Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Целищев Алексей Олегович
Должность: Проректор по учебно-научной работе
Дата подписания: 04.09.2025 13:02:31
Уникальный программный ключ:
a8cad4623edd7219a3b0897308bb14769288026a

Приложение № 2 к приказу
от « 18 »июня 2025 г. №112/к

ПОЛИТИКА
в отношении обработки персональных данных

1 Общие положения

1.1 Термины и определения

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

1.1.2 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.

1.1.3 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.

1.1.4 Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

1.1.5 Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.1.6 Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.1.7 Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.1.8 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.

1.1.9 Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

1.1.11 Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.2 Назначение и правовая основа документа

1.2.1 Политика определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется частное образовательное учреждение высшего образования «Восточная экономико-юридическая гуманитарная академия» (далее – Академия) в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

1.2.2 Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский, Уголовный и Трудовой кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

1.2.3 Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных Академии позволит оптимизировать затраты на ее построение.

1.2.4 При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

1.2.5 Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

2 Объекты защиты

2.1 Основными объектами системы безопасности персональных данных в Академии являются:

– информационные ресурсы с ограниченным доступом, содержащие конфиденциальную информацию, в том числе и персональные данные;

– процессы обработки персональных данных в информационной системе персональных данных Академии, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

– информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты

информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

3 Цели и задачи обеспечения безопасности персональных данных

3.1 Интересы затрагиваемых субъектов информационных отношений

3.1.1 Субъектами информационных отношений при обеспечении безопасности персональных данных Академии являются:

– Академия, как собственник информационных ресурсов;

– руководство и сотрудники Академии, в соответствии с возложенными на них функциями;

– физические лица, состоящие с Академией в гражданско-правовых отношениях (граждане);

3.1.2 Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

– своевременного доступа к необходимым им персональным данным (их доступности);

– достоверности (полноты, точности, адекватности, целостности) персональных данных;

– конфиденциальности персональных данных;

– защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;

– разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;

– возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;

– защиты персональных данных от незаконного распространения.

3.2 Цели защиты

3.2.1 Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Академии от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

3.2.2 Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

– доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем Академии, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);

– целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах Академии и передаваемой по каналам связи;

– конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

3.2.3 Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

3.3 Основные задачи системы обеспечения безопасности персональных данных

3.3.1 Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности Академии должна обеспечивать эффективное решение следующих задач:

– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Академии;

– создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

– защиту от вмешательства в процесс функционирования информационных систем Академии посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

– разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Академии (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

– обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

– защиту от несанкционированной модификации используемых в информационных системах Академии программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

– защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.4 Основные пути решения задач системы защиты

3.4.1 Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

– строгим учетом всех подлежащих защите ресурсов информационных систем Академии (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

– ведением журнала действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационной системы;

– полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Академии по вопросам обеспечения безопасности информации;

– подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;

– наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Академии;

– четким знанием и строгим соблюдением всеми пользователями информационных систем Академии требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

– персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Академии;

– непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Академии;

– применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

– эффективным контролем над соблюдением пользователями информационных ресурсов Академии требований по обеспечению безопасности информации;

– юридической защитой интересов Академии при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

4 Основные принципы построения системы безопасности персональных данных

4.1 Построение системы, обеспечения безопасности персональных данных Академии, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

4.2 Законность

4.2.1 Предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных Академии в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

4.2.2 Все пользователи информационной системы Академии должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

4.3 Системность

4.3.1 Системный подход к построению системы защиты информации в Академии предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени

элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

4.3.2 При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем Академии, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников). Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.4 Комплексность

4.4.1 Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

4.5 Непрерывность защиты

4.5.1 Обеспечение безопасности персональных данных - процесс, осуществляемый руководством Академии, ответственным за организацию обработки персональных данных и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри Академии и каждый сотрудник Академии должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности Академии. И ее эффективность зависит от участия руководства и сотрудников Академии в обеспечении информационной безопасности персональных данных.

4.5.2 Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

4.6 Своевременность

4.6.1 Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

4.6.2 Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

4.7 Преемственность и совершенствование

4.7.1 Предполагает постоянное совершенствование мер и средств защиты персональных данных на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем Академии и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

4.8 Разумная достаточность (экономическая целесообразность)

4.8.1 Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем Академии.

4.9 Персональная ответственность

4.9.1 Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

4.10 Минимизация полномочий

4.10.1 Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

4.11 Исключение конфликта интересов (разделение функций)

4.11.1 Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования персональными данными и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями Академии. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

4.12 Взаимодействие и сотрудничество

4.12.1 Предполагает создание благоприятной атмосферы в коллективе Академии. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственным за организацию обработки персональных данных.

4.12.2 Важным элементом эффективной системы обеспечения безопасности персональных данных в Академии является высокая культура работы с информацией. Руководство Академии несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности Академии. Все сотрудники Академии должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

4.13 Гибкость системы защиты

4.13.1 Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Академией своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры Академии;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства.

4.13.2 Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

4.14 Открытость алгоритмов и механизмов защиты

4.14.1 Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

4.15 Простота применения средств защиты

4.15.1 Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

4.16 Обоснованность и техническая реализуемость

4.16.1 Информационные технологии, технические и программные средства, средства и меры защиты персональных данных должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

4.17 Специализация и профессионализм

4.17.1 Предполагает привлечение к разработке средств и реализации мер защиты персональных данных специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственные лицензии на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Академии (ответственными за организацию обработки персональных данных).

4.18 Обязательность контроля

4.18.1 Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности персональных данных, на основе используемых систем и средств защиты персональных данных, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

4.18.2 Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

4.18.3 Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

4.18.4 Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками Академии должны немедленно доводиться до сведения руководителя Академии и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

5 Меры, методы и средства обеспечения требуемого уровня защиты информационных ресурсов

5.1 Меры обеспечения информационной безопасности

5.1.1 Все меры обеспечения безопасности информационных систем Академии подразделяются на:

- правовые (законодательные);
- морально-этические;
- технологические;
- организационные (административные);
- физические;
- технические (аппаратурные и программные).

5.2 К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих

правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем Академии.

5.3 К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в Академии. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или Академии в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

5.4 К технологическим мерам защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности

5.5 Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки персональных данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

5.6 Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности персональных данных (отражающую подходы к защите персональных данных) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

5.7 С практической точки зрения политику в области обеспечения безопасности персональных данных в Академии целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Академии в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

5.8 Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности персональных данных и детализирует (регламентирует) эти правила:

– каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных;

– кто имеет права доступа к персональным данным, кто и при каких условиях может читать и модифицировать персональные данные и т.д.

5.9 Политика нижнего уровня должна:

– предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

– определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к персональным данным;

– выбирать программно-технические (аппаратные) средства противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

5.10 Регламентация доступа в помещения

5.10.1 Компоненты информационных систем Академии должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

5.10.2 Во время обработки персональных данных в таких помещениях должен присутствовать только персонал, допущенный к работе с персональными данными. Запрещается прием посетителей в помещениях, когда осуществляется обработка персональных данных.

5.10.3 По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем Академии, должны запираться на ключ.

5.10.4 В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

5.11 Регламентация допуска сотрудников к использованию информационных ресурсов

5.11.1 В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

5.11.2 Допуск пользователей к работе с информационными системами Академии и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

5.11.3 Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

– каждый сотрудник пользуется только предписанными ему правами по отношению к персональным данным, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с ответственными за организацию обработки персональных данных;

– руководитель Академии имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

5.12 Все сотрудники Академии и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки

персональных данных, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению персональных данных Академии.

5.13 Обработка персональных данных в компонентах информационных систем Академии должна производиться в соответствии с утвержденными технологическими инструкциями.

5.14 Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

5.14.1 В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников Академии, с которых возможен доступ к ресурсам информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

5.14.2 В компонентах информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

5.14.3 Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

5.14.4 Оборудование информационной системы, используемое для доступа и хранения персональных данных, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

5.15 Подбор и подготовка персонала, обучение пользователей

5.15.1 Пользователи информационных систем Академии, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки персональных данных в Академии.

5.15.2 Обеспечение безопасности персональных данных возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами Академии. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационных систем Академии, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

5.15.3 Все пользователи информационных систем Академии должны быть ознакомлены с организационно - распорядительными документами по обеспечению безопасности персональных данных Академии, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности персональных данных. Доведение требований указанных документов до лиц, допущенных к обработке защищаемых персональных данных, должно осуществляться под роспись.

5.16 Ответственность за нарушения установленного порядка пользования ресурсами информационных систем Академии

5.16.1 Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с персональными данными, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства Академии.

5.16.2 Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

– индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;

– проверка подлинности пользователей (аутентификация) на основе паролей;

– реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

5.17 Средства обеспечения безопасности персональных данных

5.17.1 Средства защиты должны применяться ко всем ресурсам информационных систем Академии, независимо от их вида и формы представления информации в них. Для обеспечения информационной безопасности Академии используются следующие средства защиты:

– Физические меры защиты;

– Технические (аппаратно-программные) меры защиты;

– Средства идентификации и аутентификации пользователей;

– Средства разграничения доступа;

– Средства обеспечения и контроля целостности;

– Средства оперативного контроля и регистрации событий безопасности.

5.17.2 Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым персональным данным, а также технических средств визуального наблюдения, связи и охранной сигнализации. Для обеспечения физической безопасности компонентов информационных систем Академии необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки персональных данных, на:

– наличие специально внедренных закладных устройств;

– введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки персональных данных;

– оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

5.17.3 Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

5.17.4 С учетом всех требований и принципов обеспечения безопасности персональных данных по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

– средства разграничения доступа к данным;

– средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;

– средства реагирования на нарушения режима информационной безопасности.

5.17.5 На технические средства защиты возлагается решение следующих основных задач:

– идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств (Touch Memory, E-Token, Smart Card и т.п.);

– регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

– защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

– регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

– защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

5.17.6 В целях предотвращения работы с ресурсами информационных систем Академии посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

5.17.7 Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

– путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);

– путем проверки знания ими паролей;

– путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

5.17.8 Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

5.17.9 Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

– на контролируемую территорию;

– в отдельные помещения;

– к компонентам информационной среды Академии и элементам системы защиты персональных данных (физический доступ);

– к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);

– к активным ресурсам (прикладным программам, задачам и т.п.);

– к операционной системе, системным программам и программам защиты.

5.17.20 Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

5.17.21 Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

5.17.22 Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации персональных данных должен обеспечиваться:

– средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);

– средствами электронной подписи;

– средствами подсчета контрольных сумм (для используемого программного обеспечения).

5.17.23 Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

– ведения и анализа журналов регистрации событий безопасности (системных журналов);

– получения твердой копии (печати) журнала регистрации событий безопасности;

– упорядочения журналов, а также установления ограничений на срок их хранения;

– оперативного оповещения ответственного за организацию обработки персональных данных о нарушениях.

5.17.24 При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

– дата и время события;

– идентификатор субъекта, осуществляющего регистрируемое действие;

– действие (тип доступа).

5.17.25 Контроль эффективности защиты персональных данных осуществляется с целью своевременного выявления и предотвращения утечки персональных данных за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение персональных данных, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

5.17.26 Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

ЛИСТ СОГЛАСОВАНИЯ

" Политика в отношении обработки персональных данных"

№ п/п	**Должность**	**ФИО**	**Подпись**
1	Ректор	Е.К. Миннибаев	
2	Первый проректор	М.Н. Денисова	
3	Проректор по учебно-научной работе	А.О. Целищев	
4	Начальник Отдела делопроизводства	О.Е.Малышева	
5	Исполнительный директор Академии ВЭГУ	Б.О. Державец	