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором (ответственный за обработку персональных данных) с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 181 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

3. Уровни защищенности ПДн

3.1. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

3.2. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора

3.3. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора
- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных

более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора

3.4. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора

– для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора

3.5. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные

– для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора

3.6. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

– организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

– обеспечение сохранности носителей персональных данных

– утверждение директором документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей

– использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз

3.7. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

3.8. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований,

предусмотренных пунктом 3. настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

3.9. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 3.8 настоящего документа, необходимо выполнение следующих требований:

– автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе

– возложение на сотрудников функций по обеспечению такой безопасности

3.10. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

4. Основные функции Комиссии

Основными функциями Комиссии являются:

4.1. Рассмотрение и координация хода выполнения требований действующего законодательства по вопросам защиты персональных данных (далее – ПДн).

4.2. Анализ состояния работы с ПДн в школе.

4.3. Анализ и определение уровня защищенности ПДн при их обработке.

4.4. Рассмотрение и анализ результатов контроля эффективности работы по обеспечению безопасности ПДн.

5. Организация деятельности Комиссии

5.1.Основной формой деятельности Комиссии является заседание.

5.2. Заседания Комиссии проводит председатель или, по его поручению, уполномоченное лицо.

5.3. Заседания Комиссии проводятся не реже одного раза в год.

5.4. Для решения экстренных вопросов сроки проведения внеочередного заседания согласовываются с председателем Комиссии.

5.5. Члены Комиссии лично участвуют в заседаниях Комиссии. В случае невозможности присутствия на заседании член Комиссии может сообщить свое мнение по рассматриваемым вопросам письменно.

5.6. По решению председателя Комиссии, ходатайству членов Комиссии на заседания могут быть приглашены:

- представители органов власти
- представители контрольно-надзорных органов
- представители компаний – поставщиков информационных услуг, специального оборудования.

5.7. Заседание Комиссии является правомочным, если на нем присутствует не менее половины ее состава.

5.8. Решения Комиссии принимаются большинством голосов присутствующих членов Комиссии и оформляются протоколами, которые подписывает председательствующий на заседании Комиссии.

5.9. Члены Комиссии обладают равными правами при обсуждении и при голосовании по вопросам, внесенным в повестку заседания Комиссии.

5.10. При равенстве голосов членов Комиссии голос председателя Комиссии является решающим.

5.11. Для предварительной подготовки вопросов, вносимых в повестку заседания Комиссии, могут быть созданы рабочие группы. В состав рабочих групп могут быть могут быть включены специалисты из состава сотрудников школы и/или иных организаций. Регламент, определяющий порядок деятельности рабочих групп, разрабатывается Комиссией.

5.12. Решения Комиссии рассылаются членам Комиссии и иным заинтересованным лицам в установленном порядке.

5.13. По решениям Комиссии, принятым в пределах ее компетенции, могут разрабатываться проекты локальных нормативных актов школы.

5.14. Итоговым документом работы Комиссии является Акт определения уровня защищенности ПДн в информационных системах ПДн (далее – ИСПДн) (Приложение 1).

6. Права Комиссии

Комиссия для решения возложенных на нее задач имеет право:

6.1. Взаимодействовать в установленном порядке с территориальными органами федеральных органов исполнительной власти, органами местного самоуправления, а также с организациями и должностными лицами по вопросам, входящим в ее компетенцию.

6.2. Запрашивать и получать в установленном порядке необходимые материалы и информацию от территориальных органов федеральных органов исполнительной власти, органов местного самоуправления и иных организаций.

6.3. Пользоваться в установленном порядке базами данных, системами связи и коммуникации школы.

6.4. Пользоваться в установленном порядке базами данных, к которым имеет право доступа школа.

6.5. Привлекать в установленном порядке для осуществления аналитических и экспертных работ сторонних специалистов.

6.6. Вносить предложения по обеспечению информационной безопасности.

7. Обязанности членов Комиссии

7.1.Члены Комиссии обязаны:

- участвовать в заседаниях Комиссии
- давать свои заключения, предложения и замечания по подготавливаемым Комиссией документам
- участвовать в проведении экспертиз по направлениям деятельности Комиссии.
- принимать участие в голосовании по вопросам, внесенным на обсуждение Комиссии, быть готовым аргументировать свою позицию.

7.2.Председатель Комиссии в дополнение к указанным в п.5.1 обязанностям:

- организует подготовку заседаний Комиссии, осуществляет контроль за деятельностью рабочих групп
- привлекает в установленном порядке из состава сотрудников школы и/или иных организаций
- обеспечивает взаимодействие со сторонними организациями
- организует подготовку информационных материалов о работе Комиссии

7.3.Секретарь Комиссии в дополнение к указанным в п.5.1. обязанностям:

- осуществляет подготовку проектов заседаний работы Комиссии и контроль за их реализацией, а также подготовку необходимых документов и аналитических материалов к заседаниям Комиссии
- обеспечивает проведение заседаний Комиссий в установленный срок

– оформляет протоколы заседаний Комиссии, участвует в подготовке проектов докладов, а также информационных материалов для председателя и членов Комиссии (Приложение 2)

– принимает участие в подготовке проектов документов для представления в органы власти и контрольно-надзорные органы в части обеспечения информационной безопасности.