МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное
образовательное учреждение высшего образования
«Пермский государственный национальный исследовательский университет»

ПРИКАЗ

27 декабря 2016 г. № 1261

г. Пермь

Об утверждении Политики в отношении обработки персональных данных

В целях исполнения требований Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Отменить приказ № 244 от 24 марта 2014 года «Об утверждении «Политики в отношении обработки персональных данных».

2. Утвердить Политику ПГНИУ в отношении обработки персональных данных согласно Приложению № 1.

3. Утвердить Положение об обработке и защите персональных данных согласно Приложению №2.

4. Утвердить следующие инструкции:

- Инструкция по обработке персональных данных без использования средств автоматизации (Приложение № 3);
- Инструкция пользователя информационной системы персональных данных (Приложение № 4);
- инструкция по организации парольной защиты ИСПД ПГНИУ (Приложение № 5);
- инструкция по антивирусной защите информационных систем персональных данных ПГНИУ (Приложение № 6);
- инструкция администратора информационной безопасности информационных систем персональных данных ПГНИУ (Приложение № 7);

- инструкция администратора информационной безопасности ИСПД на случай возникновения внештатных ситуаций (Приложение № 8);

5. Начальнику управления общественных связей разместить текст Приложений на сервере ПГНИУ.

6. Контроль за исполнением настоящего приказа оставляю за собой.

Основание: представления проректора, ректора.

Ректор И.Ю. Макарихин

ЗАВИЗИРОВАЛИ:
Начальник ФЭУ – главный бухгалтер
Зам. начальника ФЭУ – зам. гл. бухгалтера по ПиФ
Юрист
АГ-20

Приложение № 1 к приказу № 1261
от 27 декабря 2016 года

УТВЕРЖДАЮ:
Ректор ПГНИУ
_____И.Ю. Макарихин
«___» _____ 2016 г.

ПОЛИТИКА
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ “ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ”
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения.

1.1. Политика ПГНИУ в отношении обработки персональных данных (далее – Политика) направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в ПГНИУ, в том числе,

защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика ПГНИУ разработана в соответствии с Федеральным законом “О персональных данных” и иными нормативными правовыми актами Российской Федерации, содержащими нормы, регулирующие отношения при обработке персональных данных, и определяющими случаи и особенности обработки персональных данных.

1.3. Основные понятия, используемые в нормативных актах, регулирующих отношения при обработке персональных данных:

1) персональные данные (ПД) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПД);

2) обработка ПД - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПД, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПД;

3) автоматизированная обработка ПД - обработка ПД с помощью средств вычислительной техники;

4) распространение ПД - действия, направленные на раскрытие ПД неопределенному кругу лиц;

5) предоставление ПД - действия, направленные на раскрытие ПД определенному лицу или определенному кругу лиц;

6) блокирование ПД - временное прекращение обработки ПД (за исключением случаев, если обработка необходима для уточнения персональных данных);

7) уничтожение ПД - действия, в результате которых становится невозможным восстановить содержание ПД в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители ПД;

8) обезличивание ПД - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПД конкретному субъекту ПД;

9) информационная система персональных данных (ИСПД) - совокупность содержащихся в базах данных ПД и обеспечивающих их обработку информационных технологий и технических средств.

2. Принципы обработки персональных данных

2.1. Обработка ПД ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.2. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2.3. Обработке подлежат только ПД, которые отвечают целям их обработки.

2.4. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

2.5. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

2.6. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3. Условия обработки персональных данных

3.1. Обработка ПД необходима для осуществления и выполнения функций, полномочий и обязанностей, возложенных на ПГНИУ законодательством Российской Федерации, Уставом ПГНИУ и (или) договором.

3.2. Обработка ПД осуществляется с согласия субъекта ПД на обработку его ПД, за исключением случаев, определенных федеральными законами.

3.3. ПГНИУ вправе поручить обработку ПД другому лицу с согласия субъекта ПД, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта. Лицо, осуществляющее обработку персональных данных по поручению ПГНИУ, обязано соблюдать принципы и правила обработки ПД, предусмотренные законодательством Российской Федерации.

4. Конфиденциальность персональных данных

4.1. Лица, получившие доступ к ПД, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5. Меры по обеспечению безопасности персональных данных

5.1. В ПГНИУ принимаются необходимые правовые, организационные и технические меры для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

5.2. Обеспечение безопасности ПД в ПГНИУ достигается, в частности:

1) назначением лица, ответственного за организацию обработки персональных данных;

2) изданием локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на

предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) определением угроз безопасности ПД при их обработке в информационных системах персональных данных;

4) учетом машинных носителей персональных данных;

5) обнаружением фактов несанкционированного доступа к ПД и принятием мер;

6) восстановлением ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

7) установлением правил доступа к ПД, обрабатываемым в ИСПД, а также обеспечением регистрации и учета всех действий, совершаемых с ПД в ИСПД;

8) ознакомлением работников ПГНИУ, непосредственно осуществляющих обработку ПД, с положениями законодательства Российской Федерации о персональных данных (в том числе требованиями к защите ПД) и локальными актами ПГНИУ по вопросам обработки персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности ПД и уровня защищенности ИСПД.

5.3. ПГНИУ на сервере университета (www.psu.ru) в разделе “Работа с персональными данными” размещает Федеральный закон “О персональных данных” 152-ФЗ от 27.07.2006 и локальные акты ПГНИУ по вопросам обработки и защиты ПД. Работники ПГНИУ, непосредственно осуществляющие обработку ПД, обязаны знать и соблюдать требования законодательства и локальных актов ПГНИУ в отношении обработки и защиты ПД.

5.4. Работники ПГНИУ, получившие доступ к ПД, несут персональную ответственность за сохранность носителей и конфиденциальность полученных данных.

5.5. Лица, виновные в нарушении норм, регулирующих получение, обработку, защиту и распространение ПД несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность.

Проректор по учебной работе С.О. Макаров

Приложение № 2 к приказу № 1261

от 27 декабря 2016 года

УТВЕРЖДАЮ:
Ректор ПГНИУ
_____И.Ю. Макарихин
«___» _____ 2016 г.

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ “ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ”

1. Цель обработки персональных данных

1.1. Основными целями обработки персональных данных (далее –ПД) является:

- осуществление и выполнение функций, полномочий и обязанностей, возложенных на ПГНИУ законодательством Российской Федерации в области трудовых отношений и в сфере образования;
- осуществление деятельности в соответствии с Уставом ПГНИУ;
- исполнение договора, стороной которого либо выгодоприобретателем по которому является субъект ПД.

1.2. Дополнительными целями обработки ПД являются:

- обеспечение оперативного планирования и управления учебным процессом;
- автоматизация административно-хозяйственной деятельности и управления;
- обеспечение автоматизации бухгалтерского и налогового учета;
- формирование оперативной отчетности;
- автоматизация библиотечных процессов, включая подключение к электронной библиотечной системе.

2. Организация работы с персональными данными в ПГНИУ

2.1. Обработка ПД в ПГНИУ осуществляется с использованием средств автоматизации или без использования таких средств и включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление и уничтожение персональных данных.

2.2. В ПГНИУ приказом ректора назначается лицо, ответственное за организацию обработки ПД.

2.3. В ПГНИУ в соответствии с планом мероприятий осуществляется внутренний контроль соответствия обработки ПД законодательству Российской Федерации.

2.4. Автоматизированная обработка персональных данных

2.4.1. Автоматизированная обработка (обработка с помощью средств автоматизации) осуществляется в информационных системах персональных данных (ИСПД).

2.4.2. Перечень ИСПД, используемых в ПГНИУ, и места для хранения носителей ПД, обрабатываемых в ИСПД, утверждается приказом ректора.

2.4.3. Для каждой ИСПД в ПГНИУ:

- составляется Частная модель угроз безопасности ИСПД;
- составляется Акт об установлении уровня защищенности ПД при их обработке в ИСПД;
- назначается администратор информационной безопасности ИСПД;
- назначается лицо, ответственное за допуск работников к ИСПД (в случае, если такое лицо не назначено его функции выполняет руководитель структурного подразделения);
- назначается лицо, ответственное за оформление допуска работников к обработке ПД.

2.4.4. Для организации работы с ИСПД и защиты ПД в ПГНИУ разработаны и приняты следующие нормативные документы:

- Инструкция пользователя ИСПД;
- Инструкция по организации парольной защиты ИСПД;
- Инструкция по антивирусной защите ИСПД;
- Инструкция администратора информационной безопасности ИСПД;
- Инструкция администратора ИСПД на случай возникновения внештатных ситуаций.

2.5. Неавтоматизированная обработка персональных данных

2.5.1. Неавтоматизированная обработка ПД (обработка ПД без использования средств автоматизации) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях.

2.5.2. Перечень подразделений ПГНИУ, осуществляющих неавтоматизированную обработку ПД и места хранения носителей ПД, утверждаются приказом ректора.

2.5.3. В подразделениях ПГНИУ, осуществляющих неавтоматизированную обработку ПД, назначается:

- лицо, ответственное за допуск работников к ПД и за организацию работы с ПД в подразделении, если такое лицо не назначено, то ответственный за обработку ПД в подразделении – руководитель данного подразделения;
- лицо, ответственное за оформление допуска работников к обработке ПД.

2.5.4. Для организации работы и защиты ПД при неавтоматизированной обработке ПД разработана и принята Инструкция по обработке персональных данных без использования средств автоматизации.

3. Обработка и уничтожение персональных данных

3.1. Обработка ПД допускается в случаях, указанных в пункте 1 статьи 6 Федерального закона “О персональных данных”.

3.2. Обработка ПД в ПГНИУ осуществляется работниками ПГНИУ в связи с исполнением ими должностных обязанностей.

3.3. Обработка ПД прекращается в случае достижения цели обработки ПД.

3.4. Уничтожение ПД осуществляется в срок, не превышающий тридцать дней с даты достижения цели обработки ПД, если иное не предусмотрено федеральным законодательством или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПД.

3.5. В случае отсутствия возможности уничтожения ПД в течение срока, указанного в п. 3.4 настоящего Положения, ПГНИУ осуществляет блокирование таких ПД или обеспечивает их блокирование (если обработка ПД осуществляется другим лицом, действующим по поручению ПГНИУ) и обеспечивает уничтожение ПД в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

3.6. Факт прекращения обработки ПД и уничтожения ПД фиксируется в Акте об уничтожении ПД. Уничтожение ПД осуществляется комиссией из трех человек с обязательным присутствием администратора информационной безопасности (при автоматизированной обработке ПД) или лица, ответственного за организацию работы с ПД в подразделении (при неавтоматизированной обработке ПД).

4. Доступ к ПД

4.1. В ПГНИУ установлен разрешительный порядок доступа к ПД. Работникам ПГНИУ предоставляется доступ к работе с ПД исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

4.2. Работники ПГНИУ, которые в силу выполняемых служебных обязанностей постоянно работают с ПД, получают допуск к необходимым категориям ПД на срок выполнения ими соответствующих должностных обязанностей.

4.3. Временный или разовый допуск к работе с ПД в связи со служебной необходимостью может быть получен работником ПГНИУ по согласованию с

руководителем структурного подразделения и осуществлен в присутствии работника, имеющего постоянный доступ к работе с этой категорией ПД.

4.4. Доступ работника ПГНИУ к ПД прекращается с даты, прекращения трудовых отношений, либо даты изменения должностных обязанностей работника и/или исключения работника из списка лиц, имеющих право доступа к ПД. В случае увольнения все носители, содержащие ПД, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы, должны быть переданы соответствующему должностному лицу.

4.5. Допуск работников ПГНИУ к обработке ПД производится после их информирования о требованиях Федерального закона “О персональных данных” и локальных актов ПГНИУ в сфере обработки и защиты ПД и подписания соглашения о неразглашении персональных данных.

4.6. Доступ к ПД третьих лиц, не являющихся работниками ПГНИУ, возможен только при выполнении всех следующих условий:

- получения письменного согласия субъекта ПД, оформленного с соблюдением требований Федерального закона “О персональных данных”;
- наличия, заключенного с третьей стороной, договора, в том числе государственного или муниципального контракта, либо принятого государственным или муниципальным органом соответствующего акта;
- согласия лица, осуществляющего обработку ПД по поручению ПГНИУ, соблюдать конфиденциальность, принципы и правила обработки ПД, предусмотренные федеральным законодательством.

5. Права субъекта ПД в отношении его ПД, обрабатываемых в ПГНИУ

5.1. Субъект ПД имеет право:

- на получение информации, касающейся обработки его ПД. Сведения должны быть предоставлены субъекту ПД в доступной форме, и в них не должны содержаться ПД, относящиеся к другим субъектам ПД, за исключением случаев, если имеются законные основания для раскрытия таких ПД. Перечень сведений и порядок получения сведений предусмотрен действующим законодательством РФ;
- требовать уточнения его ПД, их блокирования или уничтожения в случае, если ПД являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством РФ меры по защите своих прав;
- на условие предварительного письменного согласия при обработки ПД в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;
- на условие письменного согласия при принятии на основании исключительно автоматизированной обработки ПД решений, порождающих юридические последствия в отношении субъекта ПД или иным образом затрагивающих его права и законные интересы;

- заявлять возражения на решения, основанные на автоматизированной обработки его ПД и возможные юридические последствия такого решения;
- обжаловать действия или бездействие работников ПГНИУ в уполномоченный орган по защите прав субъектов ПД или в судебном порядке.

5.2. Для получения информации, касающейся обработки ПД, субъект ПД или его представитель должен направить запрос на имя ректора. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПД в отношениях с ПГНИУ (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5.3. Субъект ПД имеет право на получение информации, касающейся обработки его ПД, в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки ПД;
- цели и применяемые способы обработки ПД;
- сведения о лицах (за исключением работников ПГНИУ), которые имеют доступ к ПД или которым могут быть раскрыты ПД на основании договора с ПГНИУ или на основании федерального закона;
- обрабатываемые ПД, относящиеся к соответствующему субъекту ПД, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПД, в том числе сроки их хранения;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению ПГНИУ, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные федеральными законами.

5.4. Запросы субъектов ПД фиксируются в Журнале учета обращений субъектов ПД.

6. Заключительные положения

6.1. В ПГНИУ принимаются необходимые правовые, организационные, технические и другие меры для обеспечения безопасности ПД. Используются необходимые технические средства и программное обеспечение.

6.2. Все лица, допущенные к работе с ПД, а также связанные с эксплуатацией и техническим сопровождением ИСПД ознакомлены с требованиями федерального законодательства в сфере защиты ПД и локальными актами ПГНИУ.

6.3. Лица, виновные в нарушении норм, регулирующих получение, обработку, защиту и распространение ПД несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность.

Проректор по учебной работе С.О. Макаров

Приложение № 3 к приказу № 1261

от 27 декабря 2016 года

УТВЕРЖДАЮ:
Ректор ПГНИУ
_____И.Ю. Макарихин
«___» _____ 2016 г.

ИНСТРУКЦИЯ

по обработке персональных данных

без использования средств автоматизации

1. Общие положения

Настоящая Инструкция разработана в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным постановлением Правительства РФ от 15.09.2008 № 687 и определяет правила работы с персональными данными и их материальными носителями без использования средств автоматизации.

Обработка персональных данных (далее –ПД) считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПД, как использование, уточнение, распространение, уничтожение ПД в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека, при этом ПД могут быть, как извлеченными из информационной системы персональных данных (далее ИСПД) так и не связанными с ИСПД.

Материальный носитель, содержащие ПД - материальный носитель (дела, книги и журналы учета, договоры, иные съемные носители информации, содержащие ПД) с зафиксированной на нем в любой форме информацией, содержащей ПД субъектов ПД в виде текста, фотографии и (или) их сочетания.

С учетом большого объема документов, содержащих персональные данные, и строго регламентированного порядка их хранения пометка конфиденциальности на них не ставится.

2. Порядок обработки персональных данных

2.1. ПД должны обособляться от иной информации путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

2.2. При фиксации ПД на материальных носителях не допускается фиксации на одном материальном носителе ПД, цели обработки которых заведомо не

совместимы. Для обработки различных категорий ПД необходимо использовать отдельный материальный носитель для каждой из категорий.

2.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПД (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПД, осуществляемой без использования средств автоматизации, наименование и адрес ПГНИУ, фамилию, имя, отчество и адрес субъекта ПД, источник получения ПД, сроки обработки ПД, перечень действий с ПД, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки ПД;

б) типовая форма должна предусматривать поле, в котором субъект ПД может поставить отметку о своем согласии на обработку ПД, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПД;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПД, содержащихся в документе, имел возможность ознакомиться со своими ПД, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПД;

г) типовая форма должна исключать объединение полей, предназначенных для внесения ПД, цели обработки которых заведомо не совместимы.

2.4. При несовместимости целей обработки ПД, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПД отдельно от других зафиксированных на том же носителе ПД, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных ПД отдельно от находящихся на том же материальном носителе других ПД осуществляется копирование ПД, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПД, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части ПД уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПД, подлежащих уничтожению или блокированию.

2.5. Уничтожение или обезличивание части ПД, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПД с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.6. Уточнение ПД при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе

сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПД.

3. Особенности обеспечения безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

3.1. Обработка ПД, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПД можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку ПД либо имеющих к ним доступ.

3.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

3.4. Руководитель подразделения, в котором обрабатываются ПД, принимает все необходимые организационные и технические меры, исключающие возможность несанкционированного доступа к материальным носителям ПД лиц, не допущенных к их обработке. Материальные носители с ПД должны храниться в запирающихся на ключ помещениях, металлических шкафах, сейфах, иных шкафах, имеющих запираемые блок-секции.

3.5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

3.6. Должностным лицам, работающим с ПД, запрещается разглашать информацию, содержащую персональные данные, устно или письменно кому бы то ни было.

3.7. Руководитель подразделения, осуществляющего обработку ПД без использования средств автоматизации:

- определяет места хранения персональных данных (материальных носителей);
- осуществляет контроль наличия в подразделении условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ;
- организует раздельное хранение материальных носителей персональных данных (документов, дисков, USB флеш-накопителей, пр.), обработка которых осуществляется в различных целях.

4. Порядок предоставления доступа к персональным данным, обрабатываемым без использования средств автоматизации

4.1. Работник ПГНИУ наделяется правом доступа к ПД в соответствии с занимаемой должностью, должностной инструкцией и/или на основании разрешения руководителя подразделения.

4.2. Временный или разовый допуск к работе с ПД в связи со служебной необходимостью может быть получен работником ПГНИУ по разрешению

руководителя структурного подразделения и осуществлен в присутствии работника, имеющего постоянный доступ к работе с этой категорией ПД.

5. Обязанности работника, допущенного к обработке ПД

5.1. При работе с материальными носителями, содержащими ПД, работник обязан исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними (в том числе другими работниками своего структурного подразделения).

5.2. При выносе материальных носителей, содержащих ПД, за пределы помещения, в котором проводится обработка ПД, по служебной необходимости, а так же при передаче материальных носителей и/ или их копий лицам, имеющим временный или разовый допуск к работе с ПД в связи со служебной необходимостью работник должен сделать отметку в Журнале учета материальных носителей, в том числе распечаток текстов, графической и иной информации, содержащих ПД и принять все возможные меры, исключающие утрату (утерю, хищение) таких материальных носителей.

5.3. При утрате (утере, хищении) документов, содержащих ПД, работник обязан немедленно доложить о таком факте руководителю подразделения. Руководитель подразделения должен сообщить о факте утраты (утере, хищении) материальных носителей, содержащих ПД, руководителю ПГНИУ, ответственному за организацию обработки ПД в ПГНИУ. По каждому такому факту назначается служебное расследование.

5.4. Работникам, допущенным к обработке ПД, запрещается:

- сообщать сведения, являющиеся ПД, лицам, не имеющим права доступа к этим сведениям.
- делать неучтенные копии документов, содержащих ПД.
- оставлять документы, содержащие ПД, на рабочих столах без присмотра.
- выносить документы, содержащие ПД, из помещений без служебной необходимости.

6. Ответственность

6.1. Ответственность за неисполнение или ненадлежащее выполнение требований настоящей Инструкции возлагается на работников и руководителей подразделений.

6.2. Контроль за выполнением положений настоящей Инструкции возлагается на руководителя ПГНИУ, ответственного за организацию обработки ПД в ПГНИУ.

Проректор по учебной работе С.О. Макаров

Приложение № 4 к приказу № 1261

от 27 декабря 2016 года

УТВЕРЖДАЮ:
Ректор ПГНИУ
_____И.Ю. Макарихин
«___» _____ 2016 г.

ИНСТРУКЦИЯ

пользователя информационной системы персональных данных

Настоящая Инструкция устанавливает порядок предоставления доступа к ПД в информационной системе персональных данных (далее – ИСПД) и обязанности пользователя ИСПД по обеспечению безопасности обрабатываемых в ней ПД, запреты на действия пользователя в ИСПД, а также права пользователя ИСПД.

1. Порядок предоставления доступа к информационной системе персональных данных

1.1. Работник ПГНИУ наделяется правом доступа к ПД в ИСПД в соответствии с занимаемой должностью, должностной инструкцией и/или на основании заявления руководителя подразделения.

1.2. Лицо, ответственное за допуск работников к ИСПД обеспечивает организацию учета лиц, допущенных к работе с ПД, прав и паролей доступа.

1.3. Контроль за выполнением настоящей Инструкции возлагается на администратора информационной безопасности ИСПД.

2. Обязанности пользователя ИСПД

Пользователь обязан:

2.1. Не реже 1 раза в год посещать раздел “Работа с персональными данными” на сервере ПГНИУ (www.psu.ru) для актуализации знаний в сфере обработки и защиты ПД.
2.2. Знать и соблюдать требования федерального закона “О персональных данных” и локальных актов ПГНИУ в сфере обработки и защиты ПД.
2.3. Исключить возможность неконтролируемого пребывания посторонних лиц в помещениях, где ведутся работы с ПД.
2.4. Руководствоваться требованиями организационно-распорядительных документов ИСПД. Строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами ИСПД.
2.5. Использовать ИСПД для выполнения служебных задач в соответствии с должностной инструкцией.
2.6. Использовать для доступа к ИСПД собственную уникальную учетную запись (логин) и пароль.
2.7. Не допускать при работе с ИСПД просмотр посторонними лицами персональных данных, отображаемых на дисплее автоматизированного рабочего места (далее – АРМ) или иных носителях.

2.8. Блокировать экран дисплея АРМ парольной заставкой при оставлении рабочего места.
2.9. По всем вопросам, связанным с обеспечением защиты персональных данных, содержащихся в базах данных, и работе со средствами защиты информации, возникающими при работе в ИСПД, обращаться к администратору информационной безопасности.
2.10. Немедленно прекращать обработку персональных данных и ставить в известность администратора информационной безопасности при подозрении компрометации пароля, а также при обнаружении:

- несанкционированных изменений в конфигурации программных или аппаратных средств АРМ;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования АРМ;

- непредусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств;

- сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ или возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов ПГНИУ.

- других попыток несанкционированного доступа к ИСПД.

3. Действия, запрещенные пользователю ИСПД

Пользователю ИСПД запрещается:
3.1. Предоставлять доступ к информации, содержащей ПД, лицам, не допущенным к их обработке. Обрабатывать ПД в присутствии лиц, не допущенных к их обработке.
3.2. Осуществлять ввод ПД под диктовку.
3.3. Сообщать (или передавать) посторонним лицам личные ключи или атрибуты доступа к ресурсам ИСПД.
3.4. Копировать информацию, содержащую ПД на узлы сети, не входящие в ИСПД.
3.5. Выводить на печать информацию, содержащую ПД на принтеры, печать на которых не согласована с администратором информационной безопасности.
3.6. Осуществлять доступ к ИСПД с узлов сети, не назначенных администратором информационной безопасности в качестве АРМ ИСПД.
3.7. Самостоятельно изменять конфигурацию аппаратно-программных средств ИСПД.
3.8. Осуществлять действия по преодолению установленных ограничений на доступ к ИСПД.
3.9. Устанавливать на АРМ программное обеспечение, не связанное с исполнением служебных обязанностей.
3.10. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с администратором информационной безопасности ИСПД.

4. Права пользователя ИСПД

Пользователь ИСПД имеет право:

4.1. Получать помощь по вопросам эксплуатации ИСПД от администратора информационной безопасности.

4.2. Обращаться к администратору информационной безопасности по вопросам дооснащения АРМ техническими и программными средствами, не входящими в штатную конфигурацию АРМ и ИСПД, необходимыми для автоматизации деятельности в соответствии с возложенными на него должностными обязанностями.

5. Правила работы в информационно-телекоммуникационных сетях международного информационного обмена

5.1. Работа в информационно-телекоммуникационных сетях международного информационного обмена - сети Интернет и других (далее – Сеть) на элементах ИСПД должна проводиться только при служебной необходимости.

5.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирусных, межсетевых экранов и других);
- передавать по Сети защищаемую информацию;
- скачивать из Сети программное обеспечение и другие файлы в неслужебных целях;
- посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение, сайты знакомств, онлайн игры и другие).

Проректор по учебной работе С.О. Макаров

Приложение № 5 к приказу № 1261

от 27 декабря 2016 года

УТВЕРЖДАЮ:
Ректор ПГНИУ
_____И.Ю. Макарихин
«___» _____ 2016 г.

ИНСТРУКЦИЯ

по организации парольной защиты ИСПД ПГНИУ

1. Общие положения

Настоящая инструкция устанавливает основные правила парольной защиты и регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

- **Идентификация** - присвоение субъектам и объектам доступа уникального и однозначно определяющего их в пределах ИСПД идентификатора, и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
- **ИСПД** - информационная система персональных данных.
- **Компрометация** - факт доступа постороннего лица к защищаемой информации, а также подозрение на него.
- **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
- **Пароль** – признак субъекта доступа, предъявляемый совместно с идентификатором субъекта в процессе идентификации.
- **Правила доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- **Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- **Несанкционированный доступ** - доступ к информации, нарушающий правила разграничения доступа в ИСПД.

2. Правила генерации паролей

2.1. Персональные пароли должны генерироваться специальными программными средствами административной службы либо задаваться субъектом самостоятельно в соответствии с требованиями данной инструкции.

2.2. Длина пароля должна быть не менее 12 символов.

2.3. В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы либо пароль должен представлять собой фразу из нескольких слов.

2.4. Пароль не должен включать в себя:

- номера телефонов, автомобилей;
- персональные данные (ФИО, дата рождения, номер паспорта, номер зачетной книжки, адрес и т.п.);
- при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

2.5. Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПД.

2.6. Срок действия пароля задается администратором информационной безопасности. Субъект обязан сменить пароль по истечению срока его действия.

3. Порядок смены паролей

3.1. Полная плановая смена паролей пользователей должна проводиться по предложению администратора информационной безопасности ИСПД и на основании распоряжения руководителя структурного подразделения.

3.2. В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

4. Обязанности пользователей при работе с парольной защитой

4.1. При работе с парольной защитой пользователям запрещается:

- разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
- предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПД, посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

4.2. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля, сейфе.

4.3. При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

5. Компрометация паролей

5.1. Под компрометацией следует понимать следующее:

- физическая утеря носителя с парольной информацией;
- передача идентификационной информации по открытым каналам связи вне ИСПД;
- проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма, или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
- перехват пароля при распределении идентификаторов;
- сознательная передача информации постороннему лицу.

5.2. Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен вводятся запасной или новый пароль;
- о компрометации немедленно оповещаются все участники обмена информацией.

6. Ответственность пользователей при работе с парольной защитой

6.1. Ответственность за организацию парольной защиты возлагается на администратора информационной безопасности ИСПД.

6.2. Повседневный контроль за действиями работников ПГНИУ при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на администратора информационной безопасности ИСПД.

6.3. Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

6.4. Ответственность в случае несвоевременного уведомления ответственного за систему защиты информации в ИСПД о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

Проректор по учебной работе С.О. Макаров

Приложение № 6 к приказу № 1261

от 27 декабря 2016 года

УТВЕРЖДАЮ:
Ректор ПГНИУ

_____И.Ю. Макарихин
«___» _____ 2016 г.

ИНСТРУКЦИЯ

по антивирусной защите информационных систем персональных данных

ПГНИУ

1. Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты и защиты от вредоносного программного обеспечения (далее – ПО) информационных систем персональных данных (далее – ИСПД), используемых в ПГНИУ.

2. Инструкция по применению средств антивирусной защиты

2.1 Защита программного обеспечения ИСПД от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

2.2 К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами уполномоченных органов РФ.

2.3 Решение задач по установке и сопровождению средств антивирусной защиты возлагается на администратора информационной безопасности ИСПД.

2.4 Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.

2.5 Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.

2.6 Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места администратора ИСПД.

2.7 Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ПГНИУ.

2.8 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.

2.9 Контроль входящей информации необходимо проводить непосредственно после ее приема.

2.10 Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

2.11 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

2.12 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться к администратору ИСПД.

2.13 В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса администратора информационной безопасности ИСПД;
- провести лечение зараженных файлов.

2.14 Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.

2.15 Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

Проректор по учебной работе С.О. Макаров

Приложение № 7 к приказу № 1261

от 27 декабря 2016 года

УТВЕРЖДАЮ:
Ректор ПГНИУ
_____И.Ю. Макарихин
«___» _____ 2016 г.

ИНСТРУКЦИЯ
администратора информационной безопасности
информационных систем персональных данных
ПГНИУ

1. Общие положения

1.1. Настоящая инструкция определяет функции администратора информационной безопасности информационных систем персональных данных ПГНИУ (далее – ИСПД) по вопросам обеспечения конфиденциальности при проведении в ИСПД работ с использованием персональных данных.

1.2. Администратор информационной безопасности назначается приказом ректора ПГНИУ.

2. Основные функции администратора информационной безопасности

2.1. Организация доступа пользователей ИСПД к защищаемым информационным ресурсам ИСПД.

2.2. Выполнение требований по парольной защите ИСПД в соответствии с Инструкцией по организации парольной защиты.

2.3. Установка, настройка и сопровождение средств защиты информации, восстановление настроек средств защиты информации после сбоев.

2.4. Контроль за появлением новых версий программного обеспечения средств защиты.

2.5. Периодическое тестирование функций установленных средств защиты информации при изменении программной среды и/или полномочий пользователей.

2.6. Обеспечение целостности данных в защищаемом сегменте компьютерной сети.

2.7. Обеспечение резервного копирования данных защищаемого сегмента компьютерной сети, восстановление ПД, уничтоженных вследствие несанкционированного доступа.

2.8. Анализ событий информационной безопасности, получаемых от средств защиты информации, а также обеспечение необходимых мер по устранению ситуаций нарушения информационной безопасности в будущем (оперативное реагирование на поступающие сигналы о нарушениях установленных правил доступа, анализ журналов регистрации событий безопасности и т.п.).

2.9. Проведение расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению. При получении информации о возникновении вирусной эпидемии вне ПГНИУ осуществляет информирование пользователей о возможной эпидемии и рекомендуемых действиях.

2.10. При необходимости и с разрешения руководителя подразделения сопровождение третьих лиц в помещения-места хранения носителей ПД.

2.11. Администратор информационной безопасности ведет следующие журналы:

- Журнал учета применяемых средств защиты информации в системе защиты информации в ИСПД;
- Журнал учета фактов несанкционированного доступа к персональным данным.

2.12. Администратор информационной безопасности осуществляет контроль за целостностью печатей (пломб) на технических средствах ИСПД (при наличии таковых), а также за соответствием установленного программного обеспечения и технических средств, заявленных в служебной документации на ИСПД.

Проректор по учебной работе С.О. Макаров

Приложение № 8 к приказу № 1261

от 27 декабря 2016 года

УТВЕРЖДАЮ:
Ректор ПГНИУ
_____И.Ю. Макарихин
«___» _____ 2016 г.

ИНСТРУКЦИЯ

администратора информационной безопасности ИСПД
на случай возникновения внештатных ситуаций

1. Общие положения

1.1. Настоящая Инструкция определяет действия администратора информационной безопасности ИСПД по применению основных мер, методов и средств сохранения (поддержания) работоспособности ИСПД, используемой в ПГНИУ, при возникновении различных кризисных ситуаций, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности ИСПД и их основных компонентов.

1.2. Под кризисной ситуацией понимается ситуация, возникшая в результате нежелательного воздействия на ИСПД, не предотвращенная средствами защиты. Кризисная ситуация может возникнуть в результате злого умысла или случайно (в результате непреднамеренных действий, пожаров, аварий, стихийных бедствий и т.п.).

Под умышленным нападением понимается кризисная ситуация, которая возникла в результате выполнения злоумышленниками в определенные моменты времени заранее обдуманных и спланированных действий.

Под случайной (непреднамеренной) кризисной ситуацией понимается такая кризисная ситуация, которая не была результатом заранее обдуманных

действий, и причиной возникновения которой явился результат объективных причин случайного характера, халатности, небрежности или случайного стечения обстоятельств.

По степени серьезности и размерам наносимого ущерба кризисные ситуации разделяются на следующие категории:

Угрожающая - приводящая к полному выходу ИСПД из строя и их неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации;

Серьезная - приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа.

Требующая внимания - Ситуации, возникающие в результате нежелательных воздействий, не наносящих ощутимого ущерба, но, тем не менее, требующие внимания и адекватной реакции (например, зафиксированные неудачные попытки проникновения или несанкционированного доступа к ресурсам системы).

1.3. Источники информации о возникновении кризисной ситуации:

- пользователи, обнаружившие несоответствия или иные подозрительные изменения в работе или конфигурации системы или средств ее защиты в своей зоне ответственности;
- средства защиты или сигнализации, обнаружившие кризисную ситуацию;
- системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

2. Общие требования

Все пользователи, работа которых может быть нарушена в результате возникновения угрожающей или серьезной кризисной ситуации, должны немедленно оповещаться. Дальнейшие действия по устранению причин нарушения работоспособности ИСПД, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями работников.

Каждая кризисная ситуация должна анализироваться администратором информационной безопасности, и по результатам этого анализа должны вырабатываться предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.д.

Серьезная и угрожающая кризисная ситуация могут требовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи в серьезной или угрожающей кризисной ситуации обеспечивается резервным

(страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность ИСПД и выполнение ею своих задач (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

Ликвидация последствий угрожающей или серьезной кризисной ситуации подразумевает восстановление программных, аппаратных, информационных и других поврежденных компонентов системы. Для восстановления используются архивные и резервированные данные.

В случае возникновения любой кризисной ситуации должно производиться расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

Расследование кризисной ситуации производится группой, назначаемой ректором ПГНИУ. Выводы группы докладываются непосредственно ректору ПГНИУ.

Если причиной угрожающей или серьезной кризисной ситуации явились недостаточно жесткие меры защиты и контроля, а ущерб превысил установленный уровень, то такая ситуация является основанием для полного пересмотра планов обеспечения непрерывной работы и восстановления.

4. Обязанности и действия администратора информационной безопасности по обеспечению непрерывной работы и восстановлению ИСПД

Действия администратора информационной безопасности в кризисной ситуации зависят от степени ее тяжести.

4.1. В случае возникновения ситуации, требующей внимания, администратор информационной безопасности должен провести ее анализ (расследование) собственными силами. О факте систематического возникновения таких ситуаций и принятых мерах необходимо ставить в известность руководителя подразделения.

4.2. В случае возникновения угрожающей или серьезной критической ситуации действия администратора информационной безопасности включают следующие этапы:

4.2.1. Немедленная реакция - администратор информационной безопасности должен**:**

- поставить в известность пользователей, обрабатывающих информацию о факте возникновения кризисной ситуации для их перехода на аварийный режим работы (приостановку работы);
- оповестить о сложившейся ситуации системного программиста или администратора, обслуживающего ИСПД и руководителя подразделения;
- определить степень серьезности и масштабы кризисной ситуации, размеры и область поражения;
- оповестить персонал взаимодействующих подсистем о характере кризисной ситуации и ориентировочном времени возобновления обработки.

4.2.2. Частичное восстановление работоспособности (минимально необходимой для возобновления работы системы в целом, возможно с потерей производительности) и возобновлении обработки:

- отключить пораженные компоненты или переключиться на использование дублирующих ресурсов (горячего резерва);
- если не произошло повреждения программ и данных, возобновить обработку и оповестить об этом персонал взаимодействующих подсистем.
- восстановить работоспособность поврежденных критичных аппаратных средств и другого оборудования, при необходимости произвести замену отказавших узлов и блоков резервными;
- восстановить поврежденное критичное программное обеспечение, используя эталонные (страховые) копии;
- восстановить необходимые данные, используя резервные копии;
- проверить работоспособность поврежденной подсистемы, удостовериться в том, что последствия кризисной ситуации не оказывают воздействия на дальнейшую работу системы;
- уведомить администраторов смежных подсистем о готовности к работе.

Затем необходимо внести все изменения данных за время с момента создания последней страховой копии (за текущий период, операционный день) на основании информации из журналов транзакций либо все связанные с поврежденной подсистемой пользователи должны повторить действия, выполненные в течение последнего периода (дня).

4.2.3. Полное восстановление в период неактивности системы:

- восстановить работоспособность всех поврежденных аппаратных средств, при необходимости произвести замену отказавших узлов и блоков резервными;
- восстановить и настроить все поврежденные программы, используя эталонные (страховые) копии;
- восстановить все поврежденные данные, используя страховые копии и журналы транзакций;
- настроить средства защиты подсистемы в соответствии с планом защиты;

4.2.4. Далее необходимо провести расследование причин возникновения кризисной ситуации.

Проректор по учебной работе С.О. Макаров