Утверждаю

Генеральный директор
ОАО «Нефтеавтоматика»
_____ А.П. Иванов
<____>_____2010г.

Политика защиты персональных данных.

Разработано:

<27> дек. 2010г. _____ И.В. Игумнов

Согласовано:

<__>_____2010г. _____ А.Ю. Вергай
<29> 12 2010г. _____ Э.И. Глушков
<29> 12 2010г. _____ М.Г. Каримов
<__>_____2010г. _____ Д.Н. Дунюшкин
<__>_____2010г. _____ И.Р. Муллануров
<29> 12 2010г. _____ Е.П. Свиридова
<__>_____2010г. _____ И.Д. Кизина
<__>_____2010г. _____ Г.А. Книсс
<29> 12 2010г. Шарапов Е.А. Шарапов

Уфа 2010г.

1. **Введение.** 3
2. **Общие положения.** 3
3. **Цели политики.** 4
4. **Требования к системам защиты персональных данных.** 6
   - **4.1. Системы управления доступом, регистрации и учета.** 6
   - **4.2. Система обеспечения целостности и доступности.** 7
   - **4.3. Система антивирусной защиты.** 7
   - **4.4. Системы межсетевого экранирования.** 8
   - **4.5. Система анализа защищенности.** 8
   - **4.6. Система обнаружения вторжений.** 9
   - **4.7. Система криптографической защиты.** 9
5. **Определение пользователей ИСПДн.** 9
   - **5.1. Администратор ИСПДн.** 9
   - **5.2. Администратор безопасности.** 10
   - **5.3. Системный администратор.** 10
   - **5.4. Оператор АРМ.** 11
   - **5.5. Технический специалист по обслуживанию периферийного оборудования.** 11
   - **5.6. Программист-разработчик ИСПДн.** 11
6. **Требования к персоналу по обеспечению защиты ПДн.** 12
7. **Должностные обязанности пользователей ИСПДн.** 13
8. **Ответственность.** 14

1. Введение.

Настоящая политика определяет цели, принципы и правила обработки персональных данных (далее по тексту ПДн), мониторинг действий над ними, зоны ответственности персонала, осуществляющего обработку, классификацию и уровни защиты ПДн, в рамках Федерального закона о персональных данных №152-ФЗ от 27.06.2006г., Федерального закона №160 от 19.12.2005г. о ратификации конвенции совета Европы, постановления правительства РФ №687 от 15.09.2008, постановления правительства РФ №512 от 6.07.2008г., постановления правительства РФ №781 от 17.11.2007г., методическими документами Роскомнадзора, методическими документами ФСТЭК РФ, методическими документами ФСБ РФ, УК РФ (статьи №137, 140, 272), КОАП РФ (статьи 5.39, 13.11, 13.14) и политикой информационной безопасности предприятия.

2. Общие положения.

В настоящее время, на территории Российской Федерации осуществляется государственное регулирование в области обеспечения безопасности персональных данных. Правовое регулирование вопросов обработки ПДн осуществляется в соответствии с Конституцией РФ и международными договорами РФ, на основании федерального закона №152-ФЗ от 27.07.2006г. о ПДн и принятых во исполнение его положений, нормативно-правовых актов и методических документов.

Основными направлениями деятельности по защите персональных данных являются:

1. Меры, принимаемые для защиты ПДн, относящиеся к сфере деятельности, регулируемой ФСТЭК России:
   - 1.1. Защита ПДн от несанкционированного доступа:
     - 1.1.1. Обеспечение целостности.
     - 1.1.2. Управление доступом.
     - 1.1.3. Межсетевое разграничение доступа.
     - 1.1.4. Антивирусная защита.
     - 1.1.5. Мониторинг и учет деятельности при обработке ПДн.
     - 1.1.6. Анализ защищенности с применением специализированных средств.
   - 1.2. Защита ПДн от утечки по техническим каналам:
     - 1.2.1. Использование сертифицированных технических средств защиты ПДн.
     - 1.2.2. Размещение объектов защиты на максимально возможном расстоянии от границ охраняемой территории.
     - 1.2.3. Обеспечение электромагнитной развязки.

1.2.4. Обеспечение развязки цепей электропитания и заземления.

1.2.5. Размещение трансформаторных подстанций внутри контура защиты.

2. Меры, принимаемые для защиты ПДн, относящиеся к сфере деятельности, регулируемой ФСБ России:

2.1. Применение сертифицированных средств криптографической защиты информации, организация шифрованных каналов связи.

2.2. Применение сигнатурных и аномальных систем обнаружения вторжений.

3. Цели политики.

Основываясь на требованиях законодательства и нормативных документах ФСТЕК и ФСБ по защите ПДн, цели политики защиты персональных данных сводятся к:

1. Разработке материалов проектирования средств защиты информации от несанкционированного доступа к ИСПДн, которые включают в себя:

1.1. Материалы предпроектного исследования:

1.1.1. Определение обрабатываемых ПДн и объектов защиты.

1.1.2. Определение круга лиц, участвующих в обработке ПДн.

1.1.3. Определение ответственности лиц, участвующих в обработке ПДн.

1.1.4. Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей.

1.1.5. Назначение ответственного за безопасность ПДн.

1.1.6. Классификация всех используемых ИСПДн.

1.1.7. Определение контролируемых зон вокруг ИСПДн.

1.1.8. Разработка положения о защите ПДн.

1.1.9. Приведение в соответствие помещений для установки средств ИСПДн, с целью исключения несанкционированного доступа (НСД) лиц, не допущенных к обработке ПДн.

1.1.10. Организация режима контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.

1.1.11. В рамках положения о защите ПДн, разработка схемы обращения ПДн внутри организации.

1.2. Результаты технического проектирования и мероприятия по защите ПДн.

1.2.1. Разработка проекта реализации систем и средств защиты ИСПДН

1.2.2. Разработка проекта по резервному копированию защищаемой информации на твердые носители.

1.2.3. Разработка ОТМ по восстановлению работоспособности технических средств, программного обеспечения и баз данных с подсистем СЗПДн.

1.2.4. Разработка проекта по мониторингу за действиями персонала, процессами информационного обмена внутри ИСПДн и систем обнаружения вторжений и неправомочных действий.

1.2.5. Разработка положения о системе обработки ПДн на бумажных носителях.

1.3. Результаты опытной эксплуатации и итоговых испытаний:

1.3.1. Введение режима защиты ПДн.

1.3.2. Доведение до сведения сотрудников приказа о введении режима защиты ПДн.

1.3.3. Организация обучения сотрудников работе с ПДн и ИСПДн.

1.3.4. Разработка должностных инструкций о порядке обработки ПДн и обеспечении введенного режима защиты.

1.3.5. Разработка инструкций по работе с сетями общего пользования(Internet).

1.3.6. Разработка инструкций о действиях в случае возникновения нештатных ситуаций.

1.3.7. Разработка положения (если возникнет необходимость) о внесении изменений в штатное программное обеспечение элементов ИСПДн.

1.3.8. Организация реестра технических средств, средств защиты ПДн и документации к ним.

2. Разработке эксплуатационной документации, которая включает в себя:

2.1. Акты:

2.1.1. Классификации всех систем ИСПДн.

2.1.2. Внедрения систем единого учета действий пользователей с ПДн.

2.1.3. Внедрения системы управления доступом к ПДн.

2.1.4. Внедрения межсетевого экранирования.

2.1.5. Внедрения антивирусной защиты.

2.1.6. Внедрения систем анализа защищенности.

2.1.7. Внедрения подсистем обнаружения вторжений.

2.1.8. Внедрения систем криптографической защиты.

2.2. Журналы учета:

2.2.1. Журнал внутренних проверок работоспособности систем защиты ИСПДн.

2.2.2. Журнал внесения изменений в ПО защиты ИСПДн. Или обновлений его версий.

2.2.3. Журнал учета внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн.

2.2.4. Журнал учета мероприятий по контролю состояния защиты ПДн.

2.2.5. Журнал учета обращений субъектов ПДн о выполнении их законных прав.

2.2.6. Журнал регистрации внештатных ситуаций и реализаций угроз ПДн.

2.3. Матрица доступа.

2.4. Протоколы испытаний и предписания на эксплуатацию.

3. Внедрению систем защиты персональных данных и подписание актов ввода в опытно-промышленную эксплуатацию систем:
   3.1. Управления доступом.
   3.2. Межсетевого экранирования.
   3.3. Антивирусной защиты.
   3.4. Мониторинга и учета деятельности при обработке ПДн.
   3.5. Анализа защищенности с применением специализированных средств.
4. Выявление и устранение уязвимостей в СЗПДн по результатам опытно-промышленной эксплуатации, уточнение положений и инструкций по эксплуатации ИСПДн и СЗПДн..
5. Ввод ИСПДн и СЗПДн в промышленную эксплуатацию.

4. Требования к системам защиты персональных данных.

СЗПДн организации состоит из следующих систем:

1. управления доступом, регистрации и учета;
2. обеспечения целостности и доступности;
3. антивирусной защиты;
4. межсетевого экранирования;
5. анализа защищенности;
6. обнаружения вторжений;
7. криптографической защиты

Для каждой ИСПДн организации, в зависимости от ее класса, определяемого в Акте классификации, необходим свой набор систем защиты, который детально рассмотрен в Модели угроз безопасности ПДн и в Плане мероприятий по обеспечению защиты ПДн.

4.1. Системы управления доступом, регистрации и учета.

Система управления доступом, регистрации и учета необходима для реализации следующего функционала:

Идентификация и проверка подлинности субъектов доступа при входе в ИСПДн.

Идентификация терминалов, узлов сети, внешних устройств.

Идентификации программ, каталогов, файлов, записей, полей записей.

Регистрации входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки или останова операционной системы.

Регистрация попыток доступа программ, процессов, задач, к защищаемой информации.

Регистрации попыток доступа к терминалам, каналам связи, программам, каталогам, файлам, записям.

Система управления доступом может быть реализована как с помощью штатных средств обработки ПДн: на базе ОС, Active Directory, СУБД, так и с помощью специальных технических средств, осуществляющих дополнительные меры по аутентификации и контролю.

4.2. Система обеспечения целостности и доступности.

Назначение Системы обеспечения целостности и доступности в недопущении нарушения работы программных и аппаратных средств ИСПДн от случайной или намеренной модификации. Система реализуется способом резервного копирования информации с оговоренным сроком восстановления и резервированием аппаратной части основных элементов системы.

4.3. Система антивирусной защиты.

Система антивирусной защиты необходима для обеспечения защиты серверов и АРМ пользователей ИСПДн от вирусных атак и Adware.

Средства антивирусной защиты реализуют следующие функции:

4.3.1. Антивирусный мониторинг в реальном масштабе времени.

4.3.2. Полное антивирусное сканирование системы.

4.3.3. Блокирование активных скриптов.

4.3.4. Автоматическое обновление вирусных сигнатур.

4.3.5. Централизованное управление антивирусным продуктом на серверах и АРМ пользователей.

4.3.6. Централизованное управление доступом пользователя к аппаратным ресурсам АРМ, возможностям запуска тех или иных задач, удаленной

инсталляции/деинсталляции программных продуктов на АРМ пользователя, мониторингу действий пользователя и ведению логов.

4.4. Системы межсетевого экранирования.

Предназначена для реализации следующих функций:

4.4.1. Фильтрации IP-трафика в соответствии с правилами, заранее определенными системным администратором.

4.4.2. Фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.

4.4.3. Логирования информации о всех состоявшихся и не состоявшихся сетевых подключениях.

4.4.4. Логирования информации об изменениях в конфигурации правил.

4.4.5. Аутентификации системного администратора при его запросах на доступ.

4.4.6. Контроля целостности программного обеспечения межсетевого экрана.

4.4.7. Блокирования доступа объекта или субъекта, подлинность которого при аутентификации не подтвердилась.

4.4.8. Блокирования фишинга, спуффигна, DoS атак.

4.4.9. Контроля за сетевой активностью внутренних и внешних приложений для обнаружения сетевых атак.

Система реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, в соответствии с требуемым классом защиты ИСПДн.

4.5. Система анализа защищенности.

Система анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с:

4.5.1. Неправильной конфигурацией межсетевых экранов.

4.5.2. Неправильной конфигурацией серверов.

4.5.3. Наличием лишних открытых портов без видимых на то причин.

4.5.4. Ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Системы может быть реализована программными и программно-аппаратными средствами.

4.6. Система обнаружения вторжений.

Система обнаружения вторжений, служит для выявления несанкционированной сетевой активности как снаружи защищаемого периметра, так и изнутри. Система анализирует весь трафик сети и выдает предупреждения администратору, в случае, если какой-либо объект начинает генерировать сетевой трафик, не разрешенный параметрами безопасности.

Система может быть реализована программными и программно-аппаратными средствами.

4.7. Система криптографической защиты.

Система криптографической защиты служит для предотвращения несанкционированного доступа к ПДн, передаваемым по каналам связи сетей общего пользования и (или) международного обмена. В ряде случаев, шифрование может применяться и для передачи ПДн внутри охраняемого периметра, если, согласно модели угроз, существует вероятность утечки информации в силу тех или иных обстоятельств.

Система реализуется внедрением аппаратных или программных криптографических средств.

5. Определение пользователей ИСПДн.

Все пользователи ИСПДн организации делятся на администраторов ИСПДн, системных администраторов, администраторов безопасности, операторов АРМ, технических специалистов по обслуживанию оборудования, разработчиков ИСПДн.

Разбиение пользователей на группы рассматривается в Положении о разграничении прав доступа к обрабатываемым персональным данным.

5.1. Администратор ИСПДн.

Администратор ИСПДн, сотрудник организации, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает управление доступом в ИСПДн конечного пользователя (Оператора АРМ).

Администратор ИСПДн обладает:

4.5.1. Полной информацией о системном и прикладном программном обеспечении ИСПДн.

4.5.2. Полной информацией о технических средствах и конфигурации ИСПДн.

4.5.3. Правами конфигурирования и административной настройки технических средств ИСПДн.

4.5.4. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.

5.2. Администратор безопасности.

Администратор безопасности, сотрудник организации, ответственный за функционирование СЗПДн.

Администратор безопасности обладает:

1. Правами Администратора ИСПДн;
2. Полной информацией об ИСПДн;
3. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
4. Не имеет прав доступа к конфигурированию технических средств сети.

Администратор безопасности уполномочен:

1. Администрировать средства криптозащиты информации, межсетевые экраны и системы обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн.
2. Осуществлять аудит средств защиты.
3. Устанавливать доверительные отношения своей защищенной сети с сетями филиалов.

5.3. Системный администратор.

Системный администратор, сотрудник Учреждения, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления системами обработки данных.

Системный администратор обладает:

5.3.1. Частью информации о системном и прикладном программном обеспечении ИСПДн.

5.3.2. Частью информации о технических средствах и конфигурации ИСПДн.

5.3.3. Имеет физический доступ к техническим средствам обработки информации и средствам защиты, включая обслуживание и настройку административной, серверной и клиентской компонент.

5.3.4. Знает, по меньшей мере, одно легальное имя доступа.

5.4. Оператор АРМ.

Оператор АРМ, сотрудник организации, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает:

5.4.1. Всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству ПДн.

5.4.2. Располагает конфиденциальными данными, к которым имеет доступ.

5.5. Технический специалист по обслуживанию периферийного оборудования.

Технический специалист по обслуживанию, сотрудник организации, осуществляет обслуживание и настройку оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает:

5.5.1. Частью информации о системном и прикладном программном обеспечении ИСПДн.

5.5.2. Частью информации о технических средствах и конфигурации ИСПДн.

5.5.3. Знает, по меньшей мере, одно легальное имя доступа в ОС.

5.6. Программист-разработчик ИСПДн.

Разработчики прикладного программного обеспечения обеспечивают его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники организации, так и сотрудники сторонних организаций.

Разработчик прикладного ПО обладает:

Информацией об алгоритмах и программах обработки информации в ИСПДн.

Возможностью внесения ошибок, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения.

Может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

6. Требования к персоналу по обеспечению защиты ПДн.

Все пользователи ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к конфиденциальной информации.

При приеме на работу, сотрудник проходит инструктаж у начальника отдела безопасности, начальника департамента информационной безопасности. Начальник подразделения, в которое принимается сотрудник, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен с Политикой информационной безопасности и настоящей Политикой защиты ПДн, а также с инструкциями по работе с элементами ИСПДн и СЗПДн.

Сотрудники Учреждения, использующие технические средства аутентификации, должны обеспечивать сохранность ключей и паролей и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за их сохранность.

Сотрудники Учреждения должны следовать установленным процедурам при использовании паролей, при отсутствии технических средства аутентификации.

Сотрудники Учреждения должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Учреждения, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Учреждения обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки или выключения.

Сотрудники Учреждения должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

7. Должностные обязанности пользователей ИСПДн.

Должностные обязанности пользователей ИСПДн детально рассматриваются в следующих документах:

7.1. Инструкция администратора ИСПДн.

7.2. Инструкция администратора безопасности ИСПДн.

7.3. Инструкция системного администратора.

7.4. Инструкция Оператора ИСПДн.

7.5. Инструкция технического специалиста по обслуживанию оборудования.

7.6. Инструкция оператора при возникновении внештатных ситуаций.

8. Ответственность.

Политика защиты персональных данных формируется Советом по вопросам информационной безопасности и утверждается Генеральным директором предприятия.

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ "О персональных данных" лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

При нарушениях сотрудниками организации настоящей Политики защиты ПДн и правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

Требования нормативных документов по защите информации, сведения об ответственности сотрудников и руководителей подразделений за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки, должны быть отражены в Положениях о подразделениях, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников организации.

Руководство организации берет на себя ответственность за реализацию требований политики защиты персональных данных в рамках законодательства РФ, обеспечивая ее поддержку и понимание среди сотрудников и партнеров организации.