УТВЕРЖДАЮ

Ректор ФГБОУ ВО «ИГУ»

_____ Аргучинцев А.В.

«01» марта 2016 г.

Концепция информационной безопасности информационных систем персональных данных ФГБОУ ВО «ИГУ»

СОГЛАСОВАНО

Проректор по административно-хозяйственной деятельности и капитальному строительству _____ Гагаров А.А.

Директор ЦНИТ _____ Абдрахимов И.С

г. Иркутск, 2016

СОДЕРЖАНИЕ

1. Определения

В настоящем документе используются следующие термины и их определения.

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, не предназначенные 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.

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.

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 ПДн (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.

Побочные электромагнитные излучения и наводки – 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

информационно-телекоммуникационных 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).

2. Обозначения и сокращения

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

АИС – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУИ – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

3. Введение

3.1. Настоящая Концепция является Концепцией информационной безопасности информационных систем персональных данных(далее – автоматизированная информационная система (АИС))федерального государственного бюджетного образовательного учреждения высшего образования «Иркутский государственный университет» (ФГБОУ ВО «ИГУ»).

3.2. Необходимость разработки Концепции обусловлена расширением сферы применения информационных технологий и процессов в ФГБОУ ВО «ИГУ», при обработке персональных данных.

3.3. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) АИС. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

3.4. Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

3.5. Под информационной безопасностью ПДнпонимается защищенность персональных данных и обрабатывающей их инфраструктуры от случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

3.6. Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ПДн, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

3.7. Концепция является методологической основой для:

3.7.1. формирования и проведения единой политики в области обеспечения безопасности ПДн в АИСФГБОУ ВО «ИГУ»;

3.7.2. принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера,

направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;

3.7.3. разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в АИС.

3.8. Область применения Концепции распространяется на структурные подразделения ФГБОУ ВО «ИГУ», эксплуатирующие технические и программные средства АИС, в которых осуществляется автоматизированная обработка ПДн, а также осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования АИС.

3.9. Правовой базой для разработки настоящей Концепции служат требования действующих в Российской Федерации законодательных и нормативных документов по обеспечению безопасности персональных данных (ПДн).

4. Общие положения

4.1. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) АИС. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

4.2. СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

4.3. 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.

4.4. Структура, состав и основные функции СЗПДн определяются исходя из уровня защищенности АИС. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

4.5. Эти меры призваны обеспечить:

конфиденциальность информации (защиту от несанкционированного ознакомления);

целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

4.6. Стадии создания СЗПДн включают:

4.6.1. предпроектная стадия, включающая предпроектное обследование АИС, разработку технического задания на ее создание;

4.6.2. стадия проектирования (разработки проектов) и реализации АИС, включающая разработку СЗПДн в составе АИС;

4.6.3. стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия АИС требованиям безопасности информации.

4.7. Организационные мерыпредусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) предусмотренных Политикой информационной безопасности АИС следующих организационно-распорядительных документов:

4.7.1. план мероприятий по обеспечению защиты ПДн при их обработке в АИС;

4.7.2. план мероприятий по контролю обеспечения защиты ПДн;

4.7.3. порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;

4.7.4. инструкцияадминистратора АИС в части обеспечения безопасности ПДн при их обработке в АИС;

4.7.5. инструкция администратора безопасности АИС;

4.7.6. инструкция пользователя АИС в части обеспечения безопасности ПДн при их обработке в АИС;

4.7.7. рекомендации по использованию программных и аппаратных средств защиты информации.

4.8. Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности АИС.

5. Задачи системы защиты персональных данных

5.1. Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

5.2. Для достижения основной цели система безопасности ПДнАИС должна обеспечивать эффективное решение следующих задач:

5.2.1. защиту от вмешательства в процесс функционирования АИС посторонних лиц (возможность использования АИС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

5.2.2. разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам АИС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям АИС для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

- к информации, циркулирующей в АИС;
- средствам вычислительной техники АИС;
- аппаратным, программным и криптографическим средствам защиты, используемым в АИС;

5.2.3. регистрацию действий пользователей при использовании защищаемых ресурсов АИС в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

5.2.4. контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

5.2.5. защиту от несанкционированной модификации и контроль целостности используемых в АИС программных средств, а также защиту системы от внедрения несанкционированных программ;

5.2.6. защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

5.2.7. обеспечение работоспособности криптографических средств защиты информации при компрометации части ключевой системы;

5.2.8. своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;

5.2.9. создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

6. Объекты защиты

6.1. Перечень информационных систем

6.1.1. В ФГБОУ ВО «ИГУ»производится обработка персональных данных в информационных системах персональных данных (АИС).

6.1.2. Перечень АИС определяется на основании Приказов об организации информационныхсистем персональных данных.

6.2. Перечень объектов защиты

6.2.1. Объектами защиты являются – информация, обрабатываемая в АИС, и технические средства ее обработки и защиты. Перечень персональных данных,подлежащих защите, определен в Перечне персональных данных, подлежащих защите в АИС.

6.2.2. Объекты защиты включают:

- обрабатываемую информацию,
- технологическую информацию,
- программно-технические средства обработки,
- средства защиты ПДн,
- каналы информационного обмена и телекоммуникации,
- объекты и помещения, в которых размещены компоненты АИС.

7. Классификация пользователей информационной системы персональных данных

7.1. Пользователем АИС является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. ПользователямиАИС являютсяработникиФГБОУ ВО «ИГУ», имеющие доступ к АИС и ее ресурсам в соответствии с установленным порядком для исполнения своих функциональных обязанностей.

7.2. Пользователи АИС делятся на двеосновные категории:

7.2.1. АдминистраторыАИС. РаботникиФГБОУ ВО «ИГУ»,которые занимаются настройкой, внедрением и сопровождением системы. АдминистраторыАИС обладают следующим уровнем доступа:

- обладают полной информацией о системном и прикладном программном обеспечении АИС;
- обладают полной информацией о технических средствах и конфигурации АИС;
- имеют доступ ко всем техническим средствам обработки информации и данным АИС;
- обладают правами конфигурирования и административной настройки технических средств АИС.

7.2.2. ОператорыАИС. РаботникиФГБОУ ВО «ИГУ», участвующие в процессе эксплуатации АИС.Операторы АИС обладают следующим уровнем доступа:

- обладают всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагают конфиденциальными данными, к которым имеют доступ.

7.2.3. Категории пользователей должны быть определены для каждой АИС. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей определенными в Политике информационной безопасности.

7.2.4. Все выявленные группы пользователей отражаются в Отчете по результатам внутренней проверкиобеспечения защиты персональных данных в информационной системе персональных данных. На основании Отчета определяются права доступа к элементам АИС для всех групппользователей и отражаются в Матрице доступа пользователей к защищаемым ресурсаминформационной системы.

8. Основные принципы построения системы комплексной защиты информации

8.1. Построение системы обеспечения безопасности ПДнАИСи ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

8.1.1. Законность

Предполагает осуществление защитных мероприятий и разработку СЗПДнАИСв соответствии с действующим законодательством в области защиты ПДни других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал ПДнАИС должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защитуПДн.

8.1.2. Системность

Системный подход к построению СЗПДнАИСпредполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДнАИС.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты

должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

8.1.3. Комплексность

Комплексное использование методов и средств защиты 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.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать один или несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

8.1.4. Непрерывность защиты ПДн

Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АИС.

АИС должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода АИС в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, 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 системы защиты после восстановления ее функционирования.

8.1.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите АИС и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки АИС в целом и ее системы защиты информации, в частности.

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

8.1.6. Преемственность и совершенствование

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

8.1.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности ПДн 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.

8.1.8. Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

8.1.9. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность АИС, для снижения вероятности возникновения негативных действийсвязанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

8.1.10. Гибкость системы защиты ПДн

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

8.1.11. Открытость алгоритмов и механизмов защиты

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). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

8.1.12. Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов АИС.

8.1.13. Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли теоретическую и практическую проверку.

8.1.14. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация

административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами ФГБОУ ВО «ИГУ».

8.1.15. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасностиПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

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.

9. Меры, методы и средства обеспечения требуемого уровня защищенности

9.1. Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности АИС подразделяются на:

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

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению безопасности в ИСПДн.

9.1.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

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

9.1.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), 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 коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

9.1.3. Организационные(административные) меры защиты

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

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политикиинформационной безопасности ПДн в АИСсостоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность АИС в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;
- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;
- принятие решений по вопросам реализации программы безопасностиПДн, которые рассматриваются на уровне ФГБОУ ВО «ИГУ» в целом;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью АИС.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасностиПДн.Эти правила определяют:

- какова область применения политики безопасности ПДн;
- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а так же их установить ответственность;
- кто имеет права доступа к ПДн;
- какими мерами и средствами обеспечивается защита ПДн;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;
- определятьпорядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;
- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные мерывключают в себя:

- правиладоступа в помещения АИС;
- порядок допуска сотрудников к использованию ресурсов АИС (матрица доступа);
- инструкция по модификации технических средств ИСПДн;
- инструкции пользователей АИС (администратора АИС, администратора безопасности, оператора АИС);

9.1.4. Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

9.1.5. Аппаратно-программные средства защитыПДн

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АИС 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.).

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

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей АИС;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам АИС;
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты ПДн.

Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент АИС;
- каждый сотрудник (пользователь АИС) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- в АИСразработка и отладка программ осуществляется за пределами АИС, на испытательных стендах;
- все изменения конфигурации технических и программных средств АИС производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряженийлиц, ответственных за внедрение и эксплуатацию АИС;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).

В ФГБОУ ВО «ИГУ»осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

10. Контроль эффективности системы защиты информационной системы персональных данных

Контроль эффективности СЗПДн осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так же прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности АИС (оперативный контроль в процессе информационного взаимодействия в АИС), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

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

11. Сферы ответственности за безопасность персональных данных в АИС

Ответственным за разработку мер и контроль над обеспечением безопасностиперсональных данных в АИСявляется работник, назначаемый ректором ФГБОУ ВО «ИГУ». Работник,ответственный за разработку мер и контроль над обеспечением безопасностиперсональных данных в АИС может делегировать часть полномочий по обеспечению безопасности персональных данных.

Сфера ответственности ответственного за разработку мер и контроль над обеспечением безопасностиперсональных данных в АИС включает следующие направления обеспечения безопасности ПДн:

- Планирование и реализация мер по обеспечению безопасности ПДн в АИС;
- Организация анализа угроз безопасностиПДн в АИС;
- Организация разработки, внедрения, контроля исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности в АИС;
- Организация контроля защищенности ИТ инфраструктуры ФГБОУ ВО «ИГУ» от угроз безопасности ПДн в АИС;
- Организация обучения и информирования пользователей АИС, о порядке работы с ПДнв АИС и средствами защиты;
- Организация предотвращения, выявления, реагирования и расследования нарушений безопасности ПДн в АИС.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты, с этими организациями должно быть заключено «Соглашение о конфиденциальности» (Приложение 1).

12. Модель нарушителя безопасности

Под нарушителем в ФГБОУ ВО «ИГУ»понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

Нарушители подразделяются по признаку принадлежности к АИС. Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование АИС;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование АИС.

13. Модель угроз безопасности

Для АИС выделяются следующие основные категории угроз безопасности персональных данных:

1) Угрозы несанкционированного доступа к информации:

- Угрозы уничтожения, хищения аппаратных средств АИС, носителей информации путем физического доступа к элементам АИС;
- Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
- Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования АИС и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;
- Угрозы преднамеренных действий внутренних нарушителей;
- Угрозы несанкционированного доступа по каналам связи.

14. Механизм реализации Концепции

Реализация Концепции должна осуществляться на основе планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;

- постановлений Правительства Российской Федерации;

- руководящих, организационно-распорядительных и методических документов ФСТЭК России;

- потребностей АИС в средствах обеспечения безопасности информации.

15. Ожидаемый эффект от реализации Концепции

Реализация Концепции безопасности ПДн в АИС позволит:

- оценить состояние безопасности информации АИС, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

- разработать распорядительные и нормативно-методические документы применительно к АИС;

- провести классификацию и сертификацию АИС;

- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в АИС;

- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности АИС и создаст условия для ее дальнейшего совершенствования.

16. Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящаяКонцепция являются:

1 Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

2 Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119);

3 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 14.02.2008 г.);

4 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 15.02.2008 г.) (ДСП);

5 Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационной системе персональных данных с использованием средств автоматизации (утв. ФСБ России 21.02.2008 г. №149/54-144);

6 Утверждение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. Приказом ФСТЭК России от 18.02.2013 г. №21).

ПРИЛОЖЕНИЕ №1
к Концепции информационной безопасности
информационных систем персональных данных
ФГБОУ ВО «ИГУ»

Примерная форма Соглашения о конфиденциальности

Соглашение о конфиденциальности

г. Иркутск

Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский государственный университет»(ФГБОУ ВО «ИГУ»), именуемое в дальнейшем «_____» или «сторона-Обладатель», в лице _____, действующего на основании _____, с одной стороны, и

_____ (_____), именуемое в дальнейшем «_____» или «сторона-Получатель», в лице _____, действующего на основании _____, заключили настоящее Соглашение о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1 В соответствие с настоящим Соглашением стороны обязуются сохранять конфиденциальность информации, включая информацию о персональных данных (далее – Конфиденциальная информация), обладателем которой является сторона (стороны) или третьи лица, в случаях, когда сторона (стороны) получили эту информацию законным способом.

1.2 Действие настоящего Соглашения распространяется на Конфиденциальную информацию, которая:

- передана стороной-Обладателем другой стороне (далее – сторона-Получатель) в рамках (во исполнение) заключенных договоров (соглашений), а также договоренностей любого рода, переговоров, включая преддоговорные переговоры и переписку, или в связи с ними;
- получена стороной-Получателем иным законным способом, включая получение ноу-хау при выполнении договора.

1.3 К Конфиденциальной информации для целей настоящего Соглашения приравниваются результаты копирования, выписки, обработки, обобщений, аналитических выкладок или иного использования Конфиденциальной информации.

2. ПОРЯДОК ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

2.1 Действие настоящего Соглашения распространяется на Конфиденциальную информацию переданную (полученную) как до, так и после заключения настоящего Соглашения.

2.2 Конфиденциальная информация может быть передана (получена) стороной (сторонами) в любой возможной форме, в том числе в письменной, устной форме, в форме изображения, в форме звуко- или видеозаписи, в объемно-пространственной форме или иной форме, в том числе с использованием технических средств.

2.3 При передаче (получении) Конфиденциальная информация должна быть обозначена стороной (сторонами) как конфиденциальная путем нанесения соответствующей информации (грифа конфиденциальности) на материальный носитель (документ), содержащий Конфиденциальную информацию, и/или оговоркой в документе о передаче (получении) согласно пункту 2.4. настоящего Соглашения.

2.4 Передача (получение) Конфиденциальной информации оформляется письменно путем оформления акта, протокола или иного документа, оговорки (ссылки) в документе, письме, включая переписку по электронной почте. По требованию стороны-Обладателя сторона-Получатель обязана в трехдневный срок, если иное не согласовано дополнительно, предоставить письменное подтверждение передачи (получения) Конфиденциальной информации.

2.5 Передача (получение) Конфиденциальной информации осуществляется лично соответствующей стороной (ее уполномоченным лицом). По решению стороны-Обладателя передача (получение) Конфиденциальной информации может осуществляться по почте, курьерской доставкой или иным способом, обеспечивающим защиту данной информации от доступа третьих лиц.

3. ПРАВА И ОБЯЗАНОСТИ СТОРОН

3.1 Сторона-Получатель обязуется:

3.1.1 сохранять конфиденциальность Конфиденциальной информации в течение срока действия настоящего Соглашения;

3.1.2 не разглашать Конфиденциальную информацию и не использовать эту информацию, кроме как в целях, для которых данная информация была передана (получена), или согласованных со стороной-Обладателем целях;

3.1.3 соблюдать и принимать установленные стороной-Обладателем меры по охране конфиденциальности Конфиденциальной информации, переданной (полученной) на материальных носителях:

- Хранение и использование Конфиденциальной информации должно осуществляться стороной-Получателем в служебных (офисных) помещениях, обеспечивающих физическую сохранность Конфиденциальной информации.
- Если не согласовано иное, на персональных компьютерах, в памяти которых осуществляется хранение Конфиденциальной информации, должны быть установлены пароли, с целью обеспечить сохранность данной информации и исключить доступ к Конфиденциальной информации всех лиц, кроме лиц, уполномоченных на такой доступ в соответствие с настоящим Соглашением.
- Хранение и использование Конфиденциальной информации должно осуществляться стороной-Получателем отдельно (обособлено) от информации третьих лиц в отдельных папках, файлах, каталогах и т. д.
- Если не согласовано иное, вынос Конфиденциальной информации за пределы мест их хранения/использования не допускается.
- Запрещается оставлять Конфиденциальную информацию без присмотра.
- Документы и иные материальные носители, содержащие Конфиденциальную информацию, во время работы (выполнения действий, операций) располагать так, чтобы исключить возможность ознакомления с ними лиц, не уполномоченных на такое ознакомление (доступ).
- Копирование или иное воспроизведение Конфиденциальной информации и/или ее материальных носителей, включая любые выписки и цитаты, допускается лишь с письменного согласия стороны-Обладателя. При этом неудачные или ненужные копии и иные результаты воспроизведения Конфиденциальной информации (ее материальных носителей) подлежат обязательному уничтожению с помощью специальных механических устройств или вручную. В отношении копий и иных результатов воспроизведения Конфиденциальной информации и/или ее материальных носителей, включая любые выписки и цитаты, сторона-Получатель сторона обязана придерживаться тех же мер защиты, как и в отношении оригиналов.
- При утере (повреждении) или разглашении либо угрозе утери (повреждении) или разглашения Конфиденциальной информации, а равно при обнаружении признаков незаконного получения (использования) Конфиденциальной информации третьими лицами или такой угрозы, незамедлительно сообщить об этом стороне-Обладателю.

3.1.4 При предоставлении Конфиденциальной информации в установленных законодательством случаях органу государственной власти, иным государственным органам, органам местного самоуправления одновременно с таким предоставлением уведомить об этом сторону-Обладателя.

3.1.5 Вернуть Конфиденциальную информацию и ее материальные носители стороне-Обладателю:

- по требованию стороны-Обладателя; и/или
- по прекращении действия настоящего Соглашения по любым основаниям; и/или
- по достижении целей согласно пункту 3.1.2. настоящего Соглашения, в том числе после выполнения обязательств по договорам (соглашениям), а равно по прекращению обязательств стороны (сторон) по иным основаниям и/или в иных случаях.

Возврат в соответствиис настоящим пунктом осуществляется в течение 2 (Двух) рабочих дней с момента получения стороной-Получателем соответствующего требования стороны-Обладателя или достижения целей, выполнения или прекращения обязательств, как описано выше, если иной срок не согласован сторонами дополнительно или не установлен соответствующим договором (соглашением).

3.1.6 Одновременно с возвратом согласно пункту 3.1.5. настоящего Соглашения уничтожить результаты копирования, выписки, обработки, обобщений, аналитических выкладок или иного использования Конфиденциальной информации, если не поступят иные указания стороны-Обладателя.

3.2 Сторона-Получатель гарантирует:

- что доступ к Конфиденциальной информации имеют лишь те работники, которым такой доступ необходим в связи с выполнением задач в соответствие с целями согласно 3.1.2. настоящего Соглашения;
- что стороной-Получателем надлежащим образом в соответствие с действующим законодательством образом оформлен доступ его работников к Конфиденциальной информации и созданы необходимые условия для соблюдения условий настоящего Соглашения.
- сохранение своими работниками конфиденциальности Конфиденциальной информации в соответствие с условиями настоящего Соглашения, включая надлежащее выполнение ими мер по охране конфиденциальности Конфиденциальной информации.

  К работникам стороны-Получателя приравниваются иные третьи лица, как физические, так и юридические, а также их работники, привлекаемые стороной-Получателем согласно статье 313 ГК РФ с выполнением задач в соответствие с целями согласно 3.1.2. настоящего Соглашения, включая исполнение договоров (соглашений).

3.3 Сторона-Обладатель вправе в любое время проводить проверки у Стороны-Получателя на предмет соблюдения порядка использования и хранения Конфиденциальной информации.

4. ОТВЕТСТВЕННОСТЬ СТОРОН И ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

4.1 В случае неисполнения или ненадлежащего исполнения настоящего Соглашения сторона возмещает другой стороне причиненные убытки.

4.2 За разглашение Конфиденциальной информации стороной-Получателем, повлекшее причинение убытков стороне-Обладателю, сторона-Обладатель вправе потребовать возмещения причиненных ей убытков и сверх того уплаты неустойки в размере, равном понесенным убыткам.

4.3 Сторона, не исполнившая или ненадлежащим образом исполнившая настоящее Соглашение, несет ответственность, если не докажет, что надлежащее исполнение оказалось невозможным вследствие непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств.

4.4 Срок рассмотрения претензий по настоящему Соглашению – 5 (Пять) рабочих дней с момента получения претензии.

4.5 Стороны приложат все необходимые усилия для урегулирования путем переговоров любых споров, возникающих из настоящего Соглашения, в связи с ним либо с его нарушением, расторжением.

4.6 При невозможности урегулирования таких споров путем переговоров они разрешаются в суде в соответствие с действующим законодательством РФ.

5. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ. ВНЕСЕНИЕ ИЗМЕНЕНИЙ

5.1 Любые поправки, изменения и дополнения к настоящему Соглашению имеют силу только в том случае, если они составлены в письменном виде и подписаны должным образом уполномоченными представителями каждой из сторон, подписи которых заверены печатью.

5.2 Настоящее Соглашение вступает в силу с момента его подписания и действует в течение срока действия грифа конфиденциальности документов, но менее 5 (Пяти) лет. *Стороны пришли к соглашению, что действие настоящего Соглашения применяется к отношениям сторон, возникшим до заключения настоящего Соглашения, начиная с «___» _____201_г.*

5.3 По всем вопросам, не нашедшим отражение в настоящем Соглашении, стороны руководствуются действующим законодательством Российской Федерации.

5.4 Настоящее соглашение составлено и подписано в двух экземплярах по одному для каждой стороны.

6. ЮРИДИЧЕСКИЕ АДРЕСА И РЕКВИЗИТЫ СТОРОН

ФГБОУ ВО «ИГУ»
Адрес: 664003, г. Иркутск, ул. К.Маркса, 1
Телефон: (3952) 24-34-53
Банковские реквизиты:
ИНН 3808013278 КПП 380801001
УФК по Иркутской области
(ФГБОУ ВО «ИГУ» л/с 20346U26080)
р/с 40501810000002000001
ОТДЕЛЕНИЕ ИРКУТСК Г. ИРКУТСК
БИК 042520001

_____	_____
_____ /_____/	_____ /_____/
«_____»_____201__ г.	«_____»_____201__ г.
М.П.	М.П.