Приложение № 7 к приказу «Об обеспечении безопасности персональных данных в ГБОУВО РК КИПУ имени Февзи Якубова» от 05.09.2023 г. № 449

Положение
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ГБОУВО РК КИПУ имени Февзи Якубова

1. Общие положения

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ГБОУВО РК КИПУ имени Февзи Якубова (далее соответственно – Положение, Университет) устанавливает основные процессы по обеспечению безопасности персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн) в Университете.

1.2. Настоящее Положение разработано в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа 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».

1.3. Термины и определения

В настоящем Положении используются следующие термины и их определения:

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

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания, если иное не предусмотрено федеральным законом.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

Обработка персональных данных – действия (операции) 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 – Университет, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и

обработки ПДн (средства изготовления, тиражирования документов и другие технические средства обработки графической и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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

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.

Утечка (защищаемой) **информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

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

2. Организация и проведение работ по обеспечению безопасности персональных данных

2.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности мероприятий, осуществляемых на всех стадиях жизненного цикла ИСПДн, согласованных по цели, задачам, месту и времени, направленных на нейтрализацию угроз безопасности ПДн в ИСПДн, восстановление нормального функционирования ИСПДн после нейтрализации угроз с целью минимизации как непосредственного, так и опосредованного ущерба от

персональных данных при их обработке в информационных системах персональных данных».

2.7. Меры по обеспечению безопасности ПДн реализуются в том числе посредством применения в ИСПДн средств защиты информации, прошедших процедуру оценки соответствия согласно Федеральному закону от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПДн.

2.8. Оценка эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн проводится Университетом самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации в соответствии с Федеральным законом от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». Указанная оценка проводится не реже одного раза в 3 года.

2.9. 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 ИСПДн, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения (разрешительная система доступа);

– проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей ИСПДн и ответственного за обеспечение безопасности ПДн в ИСПДн, а также реализация организационных мер защиты информации.

2.10. Ввод в эксплуатацию СЗПДн осуществляется на основании нормативного правовых актов Университета, которые издаются на основании положительных результатов оценки соответствия ИСПДн требованиям безопасности ПДн (аттестации или декларации ИСПДн на соответствие требованиям безопасности информации).

2.11. Эксплуатация СЗПДн осуществляется в полном соответствии с разработанной, утвержденной и введенной в действие организационно-распорядительной и эксплуатационной документацией Университета, с учетом требований и положений, изложенных в настоящем документе.

2.12. При определении порядка проведения технического обслуживания и ремонтных работ оборудования ИСПДн, исполнение таких

работ осуществляется специалистом по защите информации Университета либо уполномоченными работниками Университета в его присутствии.

2.13. Все процедуры, связанные с изменением конфигурации СЗПДн, проведением технического обслуживания и ремонтных работ на технических средствах СЗПДн предусматривают документирование объемов и сроков выполненных работ, а также лиц (организаций), проводивших эти работы.

2.14. Примерный план проведения работ по обеспечению безопасности ПДн в ИСПДн Университета приведен в Приложении 1.

3. Порядок организации обучения пользователей информационных систем персональных данных

3.1. Решение основных вопросов обеспечения защиты ПДн предусматривает соответствующую подготовку пользователей ИСПДн. Проведение обучения позволит организовать обработку информации в соответствии с требованиями законодательства и нормативно-методических документов в области обеспечения безопасности ПДн при её обработке в информационной системе и реализовать установленный комплекс организационных и технических мер по защите ПДн.

3.2. Систему внутреннего обучения пользователей ИСПДн в области защиты ПДн составляют:

– проведение инструктажа пользователей ИСПДн;

– самостоятельное изучение пользователями ИСПДн необходимых для работы документов, средств и программных продуктов;

– повышение квалификации пользователей ИСПДн на курсах повышения квалификации в области защиты ПДн.

3.3. В результате прохождения обучения пользователи ИСПДн получат необходимые знания и навыки в отношении:

– правил использования СЗИ ИСПДн;

– содержания основных нормативных правовых актов, руководящих и нормативно-методических документов в области обеспечения безопасности ПДн при их обработке в ИСПДн;

– основных мероприятий по организации и техническому обеспечению безопасности ПДн при их обработке в ИСПДн;

– планирования, организации и контроля выполнения мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн.

3.4. Пользователи ИСПДн, допущенные к работе с ПДн, обязаны пройти инструктаж по вопросам обеспечения безопасности ПДн с целью

подтверждения своих знаний и уяснения своих обязанностей по поддержанию установленного режима защиты ПДн.

3.5. Инструктаж представляет собой ознакомление пользователей ИСПДн с требованиями настоящего Положения и действующих нормативных документов по обеспечению безопасности информации при их обработке в ИСПДн, в том числе с Инструкцией пользователя ИСПДн, а также устный инструктаж Администратора безопасности ИСПДн по вопросам эксплуатации средств защиты ПДн.

3.6. Ознакомление с положениями нормативной документации пользователь ИСПДн подтверждает своей личной подписью.

3.7. Контроль проведения инструктажа и периодическая проверка знания пользователями ИСПДн положений нормативной документации по вопросам обеспечения безопасности ПДн возлагается на специалиста по защите информации Университета.

3.8. Пользователи ИСПДн, не прошедшие инструктаж, к работе в ИСПДн не допускаются.

3.9. Проверка знаний пользователями ИСПДн положений нормативной документации по вопросам обеспечения безопасности ПДн проводится специалистом по защите информации Университета не реже одного раза в три года. Указанную проверку рекомендуется проводить в ходе периодического контроля соблюдения режима безопасности информации.

3.10. При самостоятельной подготовке пользователями ИСПДн, а также ответственным за обеспечение безопасности ПДн в ИСПДн самостоятельно изучаются (в части, касающейся):

– руководящие и нормативно-методические документы в области обеспечения безопасности ПДн;

– правила (инструкции) по использованию программных и аппаратных СЗИ;

– внутренние положения (локальные акты) Университета, устанавливающие порядок обращения с ПДн и обеспечения их безопасности.

3.11. Время для самостоятельного изучения определяется ректором Университета или лицом, его замещающим.

4. Планирование работ по защите персональных данных и контролю

4.1. Работа по защите ПДн проводится в рамках выполнения годовых планов мероприятий по защите информации, разработанных специалистом по защите информации Университета и утвержденных ректором Университета или лицом, его замещающим.

– оперативное принятие мер по пресечению нарушений требований защиты ПДн в ИСПДн;

– разработка предложений по устранению (ослаблению) угроз безопасности ПДн, обрабатываемых в ИСПДн.

5.3. В ходе контроля проверяются:

– соответствие принятых мер установленным нормам и требованиям безопасности информации;

– своевременность и полнота выполнения требований настоящего Положения и других руководящих документов по защите ПДн;

– полнота выявления возможных каналов НСД к ИСПДн и программно-технических воздействий на ИСПДн (или её элементы);

– эффективность применения организационных и технических мероприятий по защите ПДн;

– устранение ранее выявленных недостатков.

5.4. Контроль за соблюдением установленных требований безопасности ПДн осуществляется путем проведения внутренних проверок режима обработки и защиты ПДн.

5.5. Примерный план проведения внутреннего контроля режима обработки и защиты персональных данных приведён в Приложении 2. Специалист по защите информации Университета должен ежегодно составлять план проведения внутреннего контроля режима обработки и защиты ПДн и утверждать его у ректора Университета или лица, его замещающего. При необходимости в утвержденный план проведения внутреннего контроля режима обработки и защиты ПДн вносятся изменения, утверждаемые ректором Университета или лицом, его замещающим.

5.6. Внутренние проверки режима обработки и защиты ПДн (далее – Проверка) проводятся специалистом по защите информации, в соответствии с Планом проведения внутреннего контроля режима обработки и защиты ПДн, с привлечением:

– ответственного за организацию обработки ПДн в Университете;

– ответственного за обеспечение безопасности ПДн в ИСПДн Университета;

– пользователей ИСПДн.

5.7. Проверка проводится не реже одного раза в три года (при неизменности условий эксплуатации ИСПДн).

5.8. В ходе Проверки проверяется:

– соответствие уровня защищенности ИСПДн условиям, сложившимся на момент проверки;

– выполнение требований по защите ПДн от НСД;

– выполнение требований к подсистемам СЗПДн.

5.9. Результаты внутренних проверок режима обработки и защиты ПДн регистрируются в Журнале учёта внутренних проверок режима обработки и защиты ПДн, форма которого приведена в Приложении 3.

5.10. Периодический контроль состояния защиты ПДн в ходе обработки в ИСПДн осуществляется специалистом по защите информации Университета.

5.11. В случае невыполнения требований по защите информации в ИСПДн, работа в ИСПДн приостанавливается. Возобновление работы в ИСПДн разрешается только после устранения выявленных недостатков.

6. Дополнительные положения

6.1. Требования к помещениям и размещению аппаратных средств ИСПДн в них отражены в Порядке доступа работников Университета в помещения, в которых ведётся обработка ПДн в Университете.

6.2. В ходе обработки ПДн в ИСПДн Университета производится распространение ПДн, разрешённых субъектом ПДн для распространения.

Приложение 1
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ГБОУВО РК КИПУ имени Февзи Якубова

ПЛАН
проведения работ по обеспечению безопасности ПДн в ИСПДн в ГБОУВО РК КИПУ имени Февзи Якубова

№ п/п	Наименование мероприятия	Срок выполнения	Примечания
1.	Документальное регламентирование работы с ПДн	При необходимости	Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие
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 Правилах рассмотрения запросов субъектов персональных данных или их представителей, поступивших в Университет. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью в соответствии с федеральным законом
3.	Получение согласий субъектов ПДн на обработку персональных данных, разрешенных субъектом персональных данных для распространения	При необходимости	В случаях, предусмотренных Федеральным законом «О персональных данных», обработка ПДн, разрешенных субъектом ПДн для распространения, осуществляется только с согласия в письменной форме субъекта ПДн. Форма согласия приведена в Правилах рассмотрения запросов субъектов персональных

№ п/п	Наименование мероприятия	Срок выполнения	Примечания
			данных или их представителей, поступивших в Университет. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью в соответствии с федеральным законом
4.	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необходимости	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»
5.	Ограничение доступа работников к ПДн	При необходимости	В случае создания или изменения ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона необходимо разграничить доступ работников к ПДн
6.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц
7.	Ведение журналов учета отчуждаемых электронных носителей персональных данных, средств защиты информации	Постоянно	
8.	Повышение квалификации работников в области	Постоянно	Повышение квалификации работников, ответственных за выполнение работ – не менее раза в

№ п/п	Наименование мероприятия	Срок выполнения	Примечания
	защиты ПДн		три года, повышение осведомленности работников – постоянно (данное обучение проводит ответственный за обеспечение безопасности ПДн в ИСПДн)
9.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия ПДн
10	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для обрабатываемых ПДн, устанавливаются сроки обработки ПДн. При пересмотре сроков необходимые изменения вносятся в соответствующие документы
11.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации
12.	Определение уровня защищенности ПДн при их обработке в ИСПДн	При необходимости	Определение уровня защищенности ПДн при их обработке в ИСПДн осуществляется при создании ИСПДн, при изменении состава ПДн, объема обрабатываемых ПДн, категорий субъектов ПДн
13.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании системы защиты ИСПДн
14.	Аттестация ИСПДн на соответствие требованиям по обеспечению безопасности ПДн	При необходимости	Проводится совместно с предприятиями – лицензиатами ФСТЭК России
15.	Эксплуатация ИСПДн и контроль безопасности ПДн	Постоянно	
16.	Понижение требований по защите ПДн путем сегментирования ИСПДн, отключения от сетей общего пользования,	При необходимости	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона

№ п/п	Наименование мероприятия	Срок выполнения	Примечания
	обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных автоматизированных рабочих местах и прочих доступных мер		

Приложение 2
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ГБОУВО РК КИПУ имени Февзи Якубова

ПЛАН
проведения внутреннего контроля режима обработки и защиты персональных данных в ГБОУВО РК КИПУ имени Февзи Якубова

№ п/п	Мероприятие	Периодичность	Исполнитель
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 три года	Специалист по защите информации
2.	Проверка ознакомления работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн	Раз в три года	Специалист по защите информации
3.	Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство	Раз в три года	Специалист по защите информации
4.	Проверка подписания работниками, 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; – разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн	Раз в три года	Специалист по защите информации
5.	Проверка уничтожения материальных носителей ПДн с составлением	Раз в три года	Специалист по защите информации

№ п/п	Мероприятие	Периодичность	Исполнитель
	соответствующего акта		информации
6.	Проверка ведения журнала по учету обращений субъектов ПДн	Раз в три года	Специалист по защите информации
7.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Раз в три года	Специалист по защите информации
8.	Проверка соблюдения условий хранения материальных носителей ПДн	Раз в три года	Специалист по защите информации
9.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику Университета в отношении обработки ПДн	Раз в три года	Специалист по защите информации
10.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Раз в три года	Специалист по защите информации
11.	Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ-152 «О персональных данных»	Раз в три года	Специалист по защите информации
12.	Проверка применения для обеспечения безопасности ПДн средств защиты информации, прошедших в установленном порядке процедуру соответствия	Раз в три года	Специалист по защите информации
13.	Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн	При необходимости	Специалист по защите информации
14.	Контроль учета машинных носителей ПДн	Раз в три года	Специалист по защите информации
15.	Контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ПДн в ИСПДн	Раз в три года	Специалист по защите информации
16.	Контроль правил генерации и смены паролей пользователей ИСПДн, заведения и удаления учетных записей пользователей ИСПДн, реализации правил разграничения доступом, полномочий пользователей ИСПДн	Раз в три года	Специалист по защите информации
17.	Контроль внесения изменений в структурно-функциональные	Раз в три года	Специалист по защите информации

№ п/п	Мероприятие	Периодичность	Исполнитель
	характеристики ИСПДн		
18.	Контроль корректности настроек средств защиты информации	Раз в три года	Специалист по защите информации
19.	Контроль за обеспечением резервного копирования	Раз в три года	Специалист по защите информации
20.	Контроль поддержания в актуальном состоянии организационно-распорядительных документов по вопросам защиты ПДн	Раз в три года	Специалист по защите информации

Приложение 3
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ГБОУВО РК КИПУ имени Февзи Якубова

ФОРМА

Журнал

учёта внутренних проверок режима обработки и защиты персональных данных в ГБОУВО РК КИПУ имени Февзи Якубова

№ п/п	Мероприятие	Дата	Исполнитель	Результат