Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
**«СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ИМЕНИ М.К. АММОСОВА»**
(СВФУ)

ПРИКАЗ

_____ № _____

г. Якутск

О проведении мероприятий по защите информации

Во исполнение требований Федерального закона Российской Федерации 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", приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Федерального закона Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Федерального закона Российской Федерации от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», руководящих документов ФСТЭК РФ по защите конфиденциальной информации, в том числе персональные данные, и в целях обеспечения защиты конфиденциальной информации и режима безопасности персональных данных п р и к а з ы в а ю:

ЭП: Николаев Анатолий Николаевич
Серт.: 01EB5C2C00E2AA27AE42D0EE35F0C5F511
действ. 10.10.2019-10.10.2020
утверждающая ЭП, ЭП достоверна
Рег №613 от 11.09.2020

1. Утвердить Положение по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (ПРИЛОЖЕНИЕ № 1).

2. Утвердить Политику в отношении обработки персональных данных полученных на веб-сайте https://priem2020.s-vfu.ru/ (ПРИЛОЖЕНИЕ № 2).

3. Утвердить Политику в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (ПРИЛОЖЕНИЕ № 3).

4. Утвердить Порядок хранения, использования и передачи персональных данных сотрудников ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (ПРИЛОЖЕНИЕ № 4).

5. Утвердить Положение о дополнительных требованиях по защите детей от информации, распространяемой посредством информационно-телекоммуникационных сетей, причиняющей вред здоровью и (или) развитию детей (ПРИЛОЖЕНИЕ № 5).

6. Контроль за исполнением настоящего приказа возложить на проректора по цифровому развитию Иванова П.П.

Ректор СВФУ А.Н. Николаев

ЭП: Николаев Анатолий Николаевич
Серт.: 01EB5C2C00E2AA27AE42D0EE35F0C5F511
действ. 10.10.2019-10.10.2020
утверждающая ЭП, ЭП достоверна
Рег №613 от 11.09.2020

Приложение 1
Приказа СВФУ
От _____№_____

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»

1. Общие положения

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (далее - Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Цель разработки настоящего Положения - установление порядка организации и проведения работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее - защищаемая информация, информация), в информационных системах (далее - ИС) ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (далее - СВФУ) на всех стадиях (этапах) создания ИС, в ходе ее эксплуатации и вывода из эксплуатации.

1.3. К защищаемой информации, обрабатываемой в ИС СВФУ, относится следующая информация:

– персональные данные, содержащиеся в информационных системах персональных данных СВФУ;

– информация, не содержащая сведения, составляющие государственную тайну, содержащаяся в государственных информационных системах СВФУ.

2. Термины и определения

2.1. В настоящем Положении используются следующие термины и их определения:

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

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

Несанкционированный доступ (несанкционированные действия)- доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Обработка информации - действия (операции) с информацией, включая сбор, запись,

систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение информации.

Оператор - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных. В случае обработки персональных данных под оператором понимается 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.

Технические средства информационной системы - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

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

Пользователь информационной системы - лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Угрозы безопасности информации - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при ее обработке в информационной системе.

Уничтожение информации - действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации.

Уровень защищенности персональных данных - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Порядок организации и проведения работ по обеспечению безопасности информации

3.1. Под организацией обеспечения безопасности защищаемой информации при ее обработке в ИС понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности защищаемой информации, реализуемых в рамках создаваемой системы защиты информации (далее - СЗИ).

3.2. СЗИ включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности защищаемой информации, уровня защищенности персональных данных (далее - ПДн), который необходимо обеспечить, класса защищенности государственной информационной системы (далее- ГИС) и информационных технологий,

используемых в ИС.

3.3. Безопасность защищаемой информации при ее обработке в ИС обеспечивает СВФУ или лицо, осуществляющее обработку защищаемой информации по поручению СВФУ на основании заключаемого с этим лицом договора (далее - уполномоченное лицо). Договор между СВФУ и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность защищаемой информации при ее обработке в ИС.

3.4. Защита информации, содержащейся в ИС, обеспечивается путем выполнения СВФУ требований к организации защиты информации, содержащейся в ИС, и требований к мерам защиты информации, содержащейся в ИС.

3.5. СВФУ назначается лицо, ответственное за организацию обработки персональных данных при их обработке в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова».

3.6. Для обеспечения безопасности защищаемой информации, содержащейся в ИС, СВФУ назначается структурное подразделение или должностное лицо (работник), ответственное за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (далее - Ответственный).

3.7. Для проведения работ по защите информации в ходе создания, эксплуатации и вывода из эксплуатации ИС СВФУ в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. №99-ФЗ «О лицензировании отдельных видов деятельности».

3.8. Для обеспечения защиты информации, содержащейся в ИС, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании».

3.9. Защита информации, содержащейся в ИС, является составной частью работ по созданию и эксплуатации ИС и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках СЗИ.

3.10. Организационные и технические меры защиты информации, реализуемые в рамках СЗИ должны быть направлены на исключение:

– неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

– неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

– неправомерного блокирования информации (обеспечение доступности информации).

3.11. Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

– формирование требований к защите информации, содержащейся в ИС;

– разработка СЗИ;

– внедрение СЗИ;

– аттестация ИС по требованиям защиты информации (далее - аттестация ИС);

– обеспечение защиты информации в ходе эксплуатации аттестованной ИС;

– обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации.

4. Порядок резервного копирования и восстановления информации в информационных системах СВФУ

4.1. Настоящий порядок определяет правила проведения резервного копирования данных, обрабатываемых в ИС СВФУ.

4.2. Целью резервного копирования является предотвращение потери информации при сбоях оборудования, программного обеспечения, в критических и кризисных ситуациях и т.д.

4.3. Резервному копированию подлежит информация, обрабатываемая в ИС СВФУ.

4.4. В СВФУ должна быть реализована централизованная система резервного копирования.

4.5. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации в установленные сроки и с заданной периодичностью.

4.6. Перед выполнением процедур резервного копирования или восстановления информации и ПО средств защиты необходимо провести проверку:

– доступности резервного носителя, достаточности свободного места в хранилище для записи или восстановления данных:

– работоспособности средств резервного копирования и восстановления;

– готовности информационных ресурсов к осуществлению их резервного копирования или восстановления;

– завершения работы ПО и процессов, способных повлиять на процесс создания или восстановления копий.

4.7. Расписание проведения резервного копирования определяется Ответственным.

4.8. Резервное копирование проводится Ответственным и регистрируется в Журнале резервного копирования и восстановления информации (ПРИЛОЖЕНИЕ № 1).

4.9. Перечень информационных ресурсов, подлежащих резервному копированию, время и дата создания копии, пометки об успешном/неуспешном завершении, а также, при необходимости, комментарии Ответственного заносятся в Журнал резервного копирования и восстановления информации.

4.10. В случае выявления нарушений Ответственному необходимо в кратчайшие сроки устранить неисправности в системе резервного копирования и восстановить работоспособность подсистем в штатный режим работы.

4.11. О выявленных попытках несанкционированною доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования. Ответственный сообщает руководству СВФУ немедленно.

4.12. Ответственный должен контролировать проведение резервного копирования в целях выполнения требований по защите информации.

4.13. В случае обнаружения ошибки резервного копирования Ответственный выполняет повторное копирование информации вручную в максимально сжатые сроки, не нарушая технологические процессы обработки информации пользователями СВФУ, в Журнал резервного копирования и восстановления информации заносятся соответствующие отметки.

4.14. Хранение резервных копий данных осуществляется на сменных носителях информации (CD DVD. внешние жесткие диски и т.п.), промаркированных Ответственным в соответствие с расписанием резервного копирования. Маркировка должна содержать номер копии, дату ее создания, наименование ИС.

4.15. Использование носителей информации при резервном хранении должно подчиняться принципу ротации носителей, при котором для записи текущей копии используется носитель с самой ранней датой создания предыдущей копии.

4.16. Срок хранения резервных копий определяется Ответственным.

4.17. Очистка устаревших резервных копий из хранилища должна производиться

Ответственным регулярно по мере заполнения выделенной области памяти или по истечении предусмотренного срока хранения.

4.18. Удаление резервных копий для повторного использования носителя информации, либо окончательное удаление производится Ответственным.

4.19. Основанием для инициирования процедуры восстановления служит полная или частичная утрата информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях. Восстановление данных производится Ответственным.

4.20. Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

4.21. В зависимости от характера и уровня повреждения информационных ресурсов. Ответственный восстанавливает либо весь архив копии данных, либо отдельные потерянные части или технические средства из соответствующих хранилищ.

4.22. После завершения процесса восстановления Ответственным проверяется целостность информационных ресурсов и корректная работа технических средств информационных систем, также заполняются соответствующие ноля в Журнале резервного копирования и восстановления информации.

5. Формирование требований к защите информации, содержащейся в информационной системе

5.1. Формирование требований к защите информации, содержащейся в ИС, осуществляется СВФУ.

5.2. Формирование требований к защите информации, содержащейся в ИС, включает:

– принятие решения о необходимости защиты информации, содержащейся в ИС;

– классификацию ИС по требованиям защиты информации, определение уровня защищенности ПДн, при их обработке в ИС;

– определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в ИС, и разработку на их основе модели угроз безопасности информации;

– определение требований к СЗИ.

5.3. При принятии решения о необходимости защиты информации, содержащейся в ИС, осуществляется:

– анализ целей создания ИС и задач, решаемых этой ИС;

– определение информации, подлежащей обработке в ИС;

– анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС;

– принятие решения о необходимости создания СЗИ, а также определение целей и задач защиты информации в ИС, основных этапов создания СЗИ и функций по обеспечению защиты информации, содержащейся в ИС.

5.4. Результаты классификации ИС оформляются актом классификации.

5.5. Результаты определения уровня защищенности ПДн при их обработке в ИС оформляются актом определения уровня защищенности.

5.6. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

5.7. В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России.

5.8. При определении угроз безопасности информации учитываются структурно-функциональные характеристики ИС, включающие структуру и состав ИС, физические, логические, функциональные и технологические взаимосвязи между сегментами ИС, с иными ИС и информационно-телекоммуникационными сетями, режимы обработки информации в ИС и в ее отдельных сегментах, а также иные характеристики ИС, применяемые информационные технологии и особенности ее функционирования.

5.9. По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно- функциональных характеристик ИС, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

5.10. Модель угроз безопасности информации должна содержать описание ИС и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИС, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

5.11. Требования к СЗИ определяются в зависимости от класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС и угроз безопасности информации, включенных в модель угроз безопасности информации.

5.12. При определении требований к СЗИ учитываются положения политики СВФУ в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну.

6. Разработка системы защиты информации

6.1. Разработка СЗИ организуется СВФУ.

6.2. Разработка СЗИ осуществляется в соответствии с техническим заданием на создание СЗИ, и в том числе, включает:

- проектирование СЗИ;
- разработку эксплуатационной документации на СЗИ;
- макетирование и тестирование СЗИ (при необходимости).

6.3. СЗИ не должна препятствовать достижению целей создания ИС и ее функционированию.

6.4. При разработке СЗИ учитывается ее информационное взаимодействие с иными ИС и информационно-телекоммуникационными сетями.

6.5. При проектировании СЗИ осуществляются следующие мероприятия:

- определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);
- определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в ИС;
- выбираются меры защиты информации, подлежащие реализации в СЗИ;
- определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации:
- определяется структура СЗИ, включая состав (количество) и места размещения ее элементов;
- осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости,

совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС;

– определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей ИС, приводящих к возникновению угроз безопасности информации;

– определяются меры защиты информации при информационном взаимодействии с иными ИС и информационно-телекоммуникационными сетями.

6.6. Результаты проектирования СЗИ отражаются в проектной документации на ИС.

6.7. При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по ИС и (или) ее СЗИ с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.

6.8. Разработка эксплуатационной документации на СЗИ осуществляется в соответствии с техническим заданием на создание СЗИ.

6.9. При макетировании и тестировании СЗИ, в том числе, осуществляются:

– проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

– проверка выполнения выбранными средствами защиты информации требований к СЗИ,

– корректировка проектных решений, разработанных при создании СЗИ.

6.10. Макетирование СЗИ и ее тестирование может проводиться, в том числе, с использованием средств и методов моделирования ИС и технологий виртуализации.

7. Внедрение системы защиты информации

7.1. Внедрение СЗИ организуется СВФУ.

7.2. Внедрение СЗИ осуществляется в соответствии с проектной и эксплуатационной документацией на СЗИ и, в том числе, включает:

– установку и настройку средств защиты информации в ИС;

– разработку документов, определяющих правила и процедуры, реализуемые СВФУ для обеспечения защиты информации в ИС в ходе ее эксплуатации (далее организационно-распорядительные документы по защите информации);

– внедрение организационных мер защиты информации;

– предварительные испытания СЗИ (при необходимости);

– опытную эксплуатацию СЗИ (при необходимости);

– анализ уязвимостей ИС и принятие мер защиты информации по их устранению;

– приемочные испытания СЗИ (при необходимости).

7.3. Установка и настройка средств защиты информации в ИС должна проводиться в соответствии с эксплуатационной документацией на СЗИ и документацией на средства защиты информации.

7.4. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

– планирования мероприятий по защите информации в ИС;

– управления (администрирования) СЗИ;

– выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности

информации (далее - инциденты), и реагирования на них;

– управления конфигурацией аттестованной ИС и СЗИ:

– контроля за обеспечением уровня защищенности информации, содержащейся в ИС;

– информирования и обучения персонала ИС;

– защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации.

7.5. При внедрении организационных мер защиты информации осуществляются:

– реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

– проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов ИС по реализации организационных мер защиты информации;

– отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

7.6. Предварительные испытания СЗИ включают проверку работоспособности СЗИ, а также принятие решения о возможности опытной эксплуатации СЗИ.

7.7. Опытная эксплуатация СЗИ включает проверку функционирования СЗИ, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации СЗИ.

7.8. Анализ уязвимостей ИС проводится в целях оценки возможности преодоления нарушителем СЗИ и предотвращения реализации угроз безопасности информации. Анализ уязвимостей ИС включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения ИС. При анализе уязвимостей ИС проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением. В случае выявления уязвимостей ИС, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей. По результатам анализа уязвимостей должно быть подтверждено, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

7.9. Приемочные испытания СЗИ включают проверку выполнения требований к СЗИ в соответствии с техническим заданием на создание СЗИ.

8. Аттестация информационной системы

8.1. Аттестация ИС организуется СВФУ и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие СЗИ требованиям по безопасности информации.

8.2. Проведение аттестационных испытаний ИС должностными лицами, осуществляющими проектирование и (или) внедрение СЗИ ИС. не допускается.

8.3. В качестве исходных данных, необходимых для аттестации ИС, используются модель угроз безопасности информации, акт классификации ИС, акт определения уровня

защищенности ПДн при их обработке в ИС, техническое задание на создание СЗИ, проектная и эксплуатационная документация па СЗИ, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей ИС, материалы предварительных и приемочных испытаний СЗИ (при наличии).

8.4. Аттестация ИС проводится в соответствии с программой и методиками аттестационных испытаний. Для проведения аттестации ИС применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. №1085. По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии (не соответствии) ИС требованиям по защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.

8.5. При проведении аттестационных испытаний должны применяться следующие методы проверок (испытаний):

– экспертно-документальный метод, предусматривающий проверку соответствия СЗИ ИС установленным требованиям по защите информации, на основе оценки эксплуатационной документации, организационно-распорядительных документов по защите информации, а также условий функционирования ИС;

– анализ уязвимостей ИС, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации:

– анализ уязвимостей ИС, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации;

– испытания СЗИ путем осуществления попыток несанкционированною доступа (воздействия) к ИС в обход ее СЗИ.

8.6. Допускается аттестация ИС на основе результатов аттестационных испытаний выделенного набора сегментов ИС, реализующих полную технологию обработки информации. В этом случае распространение аттестата соответствия на другие сегменты ИС осуществляется при условии их соответствия сегментам ИС, прошедшим аттестационные испытания. Сегмент считается соответствующим сегменту ИС, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищенности, уровни защищенности, уровни важности, угрозы безопасности информации, реализованы одинаковые проектные решения по ИС и ее СЗИ. В сегментах ИС, на которые распространяется аттестат соответствия, СВФУ обеспечивается соблюдение эксплуатационной документации на СЗИ и организационно-распорядительных документов по защите информации.

8.7. Особенности аттестации ИС на основе результатов аттестационных испытаний выделенного набора се сегментов, а также условия и порядок распространения аттестата соответствия на другие сегменты ИС определяются в программе и методиках аттестационных испытаний, заключении и аттестате соответствия.

8.8. Повторная аттестация информационной системы осуществляется по окончании срока действия аттестата соответствия, который не может превышать 5 лет, или повышения класса защищенности информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании СЗИ, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

9. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

9.1. Обеспечение защиты информации в ходе эксплуатации аттестованной ИС осуществляется СВФУ в соответствии с эксплуатационной документацией на СЗИ и

организационно-распорядительными документами по защите информации и в том числе включает:

- планирование и контроль мероприятий по защите информации в ИС;
- анализ угроз безопасности информации в ИС;
- управление (администрирование) СЗИ;
- выявление инцидентов и реагирование на них;
- управление конфигурацией ИС и ее СЗИ;
- информирование и обучение персонала ИС;
- контроль за обеспечением уровня защищенности информации, содержащейся в ИС.

9.2. В ходе планирования мероприятий по защите информации в ИС осуществляется:

- определение лиц. ответственных за планирование и контроль мероприятий по защите информации в ИС;
- определение лиц. ответственных за выявление инцидентов и реагирование на них;
- разработка, утверждение и актуализация плана мероприятий по защите информации в ИС;
- определение порядка контроля выполнения мероприятий по защите информации в ИС, предусмотренных утвержденным планом.

Планирование мероприятий по защите информации в ИС и контроль выполнения мероприятий должны осуществляться в соответствии с порядком планирования мероприятий по защите информации в ИС и контроля их выполнения, разработанным в рамках внедрения СЗИ ИС.

9.3. В ходе анализа угроз безопасности информации в ИС осуществляется:

- выявление, анализ и устранение уязвимостей ИС;
- анализ изменения угроз безопасности информации в ИС;
- оценка возможных последствий реализации угроз безопасности информации в ИС.

Периодичность проведения указанных работ определена в Плане мероприятий по защите информации (ПРИЛОЖЕНИЕ № 2) и в Плане внутренних проверок режима защиты информации (ПРИЛОЖЕНИЕ № 3).

9.4. В ходе управления (администрирования) СЗИ осуществляются:

- определение лиц, ответственных за управление (администрирование) СЗИ ИС;
- управление учетными записями пользователей ИС и поддержание в актуальном состоянии правил разграничения доступа в ИС;
- управление средствами защиты информации в ИС;
- управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования ИС;
- централизованное управление СЗИ ИС (при необходимости);
- мониторинг и анализ зарегистрированных событий в ИС, связанных с защитой информации (далее - события безопасности);
- обеспечение функционирования СЗИ ИС в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

9.5. В ходе выявления инцидентов и реагирования на них осуществляются:

- обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий,

приводящих к возникновению инцидентов;

– своевременное информирование пользователями ИС и администраторами ИС лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

9.6. В ходе управления конфигурацией ИС и ее СЗИ осуществляются:

– определение лиц, которым разрешены действия по внесению изменений в конфигурацию ИС и ее СЗИ, их полномочия;

– определение компонентов ИС и ее СЗИ, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

– управление изменениями ИС и ее СЗИ: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на защиту информации, санкционирование внесения изменений в ИС и ее СЗИ, документирование действий по внесению изменений в ИС и сохранение данных об изменениях конфигурации ИС;

– контроль действий по внесению изменений в ИС и ее СЗИ.

9.7. В ходе информирования и обучения персонала ИС осуществляется:

– информирование персонала ИС о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС;

– доведение до персонала ИС требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;

– обучение персонала ИС правилам эксплуатации отдельных средств защиты информации;

– проведение практических занятий и тренировок с персоналом ИС по блокированию угроз безопасности информации и реагированию на инциденты;

– контроль осведомленности персонала ИС об угрозах безопасности информации и уровня знаний персонала ИС по вопросам обеспечения защиты информации.

Периодичность проведения указанных работ определена в Плане мероприятий по защите информации и в Плане внутренних проверок режима защиты информации.

9.8. В ходе контроля за обеспечением уровня защищенности информации, содержащейся в ИС, осуществляются:

– контроль (анализ) защищенности информации с учетом особенностей функционирования ИС;

– анализ и оценка функционирования ИС и ее СЗИ, включая анализ и устранение уязвимостей и иных недостатков в функционировании СЗИ ИС;

– документирование процедур и результатов контроля за обеспечением уровня

защищенности информации, содержащейся в ИС;

– принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в ИС, о необходимости доработки (модернизации) ее СЗИ.

9.9. Регулярные мероприятия по обеспечению безопасности защищаемой информации проводятся в соответствии с Планом мероприятий по защите информации. Внутренние проверки режима защиты информации проводятся в соответствии с Планом внутренних проверок режима защиты информации. По результатам проведения внутренней проверки составляется Отчет о результатах внутренней проверки режима защиты информации в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (ПРИЛОЖЕНИЕ №4).

10. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации

10.1. Обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации осуществляется СВФУ в соответствии с эксплуатационной документацией на СЗИ и организационно-распорядительными документами по защите информации и, в том числе, включает:

– архивирование информации, содержащейся в ИС;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

10.2. Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности СВФУ.

10.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

ПРИЛОЖЕНИЕ № 1
к Положению по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»
от «__»_____20__г.

Журнал резервного копирования/ восстановления данных

№ п/п	Схема резервного копирования/восстановления данных	Копируемые/ восстанавливаемые ресурсы	Хранилище	Дата/время создания копии/ восстановления	Фамилия ответственного	Подпись ответственного	Результат резервного копирования/ восстановления данных	Комментарий
1	2	3	4	5	6	7	8	9

ПРИЛОЖЕНИЕ № 3
к Положению по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»
от «__»_____20__г.

План мероприятий по обеспечению безопасности защищаемой информации в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
1.	Документальное регламентирование работы с информацией	При необхо-димости	Разработка и (или) актуализация организационно- распорядительных документов по защите информации
2.	Получение согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство	Постоянно	В случаях, предусмотренных Федеральным законом «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Форма согласия приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области защиты информации». Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью
3.	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необхо-димости	В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных»
4.	Ограничение доступа сотрудников к защищаемой информации	При необхо-димости	В случае создания ИС, а также приведения имеющихся ИС в соответствие с требованиями по безопасности ин-формации необходимо разграничить доступ сотрудников СВФУ к защищаемой информации
5.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передачи ПДн, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки,

			устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц
6.	Ведение журналов учета машинных носителей защищаемой информации, средств защиты информации	Постоянно	-
7.	Повышение квалификации сотрудников в области защиты информации	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ - не менее раза в три года, повышение осведомленности сотрудников - постоянно (данное обучение проводит ответственный за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах СВФУ)
8.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия защищаемой информации
9.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необхо-димости	Для ПДн СВФУ устанавливаются сроки обработки, которые документально подтверждаются в локальных актах СВФУ. При пересмотре сроков необходимые изменения вносятся в соответствующие документы
10.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации	При необхо-димости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Приказе «О комиссии по уничтожению защищаемой информации, не содержащей сведения, составляющие государственную тайну»
11.	Определение класса защищенности ИС	При необхо-димости	Определение класса защищенности ИС осуществляется при создании ИС, при изменении состава ИС, масштаба ИС, степеней ущерба для характеристик ИС (конфиденциальности, целостности, доступности)
12.	Определение уровня защищенности ПДн при их обработке в ИС	При необхо-димости	Определение уровня защищенности ПДн при их обработке в ИС осуществляется при создании ИС, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн
13.	Выявление угроз безопасности и	При необхо-димости	Разрабатывается при создании СЗИ

	разработка моделей угроз и нарушителя		
14.	Аттестация ИС на соответствие требованиям по обеспечению безопасности информации	При необхо-димости	-
15.	Эксплуатация ИС и контроль безопасности защищаемой информации	Постоянно	-
16.	Анализ угроз безопасности в информационной системе	При необхо-димости	В рамках данного мероприятия проводится: -выявление, анализ и устранение уязвимостей или принятие мер по предотвращению возможности эксплуатации выявленных уязвимостей; -анализ изменения угроз безопасности информации в информационных системах; -оценка возможных последствий реализации угроз безопасности информации. По результатам разрабатывается/корректируется модель нарушителей и угроз безопасности информации. При проведении работ необходимо руководствоваться действующими нормативно-методическими документами в области защиты информации
17.	Обновление программного обеспечения (в том числе средств защиты информации)	При необхо-димости	Получение обновлений производится из доверенных источников
18.	Информирование персонала информационных систем о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации информационных систем	Постоянно	-
19.	Доведение до персонала информационных	При необхо-димости	-

	систем требований по защите информации, а также положений организационно-распорядительных документов по защите информации		
20.	Обучение персонала информационных систем правила эксплуатации отдельных средств защиты информации	Постоянно	Мероприятие проводится при: - вводе средств защиты информации в эксплуатацию; - изменении правил эксплуатации средств защиты информации, предусмотренных эксплуатационной и технической документацией; - изменении пользователей средств защиты информации; - по запросу пользователей, но не реже одного раза в два года
21.	Проведение практических занятий и тренировок с персоналом информационных систем по блокированию угроз безопасности информации и реагированию на инциденты	Постоянно	Мероприятие проводится не реже одного раза в два года
22.	Контроль за обеспечением уровня защищенности информации, содержащейся в информационных системах	Постоянно	Проводится ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» самостоятельно или с привлечением организации, имеющей лицензию на деятельность по технической защите информации, для: информационных систем с установленным 2 или 3 классом защищенности не реже одного раза в два года; для информационных систем с установленным 1 классом защищенности не реже одного раза в год. Процедура контроля и результаты должны быть задокументированы
23.			

ПРИЛОЖЕНИЕ № 3
к Положению по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»
от «__»_____20__г.

План внутренних проверок режима защиты информации в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»

№ п/п	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ-152 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Раз в пол года	
2.	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн	Раз в пол года	
3.	Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство	Раз в пол года	
4.	Проверка подписания сотрудниками, осуществляющими обработку ПДн. основных форм, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПДн: - Уведомления о факте обработки ПДн без использования средств автоматизации; - Обязательства о соблюдении конфиденциальности ПДн; Формы ознакомления с положениями законодательства Российской Федерации о ПДн. локальными актами ФГАОУ ВО «Северо- восточный федеральный университет имени М.К. Аммосова» по вопросам обработки ПДн,	Раз в пол года	
5.	Проверка уничтожения материальных носителей ПДн с составлением соответствующего акта	Ежегодно	
6.	Проверка ведения журналов по учету обращений субъектов ПДн и учету передачи ПДн субъектов третьим лицам	Раз в пол года	
7.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	
8.	Проверка соблюдения условий хранения материальных носителей ПДн	Раз в пол года	

9.	Проверка состояния актуальности Уведомления об обработке (намерении осуществлять обработку) ПДн	Раз в пол года	
10.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» в отношении обработки ПДн	Раз в пол года	
11.	Организация анализа и пересмотра имеющихся угроз безопасности информации, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
12.	Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ-152 «О персональных данных»	Ежегодно	
13.	Проверка применения для обеспечения безопасности информации средств защиты информации, прошедших в установленном порядке процедуру соответствия	Раз в пол года	
14.	Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИС	При необхо-димости	
15.	Контроль учета машинных носителей информации	Раз в пол года	
16.	Контроль за принимаемыми мерами по обеспечению безопасности информации, класса защищенности ИС и уровня защищенности ПДн в ИС	Раз в пол года	
17.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС	Ежеквартально	
18.	Контроль внесения изменений в структурно-функциональные характеристики ИС	Ежеквартально	
19.	Контроль корректности настроек средств защиты информации	Раз в пол года	
20.	Контроль за обеспечением резервного копирования	Ежеквартально	
21.	Поддержание в актуальном состоянии организационно-распорядительных документов но вопросам защиты информации	Раз в пол года	

ПРИЛОЖЕНИЕ № 4
к Положению по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»
от «__»_____20__г.

Отчет о результатах внутренней проверки режима защиты информации в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»

1.1 Внутренняя проверка произведена на основании Положения по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» от «__»_____20__г.

1.2 Проверка проводилась «__»_____20 __г. по адресу:
_____
_____

1.3 В ходе проверки были проведены следующие мероприятия:
1)_____
2)_____
3)_____
4)_____
5)_____

1.4 Результаты проведения проверки:
1)_____
2)_____
3)_____
4)_____
5)_____

1.5 Необходимые мероприятия.
На основании проведения внутренней проверки режима защиты информации рекомендуется осуществить следующие мероприятия:
1)_____
2)_____
3)_____
4)_____
5)_____

Подписи ответственных лиц, проводивших внутреннюю проверку режима защиты информации:

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)
_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)
_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)

Приложение 2
Приказа СВФУ
От _____№_____

Политика в отношении обработки персональных данных полученных на веб-сайте https://priem2020.s-vfu.ru/.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая политика обработки персональных данных (далее-Политика) составлена в соответствии с требованиями Федерального закона от 27.07.2006. №152-ФЗ «О персональных данных» и определяет порядок обработки персональных данных и пользователей веб-сайта https://priem2020.s-vfu.ru/ (далее - веб-сайт), и обеспечивается соблюдение требований защиты прав граждан при обработке персональных данных Федеральным государственным автономным образовательным учреждением высшего образования "Северо-Восточный федеральный университет имени М.К. Аммосова" (далее – Университет, Оператор).

Политика в отношении обработки персональных данных применяется ко всей информации, которую Оператор может получить от посетителях веб-сайта.

Настоящая Политика утверждена Ректором Университета и действует до его отмены или до его замены иным аналогичным внутренним документом.

Настоящая Политика является обязательным для исполнения всеми сотрудниками Оператора, имеющими доступ к персональным данным пользователей веб-сайта.

Пользователь может получить любые разъяснения по интересующим вопросам, касающимся обработки его персональных данных, обратившись к Оператору с помощью электронной почты priem2020@s-vfu.ru.

2. ЦЕЛИ ПОЛИТИКИ

Целью Политики является обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

3. ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В ПОЛИТИКЕ

– Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

– Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

– Веб-сайт – совокупность графических и информационных материалов, а также программ для ЭВМ и баз данных, обеспечивающих их доступность в сети интернет по сетевому адресу https://priem2020.s-vfu.ru/;

– Использование персональных данных — действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

– Обезличивание персональных данных — действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному Пользователю или иному субъекту персональных данных;

– 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;

– 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;

– Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому пользователю веб-сайта

– Субъект персональных данных - физическое лицо, являющееся пользователем веб-сайта;

– Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

– Распространение персональных данных – любые действия, направленные на раскрытие персональных данных неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

– Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу;

– Уничтожение персональных данных – любые действия, в результате которых персональные данные уничтожаются безвозвратно с невозможностью дальнейшего восстановления содержания персональных данных в информационной системе персональных данных и (или) результате которых уничтожаются материальные носители персональных данных.

4. ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оператор может обрабатывать следующие персональные данные, самостоятельно представляемые пользователем веб-сайта:

– Фамилия, имя, отчество;

– Электронный адрес;

– Номера телефонов;

– Год, месяц, дата и место рождения;

– Пол;

– Фотография;

– Гражданство;

– Реквизиты документа, удостоверяющего личность;

– Идентификационный номер налогоплательщика, дата постановки его на учет, реквизиты свидетельства постановки на учет в налоговом органе;

– Номер свидетельства обязательного пенсионного страхования, дата регистрации в системе обязательного пенсионного страхования;

– Номер полиса обязательного медицинского страхования;

– Адрес фактического места проживания и регистрации по месту жительства и (или) по месту пребывания;

– Сведения о семейном положении;

– Скан копии документа удостоверяющего личность (все страницы);

– Скан документа об образовании (профессии, специальности и квалификации);

– Информация о результатах ЕГЭ;

– Скан копии документов подтверждающих наличие льгот на поступление в Университет;

– Информация о выбранный образовательной программе (уровень образовательной программы, форма обучения, план приема).

На сайте происходит обработка файлов «cookie» с целью авторизации пользователей веб-сайта.

5. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных пользователей веб-сайта в следующих целях:

– прием документов абитуриентов во время приемной кампании;

– заключением типовых договоров на предоставление платных образовательных услуг, а также договоров с типовыми льготами;

– проведением вступительных испытаний;

– подготовкой исходных данных для проведения зачисления, подготовкой приказов на зачисление, проведением зачисления;

– распределением студентов по учебным группам;

– предоставление отчетности в государственные структуры.

6. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Срок обработки персональных данных является неограниченным.

7. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оператор обрабатывает персональные данные Пользователя только в случае их заполнения и/или отправки Пользователем самостоятельно через специальные формы, расположенные на веб-сайте. Заполняя соответствующие формы и/или отправляя свои персональные данные Оператору, Пользователь выражает свое согласие, в соответствии со статьей 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», на автоматизированную, а также без использования средств автоматизации, обработку и использование своих персональных данных.

Оператор обрабатывает файлы «cookie» в случае, если это разрешено в настройках браузера Пользователя (включено сохранение файлов «cookie» и использование технологии JavaScript).

8. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сведения, перечисленные в статье 3 настоящей Политики, являются конфиденциальными. Оператор обеспечивает конфиденциальность персональных данных и обязан не допускать их распространения без согласия пользователей, либо наличия иного законного основания.

9. ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных пользователей осуществляется Оператором с согласия субъектов персональных данных. Обязанность представить доказательство получения согласия на обработку персональных данных по основаниям данного пункта в соответствии с законом возлагается на

Оператора.

В целях обеспечения прав и свобод человека и гражданина Оператор и его работники при обработке персональных данных пользователя обязаны соблюдать следующие общие требования:

– при определении объема и содержания персональных данных пользователя подлежащих обработке, сотрудники Оператора руководствуются Федеральным законом «О персональных данных». Оператор получает персональные данные Пользователя только в объеме, необходимом для достижения законных целей сбора и обработки персональных данных.

– сотрудники Оператора не должны обрабатывать не являющиеся общедоступными персональные данные пользователя о его судимости, политических, религиозных и иных убеждениях и частной жизни.

Оператор обеспечивает защиту персональных данных пользователя от неправомерного их использования или утраты за собственный счет в порядке, установленном федеральным законодательством.

Оператор не передает персональные данные пользователей на обработку другому лицу.

10. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

В случае соответствующего обращения субъекта персональных данных,

Оператор обязан произвести необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

В случае выявления неточностей в персональных данных, Пользователь может актуализировать их самостоятельно или путем направления Оператору уведомление на адрес электронной почты Оператора priem2020@s-vfu.ru с пометкой «Актуализация персональных данных».

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю Оператора при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его

персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных Оператором, а также цель такой обработки;

– способы обработки персональных данных, применяемые Оператором;

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Субъект персональных данных имеет право отозвать согласие на обработку персональных данных, ограничить способы и формы обработки персональных данных, запретить распространение персональных данных без его согласия.

Пользователь может в любой момент отозвать свое согласие на обработку персональных данных, направив Оператору уведомление посредством электронной почты на электронный адрес Оператора priem2020@s-vfu.ru с пометкой «Отзыв согласия на обработку персональных данных».

Субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда в судебном порядке.

11. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных осуществляется Оператором

исключительно для достижения целей, определенных настоящей Политикой.

Обработка персональных данных Оператором заключается в получении, систематизации, накоплении, хранении, уточнении (обновлении, изменении), использовании, распространении, обезличивании, блокировании, уничтожении и в защите от несанкционированного доступа.

Обработка персональных данных ведется методом смешанной (в том числе автоматизированной) обработки.

К обработке персональных данных Пользователя могут иметь доступ только работники Оператора, чьи должностные обязанности непосредственно связаны с доступом и работой с персональными данными пользователя.

12. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

Передача персональных данных третьим лицам осуществляется Оператором исключительно с согласия пользователя.

Передача персональных данных третьим лицам осуществляется Оператором только на основании соответствующего договора, существенным условием которого является обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Передача персональных данных государственным органам осуществляется в рамках их полномочий в соответствии с применимым законодательством.

13. ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

Оператор не осуществляет трансграничную передачу персональных данных.

14. ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оператор осуществляет хранение персональных данные в электронном виде на территории России.

15. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ КЛИЕНТОВ

Право доступа к персональным данным Клиентов имеют: Ректор

Университета, сотрудники Оператора.

Доступ субъекта персональных данных к своим персональным данным предоставляется при личном обращении либо при получении письменного запроса. Оператор обязан сообщить субъекту персональных данных информацию о наличии персональных данных о нем, а также предоставить возможность ознакомления с ними в течение десяти рабочих дней с момента обращения.

16. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ

Оператор обязан при обработке персональных данных Пользователей принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Защита персональных данных пользователей, хранящихся в электронных базах данных Оператора, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается работниками Оператора.

Сотрудники Оператора имеют доступ к персональным данным пользователя в связи с исполнением трудовых обязанностей.

Допуск к персональным данным пользователей других сотрудников Оператора, не имеющих надлежащим образом оформленного доступа, запрещается.

Защита доступа к электронным базам данных, содержащим персональные данные пользователей, обеспечивается:

– использованием программно-технических средств защиты периметра внутренней сети, не допускающих несанкционированный вход в локальную сеть Оператора;

– разграничением прав доступа с использованием учетной записи;

Ответы на письменные запросы уполномоченных государственных органов, других организаций и учреждений о персональных данных

пользователей даются только с письменного согласия субъектов персональных данных, если иное не установлено законодательством. Ответы оформляются в письменном виде, на бланке Оператора, и в том объеме, который позволяет не разглашать излишний объем персональных данных.

17. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Работники Оператора, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Приложение 3
Приказа СВФУ
От _____№_____

ПОЛИТИКА
в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1.Настоящая Политика в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (далее - Политика) разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2.Политика определяет основные цели и назначение, а также особенности обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (далее - СВФУ), а именно:

– информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах СВФУ;

– персональных данных, содержащихся в информационных системах персональных данных СВФУ.

1.3.Политика вступает в силу с момента ее утверждения ректором федерального государственного автономного образовательного учреждения высшего образования «Северо-Восточный федеральный университет имени

ЭП: Николаев Анатолий Николаевич
Серт.: 01EB5C2C00E2AA27AE42D0EE35F0C5F511
действ. 10.10.2019-10.10.2020
утверждающая ЭП, ЭП достоверна
Рег №613 от 11.09.2020

М.К. Аммосова» ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова».

1.4.Политика подлежит пересмотру в ходе периодического анализа со стороны руководства СВФУ, а также в случаях изменения законодательства Российской Федерации в области обеспечения безопасности защищаемой информации.

1.5.Политика подлежит опубликованию на официальном сайте СВФУ.

2. ЦЕЛИ

2.1.Цели Политики:

– обеспечение безопасности информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах СВФУ;

– обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных СВФУ.

2.2. Назначение Политики:

– разработка и/ или совершенствование комплекса согласованных организационных и технических мер, направленных на обеспечение безопасности защищаемой информации.

3. ОСНОВНЫЕ ПОНЯТИЯ

3.1. Для целей Политики используются следующие понятия:

1 **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2 **субъект персональных данных** - физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;

3 **оператор** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в се базах данных. В случае обработки персональных данных под оператором понимается 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;

4 **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), блокирование, удаление, уничтожение персональных данных;

5 **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники:

6 **распространение информации -** действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

7 **предоставление персональных данных-** действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

8 **блокирование персональных данных**- временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

9 **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;

10**информация** - сведения (сообщения, данные) независимо от формы их представления;

11**информационная система** - совокупность содержащейся в базах данных защищаемой информации и обеспечивающих их обработку информационных технологий и технических средств;

12**информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

13**конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

14**трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

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

4. ОБЛАСТЬ ДЕЙСТВИЯ

4.1.Положения Политики распространяются на:

4.1.1. Все отношения, связанные с обработкой информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах СВФУ.

4.1.2. Все отношения, связанные с обработкой персональных данных, осуществляемой СВФУ:

– с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств

соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным;

– без использования средств автоматизации.

4.2.Политика применяется ко всем сотрудникам СВФУ.

5. ЦЕЛИ ОБРАБОТКИ ИНФОРМАЦИИ

5.1.Обработка информации. не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах, осуществляется в следующих целях:

– организация передачи данных в Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении;

– обеспечение единой государственной политики в области государственной аттестации научных и научно-педагогических работников.

5.2.Обработка персональных данных осуществляется СВФУ в следующих целях:

– организация передачи данных в Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении;

– обеспечение единой государственной политики в области государственной аттестации научных и научно-педагогических работников.

6. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ИНФОРМАЦИИ

6.1.Основанием обработки информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова», являются следующие нормативные акты и документы:

– Постановление Правительства от 18.11.2013 № 1035 «О федеральной

информационной системе государственной научной аттестации»;

– Распоряжение Минобрнауки России от 30.12.2013 № Р-93/нк «О подключении к федеральной информационной системе государственной научной аттестации»;

– Информационное письмо Минобрнауки России от 30.12.2013 №13-2999 от 13.09.2013 «О подключении к единой информационной системе»;

– Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;

– Постановление Правительства РФ от 31.08.13 №755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»;

– Приказ Министерства образования и науки РФ от 26.12.2013 № 1400 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования».

6.2.Основанием обработки персональных данных в ФГАОУ ВО «Северо-восточный федеральный университет имени М.К. Аммосова» являются следующие нормативные акты и документы:

– Конституция Российской Федерации;

– Постановление Правительства от 18.11.2013 № 1035 «О федеральной информационной системе государственной научной аттестации»;

– Распоряжение Минобрнауки России от 30.12.2013 № Р-93/нк «О подключении к федеральной информационной системе государственной научной аттестации»;

– Информационное письмо Минобрнауки России от 30.12.2013 №13-2999 от 13.09.2013 «О подключении к единой информационной системе»;

– Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;

– Постановление Правительства РФ от 31.08.13 №755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»;

– Приказ Министерства образования и науки РФ от 26.12.2013 № 1400 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования».

– Договоры, заключаемые между оператором и субъектом персональных данных;

– Согласия субъектов персональных данных на обработку персональных данных.

6.3.В случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям СВФУ. обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

6.4.Обработка персональных данных прекращается при реорганизации или ликвидации ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова».

7. СОСТАВ ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ

7.1. Состав информации, не содержащей сведения, составляющие

государственную тайну, содержащейся в государственных информационных системах

7.1.1. В соответствии с целями обработки информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах, указанными в пункте 5.1 настоящей Политики, СВФУ осуществляется обработка следующей информации:

– информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну;

– персональные данные.

7.2.Состав обрабатываемых персональных данных

7.2.1. В соответствии с целями обработки персональных данных, указанными в пункте 5.2 настоящей Политики, СВФУ осуществляется обработка следующих категорий субъектов персональных данных:

– выпускники;

– абитуриенты;

– соискатели;

– научные руководители;

– оппоненты;

– соискатели ученого звания;

– члены диссертационного совета;

– представители ведущей организации.

7.2.2. Перечень и срок хранения обрабатываемых персональных данных утвержден локальным актом СВФУ.

8. ПРИНЦИПЫ ОБРАБОТКИ ИНФОРМАЦИИ

8.1.Обработка информации. не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах, осуществляется СВФУ в соответствии со следующими принципами:

– свобода поиска, получения, передачи, производства и распространения

информации любым законным способом;

– установление ограничений доступа к информации только федеральными законами; открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

– равноправие языков народов Российской Федерации при создании государственных информационных систем и их эксплуатации;

– обеспечение безопасности Российской Федерации при создании государственных информационных систем, их эксплуатации и защите содержащейся в них информации;

– достоверность информации и своевременность предоставления;

– недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

8.2.Обработка персональных данных осуществляется СВФУ в соответствии со следующими принципами:

– обработка персональных данных осуществляется на законной и справедливой основе;

– обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей; не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

– не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только персональные данные, которые отвечают целям их обработки;

– содержание и объем обрабатываемых персональных данных

соответствуют заявленным целям обработки; обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;

– при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных; СВФУ принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;

– хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных; обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

9. ОБРАБОТКА ИНФОРМАЦИИ, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

9.1.Обладатель информации

9.1.1. Обладателем информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах СВФУ является СВФУ.

9.1.2. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

– разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

– использовать информацию, в том числе распространять ее, по своему

усмотрению;

– передавать информацию другим лицам по договору или на ином установленном законом основании;

– защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

– осуществлять иные действия с информацией или разрешать осуществление таких действий.

9.1.3. Обладатель информации при осуществлении своих прав обязан:

– соблюдать права и законные интересы иных лиц;

– принимать меры по защите информации;

– ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

9.2.Общедоступная информация

9.2.1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

9.2.2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

9.2.3. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

9.3.Право на доступ к информации

9.3.1. Граждане (физические лица) и организации (юридические лица) (далее- организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных федеральными законами.

9.3.2. Гражданин (физическое лицо) имеет право на получение от СВФУ, его должностных лиц в порядке, установленном законодательством Российской

Федерации, информации, непосредственно затрагивающей его права и свободы.

9.3.3. Организация имеет право на получение от СВФУ информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с СВФУ при осуществлении этой организацией своей уставной деятельности.

9.3.4. Не может быть ограничен доступ к:

– нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия СВФУ;

– информации о деятельности СВФУ, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

– иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

9.3.5. СВФУ необходимо обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

9.3.6. Решения и действия (бездействие) СВФУ, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

9.3.7. В случае если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с

гражданским законодательством Российской Федерации.

9.3.8. Предоставляется бесплатно информация:

– о деятельности СВФУ, размещенная СВФУ в информационно-телекоммуникационных сетях;

– затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

– иная установленная законом информация.

9.3.9. Установление платы за предоставление СВФУ информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

9.4.Ограничение доступа к информации

9.4.1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

9.4.2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

9.4.3. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

9.5.Государственные информационные системы

9.5.1. Государственные информационные системы создаются в целях реализации полномочий СВФУ и обеспечения обмена информацией между государственными органами, а также в иных установленных федеральными законами целях.

9.5.2. Оператором государственной информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими

базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации государственной информационной системы.

9.5.3. Особенности эксплуатации государственных информационных систем могут устанавливаться в соответствии с техническими регламентами, локальными актами СВФУ.

9.5.4. Государственные информационные системы создаются и эксплуатируются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд.

9.5.5. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

9.5.6. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления - Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами. В случае если при создании или эксплуатации государственных информационных систем предполагается осуществление или осуществляется обработка общедоступной информации, предусмотренной перечнями, утверждаемыми в соответствии со статьей 14 Федерального закона от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», государственные информационные системы должны обеспечивать размещение такой информации в сети «Интернет» в форме открытых данных.

9.5.7. Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной

системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

9.5.8. Правительство Российской Федерации вправе устанавливать требования к порядку создания и ввода в эксплуатацию отдельных государственных информационных систем.

9.5.9. Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами и интеллектуальной собственности.

9.5.10. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно- технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

9.5.11. Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении СВФУ сведения и документы являются государственными информационными ресурсами. Информация, содержащаяся в государственных информационных системах, является официальной. Необходимо обеспечивать достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

9.6.Защита информации

9.6.1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой

информации;

– соблюдение конфиденциальности защищаемой информации;

– реализацию права на доступ к информации.

9.6.2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

9.6.3. СВФУ в случаях, установленных законодательством Российской Федерации, необходимо обеспечить:

– предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

– своевременное обнаружение фактов несанкционированного доступа к информации;

– предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации:

– недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

– возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

– постоянный контроль за обеспечением уровня защищенности информации.

9.6.4. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных

систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

9.6.5. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

10.ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Условия обработки персональных данных

16Условия обработки персональных данных, отличные от получения согласия субъекта персональных данных на обработку его персональных данных являются альтернативными.

10.1.1.Условия обработки специальных категорий персональных данных

17Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, СВФУ не производится.

10.1.2.Условия обработки биометрических персональных данных

18Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются СВФУ для установления личности субъекта персональных данных СВФУ не обрабатываются.

10.1.3.Условия обработки иных категорий персональных данных

19Обработка иных категорий персональных данных осуществляется СВФУ с соблюдением следующих условий:

– обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации па СВФУ функций, полномочий и обязанностей.

10.1.4.Условия обработки общедоступных персональных данных

20Осуществляется обработка персональных данных, сделанных общедоступными субъектом персональных данных.

10.1.5.Поручение обработки персональных данных

10.1.5.1 СВФУ не поручает обработку персональных данных другому лицу.

10.1.6.Передача персональных данных

10.1.6.1 ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

10.2 Конфиденциальность персональных данных

10.2.1.Сотрудники СВФУ, получившие доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

10.3 .Общедоступные источники персональных данных

10.3.1.СВФУ не создает общедоступные источники персональных данных.

10.4 .Согласие субъекта персональных данных на обработку его персональных данных

10.4.1.При необходимости обеспечения условий обработки персональных данных субъекта может предоставляться согласие субъекта персональных данных на обработку его персональных данных.

10.4.2.Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его

получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются СВФУ.

10.4.3.Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных СВФУ вправе продолжить обработку персональных данных без согласия субъекта персональных данных при выполнении альтернативных условий обработки персональных данных.

10.4.4.Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство выполнения альтернативных условий обработки персональных данных возлагается на СВФУ.

10.4.5.В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

– фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого

представителя (при получении согласия от представителя субъекта персональных данных);

– наименование или фамилию, имя. отчество и адрес СВФУ, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– наименование или фамилию, имя. отчество и адрес лица, осуществляющего обработку персональных данных по поручению СВФУ, если обработка будет поручена такому лицу;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых СВФУ способов обработки персональных данных;

– срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

– подпись субъекта персональных данных.

10.4.6.Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

10.4.7.В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

10.4.8.В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

10.4.9.В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

10.4.10 Персональные данные могут быть получены СВФУ от лица, не являющегося субъектом персональных данных, при условии предоставления СВФУ подтверждения наличия альтернативных условий обработки информации.

10.5 .Трансграничная передача персональных данных

10.5.1.Трансграничная передача персональных данных СВФУ не осуществляется.

10.6 .Права субъектов персональных данных

10.6.1.Право субъекта персональных данных на доступ к его персональным данным

10.6.1.1 Субъект персональных данных имеет право на получение информации (далее - запрашиваемая субъектом информация), касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных СВФУ;

– правовые основания и цели обработки персональных данных;

– цели и применяемые СВФУ способы обработки персональных данных;

– наименование и место нахождения СВФУ, сведения о лицах (за исключением работников СВФУ), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с СВФУ или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя. отчество и адрес лица, осуществляющего обработку персональных данных по поручению СВФУ. если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

10.6.1.2 Субъект персональных данных имеет право на получение запрашиваемой субъектом информации, за исключением следующих случаев:

– обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

– обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

– обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

– доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

– обработка персональных данных осуществляется в случаях,

предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

10.6.1.3 Субъект персональных данных вправе требовать от СВФУ уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

10.6.1.4 Запрашиваемая субъектом информация должна быть предоставлена субъекту персональных данных СВФУ в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

10.6.1.5 Запрашиваемая информация предоставляется субъекту персональных данных или его представителю СВФУ при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с СВФУ (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных СВФУ, подпись субъекта персональных данных или его представителя (далее необходимая для запроса информация). Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской

Федерации.

10.6.1.6 В случае если запрашиваемая субъектом информация, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в СВФУ или направить повторный запрос в целях получения запрашиваемой субъектом информации, и ознакомления с такими персональными данными не ранее чем через тридцать дней (далее - нормированный срок запроса) после первоначальною обращения или направления первоначальною запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

10.6.1.7 Субъект персональных данных вправе обратиться повторно в СВФУ или направить повторный запрос в целях получения запрашиваемой субъектом информации, а также в целях ознакомления с обрабатываемыми персональными данными до истечения нормированного срока запроса, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимой для запроса информацией должен содержать обоснование направления повторного запроса.

10.6.1.8 СВФУ вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на СВФУ.

10.6.2.Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров**,** работ, услуг на рынке, а также в целях политической агитации

10.6.2.1 Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации СВФУ не осуществляется.

10.6.3.Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

10.6.3.1 Принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы СВФУ не осуществляется.

10.6.4.Право на обжалование действий или бездействия СВФУ

10.6.4.1 Если субъект персональных данных считает, что СВФУ осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие СВФУ в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

10.6.4.2 Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

10.7 .Обязанности СВФУ

10.7.1Обязанности СВФУ при сборе персональных данных

10.7.1.1 При сборе персональных данных СВФУ предоставляет субъекту персональных данных по его просьбе запрашиваемую информацию, касающуюся обработки его персональных данных в соответствии с частью 7 статьи 14 Федерального закона «О персональных данных».

10.7.1.2 Если предоставление персональных данных является обязательным в соответствии с федеральным законом, СВФУ разъясняет

субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

10.7.1.3 Если персональные данные получены не от субъекта персональных данных, СВФУ до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию (далее-информация, сообщаемая при получении персональных данных не от субъекта персональных данных):

– наименование либо фамилия, имя, отчество и адрес СВФУ или представителя СВФУ;

– цель обработки персональных данных и се правовое основание;

– предполагаемые пользователи персональных данных;

– установленные Федеральным законом «О персональных данных» права субъекта персональных данных;

– источник получения персональных данных.

10.7.1.4 СВФУ не предоставляет субъекту информацию, сообщаемую при получении персональных данных не от субъекта персональных данных, в случаях, если:

– субъект персональных данных уведомлен об осуществлении обработки его персональных данных СВФУ;

– персональные данные получены СВФУ на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

– персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

– СВФУ осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные

интересы субъекта персональных данных;

– предоставление субъекту персональных данных информации, сообщаемой при получении персональных данных не от субъекта персональных данных, нарушает права и законные интересы третьих лиц.

10.7.1.5 При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», СВФУ обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации, обрабатываемых в следующих информационных системах:

– Государственная информационная система «АП ФИС ЕГЭ и ФРДО» с использованием баз данных, находящихся на территории следующий стран:

- Россия.

– Государственная информационная система «АП ЕИС ГА» с использованием баз данных, находящихся на территории следующий стран:

- Россия.

10.7.1.6 Местонахождение центра(ов) обработки данных и сведения об организации, ответственной за хранение данных, определены внутренними документами СВФУ.

10.7.2.Меры, направленные на обеспечение выполнения СВФУ своих обязанностей

10.7.2.1 СВФУ принимает меры, необходимые и достаточные для обеспечения выполнения своих обязанностей. СВФУ самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, если иное не предусмотрено федеральными законами. К таким мерам, в частности, относятся:

– назначение ответственного за организацию обработки персональных данных;

– издание Политики, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры,

направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

– осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям к защите персональных данных. Политике, локальным актам СВФУ;

– оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых СВФУ мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

– ознакомление сотрудников СВФУ, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, Политикой, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

10.7.3.Меры по обеспечению безопасности персональных данных при их обработке

10.7.3.1 СВФУ при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает 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.

10.7.3.2 Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз безопасности персональных данных при их

обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

10.7.3.3 Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения,

изменения, блокирования, копирования, предоставления, распространения.

10.7.4.Обязанности СВФУ при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя**,** а также уполномоченного органа по защите прав субъектов персональных данных

10.7.4.1 СВФУ сообщает в установленном порядке субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

10.7.4.2 В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя СВФУ дает в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

10.7.4.3 СВФУ предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, СВФУ вносит в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные

являются незаконно полученными или не являются необходимыми для заявленной цели обработки, СВФУ уничтожает такие персональные данные. СВФУ уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

10.7.4.4 СВФУ сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

10.7.5.Обязанности СВФУ по устранению нарушении законодательства, допущенных при обработке персональных данных, но уточнению, блокированию и уничтожению персональных данных

10.7.5.1 В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных СВФУ осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим но поручению СВФУ) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных СВФУ осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению СВФУ) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных нс

нарушает права и законные интересы субъекта персональных данных или третьих лиц.

10.7.5.2 В случае подтверждения факта неточности персональных данных СВФУ на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом но защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим но поручению СВФУ) в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

10.7.5.3 В случае выявления неправомерной обработки персональных данных, осуществляемой СВФУ или лицом, действующим по поручению СВФУ. СВФУ в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению СВФУ. В случае если обеспечить правомерность обработки персональных данных невозможно, СВФУ в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных СВФУ уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

10.7.5.4 В случае достижения цели обработки персональных данных СВФУ прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим но поручению СВФУ) и уничтожает персональные данные

или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению СВФУ) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между СВФУ и субъектом персональных данных либо если СВФУ не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

10.7.5.5 В случае отзыва субъектом персональных данных согласия на обработку его персональных данных СВФУ прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению СВФУ) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению СВФУ) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между СВФУ и субъектом персональных данных либо если СВФУ не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

10.7.5.6 В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, СВФУ блокирует такие персональные данные или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению СВФУ) и

обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

10.7.6.Уведомление од обработке персональных данных

10.7.6.1 СВФУ, за исключением случаев, предусмотренных Федеральным законом «О персональных данных», до начала обработки персональных данных уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

10.7.6.2 Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление содержит следующие сведения:

– наименование (фамилия, имя. отчество), адрес СВФУ;

– цель обработки персональных данных;

– категории персональных данных;

– категории субъектов, персональные данные которых обрабатываются:

– правовое основание обработки персональных данных;

– перечень действий с персональными данными, общее описание используемых СВФУ способов обработки персональных данных;

– описание мер, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

– фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

– дата начала обработки персональных данных;

– срок или условие прекращения обработки персональных данных;

– сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

– сведения о месте нахождения базы данных информации, содержащей

персональные данные граждан Российской Федерации;

– сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

10.7.6.3 В случае изменения указанных сведений, а также в случае прекращения обработки персональных данных СВФУ уведомляет об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

10.8 .Обработка персональных данных, осуществляемая без использования средств автоматизации

10.8.1Общие положения

10.8.1.1 Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

10.8.2.Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

10.8.2.1 Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее материальные носители), в специальных разделах или на полях форм (бланков).

10.8.2.2 При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для

обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных используется отдельный материальный носитель.

10.8.2.3 Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники СВФУ или лица, осуществляющие такую обработку по договору с СВФУ), проинформированы о факте обработки ими персональных данных, обработка которых осуществляется СВФУ без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами СВФУ.

10.8.2.4 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), соблюдаются следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес СВФУ, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых СВФУ способов обработки персональных данных;

– типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных

данных;

– типовая форма составляется таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

– типовая форма исключает объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

10.8.2.5 При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, принимаются меры по обеспечению раздельной обработки персональных данных, в частности:

– при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

– при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

10.8.2.6 Уничтожение части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с

сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Указанные правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

10.8.2.7 Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

10.8.3.Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

10.8.3.1 Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

10.8.3.2 Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

10.8.3.3 При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются СВФУ.

11СФЕРЫ ОТВЕТСТВЕННОСТИ

11.1 .Лица, ответственные за организацию обработки персональных данных в организации и за защиту информации, не содержащей сведении, составляющие государственную тайну

11.1.1СВФУ назначает лицо, ответственное за организацию обработки персональных данных при их обработке в информационных системах СВФУ.

11.1.2СВФУ назначает лицо, ответственное за защиту информации, не содержащей сведения, составляющие государственную тайну, в ИС СВФУ.

11.1.3Лицо, ответственное за организацию обработки персональных данных при их обработке в информационных системах СВФУ получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

11.1.4СВФУ предоставляет лицу, ответственному за организацию обработки персональных данных при их обработке в информационных системах СВФУ, необходимые сведения.

11.2 .Ответственность

11.2.1Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

11.2.2Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом «О персональных данных», а также требований к защите персональных данных, установленных в соответствии с Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

11.2.3.Нарушение требований Федерального закона «Об информации, информационных технологиях и о защите информации» влечет за собой

дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

11.2.4.Лица, права и законные интересы которых были нарушены в связи с разглашением защищаемой информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

11.2.5.В случае если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

– либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

– либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

12КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

21При достижении целей ожидаются следующие результаты:

– обеспечение безопасности информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах СВФУ;

– обеспечение защиты прав и свобод субъектов персональных данных при обработке его персональных данных СВФУ;

– повышение общего уровня информационной безопасности СВФУ;

– минимизация юридических рисков СВФУ.

13. СВЯЗНЫЕ ПОЛИТИКИ

22Связные политики отсутствуют.

Лист ознакомления с Политикой в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»

№ п/п	Ф.И.О.	Должность	Дата	Подпись

ЭП: Николаев Анатолий Николаевич
Серт.: 01EB5C2C00E2AA27AE42D0EE35F0C5F511
действ. 10.10.2019-10.10.2020
утверждающая ЭП, ЭП достоверна
Рег №613 от 11.09.2020

Приложение 4
Пркиаза
От _____№_____

ПОРЯДОК
хранения, использования и передачи персональных данных сотрудников ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок хранения, использования и передачи персональных данных сотрудников ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (далее - Порядок) разработан в соответствии с Трудовым кодексом Российской Федерации. Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1.2. Цель разработки настоящего Порядка - определение порядка обработки (хранения, использования, передачи) персональных данных сотрудников ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова» (далее - СВФУ); обеспечение защиты прав и свобод сотрудников СВФУ при обработке их персональных данных.

2. ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ

2.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить сотрудника СВФУ, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является сотрудник. Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Хранение персональных данных сотрудников СВФУ может осуществляться на бумажных и машинных носителях, доступ к которым ограничен списком лиц, допущенных к обработке персональных данных.

2.2. Все машинные носители персональных данных подлежат строгому учету. Форма журнала учета машинных носителей защищаемой информации, не содержащей сведения, составляющие государственную тайну, утверждена локальным актом СВФУ.

2.3. Персональные данные сотрудников, содержащиеся на машинных носителях информации, могут храниться на автоматизированных рабочих местах и серверах информационных систем СВФУ, установленных в пределах помещений, утвержденных локальным актом СВФУ.

2.4. Персональные данные сотрудников, содержащиеся на материальных носителях персональных данных, должны храниться в пределах помещений,

утвержденных Приказом об обеспечении безопасности материальных носителей персональных данных.

2.5. Хранение персональных данных сотрудников должно происходить в порядке, исключающем их утрату или их неправомерное использование.

2.6. Использование персональных данных сотрудников СВФУ осуществляется СВФУ исключительно в целях выполнения требований трудового законодательства Российской Федерации.

2.7. Обработка персональных данных сотрудников СВФУ осуществляется только специально уполномоченными лицами, перечень которых утверждается приказом СВФУ, при этом указанные в приказе сотрудники должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения непосредственных должностных обязанностей.

2.8. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники СВФУ или лица, осуществляющие такую обработку по договору с СВФУ), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется СВФУ без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

2.9. Передача персональных данных сотрудников между структурными подразделениями СВФУ осуществляется только между сотрудниками, включенными в перечень лиц, имеющих доступ к персональным данным.

2.10. Обработка персональных данных сотрудников должна осуществляться только в пределах помещений СВФУ и с использованием средств вычислительной техники СВФУ.

2.11. СВФУ вправе поручить обработку персональных данных сотрудников другим юридическим или физическим лицам на основании договора (далее - поручение СВФУ) с согласия сотрудника, если иное не предусмотрено Федеральным законом «О персональных данных». Лицо, осуществляющее обработку персональных данных по поручению СВФУ, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных».

2.12. Сотрудники СВФУ и иные лица, получающие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия сотрудников, если иное не предусмотрено федеральным законодательством в сфере защиты персональных данных.

3. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. При передаче персональных данных сотрудника СВФУ должны быть соблюдены следующие требования:

– не сообщать персональные данные сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а

также в случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

– предупреждать лица, получающие персональные данные сотрудников, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц обеспечения конфиденциальности полученных персональных данных;

– не сообщать персональные данные сотрудника в коммерческих целях без его письменного согласия;

– передавать персональные данные сотрудника представителям сотрудников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными сотрудника, которые необходимы для выполнения указанными представителями их функций;

– не отвечать на вопросы, связанные с передачей персональных данных сотрудника по телефону или факсу, за исключением случаев, связанных с выполнением соответствующими сотрудниками своих непосредственных должностных обязанностей, адресатам в чью компетенцию входит получение такой информации.

3.2. В целях обеспечения контроля правомерности использования переданных по запросам персональных данных лицами, их получившими, сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также состав переданной информации фиксируются в Журнале учета передачи персональных данных. Форма соответствующего журнала утверждена локальным актом СВФУ.

– **Лист ознакомления**

– **с Порядком хранении, использовании и передачи персональных данных сотрудников ФГАОУ ВО «Северо-Восточный федеральный университет имени М.К. Аммосова»**

№ п/п	Ф.И.О.	Должность	Дата	Подпись

Приложение 5
Приказа
От _____№_____

ПОЛОЖЕНИЕ
о дополнительных требованиях по защите детей от информации, распространяемой посредством информационно-телекоммуникационных сетей, причиняющей вред здоровью и (или) развитию детей

1. Общие положения

1.1. Настоящее Положение о дополнительных требованиях по защите детей от информации, распространяемой посредством информационно-телекоммуникационных сетей, причиняющей вред здоровью и (или) развитию детей (далее - Положение), определяет дополнительные требования к обороту информационной продукции, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, и меры защиты обучающихся от информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в федеральном государственное автономное образовательное учреждение высшего образования «Северо-Восточный федеральный университет имени М.К. Аммосова» (далее - СВФУ).

1.2. Настоящее Положение является локальным нормативным актом СВФУ, обязательным для исполнения всеми сотрудниками и обучающимися СВФУ.

1.3. При разработке настоящего Положения использованы следующие нормативные документы:

1.3.1 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

1.3.2 Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

1.3.3 Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

1.3.4 приказ Министерства связи и массовых коммуникаций Российской Федерации от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программноаппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию»;

1.3.5 письмо Министерства образования и науки Российской Федерации от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет»;

1.3.6 Устав и иные локальные нормативные акты СВФУ.

2. Термины, определения и сокращения

В настоящем Положении используются следующие термины и определения:

доступ обучающихся к информации - возможность получения и использования обучающимися свободно распространяемой информации;

информационная безопасность обучающихся - состояние защищенности обучающихся, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;

информационная продукция - предназначенная для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для электронных вычислительных машин (программы для ЭВМ) и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том

числе сети Интернет, и сетей подвижной радиотелефонной связи;
информационная продукция для обучающихся - информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию обучающихся;
информация, причиняющая вред здоровью и (или) развитию обучающихся - информация (в том числе содержащаяся в информационной продукции для обучающихся), распространение которой среди обучающихся запрещено или ограничено в соответствии с законодательством Российской Федерации;
оборот информационной продукции - предоставление и (или) распространение информационной продукции, включая ее продажу (в том числе распространение по подписке), аренду, прокат, раздачу, выдачу из фондов общедоступных библиотек, публичный показ, публичное исполнение (в том числе посредством зрелищных мероприятий), распространение посредством эфирного или кабельного вещания, информационно-телекоммуникационных сетей, в том числе сети Интернет, и сетей подвижной радиотелефонной связи.

3. Виды информации, распространяемой посредством информационно-телекоммуникационных сетей, причиняющей вред здоровью и (или) развитию детей и не соответствующей задачам образования

3.1. К информации, причиняющей вред здоровью и (или) развитию обучающихся, относится информация:
3.1.1 запрещенная для распространения среди обучающихся;
3.1.2 распространение которой среди обучающихся определенных возрастных категорий ограничено.
3.2. К информации, запрещенной для распространения среди обучающихся, относится информация:
3.2.1 побуждающая обучающихся к совершению действий, представляющих угрозу жизни и (или) здоровью обучающихся, в том числе к причинению вреда своему здоровью, самоубийству;
3.2.2 способная вызвать у обучающихся желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
3.2.3 обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
3.2.4 отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;
3.2.5 оправдывающая противоправное поведение;
3.2.6 содержащая нецензурную брань;
3.2.7 содержащая информацию порнографического характера;
3.2.8 о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.
3.3. К информации, распространение которой среди обучающихся определенных возрастных категорий ограничено, относится информация:
3.3.1 представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

3.3.2 вызывающая у обучающихся страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3.3.3 представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

3.3.4 содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

3.4. К информации, не соответствующей задачам образования, относится следующая информация:

3.4.1 компьютерные игры, за исключением соответствующих задачам образования;

3.4.2 ресурсы, базирующиеся либо ориентированные на обеспечение анонимности распространителей и потребителей информации;

3.4.3 банки рефератов, эссе, дипломных работ, за исключением соответствующих задачам образования;

3.4.4 онлайн-казино и тотализаторы;

3.4.5 мошеннические сайты;

3.4.6 магия, колдовство, чародейство, ясновидящие, приворот по фото, теургия, волшебство, некромантия, тоталитарные секты.

4. Дополнительные требования к обороту информационной продукции, распространяемой посредством информационно-телекоммуникационных сетей, запрещенной для обучающихся, в местах, доступных для обучающихся

4.1. Доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, в местах, доступных для обучающихся, предоставляется сотрудниками СВФУ, в должностные обязанности которых входит обеспечение технического сопровождения доступа к ресурсам сети Интернет в СВФУ, при условии применения административных и организационных мер средств защиты обучающихся от информации, причиняющей вред здоровью и (или) развитию обучающихся (пп. 3.1 - 3.3 настоящего Положения).

4.2. При использовании сети Интернет в СВФУ в научнообразовательных целях обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к научно-образовательному процессу.

4.3. Сотрудникам СВФУ, непосредственно взаимодействующим с несовершеннолетними в рамках своей трудовой деятельности, следует учитывать, что в силу особенностей информационных технологий, применяемых в сети Интернет, технические средства контентной фильтрации не могут гарантировать обеспечение полного и всестороннего ограничения доступа к информации, указанной в пп. 3.1 - 3.3 настоящего Положения.

5. Меры, направленные на предотвращение, выявление и устранение нарушений законодательства Российской Федерации о защите детей от информации, распространяемой посредством информационно-телекоммуникационных сетей, причиняющей вред здоровью и (или) развитию детей

5.1. Внутренний контроль за соблюдением законодательства Российской Федерации о защите детей от информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, причиняющей вред здоровью и (или) развитию детей, соответствием применяемых административных и организационных мер защиты обучающихся от информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, причиняющей вред здоровью и (или) развитию обучающихся, требованиям настоящего Положения, иных локальных нормативных актов СВФУ, действующих в указанной сфере, за оборотом информационной продукции, запрещенной для обучающихся, использованием ресурсов сети Интернет во время образовательного процесса, соблюдением требований Положения и законодательства

Российской Федерации осуществляют структурные подразделения СВФУ, использующие (применяющие, распространяющие и изготавливающие) информационную продукцию.

5.2. Преподаватель, ведущий занятие, обязан осуществлять контроль использования технических средств, применяемых при организации доступа к ресурсам сети Интернет, контроль доступа обучающихся к ресурсам сети Интернет, а также принимать меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

5.3. Обучающиеся и сотрудники, в случае выявления наличия доступа к ресурсам сети Интернет, содержащим информацию, перечисленную в пп 3.1-3.3 настоящего Положения, незамедлительно информируют преподавателя, ведущего занятие, непосредственного руководителя и подразделение, ответственное за обеспечение эксплуатация сети передачи данных.

5.4. При прогнозировании или выявлении ситуаций, которые могут привести к получению обучающимися информационной продукции, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, не совместимой с задачами образования, иной, распространение которой запрещено законодательством Российской Федерации, структурные подразделения, использующие (применяющие, распространяющие и изготавливающие) информационную продукцию, применяют меры по устранению таких ситуаций.

5.5. Нарушение законодательства Российской Федерации в сфере защиты детей от информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также требований настоящего Положения, влечет за собой ответственность в соответствии с законодательством Российской Федерации.

6. Ответственность

6.1. Ответственность за соблюдение требований настоящего Положения возлагается на всех сотрудников СВФУ, в трудовые обязанности которых входит организация и осуществление оборота информационной продукции.

6.2. Контроль за исполнением требований Положения в СВФУ возлагается на заведующую сектором корпоративных сайтов отдела информационных систем и управления данными департамента цифровых технологий.

7. Управление Положением

7.1. Ответственность за поддержание настоящего Положения в актуальном состоянии несет держатель документа.

7.2. Контроль за размещением на официальном сайте СВФУ в сети Интернет актуальной версии Положения осуществляет держатель документа.

7.3. Подлинник настоящего Положения хранится в департаменте цифровых технологий согласно утвержденной номенклатуре дел.

7.4. Порядок периодической проверки (внесения в документ изменений, прекращения его действия) определен Регламентом управления внутренними нормативными документами в действующей редакции.

7.5. Настоящее Положение подлежит обязательной рассылке проректорам, руководителям структурных подразделений СВФУ.