МБОУ "БАРНАУЛЬСКИЙ КАДЕТСКИЙ КОРПУС"

Подписано цифровой подписью: МБОУ "БАРНАУЛЬСКИЙ КАДЕТСКИЙ КОРПУС"
Дата: 2022.11.24 09:54:47 +07'00'

УТВЕРЖДАЮ
ДиректорМБОУ
«Барнаульский кадетский корпус»
_____В.В. Оноприенко
«____» _____ 20___ года

ПОЛОЖЕНИЕ
О КОМИССИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о комиссии по защите персональных данных (далее – Положение) определяет основные задачи, функции и права комиссии, в обязанности которой входит проведение работ по обеспечению безопасности и организации обработки персональных данных в МБОУ «Барнаульский кадетский корпус».

1.2. Комиссия по приведению Оператора в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее – Комиссия), назначается на весь период обработки персональных данных у Оператора приказом руководства Оператора.

1.3. В состав Комиссии добавляются новые члены приказом руководства Оператора.

1.4. Из состава Комиссии сотрудники исключается на основании приказа руководства Оператора.

1.5. Основной задачей Комиссии является приведение деятельности Оператора в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее – Требования) и контроль над исполнением основных положений законодательства.

1.6. Свою деятельность Комиссия осуществляет в соответствии с «Планом мероприятий по приведению МБОУ «Барнаульский кадетский корпус»в соответствие с требованиями законодательства Российской Федерации в области персональных данных», утверждаемым руководством Оператора.

1.7. Комиссия самостоятельно разрабатывает «План мероприятий по приведению МБОУ «Барнаульский кадетский корпус» в соответствие с требованиями законодательства Российской Федерации в области персональных данных» и передает руководству Оператора на утверждение.

1.8. В своей деятельности Комиссия руководствуется законодательными и нормативно-правовыми актами Российской Федерации в области персональных данных, настоящим Положением и иными нормативными актами Оператора.

1.9. Законодательные и нормативно-правовые акты Российской Федерации в области персональных данных приведены в Приложении №1 к настоящему Положению.

2. ОРГАНИЗАЦИОННАЯ СТРУКТУРА КОМИССИИ

2.1. Комиссия состоит из Председателя Комиссии и членов Комиссии.

2.2. Комиссия возглавляется Председателем Комиссии.

2.3. Комиссия подчиняется руководству Оператора.

2.4. Из состава Комиссии назначается лицо, ответственное за организацию обработки персональных данных, и администратор безопасности информационных систем персональных данных.

3. ОСНОВНЫЕ ФУНКЦИИ КОМИССИИ

3.1. Разработка проектов документов, необходимых для выполнения Требования законодательства и представленных в Приложении №2 к настоящему Положению.

3.2. Организация и проведение работ по обеспечению безопасности помещений, в которых производится обработка персональных данных, а также находятся на хранении материальные носители персональных данных.

3.3. Анализ и оценка соответствия внутренних нормативных документов Оператора, в части касающейся обработки персональных данных, а в случае выявления несоответствий – внесение необходимых изменений.

3.4. Организация и проведение работ по обучению и повышению осведомленности персонала в области персональных данных.

3.5. Анализ изменений законодательства Российской Федерации в области персональных данных.

3.6. Оценка выполнения Оператором обязанностей, установленных законодательством Российской Федерации в области персональных данных, а в случае выявления несоответствий – выработка рекомендаций по их устранению.

3.7. Организация подготовки и направления в уполномоченный орган по защите прав субъектов персональных данных Уведомления об обработке персональных данных, а в случае изменения сведений, содержащихся в Реестре операторов, осуществляющих обработку персональных данных, направление сведений о таких изменениях.

3.8. В случае выявления неправомерных действий с персональными данными, Комиссия направляет уведомление об устранении нарушений.

3.9. Анализ и оценка соответствия Требованиям законодательства типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, а в случае выявления несоответствий – выработка рекомендаций по их устранению.

3.10. Анализ и оценка соответствия договорной базы Оператора Требованиям законодательства, а в случае выявления несоответствий – внесение соответствующих изменений и дополнений.

3.11. Контроль выполнения Требований законодательства, в части касающейся согласия субъектов персональных данных на обработку их персональных данных.

3.12. Общий контроль соблюдения Оператором требований по обеспечению безопасности персональных данных и соблюдения Требований законодательства.

3.13. Организация работ и сбор необходимых документов при прохождении федерального государственного контроля (надзора) за соответствием обработки персональных данных Требованиями законодательства.

3.14. Ведение журнала по учету проверок в соответствии с Требованиями законодательства.

3.15. Организация работ по разработке моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных Оператора, в том числе:

3.15.1. оценка полноты и правильности определения угроз безопасности;

3.15.2. плановый и внеплановый пересмотр.

3.16. Организация работ по созданию системы защиты персональных данных (комплекса организационно-технических мер), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего уровня защищенности информационных систем персональных данных.

3.17. Проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.

3.18. Обучение лиц, применяющих средства защиты информации, правилам работы с ними.

3.19. Организация учета применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.

3.20. Контроль выполнения мероприятий по защите персональных данных, реализуемых в рамках подсистем защиты с учетом уровня защищенности информационной системы персональных данных (не реже 1 раза в 3 года):

3.20.1. идентификация и аутентификация субъектов доступа и объектов доступа;

3.20.2. управление доступом субъектов доступа к объектам доступа;

3.20.3. ограничение программной среды;

3.20.4. защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

3.20.5. регистрация событий безопасности;

3.20.6. антивирусная защита;

3.20.7. обнаружение (предотвращение) вторжений;

3.20.8. контроль (анализ) защищенности персональных данных;

3.20.9. обеспечение целостности информационной системы и персональных данных;

3.20.10. обеспечение доступности персональных данных;

3.20.11. защита среды виртуализации;

3.20.12. защита технических средств;

3.20.13. защита информационной системы, ее средств, систем связи и передачи данных;

3.20.14. выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

3.20.15. управление конфигурацией информационной системы и системы защиты персональных данных.

3.21. Контроль за соответствием условий эксплуатации информационных систем персональных данных требованиям организационно-технической и эксплуатационной документации.

3.22. Контроль соблюдения работниками Оператора установленных требований по обеспечению безопасности персональных данных, проведение разбирательств и составление заключений по фактам несоблюдения данных требований.

3.23. Проведение внутренних проверок состояния защиты персональных данных.

3.24. Анализ эффективности и достаточности принятых мер и применяемых средств защиты персональных данных.

3.25. Разработка предложений по совершенствованию системы защиты персональных данных.

3.26. Решение вопросов, связанных с обслуживанием и эксплуатацией информационных систем:

3.26.1. эксплуатация информационных систем персональных данных в соответствии с организационно-технической и эксплуатационной документацией;

3.26.2. обеспечение работоспособности системы защиты персональных данных, реализуемой в рамках подсистем защиты с учетом уровня защищенности информационной системы;

3.26.3. организация мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

3.26.4. организация учета и использования машинных носителей информации;

3.26.5. организация работ по привлечению сторонних организаций для формирования и сопровождения баз данных и информационного взаимодействия (центров обработки информации), выполняющих функции операторов и администраторов системы централизованной обработки данных;

3.26.6. установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

3.26.7. учет лиц, допущенных к работе с персональными данными в информационных системах персональных данных.

3.27. Организация работ по размещению оборудования информационных систем персональных данных в части выполнения требований по сохранности носителей персональных данных и средств защиты информации, а также исключения возможности проникновения и неконтролируемого пребывания посторонних лиц на охраняемую территорию.

3.28. Уточнение персональных данных субъектов.

3.29. Блокирование обработки персональных данных субъектов.

3.30. Уничтожение персональных данных (по достижении целей обработки или в случае утраты необходимости в их достижении) при их автоматизированной обработке. Инструкция по уничтожению и обезличиванию персональных данных на бумажных и электронных носителях – Приложение 1.

3.31. Обеспечение безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

3.32. Организация работ по ознакомлению работников Оператора, осуществляющих обработку персональных данных без использования средств автоматизации, а также лиц, осуществляющих такую обработку по договору с Оператором, о факте обработки ими персональных данных без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

3.33. Обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.34. Организация работ по уничтожению материальных носителей персональных данных в случае достижения целей обработки или в случае утраты необходимости в их достижении с составлением актов об уничтожении.

3.35. Контроль выполнения требований настоящего Положения.

3.36. Определение уровня защищенности информационных систем персональных данных.

4. ПРАВА КОМИССИИ

4.1. Запрос и получение необходимых материалов для организации и проведения работ по вопросам обеспечения безопасности персональных данных у Оператора.

4.2. Привлечение к проведению работ по защите персональных данных на договорной основе сторонних организаций.

4.3. Контроль деятельности структурных подразделений Оператора в части выполнения ими требований по обеспечению безопасности персональных данных.

4.4. Внесение предложений руководству Оператора о приостановке работ в случае обнаружения несанкционированного доступа, утечки персональных данных, а также в случае предпосылок нарушения безопасности персональных данных.

5. ОТВЕТСТВЕННОСТЬ

5.1. Председатель Комиссии и члены Комиссии несут ответственность в соответствии с законодательством Российской Федерации.

Приложение 1

Инструкция по уничтожению и обезличиванию персональных данных на бумажных и электронных носителях

Общие положения

1.1 Настоящая инструкция определяет порядок уничтожения и обезличивания информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в ГБОУ школы-интерната №1 им. К. К. Грота Красногвардейского района Санкт- Петербурга (далее - Школы-интерната).

1.2 Целью настоящей инструкции 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 тайну.

1.3 Основные понятия, используемые в Инструкции:

- Персональные данные (далее - ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2. Условия и порядок уничтожения, содержащих персональные данные

2.1 Документы, содержащие персональные данные, обрабатываемые в структурных подразделениях Школы-интерната, обязаны храниться в течение сроков, установленных Федеральным законом №125-ФЗ от 22.10.2004г. и перечнем утвержденном приказом Минкультуры России от 25.08. 2010 г. № 558.

2.2 Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

В случае отзыва согласия на обработку ПДн оператор обязан прекратить их обработку и в случае, если сохранение ПДн более не требуется для целей обработки, уничтожить ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва и письменно известить субъекта ПДн об окончании обработки его ПДн (приложение 3).

2.4 В случае отзыва субъектом ПДн согласия на обработку ПДн оператор вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6 части 2 статьи 10 и части 2 статьи 11 Федерального закона № от 27.07.2006 N 152-ФЗ

2.5 В случае выявления неправомерной обработки ПДн, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие персональные данные.

2.6 Отбор носителей ПДн к уничтожению осуществляется по решению руководителя соответствующего подразделения, к деятельности которого относится носитель и ответственного по защите ПДн.

2.7 По итогам создается комиссия и составляется Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами комиссии (приложение 1).

2.8 Уничтожение материальных носителей ПДн производится с участием комиссии, в состав которой входят ответственные работники, допущенные к работе с ПДн и сотрудники ответственные за защиту ПДн.

2.9 Уничтожение материальных носителей ПДн производится путем измельчения, сожжения или механического уничтожения. На каждый способ уничтожения составляется отдельный акт.

2.10 Уничтожение съемных машинных носителей информации (Flash, CD иDVD -дисков и др.) производится путем деформирования до состояния, которое исключает их повторное использование с последующим сожжением.

2.11 Перед уничтожением необходимо произвести циклы полного удаления всей информации.

2.12 После уничтожения материальных носителей членами: комиссии подписывается акт об уничтожении носителей, содержащих персональные данные.

2.13 Об уничтожении файлов делаются соответствующие отметки в Журнале уничтожения носителей персональных данных (Приложение 2).

Условия и порядок обезличивания документов, содержащие персональные данные

4.1 Оператор может обезличивать персональные данные в статистических или иных исследовательских целях, по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- замена части данных идентификаторами;
- обобщение, изменение или удаление части данных;
- деление данных на части и обработка в разных информационных системах;
- перемешивание данных;

3.3. В случае достижения целей обработки персональных данных или в случае утраты необходимости в достижении этих целей способом обезличивания является уменьшение перечня обрабатываемых данных.

3.5. Решение о необходимости обезличивания персональных данных и способе обезличивания принимает ответственный по защите персональных данных.

3.6. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Приложение 2

Типовая форма акта об уничтожении носителей, содержащих персональные данные

Акт N _____об уничтожении носителей, содержащих персональные данные

Комиссия в составе:

Председатель- _____

Члены комиссии - _____

провела отбор бумажных, электронных, магнитных и оптических носителей персональных данных и другой конфиденциальной, информации (далее носители) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению и составила настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

N п/н	Дата	Тип носителя	Учетный номер носителя	Категории информации	Примечание

Всего носителей _____
(цифрами и прописью количество)

На указанных носителях персональные данные уничтожены путем_____
_____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПД уничтожены путем_____
(разрезания/сжигания/размагничивания/физического уничтожении/механического уничтожения / иного способа)

Председатель комиссии:_____ / _____/

Члены комиссии:_____/_____/

_____/_____/

Приложение 3

Типовая форма журнала уничтожения носителей персональных данных

Журнал уничтожения носителей персональных данных

Журнал начат_____
Журнал завершен_____
Ответственный _____ (Ф.И.О.)
На_____листах

N п/п	Наименование ИСПД, в которой уничтожаются персональные данные	Ф.И.О. субъекта, переданные которого подлежащие уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположе	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных