УТВЕРЖДАЮ
Ректор ГОУ ВПО «НГГУ»
_____ С. И. Горлов
«__» _____ 2010 г.

Инструкция администратора безопасности информационной системы персональных данных

1. Общие положения

1.1. Настоящая инструкция разработана на основании:

- Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных»;
- Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации №781 от 17 ноября 2007г.;
- Приказа №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного ФСТЭК России от 05.02.2010 г.;
- Приказа №__ от «__» _____ 20__г. «Об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Ректором ГОУ ВПО «НГГУ»;
- Положения от «__» _____ 20__г. «О разрешительной системе допуска пользователей к обрабатываемой в ИСПДн информации», утвержденного Ректором ГОУ ВПО «НГГУ».

1.2. Инструкция определяет основные задачи, функции, обязанности, права и ответственность Администратора безопасности информационной системы персональных данных (далее – ИСПДн) ГОУ ВПО «НГГУ» (далее - НГГУ).

1.3. Администратор безопасности ИСПДн (далее – Администратор) назначается приказом Ректора НГГУ или лицом его заменяющим, из сотрудников отдела АСУ и является лицом, выполняющим функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники ИСПДн НГГУ, в пределах своей зоны ответственности.

1.4. Закрепление функциональных обязанностей и разделение зон ответственности производится приказом Ректора НГГУ.

1.5. В своей деятельности Администратор руководствуется требованиями действующих федеральных законов, общегосударственных, ведомственных, а также внутренних нормативных документов по вопросам защиты информации и обеспечивает их выполнение пользователями ИСПДн.

1.6. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

2. Задачи и функции администратора

2.1. Основными задачами Администратора являются:

- сопровождение средств защиты информации (в том числе криптографических, шифровальных) от несанкционированного доступа (далее – СЗИ) и основных технических средств и систем (далее – ОТСС);
- организация разграничения доступа;
- контроль эффективности защиты информации.

2.2. Для выполнения поставленных задач на Администратора возлагаются следующие функции:

2.2.1. Допуск пользователей (разработчиков, эксплуатационного персонала) к техническим, программным средствам и информационным ресурсам ИСПДн в соответствии с требованиями «Положения о разрешительной системе допуска пользователей к обрабатываемой в ИСПДн информации» на всех стадиях жизненного цикла ИСПДн.

2.2.2. Участие на стадии проектирования (внедрения) ИСПДн в разработке технологии обработки информации конфиденциального характера (далее – Информации) по вопросам:

- организация порядка учета, хранения и обращения с документами и носителями информации;
- подготовки инструкций, определяющих задачи, функции, ответственность, права и обязанности пользователей ИСПДн по вопросам защиты информации, а также ответственных по защите информации в процессе автоматизированной обработки информации;
- сопровождение СЗИ, в том числе средств криптографической защиты информации, на стадии эксплуатации ИСПДн, включая ведение служебной информации СЗИ (управление ключевой системой, сопровождение правил разграничения доступа), оперативный контроль за функционированием СЗИ;
- контроль выполнения требований действующих нормативных документов по вопросам защиты информации при обработке информации в ИСПДн;
- контроль соответствия общесистемной программной среды эталону (контроль целостности программного обеспечения) и проверка включаемых в ИСПДн новых программных средств.

3. Обязанности администратора

3.1. Для реализации поставленных задач и возложенных функций Администратор ОБЯЗАН:

3.1.1. Сопровождать СЗИ и ОТСС:

− Вести учет (по вопросам обеспечения безопасности информации) и знать перечень установленных в подразделениях НГГУ СЗИ и перечень задач, решаемых с их использованием;

− Вести журнал учета эксплуатационной и технической документации СЗИ ИСПДн.

− Вести журнал учета машинных носителей персональных данных.

− Осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на автоматизированных рабочих местах (далее – АРМ) специальных программных и программно-аппаратных СЗИ;

− Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ и серверов, осуществлять проверку работоспособности системы защиты после установки (обновления) программных средств ИСПДн;

− Периодически проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование);

− Контролировать соответствие технического паспорта ИСПДн фактическому составу (комплектности) ИСПДн и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения в ИСПДн);

− Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ;

− Вести журнал учета нештатных ситуаций, фактов вскрытия и опечатывания АРМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ИСПДн;

− Проводить периодический инструктаж сотрудников подразделения (пользователей ИСПДн) по правилам работы с используемыми средствами и системами зашиты информации.

3.1.2. Организовывать разграничения доступа:

3.1.2.1. Участвовать в разработке и знать перечень защищаемых информационных ресурсов.

3.1.2.2. Разрабатывать для ИСПДн решения по:

− составу доменов сети, системы доверительных отношений между ними;

− составу групп (локальных и глобальных) каждого домена;

− приписке пользователей с одинаковыми правами, статусом безопасности и характером решаемых задач к соответствующим группам;

− определению информационных связей между сегментами сети и требований к изоляции сегментов с использованием средств аппаратной безопасности сегментов;

− вести учет заявок пользователей на допуск к информационным ресурсам ИСПДн;

− осуществлению контроля за наличием активных компьютеров сети, состоянием активных пользователей, использованием разделяемых ресурсов, процессом печати на общих принтерах;

− разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, проектированию системы почтовых ящиков, использованию СЗИ при передаче закрытых документов);

− разработке порядка выхода пользователей в сети связи общего пользования (далее – Сети) и использованию встроенных СЗИ в сервисных программах;

− определению режимов использования СЗИ: защита паролей, защита в протоколах передачи данных, кодирование файлов, подключение дополнительных алгоритмов криптографической защиты;

− разработке политики аудита: определению состава регистрируемых событий и списка лиц, имеющих допуск к журналам аудита;

− осуществлять учет и периодический контроль за составом и полномочиями пользователей различных АРМ ИСПДн;

− контролировать и требовать соблюдения установленных правил по организации парольной защиты в ИСПДн НГГУ;

− осуществлять оперативный контроль за работой пользователей защищенных АРМ, анализировать содержимое журналов событий операционных систем (далее - ОС), систем управления базами данных (далее - СУБД), пакетов прикладных программ (далее - ППП) и СЗИ всех АРМ и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование журналов событий АРМ и надлежащий режим хранения данных архивов;

− принимать участие в работах по внесению изменений в аппаратно-программную конфигурацию серверов и АРМ ИСПДн;

− обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания АРМ и отправке их в ремонт (контролировать стирание информации на съемных носителях);

− организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль за правильностью их использования;

− осуществлять периодический контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных;

− по указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ, установленных на АРМ ИСПДн;

− требовать от пользователей стирания остаточной информации на несъёмных носителях (жестких дисках) установленным порядком, а в оперативной памяти по окончании обработки информации путем перезагрузки АРМ;

− контролировать обеспечение защиты конфиденциальной информации при взаимодействии абонентов с информационными сетями связи общего пользования.

3.1.3. Контролировать эффективность защиты информации:

− Проводить работу по выявлению возможности вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам АРМ;

− Докладывать ответственному по обеспечению безопасности о выявленных угрозах безопасности информации, обрабатываемой в ИСПДн, об имевших место попытках НСД к информации и техническим средствам АРМ;

− Проводить занятия с пользователями ИСПДн по правилам работы на АРМ, оснащенных СЗИ, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков, выявленных при контроле эффективности защиты информации;

− Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в ИСПДн.

3.2. Администратору ЗАПРЕЩАЕТСЯ:

3.2.1. Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации.

3.2.2. Использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий.

3.2.3. Самостоятельно (без согласования с подразделением автоматизации) вносить изменения в настройки серверной части ИСПДн.

3.2.4. Использовать в своих и в чьих-либо личных интересах ресурсы ИСПДн, предоставлять такую возможность другим.

3.2.5. Выключать СЗИ без письменной санкции руководства.

3.2.6. Передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки.

3.2.7. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИСПДн, блокированию доступа, потере информации без санкции руководства и предупреждения пользователей.

3.2.8. Нарушать правила эксплуатации оборудования ИСПДн.

3.2.9. Корректировать, удалять, подменять журналы аудита.

4. Права и ответственность администратора

4.1. Администратор имеет право:

− получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и АРМ пользователей;

− требовать от пользователей ИСПДн выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

− участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

− осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности;

− производить анализ защищенности ИСПДн путем применения специального программного обеспечения, осуществления попыток взлома системы защиты ИСПДн. Такие работы должны проводиться в часы наименьшей информационной нагрузки с обязательным уведомлением сотрудников подразделений автоматизации и обеспечение безопасности информации;

− вносить свои предложения по совершенствованию мер защиты в ИСПДн.

4.2. Администратор несет ответственность за:

− реализацию принятой в НГГУ политики информационной безопасности;

− программно - технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и ИСПДн обработки информации, закрепленные за ним приказом Ректора НГГУ, а также за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями;

− разглашение сведений, конфиденциального характера, ставших известными ему по роду работы;

− качество и последствия проводимых им работ по контролю действий пользователей при работе в ИСПДн.

С инструкцией ознакомлен _____ «___» _____ 20___г.
(роспись)