Государственное бюджетное образовательное учреждение
высшего профессионального образования
«Новосибирский государственный медицинский университет» Министерства здравоохранения и социального развития Российской Федерации
(ГБОУ ВПО НГМУ Минздравсоцразвития России)

УТВЕРЖДЕНО
Решением Ученого Совета
ГБОУ ВПО НГМУ
Минздравсоцразвития
России
от «20» 11 2012 № 8

КОПИЯ

ПОЛИТИКА
информационной безопасности
ГБОУ ВПО НГМУ Минздравсоцразвития
России

I. Общие положения

1.1. Настоящий документ, в соответствии с требованиями ст. 18.1 Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных", определяет политику ГБОУ ВПО НГМУ Минздравсоцразвития России (далее Университет) в области обработки персональных данных, определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется Университет в своей деятельности.

1.2. Настоящий документ утверждается, изменяется и/или отменяется решением Ученого Совета Университета, распространяет свое действие на все структурные подразделения и работников Университета, а так же на иных третьих лиц (пациентов, обучающихся, контрагентов (на договорной основе) и пр.).

1.3. Настоящий документ разработан на основании и во исполнение норм Трудового кодекса РФ, Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Федеральный закон от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации" и других законодательных актов, определяющих права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативных, отраслевых и ведомственных документов, по вопросам безопасности информации, утвержденных органами государственного управления различного уровня в пределах их компетенции.

ЭКЗЕМПЛЯР №1

1.4. Деятельность Университета в области информационной безопасности регулируется нормами настоящего документа, а так же иными локальными актами по вопросам регулирования порядка обработки персональных данных, обеспечения доступа к персональным данным, контроля за реализацией мер политики.

1.5. Политика вводится в действие приказом ректора Университета и подлежит для всеобщего ознакомления размещению на официальном сайте Университета (**www.ngmu.ru**)

1.5. В настоящем документе, а так же иных локальных актах по вопросам определения порядка обработки персональных данных используются следующие обозначения и сокращения:

АРМ – Автоматизированное рабочее место.

АС – Автоматизированная система.

БД – База данных.

ЗИ – Защита информации.

ИБ – Информационная безопасность.

ИР – Информационные ресурсы.

ИС – Информационная система.

ИТС – Информационно-телекоммуникационная система.

КЗ – Контролируемая зона.

МЭ – Межсетевой экран.

НСД – Несанкционированный доступ.

ОС – Операционная система.

ПБ – Политики безопасности.

ПДн – Персональные данные.

ПО – Программное обеспечение.

СВТ – Средства вычислительной техники.

СЗИ – Средство защиты информации.

СКЗИ – Средство криптографической защиты информации.

СПД – Система передачи данных.

СУБД – Система управления базами данных.

СУИБ – Система управления информационной безопасностью.

СЭД – Система электронного документооборота.

ЭВМ – Электронная - вычислительная машина, персональный компьютер.

ЭЦП – Электронная цифровая подпись.

ACL – Список контроля доступа.

2. Цели, задачи и принципы политики информационной безопасности

2.1. Основными целями политики информационной безопасности (далее политики ИБ) являются организация системы защиты информации Университет от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи**,** обеспечивающей эффективную работу всей информационной системы Университета при осуществлении деятельности, указанной в его Уставе**.**

2.2. Задачами политики ИБ являются:

- описание организации СУИБ в Университета;
- определение Политик ИБ, а именно:
  - Политика реализации антивирусной защиты;

– Политика учетных записей;
– Политика предоставления доступа к ИР;
– Политика использования паролей;
– Политика защиты АРМ;
– Политика конфиденциального делопроизводства;
- определение порядка сопровождения ИС Университет.

2.3.Основными принципами обеспечения ИБ являются следующие:

– постоянный и всесторонний анализ информационного пространства Университета с целью выявления уязвимостей информационных активов;

– своевременное обнаружение проблем, потенциально способных повлиять на ИБ Университета, корректировка моделей угроз и нарушителя;

– разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей Университета, а также повышать трудоемкость технологических процессов обработки информации;

– контроль эффективности принимаемых защитных мер;

– персонификация и адекватное разделение ролей и ответственности между сотрудниками Университета, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

3. Общая структура и управление политикой ИБ

3.1. Общее руководство обеспечения ИБ осуществляется ответственным за организацию обработки персональных данных. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет ответственный за организацию обработки персональных данных. Ответственность за функционирование автоматизированной системы Университета несет системный администратор- должностное лицо, назначаемое приказом ректора из числа квалифицированных специалистов.

Должностные обязанности системного администратора закрепляются в соответствующих инструкциях.

3.2. Руководители структурных подразделений Университета ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

3.3.Сотрудники Университета обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других локальных актов Университета в области организации обработки персональных и иных конфиденциальных данных.

3.4. Ответственность за разработку мер и контроль обеспечения защиты информации несёт ответственный за организацию обработки персональных данных.

3.5. Ответственность за реализацию политик возлагается:

– в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на системного администратора;

– в части, касающейся организации доведения правил политик и инструкций по работе с конфиденциальной информацией до сотрудников Университета – на начальника отдела кадров Университета;

– в части, касающейся организации доведения правил политик до иных лиц (см. область действия настоящей политики) – на ответственного за организацию защиты персональных данных;

– в части, касающейся исполнения правил политики, – на каждого сотрудника Университета, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

3.6. Локальные акты, принимаемые в целях обеспечения информационной безопасности должны в обязательном порядке быть согласованы с ответственным за организацию обработки персональных данных и системным администратором и не противоречить основным целям, задачам и принципам политики.

3.7. Локальны акты, регулирующие порядок обработки персональных данных включают, утверждаются ректором Университета и включают в себя, но не ограничиваются, следующие документы:

- Порядок обработки персональных данных;

-Приказы об утверждении лиц, ответственных за организацию обработки персональных данных, об утверждении перечня помещений, в которых осуществляется обработка персональных данных, лиц имеющих допуск к обработке персональных данных и пр.

4. Регламенты информационной безопасности

4.1.Регламент предоставления доступа к информационному ресурсу

4.1.1. Настоящий регламент определяет основные правила предоставления сотрудникам доступа к защищаемым ИР Университет.

4.1.2.К работе с ИР допускаются пользователи, ознакомленные с правилами работы с ИР и ответственностью за их нарушение, а также настоящей политикой.

Каждому сотруднику Университет, допущенному к работе с конкретным ИР, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в АС Университет одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

4.1.3.Порядок создания (продления) учетной записи пользователя.

Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Университет инициируется заявкой (Приложение № 1).

В заявке указывается:

– должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;

– основание для регистрации учетной записи (номер приказа о принятии на работу в Учреждении или иного договорного документа, определяющего необходимость предоставления сотруднику доступа к ИР Университет).

Заявку подписывает начальник отдела кадров подтверждающий, что указанный сотрудник действительно принят в штат Университета.

Заявка согласуется с ответственным за организацию обработки персональных данных и передается системному администратору.

Системный администратор рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к ресурсам Университета.

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.

Минимальные права в ИС Университета, определенные выше, а также присвоение начального пароля производится системным администратором, при согласовании заявки на предоставление (изменение) прав доступа пользователя к ИР.

4.1.4.Порядок предоставления (изменения) полномочий пользователя

Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Университета инициируется заявкой (Приложение № 1).

В заявке указывается:

– должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;

– основание для регистрации учетной записи (номер приказа о принятии на работу в Университет или иного договорного документа, определяющего необходимость предоставления сотруднику доступа к ИР Университета).

Заявку подписывает начальник отдела кадров, подтверждающий, что указанный сотрудник действительно принят в штат Университета.

Заявка согласуется с ответственным за организацию обработки персональных данных и передается системному администратору.

Системный администратор рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к ресурсам Университета.

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.

Минимальные права в ИС Университет, определенные выше, а также присвоение начального пароля производится системным администратором, при согласовании заявки на предоставление (изменение) прав доступа пользователя к ИР.

4.1.4.Порядок предоставления (изменения) полномочий пользователя

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам Университета инициируется заявкой руководителя структурного подразделения сотрудника (Приложение № 2).

В заявке указывается:

– должность, фамилия, имя и отчество сотрудника;

– имя пользователя (учетной записи) данного сотрудника;

– наименование информационного актива (системы, ресурса), к которому необходим допуск (или изменение полномочий пользователя);

– полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на конкретных ИР ИС) с указанием разрешенных видов доступа к ресурсу (ролей).

Заявка согласуется с ответственным за организацию обработки персональных данных и передается системному администратору на исполнение.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

4.1.5.Порядок удаления учетной записи пользователя

При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться.

Предпочтительно использовать механизмы автоматического блокирования учетных записей уволенных сотрудников, используя соответствующие ИС. При невозможности автоматического блокирования учетных записей, сотрудникам сопоставляются временные учетные записи (с фиксированным сроком действия), о чем делается отметка в заявке при ее исполнении и в обязательном порядке доводится до инициатора заявки.

Допускается регистрация постоянных учетных записей при отсутствии механизмов автоматической блокировки. В этом случае начальник кадровой службы обязан своевременно подавать заявки на блокирование учетной записи сотрудника (Приложение №3) не позднее, чем за сутки до момента прекращения срока действия полномочий пользователя.

В заявке указывается:

– должность сотрудника, фамилия, имя и отчество сотрудника;

– имя пользователя (учетной записи) данного сотрудника;

– дата прекращения полномочий пользователя.

Заявку подписывает начальник отдела кадров, утверждая тем самым факт прекращения срока действия полномочий пользователя.

Ответственный за организацию обработки персональных данных рассматривает представленную заявку и передает заявку на исполнение системному администратору.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

В случае необходимости сохранения персональных документов (профайла пользователя) на АРМ сотрудника, после прекращения срока действия его полномочий, сотрудник (или его непосредственный руководитель) должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия своих полномочий) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации. Заявка должна подаваться даже в случае применения механизмов автоматической блокировки учетных записей уволенных сотрудников.

Такая заявка должна быть предварительно согласована с ответственным за организацию обработки персональных данных, и после выполнения действий по

блокированию учетной записи передается системному администратору для исполнения требования по сохранению данных.

4.1.6.Порядок хранения исполненных заявок

Исполненные заявки передаются ответственному за организацию обработки персональных данных, и хранятся в архиве в течение 5 лет с момента окончания предоставления доступа к ИР Университета.

Копии исполненных заявок хранятся у системного администратора.

Они могут впоследствии использоваться:

– для восстановления полномочий пользователей после аварий в ИС Университета;

– для контроля правомерности наличия у конкретного пользователя прав доступа к ИР;

– тем или иным ресурсам системы при разборе конфликтных ситуаций;

– для проверки правильности настройки средств разграничения доступа к ресурсам системы.

В случае невозможности исполнения инициатору заявки направляется мотивированный отказ с приложением Заявки.

4.2. Регламент учетных записей

4.2.1.Настоящий регламент определяет основные правила присвоения учетных записей пользователям информационных активов Университета.

4.2.2.Регистрационные учетные записи подразделяются на:

– пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов Университета;

– системные – используемые для нужд операционной системы;

– служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

4.2.3.Каждому пользователю информационных активов Университет назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

4.3. Регламент использования паролей

4.3.1. Настоящий регламент предусмотрен для обеспечения информационной безопасности путем ограничения круга пользователей и защиты доступа к определяемому иными регламентами и локальными актами кругу информации.

4.3.2. Основные положения регламента закрепляются в «Инструкции по организации парольной защиты в автоматизированной системе».

4.4. Регламент реализации антивирусной защиты

4.4.1. Настоящий регламент определяет основные правила для реализации антивирусной защиты в Университете.

4.4.2. Основные положения регламента закрепляются в «Инструкции по проведению антивирусного контроля в АС».

4.5. Регламент защиты автоматизированного рабочего места

4.5.1. Настоящий регламент определяет основные правила и требования по защите ПДн и иной КИ Университета от неавторизованного доступа, утраты или модификации.

4.5.2.Во время работы с КИ должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие КИ, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

4.5.3.Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с локальными актами, в том числе инструкциями с носителями КИ, Перечнем сведений конфиденциального характера и пр.

4.5.4.Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только системному администратору. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

4.5.5.Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных АРМ, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

4.5.6.Копирование КИ и временное изъятие носителей КИ (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих КИ, пользователь имеет право присутствовать при дальнейшем проведении работ.

ПО должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать КИ, должны быть закреплены за соответствующими сотрудниками Университета. Запрещается использование указанных АРМ другими пользователями без согласования с ответственным за обработку персональных данных Университета. При передаче указанного АРМ другому пользователю, должна производится гарантированная очистка диска (форматирование).

4.5.7.Системный администратор вправе отказать в устранении проблемы, вызванной наличием на рабочем месте ПО или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

4.6. Регламент сопровождения информационной системы Университета.

4.6.1.Обеспечение ИБ ИС на стадиях жизненного цикла ИБ ИС должна обеспечиваться на всех стадиях ЖЦ ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии ответственного за обработку персональных данных и системного администратора. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

4.6.2.При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ 34.ххх «Стандарты информационной технологии».

Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии ответственного за обработку персональных данных и системного администратора.

4.6.3.На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

– неверной формулировки требований к ИС;

– выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;

– принятия неверных проектных решений;

– внесения разработчиком дефектов на уровне архитектурных решений;

– внесения разработчиком недокументированных возможностей в ИС;

– неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС;

– разработки некачественной документации;

– сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;

– неверного конфигурирования ИС;

– приемки ИС, не отвечающей требованиям заказчика;

– внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

4.6.4.Привлекаемые для разработки средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз информационной безопасности.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

4.6.4.В договор (контракт) о поставке ИС и их компонентов рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика.4.6.5.На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

– умышленное несанкционированное раскрытие, модификация или уничтожение информации;

– неумышленная модификация или уничтожение информации;

– недоставка или ошибочная доставка информации;

– отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения.

4.6.7.На стадии сопровождения должна быть обеспечена защита от угроз:

– внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;

– невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

4.6.8.На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб Учреждению, и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

4.6.9.Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ ИС.

4.7. Регламент профилактики нарушений политики информационной безопасности.

4.7.1.Под профилактикой нарушений политики ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в Университете и проведение разъяснительной работы по ИБ среди пользователей.

4.7.2.Проведение в ИС Университета регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования. Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной в ИС Университете степенью периодичности.

4.7.3.Задача предупреждения в ИС Университета возможных нарушений ИБ решается по мере наступления следующих событий:

– включение в состав ИС Университет новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Университета;

– изменение конфигурации программных и технических средств ИС (изменение конфигурации ПО рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Университета;

– при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или ПО технических средств, используемых в ИС Университета.

4.7.4. Системный администратор (возможно, при помощи сторонней организации специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или ПО относительно ИС Университета. Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, учреждений и иных объединений и других организаций, специализирующихся в области защиты информации.

Системный администратор (возможно, при помощи сторонней организации, специализирующейся в области ИБ) организовывает периодическую проверку СЗИ ИС Университет путем моделирования возможных попыток осуществления НСД к защищаемым ИР.

4.7.5.Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе СЗИ ИС Университета средств и функций защиты. По результатам профилактических работ, проводимых в ИС, необходимо сделать соответствующие записи в «Журнале проверки исправности и технического обслуживания».

4.7.6.Плановая разъяснительная работа по правилам настоящих регламентов и политики в целом, а также инструктаж сотрудников Университета по соблюдению

требований нормативных и регламентных документов по ИБ, принятых в Университете, проводится ответственным за организацию обработки персональных даных ежеквартально.

Внеплановая разъяснительная работа по правилам настоящих регламентов, а также инструктаж сотрудников Университета по соблюдению требований нормативных и регламентных документов по ИБ, принятых в Университете, проводится при пересмотре настоящих регламентов, при возникновении инцидента нарушения правил настоящих регламентов.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящих регламентов и иных локальных актов в области обработки персональных данных.

4.8. Ликвидация последствий нарушения регламентов информационной безопасности.

4.8.1. Системный администратор, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

4.8.2. В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР ИС рекомендуется уведомить ответственного за обработку персональных данных и/или системного администратора, и далее следовать их указаниям.

4.8.3.Действия системного администратора при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

- Инструкцией пользователя автоматизированной системы;
- Политикой информационной безопасности;
- Должностными обязанностями системного администратора.

4.8.4.После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

5. Ответственность за нарушение политики информационной безопасности.

5.1.Ответственность за выполнение правил ПБ несет каждый сотрудник Университета в рамках своих должностных обязанностей и полномочий.

5.2.На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования ПБ Университета, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор или увольнение (пп. «в» п. 6 ст. 81 ТК РФ)

5.3.Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Университету в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).

5.4.За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или

модификация защищаемой информации, сотрудники Университета могут быть привлечены к уголовной ответственности.

ПРОЕКТ ВНОСИТ:
Начальник отдела информатизации
«____»_____2012 г. Прокушев А.Ю.

СОГЛАСОВАНО:

Проректор по общим вопросам
«_____»_____2012 г. Гончаров И.Г.

Начальник юридического отдела
«_____»_____2012 г. Акимова А.Б.

Начальник отдела кадров
«_____»_____2012 г. Кох О.А.

Приложение 1

Форма заявления на создание учетной записи пользователя

СОГЛАСОВАНО
Специалист по кадрам «___» _____ 201_ г.
(для штатных сотрудников)

Ответственный за организацию обработки персональных данных «___» _____ 201_ г.

ЗАЯВЛЕНИЕ № _____
На создание (продление) учетной записи пользователя

Прошу создать (продлить) учетную запись пользователя:

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Ф.И.О. непосредственного руководителя, должность, телефон	

Сотрудник приступает к работе с: «___» _____ 20__г. по «___» _____ 20__г.
указывается при необходимости

Обоснование служебной
необходимости:_____
_____
_____
_____
_____

_____ _____ «___» _____
20__г.
фамилия И.О. руководителя подразделения подпись дата

С правилами работы в информационной системе ГБОУ ВПО НГМУ Минздравсоцразвития России ознакомлен(а)

_____ _____ «___» _____
20__г.
фамилия И.О. сотрудника подпись дата

Выполнено: _____
назначенное имя пользователя

Ответственный за техническое обслуживание _____ _____
подпись фамилия И.О.

Дата: «___» _____ 201_ г.

Приложение 2

Форма заявления на изменение полномочий

СОГЛАСОВАНО

Ответственный за организацию обработки персональных данных «___» _____ 201_ г.

ЗАЯВЛЕНИЕ № _____
На изменение полномочий пользователю

Прошу изменить полномочия по работе с информационным ресурсом:

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Имя в системе (указывается если есть)	
Ф.И.О. непосредственного руководителя, должность, телефон	
Наименование информационного ресурса	
Старые полномочия (если были)	
Новые полномочия	

Изменения вступают в силу с: «___» _____ 20__г. по «___» _____ 20__г.
(указывается при необходимости)

Обоснование служебной необходимости:_____
_____
_____
_____
_____

_____ _____ «___» _____ 20__г.
фамилия И.О. руководителя подразделения подпись дата

С правилами работы в информационной системе ГБОУ ВПО НГМУ Минздравсоцразвития России ознакомлен(на)
_____ _____ «___» _____ 20__г.
фамилия И.О. сотрудника подпись дата

Выполнено:
_____
назначенное имя пользователя, описание выполненных действий

Ответственный за техническое обслуживание _____ _____
подпись фамилия И.О.

Дата: «___» _____ 20__г.

Приложение 3

Форма заявления на блокировку учетной записи

Специалист по кадрам «___» _____ 201_ г.
(для штатных сотрудников)

Ответственный за организацию обработки персональных данных «___» _____ 201_ г.

ЗАЯВЛЕНИЕ № _____
На блокировку учетной записи пользователя

Прошу заблокировать учетную запись пользователя:

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Имя в системе	
Ф.И.О. непосредственного руководителя, должность, телефон	

Срок действия полномочий прекратить с: «___» _____ 20__г.

Обоснование
блокировки:_____
_____
_____
_____

_____ _____ «___» _____
20__г.
фамилия И.О. руководителя подразделения подпись дата

С гарантированным хранением данных в течении
_____
указывается срок хранения данных пользователя

Пользователь блокирован

Ответственный за техническое обслуживание _____ _____
подпись фамилия И.О.

Дата: «___» _____ 201_ г.