

Министерство Культуры Челябинской области
Государственное бюджетное образовательное учреждение высшего образования
«Южно-Уральский государственный институт искусств имени П.И. Чайковского»
(ГБОУ ВО «ЮУрГИИ им. П.И. Чайковского»)

УТВЕРЖДАЮ

Ректор

_____ Е.Р. Сизова

« 18 » _____ декабря _____ 20 23 г.

приказ от 18.12.2023 № 02-10/03-47

ПОЛИТИКА

информационной безопасности персональных данных при их обработке
в государственном бюджетном образовательном учреждении высшего
образования «Южно-Уральский государственный институт искусств
имени П.И. Чайковского» и в информационных системах персональных данных
ГБОУ ВО «ЮУрГИИ им. П.И. Чайковского»

СОДЕРЖАНИЕ

1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	3
2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ.....	8
3. ВВЕДЕНИЕ.....	9
4. ОБЩИЕ ПОЛОЖЕНИЯ.....	10
5. ПОЛЬЗОВАТЕЛИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	12
6. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	13
7. СУБЪЕКТЫ ПРАВООТНОШЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕМ ЕЕ БЕЗОПАСНОСТИ	14
8. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ИХ ИСТОЧНИКИ	18
9. ОЦЕНКА РИСКОВ СЕТЕВОЙ БЕЗОПАСНОСТИ	19
10. МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	19
11. СИСТЕМНЫЙ АУДИТ	20
12. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ	21
13. АНТИВИРУСНЫЙ КОНТРОЛЬ	23
14. АНАЛИЗ ИНЦИДЕНТОВ	25
15. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	26
16. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ, ЯВЛЯЮЩИХСЯ ПОЛЬЗОВАТЕЛЯМИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	29

1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. В Политике информационной безопасности персональных данных при их обработке в государственном бюджетном образовательном учреждении высшего образования «Южно-Уральский государственный институт искусств имени П.И. Чайковского» и в информационных системах персональных данных ГБОУ ВО «ЮУрГИИ им. П.И. Чайковского» (далее – Политика, институт) используются следующие термины и их определения:

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

2) аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному (ГОСТ 7498-2);

3) безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

4) 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;

5) блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи;

6) 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;

7) вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных;

8) 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;

9) 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;

10) доступ к информации– возможность получения информации и её использования;

11) 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);

12) защищаемая информация– информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

13) идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

14) 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;

15) 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;

16) информационные технологии– процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

17) 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;

18) источник угрозы безопасности информации– субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации;

19) контролируемая зона– пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;

20) 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;

21) 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;

22) 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;

23) 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;

24) не декларированные 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;

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

26) 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;

27) обезличивание персональных данных– действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

28) 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;

29) 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;

30) 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;

31) 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;

32) перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов;

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

34) 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;

35) политика «чистого стола»– комплекс организационных мероприятий, контролирующая отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа;

36) пользователь информационной системы персональных данных– лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования;

37) правила разграничения доступа– совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

38) программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства;

39) программное (программно-математическое) воздействие– несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ;

40) раскрытие персональных данных– умышленное или случайное нарушение конфиденциальности персональных данных;

41) 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;

42) ресурс информационной системы– именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;

43) специальные категории персональных данных– персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных;

44) средства вычислительной техники– совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

45) субъект доступа (субъект)– лицо или процесс, действия которого регламентируются правилами разграничения доступа;

46) технический канал утечки информации– совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

47) трансграничная передача персональных данных– передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

48) 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;

49) 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;

50) утечка (защищаемой) информации по техническим каналам– неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;

51) уязвимость– слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации;

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

2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

2.1. Обозначения и сокращения, которые используются в Политике института:

1) АРМ– автоматизированное рабочее место;

2) ИСПДн– информационная система персональных данных;

- 3) КЗ– контролируемая зона;
- 4) НСД– несанкционированный доступ
- 5) ОС– операционная система
- 6) ПДн– персональные данные
- 7) ПО– программное обеспечение
- 8) СЗИ– средства защиты информации
- 9) СЗПДн– система (подсистема) защиты персональных данных
- 10) УБПДн – угрозы безопасности персональных данных.

3. ВВЕДЕНИЕ

3.1. Настоящая Политика института является официальным документом.

3.2. Политика института разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных согласно требованиям:

- 1) Конституции Российской Федерации;
- 2) Федерального закона от 27.06.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 3) Федерального закона от 29.07.2004 №98-ФЗ «О коммерческой тайне»;
- 4) Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- 5) Национального стандарта РФ ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 01.12.2011 №683-ст);
- 6) постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 7) приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3.3. Политика института представляет собой совокупность правил, требований и принятых решений, определяющих порядок доступа к информационным ресурсам института, основные направления и способы защиты информации института.

3.4. В Политике института определены требования к персоналу информационных систем персональных данных ГБОУ ВО ЮУрГИИ им. П.И. Чайковского (далее – ИСПДн), степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в ИСПДн института.

4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1. Основными целями Политики института являются:

1) обеспечение безопасности объектов защиты института от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн);

2) защита субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба;

3) обеспечение целостности и конфиденциальности информации;

4) обеспечение соблюдения требований законодательства, руководящих и нормативных документов и общей политики безопасности.

4.2. Основными задачами Политики института являются:

1) доступность обрабатываемой информации;

2) защита информации от несанкционированного доступа к ней посторонних лиц, от утечки по техническим каналам, от специальных воздействий на информацию в целях её блокирования, уничтожения, искажения;

3) контроль целостности и аутентичности (подтверждение авторства) информации, хранимой, обрабатываемой и передаваемой по каналам связи института;

4) обеспечение конфиденциальности определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи института;

5) оценка рисков информационной безопасности.

4.3. Защите подлежит вся принимаемая, передаваемая, обрабатываемая и хранимая информация содержащая:

1) сведения, составляющие служебную и коммерческую тайну, доступ к которым ограничен, в соответствии с положениями предоставленными Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и Федеральным законом от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне";

2) персональные данные, доступ к которым ограничен в соответствии с положениями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных";

3) открытые сведения, в части обеспечения доступности и целостности информации.

4.4. Основными способами защиты ИСПДн института являются:

- 1) оценка рисков сетевой безопасности;
- 2) мониторинг информационной безопасности;
- 3) системный аудит;
- 4) антивирусный контроль;
- 5) анализ инцидентов.

4.5. Основными средствами защиты информационных ресурсов института являются:

1) криптографические средства: СКЗИ КриптоПро CSP, VipNet CSP, VipNetClient, Крипто-Арм;

2) средства обеспечения и контроля целостности программных и информационных ресурсов: SecretNetStudio, ПАК Соболев, DallasLock, Kaspersky;

3) средства разграничения доступа к ресурсам автоматизированной системы: ActiveDirectory, ALDPro;

4) средства идентификации и аутентификации пользователей: ActiveDirectory, ALDPro;

5) программные средства защиты: Kaspersky.

4.6. 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.

4.7. Состав объектов защиты представлен в Перечне персональных данных, обрабатываемых в ИСПДн.

4.8. Политика института утверждается ректором института и доводится до сведения всех работников института.

4.9. Требования настоящей Политики института распространяются на всех работников института (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

5. ПОЛЬЗОВАТЕЛИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В ИСПДн института можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- 1) ответственный за обеспечение безопасности персональных данных;
- 2) администратор безопасности ИСПДн;
- 3) оператор АРМ.

5.2. Разрешительная система доступа пользователей к информационным ресурсам ИСПДн оформляется в виде Матрицы доступа работников к защищаемым персональным данным, содержащимся в информационной системе персональных данных, утверждаемой руководителем института, и реализуется с помощью средств защиты от несанкционированного доступа. Матрица доступа должна отражать полномочия пользователей по выполнению конкретных действий в отношении информационных ресурсов ИСПДн (чтение, запись, модификация, передача).

5.3. Ответственный за обеспечение безопасности персональных данных – работник института, ответственный за организацию работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Ответственный за обеспечение безопасности персональных данных обладает следующим уровнем доступа и знаний:

8) обладает полной информацией о перечне персональных данных и технических средств, входящих в информационные системы персональных данных;

9) обладает полной информацией о списке лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей;

10) обладает полной информацией о текущем состоянии защищенности ИСПДн института;

11) имеет доступ ко всем программным и аппаратным средствам обработки информации и данным ИСПДн;

12) имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

13) имеет доступ ко всем помещениям, где ведется обработка персональных данных.

5.4. Администратор безопасности ИСПДн – работник института, ответственный за настройку, внедрение и сопровождение ИСПДн, функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент, уполномочен

осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

5.5. Администратор безопасности обладает следующим уровнем доступа и знаний:

1) обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

2) обладает полной информацией о технических средствах и конфигурации ИСПДн;

3) имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

4) обладает правами конфигурирования и административной настройки технических средств ИСПДн;

5) имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.

5.6. Администратор безопасности уполномочен:

1) реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;

2) осуществлять аудит средств защиты;

3) устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

5.7. Оператор АРМ – работникинститута, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ввод ПДн в ИСПДн, корректировка ПДн, формирование справок и отчетов по информации, полученной из ИСПДн. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

5.8. Оператор ИСПДн обладает следующим уровнем доступа и знаний:

1) обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

2) может использовать конфиденциальные данные, к которым имеет доступ, для выполнения служебных обязанностей.

6. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Работникинститута, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность

их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

6.2. Работники института должны следовать Инструкции по организации парольной защиты.

6.3. Работники института должны выполнять требования Инструкции пользователя ИСПДн.

6.4. При работе с ПДн в ИСПДн работники института обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ.

6.5. Работники института 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 работников института, которые нарушили принятые Политику института и процедуры безопасности ПДн.

6.6. Работники 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.

6.7. Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- 1) инструкция ответственного за обеспечение безопасности персональных данных;
- 2) инструкция администратора безопасности ИСПДн;
- 3) инструкция пользователя ИСПДн.

7. СУБЪЕКТЫ ПРАВООТНОШЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕМ ЕЕ БЕЗОПАСНОСТИ

7.1. К субъектам правоотношений, связанных с использованием информационных ресурсов института и обеспечением их безопасности (далее – субъекты правоотношений) относятся:

- 1) ГБОУ ВО «ЮУрГИИ им. П.И. Чайковского» как собственник информационных ресурсов;
- 2) Работники института, как пользователи, по работе с информацией в соответствии с возложенными на них трудовыми обязанностями;
- 3) структурные подразделения института, обеспечивающие эксплуатацию информационных ресурсов;

4) иные пользователи (физические и юридические лица), информация о которых обрабатывается, накапливается и хранится в институте (далее – пользователи).

7.2. В целях организации процесса использования информационных ресурсов института необходимо соблюдать следующие требования:

1) получение пользователями доступа к информационным ресурсам основывается на аутентификации этих пользователей и разграничении доступа;

2) в качестве объектов доступа рассматриваются информационные ресурсы института, в отношении которых институт имеет права владения, распоряжения, пользования: данные (информация), технические средства, программные средства, услуги (сервисы) информационных систем;

3) каждому пользователю сопоставляется учетная запись пользователя, присваиваются, по возможности, единые для различных объектов доступа института атрибуты информационной безопасности: уникальный идентификатор, права доступа – с учетом их важности и ценности для деятельности института;

4) в институте могут применяться виды аутентификации, основанные на знании пользователем пароля (базовый вид аутентификации), на владении физическим носителем «секрета» (смарт-карты, устройства контактной памяти, USB-ключи, криптографические токены), на уникальных данных пользователя (биометрические параметры). При необходимости может использоваться комбинация двух или более видов;

5) пользователи уведомляются об обязанностях по обращению с «секретами» аутентификации и сроках истечения их действия. «Секреты», в свою очередь передаются пользователям способом, исключающим несанкционированное ознакомление с ними. Передача пользователем личного «секрета» другому лицу запрещена;

6) назначение прав доступа соответствует принципу «Запрещено все, что явно не разрешено» и определяется, исходя из служебных обязанностей пользователя;

7) категорически запрещен доступ к ресурсам по принципу «Всем – Полный доступ». Запрещен также неавторизованный (анонимный, гостевой) доступ к любым ресурсам, кроме общедоступных страниц вебсайтов института;

8) пересмотр прав доступа осуществляется при возникновении производственной необходимости;

9) управление доступом к сетевым информационным ресурсам и услугам производится, в том числе, путем разделения информационной

телекоммуникационной системы института отдельные логические и физические сетевые сегменты;

10) в институте должны использоваться средства контроля над соблюдением правил доступа к объектам доступа;

11) служебный доступ к объектам доступа института, осуществляемый по внешним каналам связи, должен защищаться с применением механизмов аутентификации и криптографической защиты информации;

12) для снижения вероятности угроз несанкционированного доступа, необходимо минимизировать число устройств, имеющих легальные внешние IP-адреса сети Интернет. Оборудование, имеющее легальные внешние IP-адреса сети Интернет, должно проверяться на наличие уязвимостей и автоматически получать обновления безопасности;

13) объекты доступа института должны быть защищены от внешних угроз из сети Интернет и из локальной сети сетевыми брандмауэрами и штатными средствами защиты, входящими в состав операционной системы и приложений. Число открытых для доступа сервисов и ресурсов на этих объектах должно быть минимально необходимым;

14) в договорах с поставщиками информационно-технических услуг определяются требования по управлению доступом к этим услугам;

15) при увольнении работника обеспечивается невозможность его доступа к объектам доступа института;

16) при нарушении требований Политики института информационной безопасности доступ пользователя к информационным ресурсам может быть временно заблокирован ответственными лицами до устранения нарушения;

17) порядок работы с информационными ресурсами, содержащими сведения, отнесенные к государственной тайне либо к персональным данным, защита которых организуется в соответствии с требованиями законодательства РФ, определяется соответствующими внутренними документами института. Разработка и утверждение этих документов производится вне настоящей Политики информационной безопасности;

18) доступ к информационным ресурсам института имеют все работники;

19) уровень доступа к информационным ресурсам института определяется для каждого работника индивидуально с соблюдением следующих требований:

а) каждый работник имеет доступ только к той информации, которая необходима ему для выполнения должностных обязанностей;

б) конфиденциальная и открытая информация института размещается на разных серверах;

в) непосредственный руководитель работника имеет право на просмотр информации, используемой работником.

7.3. Все работники должны быть ознакомлены персонально под роспись с организационно-распорядительными документами по защите информации, должны знать и неукоснительно выполнять технологические инструкции и общие обязанности по обеспечению безопасности информации.

7.4. При вступлении в должность нового работника 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.

7.5. Работник должен быть ознакомлен со сведениями настоящей Политики института, принятых процедур работы с элементами ИСПДн и СЗПДн.

7.6. Каждый работник при приеме на работу подписывает обязательство о соблюдении требований по сохранению конфиденциальной информации и ответственности за их нарушение, а также о выполнении правил работы с информацией.

7.7. Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- 1) инструкция ответственного за обеспечение безопасности персональных данных;
- 2) инструкция администратора безопасности ИСПДн;
- 3) инструкция пользователя ИСПДн.

7.8. Все работники, допущенные к работе с информацией института, несут персональную ответственность за нарушение правил ее использования, передачи, хранения, а также требований по сохранению конфиденциальной информации.

7.9. Для пользователей разрабатываются инструкции о порядке использования информационных ресурсов института, включающие требования по обеспечению безопасности информации.

7.10. До предоставления доступа к информационным ресурсам института пользователи должны быть ознакомлены с перечнем конфиденциальной информации и своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки такой информации.

8. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ИХ ИСТОЧНИКИ

8.1. Угрозы безопасности информации, с которыми сталкивается институт, могут быть связаны с проблемами:

- 1) несанкционированного доступа к информации;
- 2) несанкционированной передачи информации;
- 3) внесения вредоносной программы, отказа от факта приема или источника информации;
- 4) отказа в обслуживании и недоступности информации или услуг.

8.2. Указанные угрозы могут быть связаны с утратой:

- 1) конфиденциальности информации и программы (в сетях и системах, соединенных с сетями);
- 2) целостности информации и программы (в сетях и системах, соединенных с сетями);
- 3) доступности информации и сетевых услуг (и систем, соединенных с сетями);
- 4) подлинности информации (а также аутентичности сетевых пользователей и администраторов);
- 5) достоверности информации и программы (в сетях и системах, соединенных с сетями);
- 6) способности контролировать несанкционированное использование и эксплуатацию сетевых ресурсов, включая осуществление контроля в контексте политики безопасности и выполнение обязательств в отношении законодательства и предписаний (например, в отношении хранения детской порнографии);
- 7) способности контролировать злоупотребление санкционированным доступом.

8.3. Основными источниками угроз безопасности информации являются:

- 1) некорректное использование средств аутентификации (паролей);
- 2) использование программного обеспечения, воздействие программ из сети Интернет, специально разработанных или модифицированных для несанкционированного уничтожения, блокирования, модификации либо копирования информации, а также нарушения нормального функционирования элементов информационных систем института;
- 3) некорректным информированием об инцидентах или использованием информации о них, отказы и сбои системы обеспечения.

9. ОЦЕНКА РИСКОВ СЕТЕВОЙ БЕЗОПАСНОСТИ

9.1. Для идентификации и подтверждения технических мер и средств контроля и управления безопасностью информации в институте проводится оценка риска сетевой безопасности. Для этого должны быть выполнены следующие основные действия:

1) определение степени значимости информации, выраженной с точки зрения потенциального неблагоприятного воздействия на основную деятельность института в случае возникновения нежелательных инцидентов;

2) идентификация и оценка вероятности или уровней угроз, направленных против информации;

3) идентификация и оценка степени серьезности или уровня уязвимостей (слабых мест), которые могли бы быть использованы идентифицированными угрозами;

4) оценка величины рисков, основывающихся на определенных последствиях потенциального неблагоприятного воздействия на операции деятельности института и уровнях угроз и уязвимостей;

5) идентификация аспектов специализированной архитектуры/проекта безопасности и оправданных потенциальных областей действия мер и средств контроля и управления безопасностью, необходимых для обеспечения того, чтобы оцененные риски оставались в допустимых пределах.

10. МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. Мониторинг работоспособности аппаратных компонентов автоматизированных систем, обрабатывающих информацию, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования.

10.2. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

10.3. Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

1) установление сроков действия паролей;

2) периодическую, не реже раз в 3 (Три) месяца, проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

10.4. Мониторинг целостности программного обеспечения включает следующие действия:

- 1) проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- 2) обнаружение дубликатов идентификаторов пользователей;
- 3) восстановление системных файлов администраторами систем с резервных копий.

10.5. Мониторинг попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств и предусматривает:

- 1) фиксацию неудачных попыток входа в систему в системном журнале;
- 2) протоколирование работы сетевых сервисов;
- 3) выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

10.6. Мониторинг производительности автоматизированных систем, обрабатывающих информацию, производится по обращениям пользователей в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

11. СИСТЕМНЫЙ АУДИТ

11.1. Системный аудит производится один раз в год и в особых ситуациях.

11.2. Системный аудит включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

11.3. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности.

11.4. Обзоры безопасности должны включать:

- 1) отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;

2) проверку содержимого файлов конфигурации на соответствие списку для проверки;

3) обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

4) проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);

5) проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

б) проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

11.5. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

11.6. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы.

11.7. Информация об известных уязвимостях извлекается из документации и внешних источников, затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

11.8. Внесение изменений в системное программное обеспечение осуществляется администратором систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале, уведомлением каждого работника, которого касается изменение, разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

12. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Система защиты персональных данных (СЗПДн), строится на основании:

1) перечня персональных данных, обрабатываемых в ИСПДн;

2) модели угроз безопасности персональных данных при их обработке в ИСПДн;

3) руководящих документов ФСТЭК и ФСБ России.

12.2. На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн института. На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по защите персональных данных.

12.3. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

1) АРМ пользователей;

2) СУБД;

3) каналы передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

12.4. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

1) антивирусные средства для рабочей станции пользователя;

2) модуль доверенной загрузки;

3) средства межсетевое экранирования;

4) средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

12.5. Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

1) управление и разграничение доступа пользователей;

2) регистрацию и учет действий с информацией;

3) обеспечивать целостность данных;

производить обнаружения вторжений.

12.6. Список используемых технических средств отражается в Техническом паспорте информационной системы персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Технический паспорт и утверждены ректором института или лицом, ответственным за обеспечение безопасности ПДн.

13. АНТИВИРУСНЫЙ КОНТРОЛЬ

13.1. Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

- 1) резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- 2) утилиты для обнаружения и анализа новых вирусов.

13.2. К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

13.3. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать LiveCD с другими антивирусными средствами.

13.4. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администратором соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

13.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

13.6. Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

13.7. Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных установленных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запечатанном помещении.

13.8. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы

данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флеш-накопителей и т. п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

13.9. Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

13.10. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

1) осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;

2) проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

13.11. На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

13.12. На всех рабочих станциях и серверах необходимо организовать регулярное обновление антивирусных баз.

13.13. Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которые распространяются вирусы.

13.14. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

1) отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;

2) немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т. д.) зараженного файла, типа зараженного файла,

характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

14. АНАЛИЗ ИНЦИДЕНТОВ

14.1. Если администратор системы, обрабатывающей информацию, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

- 1) факт попытки несанкционированного доступа (НСД);
- 2) продолжается ли НСД в настоящий момент;
- 3) кто является источником НСД;
- 4) что является объектом НСД;
- 5) когда происходила попытка НСД;
- 6) как и при каких обстоятельствах была предпринята попытка НСД;
- 7) точку входа нарушителя в систему;
- 8) была ли попытка НСД успешной;
- 9) определить системные ресурсы, безопасность которых была нарушена;
- 10) какова мотивация попытки НСД.

14.2. Для выявления попытки НСД необходимо:

- 1) установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях;
- 2) выявить подозрительную активность пользователей;
- 3) проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго;
- 4) проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

14.3. При анализе системных журналов администратору необходимо произвести следующие действия:

- 1) проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- 2) проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- 3) просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- 4) проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;
- 5) проверить наличие мест в журналах, которые выглядят необычно;

б) выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;

7) выявить наличие неудачных попыток входа в систему.

14.4. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

1) проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;

2) проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;

3) проверить наличие мест в журналах, которые выглядят необычно;

4) выявить попытки изменения таблиц маршрутизации и адресных таблиц;

5) проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

14.5. Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

1) составить базовую схему того, как обычно выглядит система;

2) провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;

3) проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;

4) проверить целостность системных программ;

5) проверить систему аутентификации и авторизации.

14.6. В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

15. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

15.1. В институте выделяются следующие категории персональных данных:

1) специальные категории персональных данных;

2) биометрические персональные данные;

3) общедоступные или обезличенные персональные данные;

4) персональные данные, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным.

15.2. К субъектам персональных данных относятся: граждане, обратившиеся в институт и иные лица, персональные данные которых подлежат обработке на основании полномочий института.

15.3. Все персональные сведения о субъекте персональных данных ГБОУ ВО «ЮУрГИИ им. П.И. Чайковского» может получить только от него самого.

15.4. Института обязано сообщить субъекту персональных данных о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работника дать письменное согласие на их получение.

15.5. Персональные данные субъекта персональных данных являются конфиденциальной информацией и не могут быть использованы ГБОУ ВО «ЮУрГИИ им. П.И. Чайковского» или любым иным лицом в личных целях.

15.6. При определении объема и содержания персональных данных институт руководствуется настоящим Конституцией Российской Федерации, иными федеральными законами.

15.7. Персональные данные хранятся в помещениях института на бумажных носителях, учтенных машинных носителях в соответствии с «Инструкцией по учету машинных носителей».

15.8. Право доступа к персональным данным имеют работники, внесенные в «Список лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей» и в «Журнал учета лиц, допущенных к работе с персональными данными в информационных системах».

15.9. Институт обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей по защите персональных данных, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.

15.10. Институт самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей по защите персональных данных, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам могут, в частности, относиться:

1) назначение ответственного за организацию обработки персональных данных;

2) издание документов, определяющих его политику в отношении обработки персональных данных, локальных актов института по вопросам обработки персональных данных, в том числе, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

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

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора (института);

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

б) ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

15.11. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных институт осуществляет блокирование неправомерно обрабатываемых персональных данных с момента такого обращения на период проверки.

15.12. В случае выявления неточных персональных данных при обращении субъекта персональных данных институт осуществляет блокирование персональных данных с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

15.13. В случае подтверждения факта неточности персональных данных институт на основании сведений, представленных субъектом персональных данных, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

15.14. В случае выявления неправомерной обработки персональных данных, осуществляемой институтом, вуз, в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.

15.15. В случае если обеспечить правомерность обработки персональных данных невозможно, институт в срок, не превышающий десяти рабочих дней с

даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

15.16. Об устранении допущенных нарушений или об уничтожении персональных данных институт уведомляет субъекта персональных данных.

15.17. В случае достижения цели обработки персональных данных институт прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

15.18. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных институт прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

15.19. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 15.15-15.18 настоящей Политики института, институт осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

15.20. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном Федеральными законами Российской Федерации.

16. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ, ЯВЛЯЮЩИХСЯ ПОЛЬЗОВАТЕЛЯМИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

16.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

16.2. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 Уголовного кодекса Российской Федерации).

16.3. Ответственный за обеспечение безопасности персональных данных и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

16.4. При нарушениях работниками института – пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

16.5. Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях института, осуществляющих обработку ПДн в ИСПДн, и должностных инструкциях работников института.

16.6. Необходимо внести в Положения о подразделениях института, осуществляющих обработку ПДн в ИСПДн, сведения об ответственности их руководителей и работников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

РАЗРАБОТАНА:

<u>Начальник ОУП</u> должность	_____	<u>Е.А. Соломатова</u> расшифровка подписи
<u>Начальник СИ</u> должность	_____	<u>А.А. Сериков</u> расшифровка подписи

СОГЛАСОВАНО:

<u>Проректор по АХР</u> должность	_____	<u>П.П. Сундарев</u> расшифровка подписи
--------------------------------------	-------	---