

План мероприятий по обеспечению безопасности ПДн

Мероприятие	Периодичность выполнения	Результат
1 этап (выполняют все, кто обрабатывает ПД) (срок до 10 мая 2010 года)		
Организационные мероприятия		
Создание постоянно действующей комиссии по защите информации	Разовое	Приказ о комиссии по информационной безопасности
Назначение ответственного за безопасность ПДн	Разовое	Приказ о подразделении по защите персональных данных или Приказ об ответственном за защиту персональных данных
Определение контролируемой зоны	Разовое	Приказ о контролируемой зоне
Первичная внутренняя проверка		Приказ о проведении внутренней проверки
Определение перечня ИСПДн	Разовое	Отчет о результатах проведения внутренней проверки
Определение обрабатываемых ПДн и объектов защиты, целесообразность обработки ПДн, правовые основания для обработки ПДн	Разовое	Отчет о результатах проведения внутренней проверки
Определение круга лиц, участвующих в обработке ПДн	Разовое	Отчет о результатах проведения внутренней проверки
Определение ответственности лиц, участвующих в обработке	Разовое	Отчет о результатах проведения внутренней проверки
Определение прав ограничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое	Отчет о результатах проведения внутренней проверки
Физические мероприятия		
Установление контролируемой зоны вокруг ИСПДн	Разовое	
Организация постов охраны для пропуска в контролируемую зону	Разовое	
Установка жалюзи, штор на окнах или другие меры, исключающие несанкционированный доступ к ПД снаружи здания	Разовое	
Установка решеток на окнах первого и последнего этажа здания или средств оповещения при проникновении (1класс ИСПДн)	Разовое	
Технические (аппаратные и программные) мероприятия		
Внедрение антивирусной защиты	Разовое	
Контролирующие мероприятия		
Создание журнала внутренних проверок и поддержание его в актуальном состоянии	Разовое	Ведение журнала
Контроль соблюдения режима обработки ПДн	Еженедельно	
Контроль соблюдения режима защиты	Еженедельно	
Контроль выполнения антивирусной защиты	Еженедельно	
2 этап (выполняют все, кто обрабатывает ПД) (срок до 1 июня 2010 года)		
Организационные мероприятия		
Классификация всех выявленных ИСПДн	Разовое	Приказ о проведении классификации систем обработки ПДн, Акты классификации ИСПДн
Принятие документов регламентирующих обработку ПДн	Разовое	Приказ об утверждении эксплуатационной документации ИСПДн, Приказ о назначении администратора ИСПДн, Приказ о назначении администратора безопасности ИСПДн, Положение о Порядке резервирования и восстановления

Подача уведомления об обработке персональных данных		работоспособности ТС и ПО, баз данных и СЗИ
Выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц, не Допущенных к обработке ПДн	Разовое	Направить уведомления об обработке персональных данных в соответствующий территориальный орган Роскомнадзора по месту регистрации оператора
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	Разовое	
Организация порядка резервного копирования защищаемой информации на твердые носители	Разовое	
Организация порядка восстановления работоспособности технических средств, ПО, баз данных с подсистем СЗИ ПДн	Разовое	
Создание журнала учета обращений субъектов ПДн	Разовое	Журнал учета обращений субъектов персональных данных о соблюдении их законных прав, при обработке персональных данных в ИСПДн
Контролирующие мероприятия		
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	
3 этап		
(Мероприятия осуществляются в зависимости от категории ПД, класса системы обработки ПДн и наличия передачи ПДн третьим лицам. Желательна разработка документации и проведение мероприятий организацией, имеющей лицензию в области защиты ПД).		
Организационные мероприятия		
Первичный анализ актуальности угроз безопасности персональным данным (УБПДн)	Разовое	
Введение в действие инструкции по порядку формирования, распределения и применения паролей	Разовое	Инструкция по порядку формирования, распределения и применения паролей
Организация информирования и обучения сотрудников о порядке обработки ПДн	Разовое	
Организация информирования и обучения сотрудников о введённом режиме защиты ПДн	Разовое	
Разработка должностных инструкций о порядке обработки ПДн и обеспечении введённого режима защиты	Разовое	Должностные инструкции о порядке обработки ПДн и обеспечении введённого режима защиты
Разработка инструкций о порядке работы при подключении к сетям общего пользования и (или) международного обмена	Разовое	Инструкция о порядке работы при подключении к сетям общего пользования и (или) международного обмена
Разработка инструкций о действии в случае возникновения внештатных ситуаций	Разовое	Инструкция пользователя по обеспечению безопасности обработки ПД, при возникновении внештатных ситуаций
Разработка положений о внесении изменений в штатное программное обеспечение элементов ИСПДн	Разовое	Положение о внесении изменений в штатное программное обеспечение элементов ИСПДн
Разработка положений о порядке внесения изменений в программное обеспечение собственной разработки или штатное ПО специально дорабатываемое собственными разработчиками или сторонними организациями.	Разовое	Положение о порядке внесения изменений в программное обеспечение
Положение должно включать в себя техническое задание на изменения, технический проект, приемо-сдаточные испытания, акт о		

введении в эксплуатацию.			
Организация перечня по учету технических средств и средств защиты, а так же документации к ним	Разовое	Перечень по учету технических средств и средств защиты, а так же документации к ним	
Физические мероприятия			
Внедрение технической системы контроля доступа в контролируемую зону и помещения (по электронным пропускам, токenu, биометрическим данным и т.п.)	Разовое		
Внедрение технической системы контроля доступа к элементам ИСПДн (по электронным пропускам, токenu, биометрическим данным и т.п.)	Разовое		
Внедрение видеонаблюдения	Разовое		
Установка дверей на входе в помещения с аппаратными средствами ИСПДн	Разовое		
Установка замков на дверях в помещениях с аппаратными средствами ИСПДн	Разовое		
Установка систем пожаротушения в помещениях, где расположены элементы ИСПДн	Разовое		
Установка систем кондиционирования в помещениях, где расположены аппаратные средства ИСПДн	Разовое		
Установка систем бесперебойного питания на ключевые элементы ИСПДн	Разовое		
Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн	Разовое		
Технические (аппаратные и программные) мероприятия			
Внедрение единого хранилища зарегистрированных действий пользователей с ПДн	Разовое		
Внедрение специальной подсистемы управления доступом, регистрации и учета (НАЗВАНИЕ)	Разовое		
Внедрение межсетевого экранирования (НАЗВАНИЕ)	Разовое		
Внедрение подсистемы анализа защищенности (НАЗВАНИЕ)	Разовое		
Внедрение подсистемы обнаружения вторжений (НАЗВАНИЕ)	Разовое		
Внедрение криптографической защиты (НАЗВАНИЕ)	Разовое		
Контролирующие мероприятия			
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) междугородного обмена	Еженедельно		
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно		
Контроль за обеспечением резервного копирования	Ежемесячно		
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно		
Поддержание в актуальном состоянии нормативно-организационных	Ежемесячно		

Документов
Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями.

Ежемесячно

В План включены следующие категории мероприятий:

- организационные (административные);
- физические;
- технические (аппаратные и программные);
- контролирующие.