Рассмотрено на заседании
Педагогического совета
Протокол № №1
от «27» 08 2020 г.

«Утверждаю»
Директор ЦДП КГМА
Баймуратов Т.Т.
«2» 09 2020 г.

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ЛИЦЕЯ при КГМА им.И.К.Ахунбаева

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об информационной безопасности (далее – Положение) лицея при КГМА им.И.К.Ахунбаева является официальным документом.

1.2. В Положении определены требования к персоналу информационной системы персональных данных (ИСПДн), степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн лицея.

1.3. Целью настоящего Полрожения является обеспечение безопасности объектов защиты лицея от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных (УБПДн).

1.4. Безопасность персональных данных достигается путем исключения 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.

1.5. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2. ОБЛАСТЬ ДЕЙСТВИЯ

2.1. Требования настоящего Положения распространяются на всех сотрудников лицея (штатных, совместителей).

3. ОСНОВНЫЕ ПОНЯТИЯ

В настоящем Положении используются следующие термины и их определения:

автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

аутентификация отправителя данных – подтверждение того, что

отправитель полученных данных соответствует заявленному;
безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;
биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию;
блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения (созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению);
вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных;
вспомогательные технические средства и системы – технические средства и системы, непредназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных;
доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ;
доступ к информации – возможность получения информации и ее использования;
закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации);
защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником

информации;
идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;
информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных;
информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
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;
источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации;
контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных 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;
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;
нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных;
неавтоматизированная обработка персональных данных – 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;
недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации;
несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных;
носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;
обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;
технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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, применяемые в

информационных системах;
перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов;
персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;– электромагнитные
излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания;
политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа;
пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования;
правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;
программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства;
программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ;
раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных;
распространение персональных данных – действия, направленные на передачу персональных данных определенному 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 информационнотелекоммуникационных сетях или предоставление доступа к персональным
данным каким-либо иным способом;
ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;

специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных;
средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;
субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа;
технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;
трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;
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 невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;
уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации;
целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

4. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Система защиты персональных данных (СЗПДн) строится на основании: перечня персональных данных, подлежащих защите, акта определения уровня защищенности информационной системы персональных данных, модели угроз безопасности персональных данных, положения о разрешительной системе доступа работников к защищаемым информационным ресурсам ИСПДн, руководящих документов. На основании этих документов определяется необходимый

уровень защищенности ПДн каждого сегмента ИСПДн лицея. На основании анализа актуальных угроз безопасности ПДн, описанного в модели угроз, и отчета о результатах проведения внутренней проверки делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

4.2. Для ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн: автоматизированном рабочем месте (АРМ) пользователей, сервере приложений, системе управления базами данных (СУБД), границе локальной вычислительной сети (ЛВС), каналах передачи в сети общего пользования и (или) международного обмена, – если по ним передаются ПДн.

4.3. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства: антивирусные средства для рабочих станций пользователей и серверов; средства межсетевого экранирования; средства криптографической защиты информации, при передаче защищаемой информации по каналам связи. Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным программным обеспечением (ПО) и специальными комплексами, реализующими средства защиты.

4.4. Список функций защиты: управление и разграничение доступа пользователей; регистрация и учет действий с информацией; обеспечение целостности данных; обнаружение вторжений.

4.5. Список используемых технических средств отражается в журнале по учету применяемых средств защиты информации. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн соответствующие изменения должны быть внесены в Список и утверждены ректором Университета или лицом, ответственным за обеспечение защиты ПДн.

5. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДн

СЗПДн включает в себя следующие подсистемы: управление доступом, регистрация и учет; обеспечение целостности и доступности; антивирусная защита; межсетевое экранирование; анализ защищенности; обнаружение вторжений; защита информации от утечки по техническим каналам; криптографическая защита. Подсистемы СЗПДн имеют различный функционал в зависимости от уровня защищенности ИСПДн, определенного в Акте определения уровня защищенности информационной системы персональных данных.

5.1. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций: идентификации и аутентификации; контроля доступа пользователей к защищаемым ресурсам;

регистрации событий безопасности ИСПДн согласно предъявляемым параметрам регистрации; учета всех носителей информации на различных этапах их жизненного цикла.
Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД), а также внедрением специальных технических средств, осуществляющих дополнительные меры по аутентификации и контролю: применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и др.
5.2. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Университета, а также средств защиты при случайной или намеренной модификации.
Подсистема реализуется организацией резервного копирования обрабатываемых данных, восстановлением системы защиты информационной системы, резервированием ключевых элементов ИСПДн, обеспечением целостности программных средств системы защиты, физической охраной информационной системы, тестированием функций системы защиты.
5.3. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты (АВС) серверов и АРМ пользователей ИСПДн лицея. Средства антивирусной защиты предназначены для реализации следующих функций: резидентный антивирусный мониторинг; антивирусное сканирование; скрипт-блокирование; централизованная/удаленная установка/деинсталляция антивирусного продукта, настройка, администрирование, просмотр отчетов и статистической информации по работе продукта; автоматизированное обновление антивирусных баз; ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения; автоматический запуск сразу после загрузки ОС.
Подсистема АВС реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.
5.4. Подсистема межсетевого экранирования предназначена для реализации следующих функций: фильтрации на соответствующем уровне модели OSI сетевых пакетов, пакетов служебных протоколов и запросов, согласно предъявляемым требованиям; идентификации и аутентификации администратора межсетевого экрана, а также различных запросов пользователя; регистрации событий безопасности; сохранения целостности своей программной и информационной части; восстановления после сбоев и отказов оборудования; тестирования выполняемых функций.
Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС, классом не ниже 4.
5.5. Подсистема анализа защищенности должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации

программного обеспечения ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

5.6. Подсистема обнаружения вторжений должна обеспечивать выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

5.7. Подсистема защиты информации от утечки по техническим каналам предназначена для исключения несанкционированного доступа (НСД) к защищаемой информации в ИСПДн лицея посредством побочных электромагнитных излучений и наводок (ПЭМИН). Применение данной подсистемы зависит от актуальности ПЭМИН с точки зрения построенной модели угроз, либо согласно требованиям класса ИСПДн.

5.8. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн лицея при ее передаче по каналам связи сетей общего пользования и (или) международного обмена. Подсистема реализуется путем внедрения криптографических программно-аппаратных комплексов.

6. ПОЛЬЗОВАТЕЛИ ИСПДн

В ИСПДн лицея можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн: пользователь (оператор) ИСПДн; администратор информационной безопасности; программист-разработчик ИСПДн.

6.1. Оператор АРМ – сотрудник Университета, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

6.1.1. Оператор ИСПДн обладает следующим уровнем доступа и знаний: обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; располагает конфиденциальными данными, к которым имеет доступ; имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.

6.2. Администратор информационной безопасности – сотрудник лицея, занимающийся настройкой, внедрением и сопровождением системы, конфигурированием и управлением программного обеспечения (ПО) и оборудования, включая оборудование, отвечающее за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от НСД. Администратор информационной безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, осуществляет аудит средств защиты объекта.

6.2.1. Администратор информационной безопасности обладает

следующим уровнем доступа: обладает полной информацией о системном и прикладном программном обеспечении ИСПДн; обладает полной информацией о технических средствах и конфигурации ИСПДн; имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; обладает правами конфигурирования и административной настройки технических средств ИСПДн; имеет доступ к средствам защиты информации и протоколирования; обладает полной информацией об ИСПДн; имеет доступ к средствам защиты информации и протоколирования.

7. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Все сотрудники лицея, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

7.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

7.3. Сотрудник должен быть ознакомлен со сведениями настоящего Положения, принятых процедур работы с элементами ИСПДн и СЗПДн.

7.4. Сотрудники лицея, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

7.5. Сотрудники лицея должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

7.6. Сотрудники лицея должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

7.7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

7.8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Университета, третьим лицам.

7.9. При работе с ПДн в ИСПДн сотрудники обязаны

обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.
7.10. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.
7.11. Сотрудники лицея должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.
7.12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

8. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обязанности пользователей ИСПДн описаны в следующих инструкциях:
1) Инструкция администратора информационной безопасности по обеспечению безопасности персональных данных;
2) Инструкция пользователя по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных;
3) Инструкция пользователя, участвующего в неавтоматизированной обработке персональных данных;
4) Руководство пользователя по эксплуатации средств защиты информации;
5) Инструкция по организации парольной защиты.