Иван Трещев

Организационное и правовое обеспечение информационной безопасности

для студентов и специалистов

Иван Трещев

Организационное и правовое обеспечение информационной безопасности. Для студентов и специалистов

«Издательские решения»

Трещев И. А.

Организационное и правовое обеспечение информационной безопасности. Для студентов и специалистов / И. А. Трещев — «Издательские решения»,

ISBN 978-5-44-964478-7

Данная книга может быть рассмотрена в качестве учебного пособия при организации соответствующих курсов. Изложенный в ней материал будет полезен при проведении занятий в интерактивной форме, организации деловых и ролевых игр, проектном обучении.

ISBN 978-5-44-964478-7

Содержание

Организационное и правовое обеспечение информационной безопасности Для студентов и специалистов

Иван Андреевич Трещев

«Если вы уверены, что написанная вами инструкция по правилам выбора паролей не может быть понята неправильно, всегда найдется сотрудник, который поймет ее именно так» – один из законов Мерфи.

Разработка документов Артем Александрович Богачев
Участие в разработке документов Анастасия Сергеевна Ватолина

ISBN 978-5-4496-4478-7
Создано в интеллектуальной издательской системе Ridero

Введение

Система защиты информации многогранна. Она включает в себя как вопросы защиты от утечки по техническим каналам, защиты от несанкционированного доступа, так и вопросы организационного и правового обеспечения, вопросы физической защиты и многое другое.

Данная книга содержит перечень документов, которые по мнению автора необходимы для любого предприятия. Документарное обеспечение упорядычивает работу по организации системы защиты информации. В случае отсутствия инструкции работодатель не вправе требовать от сотрудников их исполнения, поэтому к разработке документов следует отнестись серьезно.

Любые совпадения имен и фамилий являются случайными. Наименования и торговые марки использованные в книге взяты из открытых источников и являются собственностью их обладателей.

Книга построена на основе курса по организационному и правовому обеспечению информационной безопасности, который автор вот уже на протяжении более 5 лет использует при подготовке специалистов по защите информации.

Приведенные документы можно условно разделить на 3 категории:

1. Роскомнадзор – в области обеспечения исполнения законодательства по защите информации.
2. ФСТЭК – в области защиты информации некриптографическими средствами.
3. ФСБ – в области защиты информации с использованием средств криптографической защиты.

Практические занятия по дисциплине «Организационное и правовое обеспечение информационной безопасности» проводятся в интерактивной форме – форме деловых игр, отражающих проведение реальных аудиторских проверок «регуляторов». Всего в семестре устанавливается несколько контрольных точек по неделям:

2-я неделя – подача уведомления в «Роскомнадзор» (передача уведомления преподавателю).

5-я неделя – аудиторская проверка «Роскомнадзора».

10-я неделя – аудиторская проверка «ФСТЭК РФ».

15-я неделя – аудиторская проверка «ФСБ РФ».

Схемы контролируемой зоны, расположения средств вычислительной техники, средств защиты, электропитания и заземления необходимо согласовывать с преподавателем.

Ко второй неделе необходимо подготовить уведомление об обработке персональных данных. Пример уведомления приведен в книге далее, к 5-ой неделе комплект документов в соответствии со спецификацией приведенной далее для Роскомнадзора, к 10 неделе комплект документов в соответствии со спецификацией приведенной далее для ФСТЭК, к 15 неделе комплект документов в соответствии со спецификацией приведенной в далее для ФСБ. В каждом варианте обязательно в организации обеспечением информационной безопасности которой занимается студент ведется автоматизированная обработка более чем 100 000 субъектов персональных данных. Обязательно есть необходимость использовать технические средства защиты информации от утечек по техническим каналам, средства защиты от несанкционированного доступа, средства криптографической защиты информации. Ответственным за обеспечение информационной безопасности в организации назначается студент. Нужно учесть, что если количество ИСПДн в организации больше одной, то некоторые документы представляются по каждой ИСПДн в отдельности. Спецификации подаваемых документов подлежат обязательному согласованию с преподавателем.

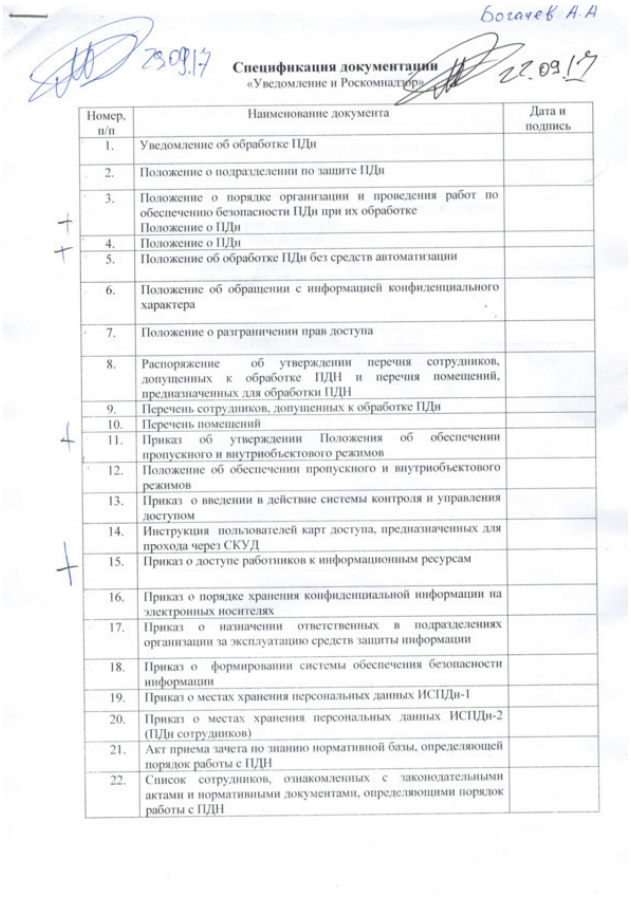
Примерный перечень средств защиты от НСД
1 Secret Net 6.5
2 Dallas Lock 7.7
3 Accord
4 Аура
5 Страж NT
Перечень средств криптографической защиты
111 АПКШ Континент клиентская часть Континент АП.
112 ФПСУ/IP клиентская часть ФПСУ/IP клиент.
113 CheckPoint Connectra клиентская часть Connectra client.
114VipNet HW 1000 клиентская часть VipNet Client.
А) Соната, ЛГШ-1000, Корунд.
Б) Барон, Вето-М, Прокруст 2000

Варианты заданий

№	Наименование организации	ФИО Руководителя	Средства защиты от НСД	Криптографические средства	Количество ИС. ПДн	Технические средства защиты
1	Медико-диагностический центр	Скорая Снежана Сергеевна	1	111	1	А
2	Аппарат Президента	Путин Владимир Владимирович	2	112	2	Б
3	Налоговая	Денежная Виктория Павловна	3	113	1	А
4	Пенсионный фонд	Бабудина Ирина Витальевна	4	111	2	Б
5	КнАГТУ	Ученый Александр Иванович	5	112	1	А
6	Архив библиотеки	Белых Сергей Сергеевич	1	113	2	Б
7	Администрация города	Медведев Илья Игоревич	2	111	1	А
8	Амурский судостроительный завод	Шорохов Сергей Иванович	3	114	2	Б
9	Отдел социальной помощи населению	Добрый Сергей Иванович	4	113	1	А
10	Завод Вымпел	Быстрый	5	111	2	Б

РОСКОМНАДЗОР

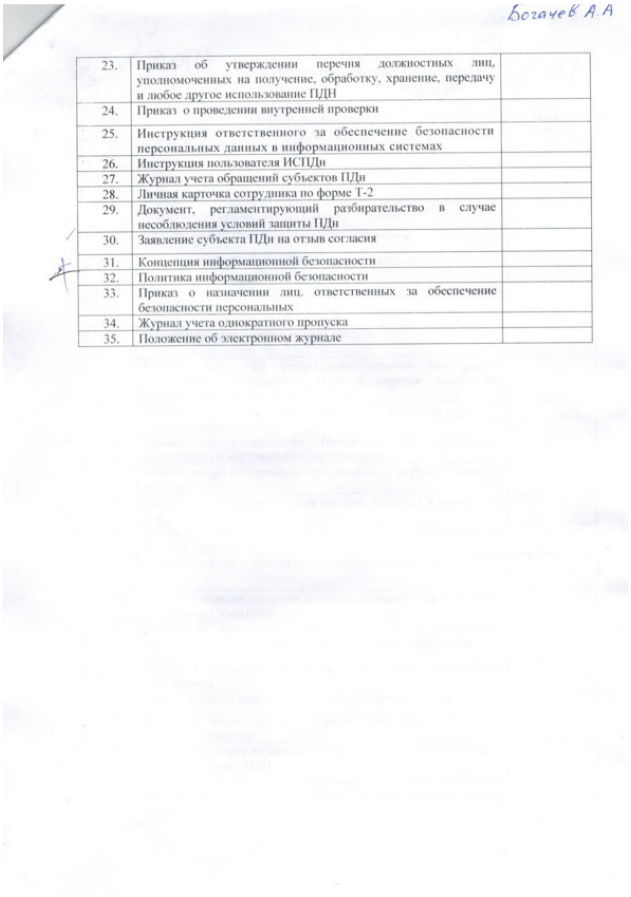
Спецификация



Богачев А.А

Спецификация документации
«Уведомление и Роскомнадзор»

Номер, п/п	Наименование документа	Дата и подпись
1.	Уведомление об обработке ПДн	
2.	Положение о подразделении по защите ПДн	
3.	Положение о порядке организации и проведения работ по обеспечению безопасности ПДн при их обработке Положение о ПДн	
4.	Положение о ПДн	
5.	Положение об обработке ПДн без средств автоматизации	
6.	Положение об обращении с информацией конфиденциального характера	
7.	Положение о разграничении прав доступа	
8.	Распоряжение об утверждении перечня сотрудников, допущенных к обработке ПДН и перечня помещений, предназначенных для обработки ПДН	
9.	Перечень сотрудников, допущенных к обработке ПДн	
10.	Перечень помещений	
11.	Приказ об утверждении Положения об обеспечении пропускного и внутриобъектового режимов	
12.	Положение об обеспечении пропускного и внутриобъектового режимов	
13.	Приказ о введении в действие системы контроля и управления доступом	
14.	Инструкция пользователей карт доступа, предназначенных для прохода через СКУД	
15.	Приказ о доступе работников к информационным ресурсам	
16.	Приказ о порядке хранения конфиденциальной информации на электронных носителях	
17.	Приказ о назначении ответственных в подразделениях организации за эксплуатацию средств защиты информации	
18.	Приказ о формировании системы обеспечения безопасности информации	
19.	Приказ о местах хранения персональных данных ИСПДн-1	
20.	Приказ о местах хранения персональных данных ИСПДн-2 (ПДн сотрудников)	
21.	Акт приема зачета по знанию нормативной базы, определяющей порядок работы с ПДН	
22.	Список сотрудников, ознакомленных с законодательными актами и нормативными документами, определяющими порядок работы с ПДН	



Богачев А.А

23.	Приказ об утверждении перечня должностных лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование ПДН	
24.	Приказ о проведении внутренней проверки	
25.	Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах	
26.	Инструкция пользователя ИСПДн	
27.	Журнал учета обращений субъектов ПДн	
28.	Личная карточка сотрудника по форме Т-2	
29.	Документ, регламентирующий разбирательство в случае несоблюдения условий защиты ПДн	
30.	Заявление субъекта ПДн на отзыв согласия	
31.	Концепция информационной безопасности	
32.	Политика информационной безопасности	
33.	Приказ о назначении лиц, ответственных за обеспечение безопасности персональных	
34.	Журнал учета однократного пропуска	
35.	Положение об электронном журнале	

1. Уведомление

Исх. № ____ от «___» _____ 20__ г. Экз. № __

Руководителю Управления

Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций

Дальневосточное управление

О. В. Шахматовой

(Управление Роскомнадзора по Дальневосточному Федеральному округу)

ул. Ленина, д. 4 г. Хабаровск, 681000

Уведомление

об обработке (о намерении осуществлять обработку) персональных данных

Тип оператора: Государственный орган

Первичная профсоюзная организация администрации президента Российской Федерации

_____

(полное и сокращенное наименования оператора)

пл. Старая, д. 4, Москва, 101000

_____

(адрес местонахождения и почтовый адрес Оператора)

ИНН: 7710155192 КПП: 771001001 ОГРН: 1037739208870 ОКВЭД: 91.20 ОКПО: 584673?6

ОКФС: 52 ОКОГУ: 4220003 ОКОПФ: 20202

руководствуясь**:** Конституцией Российской Федерации, Налоговым кодексом РФ, Федеральным законом «О государственной гражданской службе Российской Федерации» от 27.07.2004 №79- ФЗ, Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ, Указом Президента Российской Федерации «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» от 30.05.2005 №609, Указом Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 06.03.97 №188.

_____

(правовое основание обработки персональных данных)

с целью: регистрации сведений субъектов персональных данных, необходимых для осуществления деятельности в области государственного управления; персональных данных сотрудников (работников) и обращающихся лиц, сведений об профессиональной служебной деятельности работников.

_____

(цель обработки персональных данных)

осуществляет обработку следующих категорий персональных данных:

сотрудники – фамилия, имя, отчество; год, месяц, дата и место рождения; адрес места прописки; семейное, социальное, имущественное положение; образование; профессия; доходы, ИНН, паспортные данные, данные медицинского полиса, страхового свидетельства, а также специальные категории персональных данных – состояние здоровья, биометрические персональные данные – отпечатки пальцев; обращающиеся граждане – фамилия, имя, отчество; год, месяц, дата и место рождения; адрес места прописки, ИНН, паспортные данные.

_____

(категории персональных данных)

принадлежащих: работникам, лицам, делающим обращение в организацию, лицам, участвующих в конкурсах на замещение вакантных должностей, лицам, участвующих в конкурсе на зачисление в кадровый резерв, уволенным работникам, лицам, выполняющих поставки, работы, услуги по договорам, посетителям.

(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных осуществляется:

способом смешанной обработки – на бумажных, на электронных носителях и в ИСПДн с передачей по внутренней сети оператора, с передачей в сеть общего пользования Интернет;

операции с персональными данными: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение, уничтожение персональных данных.

(перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных)

Для обеспечения безопасности персональных данных принимаются следующие меры:

Ответственные должностные лица, их полномочия, обязанности и ответственность определены Положением по вопросам обработки персональных данных, осуществляемой без использования средств автоматизации, Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, Приказом о назначении ответственных за обеспечение безопасности персональных данных в ППО администрации президента.

Работники, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

Класс информационной системы персональных данных оператора: К1.

Для защиты персональных данных используются:

комплекс ФПСU-IP/Клиент, регистрационный номер СФ/124—3165, производителей ООО «АМИКОН», уровень криптографической защиты персональных данных КС1, уровень специальной защиты от утечки по каналам побочных излучений и наводок КС, уровень защиты от несанкционированного доступа АК3;

средства обеспечения безопасности: пароли, программно-аппаратные средства защиты информации: «Dallas Lock 7.7», «АМИКОН», «Прокруст 2000», пространственное зашумление: генератор вибро-акустический «Барон»; генератор радиоэлектронный «Вето-М», ключи доступа (применение следующих основных методов и способов защиты информации: а) управление доступом; б) регистрация и учет; в) обеспечение целостности; а также – анализ защищенности; использование средств обнаружения вторжений; защита информации от утечки по техническим каналам, защита информации от несанкционированных действий [НСД], использование межсетевых экранов, контроль отсутствия недекларированных возможностей [НДВ] программного обеспечения средств защиты информации [СЗИ] – при передаче персональных данных с использованием сети Интернет).

Ответственный за организацию обработки персональных данных: Богачев Артем Алексеевич; Тел.: +7 (914) -421-18-81; ул. Ленина, д. 60; 681010, г. Комсомольск-на-Амуре; artem@mail.ru

---

(Описание мер, предусмотренных статьями 18^1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименование этих средств); (Ф.И.О. физического лица или наименование юридического

лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных: Трансграничная передача персональных данных в процессе их обработки не осуществляется.

Сведения об обеспечении безопасности персональных данных:

На основании модели угроз безопасности информации (частной модели угроз безопасности персональных данных) разработана система защиты информации (СЗИ).

Хранение сведений организовано на электронных носителях (в ИСПДн) с использованием средств обеспечения безопасности, на бумажных носителях – в сейфах (шкафах исключающих несанкционированный доступ).

_____

(сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленные Правительством Российской Федерации)

Дата начала обработки персональных данных: 15.09.2017г. (число, месяц, год)

Срок или условия прекращения обработки персональных данных: бессрочно

Руководитель _____ Путин Владимир Владимирович

(должность) (подпись) (Ф.И.О.)

«15» сентября 2017 г.

2.Положение о подразделении

УТВЕРЖДАЮ
Начальник ППО «Администрация президента»
по г. Москва
В. В. Путин
от «15» сентября 2017 г.
№ _____
Положение о подразделении по защите персональных данных
Комсомольск-на-Амуре
2017
Приказ
«15» сентября 2017г.
Г г. Комсомольск-на-Амуре
№1111

О проведении работ по защите персональных данных в первичной профсоюзной организации «Администрация президента»

В целях исполнения Федерального закона №152-ФЗ от 27 июля 2006 года «О персональных данных» в государственных органах:

П Р И К А З Ы В А Ю:

1) Назначить отдел информационных технологий ответственным за обеспечение защиты персональных данных, во главе с начальником отдела информационных технологий.

2) Осуществлять режим защиты персональных данных на основании принципов и положений:

а) Концепции информационной безопасности.

б) Политики информационной безопасности.

3) Осуществлять режим защиты персональных данных в отношении данных перечисленных в Перечне персональных данных, подлежащих защите.

4) Провести внутреннюю проверку, в срок до 2017 г., на предмет:

а) Классификации информационных систем обработки данных.

б) Определения режима обработки персональных данных в информационной системе.

в) Установления круга лиц участвующих в обработке персональных данных.

г) Выявления угроз безопасности персональных данных.

5) Разработать и внедрить:

а) План мероприятий по обеспечению защиты персональных данных.

б) Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним.

в) План внутренних проверок.

г) Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

д) Инструкцию администратора безопасности информационных системах персональных данных.

е) Инструкцию пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций.

6) Контроль за исполнением настоящего приказа возложить на начальника отдела безопасности.

Путин В. В. _____
(подпись)

3.Положение о порядке организации и проведения работ по обеспечению безопасности ПДн

Приложение №1
УТВЕРЖДЕНО
Приказом ППО «Администрация президента»
по г. Москва
от «15» сентября 2017 г.
№ _____
ПОЛОЖЕНИЕ
о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в первичной профсоюзной организации «Администрация президента» по г. Москва
Комсомольск-на-Амуре
2017
Оглавление

1. Основные понятия и сокращения

В настоящем Положении используются следующие основные понятия и сокращения:

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор АС – лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

Администратор безопасности АС – лицо, ответственное за защиту АС от несанкционированного доступа к информации.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа (ВП) – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ к персональным данным – возможность получения персональных данных и их использования.

Защита от несанкционированного доступа – предотвращение или существенное затруднение несанкционированного доступа.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов.

Контролируемая зона (КЗ) – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально – распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Недекларированные возможности (НДВ) – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ {несанкционированные действия) (НСД) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим техническим характеристикам и функциональному предназначению.

Несанкционированный доступ к персональным данным (несанкционированные действия), (НСД) – доступ к персональным данным или действия с персональными данными, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, вероисповедание, национальность, другая информация.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь ИСПДн – лицо, участвующее в функционировании ИСПДн или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить персональные данные или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие (ПМВ) – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ

Ресурс информационной системы персональных данных – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы персональных данных.

Санкционированный доступ к персональным данным – доступ к персональным данным, не нарушающий правила разграничения доступа.

Средства вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Система защиты информации – совокупность органов и (или) исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Система защиты персональных данных (СЗПДн) – комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности ПДн в ИСПДн.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа

Технический канал утечки информации – совокупность носителя персональных данных (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается информация, содержащая персональные данные.

Технические средства информационной системы персональных данных (ТСИСПДн) – средства вычислительной техники, информационновычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео-и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, приложения и т. п.), средства защиты информации.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации, содержащей персональные данные, по техническим каналам – неконтролируемое распространение персональных данных от носителя персональных данных через физическую среду до технического средства, осуществляющего перехват информации, содержащей персональные данные.

Целостность информации, содержащей персональные данные – способность средства вычислительной техники или информационной системы персональных данных обеспечивать неизменность информации, содержащей персональные данные, в условиях случайного и/или преднамеренного искажения (разрушения).

2. Общие положения

2.1. Положение о порядке организации и проведения работ по обеспечению безопасности ПДн при их обработке в Администрации президента России по г. Комсомольску-на-Амуре Хабаровского края (далее – Положение) относится к основополагающим документам, определяющим общие принципы организации работ по информационной безопасно-

сти ПДн в организации. Положение разработано в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ, постановлением Правительства РФ от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности ПДн при их обработке в ИСПДн», постановлением Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»; «Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», утвержденной ФСТЭК России 14.02.08, «Базовой моделью угроз безопасности ПДн при их обработке в ИСПДн», утвержденной ФСТЭК России 15.02.08; Приказом ФСТЭК России от 05.02.2010 №58 (зарегистрированным в Минюсте России 19.02.2010 №16456) «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» и другими нормативными документами и определяет содержание и порядок осуществления мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн Администрации президента России по г. Комсомольску-на-Амуре Хабаровского края (далее – Организация), представляющих собой совокупность ПДн, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации.

2.2. Организация и проведение работ по обеспечению безопасности информации, содержащей ПДн, на объекте информатизации Организации проводится на основании законодательных и нормативных актов Российской Федерации в области защиты информации и настоящего Положения. Безопасность ПДн при их обработке в ИСПДн достигается путем исключения НСД, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

2.3. Требования настоящего Положения являются обязательными для исполнения в Организации, а также организациями, учреждениями и предприятиями, выполняющими работы по защите информации в Организации.

2.4. Положение определяет порядок организации и проведения работ по защите информации, содержащей ПДн, на объект информатизации как в период их создания, так и в процессе повседневной эксплуатации.

2.5. Принимаемые меры по защите информации на объекте информатизации должны обеспечивать выполнение действующих требований и норм по защите информации.

При обработке ПДн в ИСПДн должно быть обеспечено:

– проведение мероприятий, направленных на предотвращение НСД к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

– своевременное обнаружение фактов НСД к ПДн;

– недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

– возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;

– постоянный контроль за обеспечением уровня защищенности ПДн.

2.6. Разработка мер и обеспечение защиты информации на объекте информатизации осуществляются отделом безопасности Организации или ответственным за защиту информации работником.

Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью СЗПДн, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения НСД, утечки информации, содержащей ПДн, по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в ИСПДн информационные технологии.

Для обеспечения безопасности ПДн при обработке в ИСПДн осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Методы и способы защиты ПДн в ИСПДн устанавливаются ФСТЭК России и ФСБ России в пределах их полномочий.

Разработка мер защиты информации может осуществляться также сторонними организациями, имеющими лицензии ФСТЭК России и ФСБ России на право проведения соответствующих работ.

Достаточность принятых мер по обеспечению безопасности ПДн при их обработке в ИСПДн оценивается при проведении государственного контроля и надзора.

Согласование планируемых мер, контроль выполнения работ на местах, соответствия принятых мер и проводимых мероприятий по защите информации действующим требованиям и нормам производит отдел безопасности или администратор информационной безопасности.

2.7. Объект информатизации Организации должен соответствовать требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

Размещение ИСПДн и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и средств защиты ПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

2.8. Защита информации организуется в соответствии с действующими нормативными документами ФСТЭК России.

Мероприятия по обеспечению безопасности ПДн формулируются в зависимости от класса ИСПДн с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства. Ответственность за общее состояние и организацию работ по созданию и эксплуатации объекта информатизации возлагается на начальника Организации. Ответственность за обеспечение требований по защите информации, циркулирующей на объекте информатизации, возлагается на начальников структурных подразделений организации, эксплуатирующих объект информатизации.

2.9. Контроль выполнения требований настоящего Положения возлагается на начальника Организации.

2.10. Финансирование мероприятий по защите информации предусматривается сметами организации на планируемый год. При этом:

– расходы по защите информации при эксплуатации существующих помещений, технических систем и средств включаются в стоимость их содержания;

– затраты, связанные с защитой информации в создаваемых информационновычислительных и других технических системах, предусматриваются в стоимости создания и развития этих систем;

– расходы по защите информации при ремонте и реконструкции помещений предусматриваются в стоимости этих работ.

2.11. Настоящее положение не распространяется на ИСПДн, обрабатывающие ПДн, отнесенные в установленном порядке к сведениям, составляющим государственную тайну.

3.Классификация информационных систем персональных данных

3.1. Классификация ИСПДн в Организации осуществляется с учетом категорий и объема накапливаемых, обрабатываемых и распределяемых с их использованием ПДн с целью установления методов и способов защиты, необходимых для обеспечения безопасности ПДн.

3.2. Классификация ИСПДн проводится на этапе их создания или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем).

3.3. Состав, функциональное содержание методов и средств защиты зависит от вида и степени ущерба, возникающего вследствие реализации выявленных угроз безопасности ПДн. При этом ущерб возникает за счет неправомерного или случайного уничтожения, изменения, блокирования, копирования, распространения ПДн или от иных неправомерных действий с ними. В зависимости от объекта, причинение ущерба которому вызывается неправомерными действиями с ПДн, рассматриваются два вида ущерба: непосредственный и опосредованный.

3.4. Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту ПДн. Он возникает за счет незаконного использования (в том числе распространения) ПДн или за счет несанкционированной модификации этих данных и может проявляться в виде:

– незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта;

– потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием ПДн;

– нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь путем осуществления контактов с ним по различным поводам без его на то желания (например – рассылка персонифицированных рекламных предложений и т.п.).

3.5. Опосредованный ущерб связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности экономических, политических, военных, медицинских, правоохранительных, социальных, кредитно-финансовых и иных государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с ПДн.

3.6. Классификация ИСПДн проводится комиссией, назначаемой начальником Организации, в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. N 55/86/20, и иными руководящими документами по защите ПДн.

3.7. Проведение классификации ИСПДн включает в себя следующие этапы:

– сбор и анализ исходных данных по ИСПДн;

– присвоение ИСПДн соответствующего класса и его документальное оформление.

3.8. При проведении классификации ИСПДн комиссией учитываются следующие исходные данные:

– категория обрабатываемых ПДн в ИСПДн;

– объем обрабатываемых ПДн (количество субъектов ПДн, ПДн которых обрабатываются в ИСПДн);

– заданные характеристики безопасности ПДн, обрабатываемых в ИСПДн;

– структура ИСПДн;

– наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена;

– режим обработки ПДн;

– режим разграничения прав доступа к ИСПДн;

– местонахождение технических средств ИСПДн.

3.9. В случае выделения в составе ИСПДн подсистем, каждая из которых является ИСПДн, ИСПДн в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

3.10. Результаты классификации ИСПДн оформляются актом, подписанными членами комиссии, и утверждается начальником Организации.

3.11. Класс ИСПДн может быть пересмотрен:

– на основе проведенных комиссией анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений конкретной ИСПДн;

– по результатам мероприятий по контролю и надзору уполномоченными органами за выполнением требований по обеспечению безопасности ПДн при их обработке в ИСПДн.

4. Основные цели и задачи защиты информации на объекте информатизации Организации

4.1. В соответствии с присвоенным классом ИСПДн и моделью угроз безопасности ПДн в Организации должен выполняться комплекс организационнотехнических мероприятий по защите информации, циркулирующей в помещениях, технических системах и средствах передачи, хранения и обработки информации.

4.2. Накопление, обработка, хранение и передача защищаемой информации в Организации происходит на объекте информатизации, который представляет собой совокупность информационных ресурсов, средств и систем обработки информации, используемых» в соответствии с заданной информационной технологией, средств обеспечения, помещений, в которых они установлены, или помещений, предназначенных для ведения конфиденциальных переговоров.

К объекту информатизации в Организации относятся защищаемые, специальные помещения и средства вычислительной техники.

4.3. Целями защиты информации на объекте информатизации являются:

– предотвращение утечки информации по техническим каналам;

– предотвращение уничтожения, искажения, копирования, блокирования информации в системах информатизации за счет НСД к ней;

– соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах ее обработки;

– сохранение возможности управления процессом обработки и пользования информацией.

4.4. К основным задачам защиты информации на объекте информатизации относя гея задачи по предотвращению:

– несанкционированного доведения защищаемой информации до лиц, не имеющих права доступа к этой информации;

– получения защищаемой информации заинтересованным лицом с нарушением установленных прав или правил доступа к защищаемой информации;

– получения защищаемой информации разведкой с помощью технических средств;

– воздействия на защищаемую информацию с нарушением установленных прав или правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

– воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств АС, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

4.5. Защита информации на объекте информатизации Организации достигается выполнением комплекса организационных мероприятий с применением сертифицированных средств защиты информации от утечки или воздействия на нее по техническим каналам путем НСД к ней, по предупреждению преднамеренных программно-технических воздействий, предпринятых с целью нарушения целостности (модификации, уничтожения) информации в про-

цессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

5. Порядок определения защищаемой информации организации

5.1. К защищаемой информации Организации относится:

– информация, содержащая ПДн работников, клиентов, граждан;

– общедоступная информация, уничтожение, изменение, блокирование которой может нанести ущерб Организации.

5.2. По результатам анализа информации обрабатываемой в Организации составляются:

– «Список сотрудников, допущенных к обработке ПДн» (с указанием названия и вида обрабатываемого документа: бумажный, электронный);

– «Перечень информационных ресурсов, содержащих ПДн, подлежащих защите в АС».

5.3. Защищаемая информация Организации может быть представлена:

– на бумажных носителях в виде отдельных документов или дел с документами;

– на машинных носителях в виде файлов, массивов; баз данных, библиотек и пр.;

– в виде речевой информации, при проведении совещаний, переговоров и пр.

5.4. С целью определения технических средств и систем, с помощью которых

обрабатывается информация, содержащая ПДн, а также помещений, где проводятся обсуждения с использованием такой информации, отделом информационных технологий, отделом безопасности или администратором информационной безопасности Организации составляются и утверждаются перечни ТС ИСПДн, защищаемых и специальных помещений.

6. Технические каналы утечки защищаемой информации, циркулирующей на объекте информатизации Организации

6.1. Технический канал утечки информации (ТКУИ) представляет собой совокупность следующих факторов:

– источника информативного сигнала;

– физической среды его распространения;

– приемника, способного зарегистрировать данный сигнал.

6.2. При ведении переговоров и использовании технических средств для обработки и передачи информации на объекте информатизации Организации возможна реализация следующих ТКУИ:

– акустического излучения информативного речевого сигнала;

– электрических сигналов, возникающих при преобразовании информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющихся по проводам и линиям, выходящим за пределы КЗ;

– виброакустических сигналов, возникающих при преобразовании информативного акустического сигнала за счет воздействия его на строительные конструкции и инженерно-технические коммуникации защищаемого помещения;

– НСД к обрабатываемой в АС информации и несанкционированные действия с ней;

– воздействия на технические или программные средства ИС в целях нарушения конфиденциальности, целостности и доступности информации посредством специально внедренных программных средств;

– ПЭМИН информативных сигналов от ТС ИСПДн и линий передачи информации;

– наводок информативного сигнала, обрабатываемого ТС ИСПДн, на цепи электропитания и линии связи, выходящие за пределы КЗ;

– радиоизлучений, модулированных информативным сигналом, возникающим при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;

– радиоизлучений или электрических сигналов от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации («закладочные устройства»), модулированных информативным сигналом;

– радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

– просмотра информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;

– прослушивания телефонных и радиопереговоров;

– хищения технических средств с хранящейся в них информацией или носителей информации.

6.3. Перехват информации, циркулирующей на объекте информатизации, или воздействие на нее с использованием технических средств могут вестись:

– из-за границы КЗ из близлежащих строений и транспортных средств;

– из смежных помещений, принадлежащих другим организациям и расположенным в том же здании, что и объект информатизации;

– при посещении Организации посторонними лицами;

– за счет НСД к информации, циркулирующей в АС, как с помощью технических средств автоматизированной системы, так и через сети.

6.4. В качестве аппаратуры перехвата или воздействия на информацию и технические средства объекта информатизации могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта либо подключаемые к каналам связи или техническим средствам обработки информации, а также электронные устройства съема информации – «закладочные устройства», размещаемые внутри или вне защищаемого помещения.

6.5. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны, вследствие:

– непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемого помещения и его инженерно- технических систем;

– некомпетентных или ошибочных действий пользователей;

– непреднамеренного просмотра информации с экранов мониторов и пр.

6.6. Выявление и учет факторов, которые воздействуют или могут воздействовать на информацию, циркулирующую на объекте информатизации, проводятся в соответствии с «Базовой моделью угроз безопасности ПДн при их обработке в ИСПДн», утвержденной ФСТЭК России 15.02.2008, и составляют основу для планирования мероприятий, направленных на защиту информации на объекте информатизации.

7. Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

7.1. В целях осуществления технического обеспечения безопасности ПДн при их обработке в ИСПДн, в зависимости от класса ИСПДн в Организации реализовываются Следующие мероприятия:

– мероприятия по защите от НСД к ПДн при их обработке в ИСПДн;

– мероприятия по защите информации от утечки по техническим каналам.

7.2. Мероприятия по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий включают:

– управление доступом;

– регистрацию и учет;

– обеспечение целостности;

– контроль отсутствия НДВ;

– антивирусную защиту;

– обеспечение безопасного межсетевого взаимодействия ИСПДн;

– анализ защищенности;

– обнаружение вторжений.

7.3. Подсистему управления доступом, регистрации и учета необходимо реализовывать на базе программных средств блокирования несанкционированных действий, сигнализации и регистрации. Это специальные, не входящие в ядро какой-либо операционной системы сертифицированные программные и программно-аппаратные средства защиты самих операционных систем, электронных баз ПДн и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения опасных для ИСПДн действий пользователя или нарушителя. К ним относятся специальные утилиты и программные комплексы защиты, в которых реализуются функции диагностики, регистрации, уничтожения, сигнализации и имитации.

Средства диагностики осуществляют тестирование файловой системы и баз ПДн, постоянный сбор ПДн о функционировании элементов подсистемы обеспечения безопасности ПДн.

Средства уничтожения предназначены для уничтожения остаточных данных и могут предусматривать аварийное уничтожение данных в случае угрозы НСД, которая не может быть блокирована системой.

Средства сигнализации предназначены для предупреждения операторов при их обращении к защищаемым ПДн и для предупреждения администратора при обнаружении факта НСД к ПДн, искажении программных средств защиты, выходе или выводе из строя аппаратных средств защиты и о других фактах нарушения штатного режима функционирования ИСПДн.

Средства имитации моделируют работу с нарушителями при обнаружении попытки НСД к защищаемым ПДн или программным средствам. Имитация позволяет увеличить время на определение места и характера НСД, что особенно важно в территориально распределенных сетях, и дезинформировать нарушителя о месте нахождения защищаемых ПДн.

7.4. Подсистема обеспечения целостности реализуется преимущественно операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

7.5. Подсистема контроля отсутствия НДВ реализуется в большинстве случаев на базе систем управления базами данных, средств защиты ПДн, антивирусных средств защиты ПДн.

7.6. Для обеспечения безопасности ПДн и программно-аппаратной среды ИСПДн, обеспечивающей обработку этой информации, применяются средства антивирусной защиты, обеспечивающие:

– обнаружение и (или) блокирование деструктивных вирусных воздействий на общесистемное и прикладное программное обеспечение, реализующее обработку ПДн, а также на ПДн;

– обнаружение и удаление неизвестных вирусов;

– обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске

При выборе средств антивирусной защиты необходимо учитывать следующие факторы:

– совместимость указанных средств со штатным программным обеспечением ИСПДн;

– степень снижения производительности функционирования ИСПДн по основному назначению;

– наличие средств централизованного управления функционированием средств антивирусной защиты с рабочего места администратора сети в ИСПДн;

– возможность оперативного оповещения администратора безопасности информации в ИСПДн обо всех событиях и фактах проявления ПМВ;

– наличие подробной документации по эксплуатации средства антивирусной защиты;

возможность осуществления периодического тестирования или самотестирования средства антивирусной защиты;

– возможность наращивания состава средств защиты от ПМВ новыми дополнительными средствами без существенных ограничений работоспособности ИСПДн и «конфликта» с другими типами средств защиты ПДн.

Описание порядка установки, настройки, конфигурирования и администрирования средств антивирусной защиты, а также порядка действий в случае выявления факта вирусной атаки или иных нарушений требований по защите от ПМВ должны быть включены в руководство администратора безопасности информации в ИСПДн.

7.7. Для осуществления разграничения доступа к ресурсам ИСПДн при межсетевом взаимодействии применяется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами.

7.8. Подсистема анализа защищенности реализуется на основе использования средств тестирования (анализа защищенности) и контроля (аудита) безопасности ПДн.

Средства анализа защищенности применяются с целью контроля настроек защиты операционных систем на рабочих станциях и серверах и позволяют оценить возможность проведения нарушителями атак на сетевое оборудование, контролируют безопасность программного обеспечения. Для этого они исследуют топологию сети, ищут незащищенные или несанкционированные сетевые подключения, проверяют настройки межсетевых экранов. Подобный анализ производится на основании детальных описаний уязвимостей настроек средств защиты (например, коммутаторов, маршрутизаторов, межсетевых экранов) или уязвимостей операционных систем или прикладного программного обеспечения. Результатом работы средства анализа защищенности является отчет, в котором обобщаются сведения об обнаруженных уязвимостях.

В интересах выявления угроз НСД за счет межсетевого взаимодействия применяются системы обнаружения вторжений. Такие системы строятся с учетом особенностей реализации атак, этапов их развития и основаны на целом ряде методов обнаружения атак.

Для обнаружения вторжений в ИСПДн Организации рекомендуется использовать системы обнаружения сетевых атак, использующие как сигнатурные методы анализа, так и методы выявления аномалий.

7.9. Для защиты ПДн от утечки по техническим каналам применяются

организационные и технические мероприятия, направленные на исключение утечки акустической (речевой), видовой информации, а также утечки информации за счет ПЭМИН. При реализации технических мероприятий используются технические пассивные и активные средства защиты.

7.10. Перечень мероприятий по защите ПДн для ИСПДн Организации определяется отделом информатизации и ввода данных в зависимости от ущерба, который может быть нанесен вследствие НСД или непреднамеренного доступа к ПДн в соответствии с действующим законодательством.

8. Организация работ по защите информации на объекте информатизации организации

8.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по целям, задачам, месту и времени организационных и технических мероприятий в Управлении, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

Защита информации, циркулирующей на объекте информатизации, должна быть комплексной и дифференцированной. С этой целью для объекта информатизации создается система защиты информации.

Разработка мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн в Организации осуществляется отделом безопасности.

8.2. Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством РФ требованиям, обеспечивающим защиту ПДн.

Средства защиты ПДн, применяемые в ИСПДн, должны быть сертифицированы в соответствии с требованиями по безопасности ПДн.

8.3. Порядок организации и обеспечения безопасности ПДн в ИСПДн Управления включает в себя:

8.3.1 Оценку обстановки.

Оценка обстановки проводится работниками отдела информатизации и ввода данных и определяются возможные способы обеспечения безопасности ПДн. Она основывается на результатах комплексного обследования ИСПДн, в ходе которого, прежде всего, проводится категорирование ПДн по важности.

При оценке обстановки определяется необходимость обеспечения безопасности ПДн от угроз:

уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн;

– утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН);

– перехвата при передаче по проводным (кабельным) линиям связи;

хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе ПМВ);

– воспрепятствования функционированию ИСПДн путем преднамеренного электромагнитного воздействия на ее элементы;

– непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за

ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

При оценке обстановки учитывается степень ущерба, который может быть причинен в случае неправомерного использования соответствующих ПДн.

8.3.2. Обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн проводится в соответствии с действующим законодательством.

8.3.3. Разработку замысла обеспечения безопасности ПДн (осуществляется выбор основных способов защиты ПДн).

8.3.4. Выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты.

При выборе целесообразных способов обеспечения безопасности ПДн, обрабатываемых в ИСПДн, определяются организационные меры и технические (аппаратные, программные и программно-аппаратные) сертифицированные средства защиты.

В соответствии с выявленными сектором защиты информации угрозами безопасности ПДн осуществляется планирование и проведение мероприятий, направленных на обеспечение безопасности ПДн при их обработке в ИСПДн Организации.

Модель угроз применительно к конкретной ИСПДн разрабатывается отделом безопасности в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной

заместителем директора ФСТЭК России от 14.02.2008, на основе Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России от 15.02.2008, по представленным необходимым техническим данным об ИСПДн.

8.3.5. Решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты. Предусматривает подготовку кадров, выделение необходимых финансовых и материальных средств, закупку и разработку программного и аппаратного обеспечения.

Контроль осуществляется отделом безопасности по выполнению требований нормативных документов по защите ПДн, а также в оценке обоснованности и эффективности принятых мер.

8.3.6. Обеспечение реализации принятого замысла защиты ПДн.

8.3.7. Планирование мероприятий по защите ПДн.

8.3.8. Организацию и проведение работ по созданию СЗПДн в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних лицензированных организаций, решение основных задач взаимодействия.

8.3.9. Разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн.

8.3.10. Развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн.

8.3.11. Доработку СЗПДн по результатам опытной эксплуатации.

8.4. Комплексная защита информации на объекте информатизации проводится по следующим основным направлениям работы:

– охрана помещений объекта;

– определение перечня информации, подлежащей защите;

– классификация ИСПДн;

– создание системы защиты информации при разработке и модернизации объекта;

– составление организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;

– защита речевой информации при осуществлении конфиденциальных переговоров;

– защита информации, содержащей ПДн, при ее автоматизированной обработке, передаче с использованием технических средств, а также на бумажных или иных носителях;

– защита информации при взаимодействии абонентов с информационными сетями связи общего пользования.

8.5. Перечень необходимых мер защиты информации определяется по результатам обследования объекта информатизации с учетом соотношения затрат на защиту информации с возможным ущербом (негативным последствиям для субъектов ПДн) от ее разглашения, утраты, уничтожения, искажения, нарушения санкционированной доступности и работоспособности технических средств, обрабатывающих эту информацию, а также с учетом реальных возможностей ее перехвата и раскрываемости.

Основное внимание должно быть уделено защите информации, содержащей ПДн, в отношении которой угрозы реальны и сравнительно просто реализуемы без применения сложных технических средств перехвата информации.

К информации такого рода относится:

– речевая информация, циркулирующая в защищаемом помещении;

– информация, обрабатываемая СВТ;

– информация, выводимая на экраны мониторов;

– документированная информация, содержащая ПДн;

– информация, передаваемая по каналам связи, выходящим за пределы КЗ.

В целом обеспечение безопасности ПДн при их обработке в ИСПДн достигается реализацией совокупности организационных и технических мер, причем в интересах обеспечения безопасности ПДн в обязательном порядке подлежат защите технические и программные средства, используемые при обработке ПДн, и носители информации. При организации и осуществлении защиты ПДн необходимо руководствоваться требованиями нормативных и методических документов по защите ПДн в автоматизированных системах, учитывая при этом, что ПДн отнесены к информации ограниченного доступа.

В связи с тем что ИСПДн по своим характеристикам и номенклатуре угроз безопасности ПДн близки к наиболее распространенным информационным системам, целесообразно при их защите максимально использовать традиционные подходы к технической защите информации.

8.6. Создание системы защиты информации объекта информатизации осуществляется по следующим стадиям:

– предпроектная стадия, включающая в себя предпроектное обследование объекта информатизации (ИСПДн), разработку аналитического обоснования необходимости создания системы защиты персональных данных (далее СЗПДн) и технического задания на ее создание;

– стадия проектирования (разработки проектов) и реализации ИСПДн, включающая в себя разработку СЗПДн в составе объекта информатизации (ИСПДн);

– стадия ввода в действие СЗПДн, включающая в себя опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации

(далее СрЗИ), а также оценку соответствия ИСПДн требованиям безопасности информации.

8.6.1. Предпроектная стадия обследования объекта информатизации (ИСПДн) включает в себя:

– установление необходимости обработки ПДн в ИСПДн;

– определение ПДн, подлежащих защите от НСД;

– определение условий расположения ИСПДн относительно границ КЗ;

– определение конфигурации и топологии ИСПДн в целом и ее отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

– определение технических средств и систем, предполагаемых к использованию в разрабатываемой ИСПДн, условий их расположения, общесистемных и прикладных программных средств, имеющихся и предлагаемых к разработке;

– определение режимов обработки ПДн в ИСПДн в целом и в отдельных ее компонентах;

– определение класса ИСПДн;

– уточнение степени участия должностных лиц в обработке ПДн, характер их взаимодействия между собой;

– определение (уточнение) угроз безопасности ПДн применительно к конкретным условиям функционирования ИСПДн (разработка частной модели угроз).

8.6.2. По результатам предпроектного обследования на основе документов ФСТЭК России, с учетом установленного класса ИСПДн задаются конкретные требования по обеспечению безопасности ПДн, включаемые в техническое (частное техническое) задание на разработку СЗПДн.

8.6.3. Предпроектное обследование может быть поручено специализированной организации, имеющей соответствующую лицензию. Порядок ознакомления (при необходимости) специалистов подрядной организации с защищаемыми сведениями определяется Организацией.

8.6.4. Аналитическое обоснование необходимости создания СЗПДн должно содержать:

– информационную характеристику и организационную структуру объекта информатизации;

– характеристику комплекса ТСИСПДн и ВТСС, программного обеспечения, режимов работы, технологического процесса обработки информации;

– возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;

– перечень предлагаемых к использованию сертифицированных СрЗИ;

– обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;

– оценку материальных, трудовых и финансовых затрат на разработку и внедрение СЗПДн;

– ориентировочные сроки разработки и внедрения СЗПДн;

– перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

Аналитическое обоснование подписывается руководителем организации, проводившей предпроектное обследование, согласовывается с отделом безопасности или ответственным лицом и утверждается начальником Организации.

8.6.5. Техническое (частное техническое) задание на разработку СЗПДн должно содержать:

– обоснование разработки СЗПДн;

– исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

– класс ИСПДн;

– ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;

– конкретизацию мероприятий и требований к СЗПДн;

– перечень предполагаемых к использованию сертифицированных СрЗИ;

– обоснование проведения разработок собственных СрЗИ при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных СрЗИ;

– состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

8.6.6. В целях дифференцированного подхода к обеспечению безопасности ПДн в зависимости от объема обрабатываемых ПДн и угроз безопасности жизненно важным интересам личности, общества и государства ИСПДн подразделяются на классы.

Класс АС (ИСПДн) устанавливается в соответствии с «Порядком проведения классификации ИСНДн», утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 №55/86/20, и оформляется актом.

Пересмотр класса защищенности АС (ИСПДНн) производится в обязательном порядке, если произошло изменение хотя бы одного из критериев, на основании которых он был установлен.

8.6.7. На стадии проектирования и создания АС (ИСПДн, СЗПДн) проводятся следующие мероприятия:

– разработка задания и проекта проведения работ (в том числе строительных и строительно-монтажных) по созданию (реконструкции) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;

– выполнение работ в соответствии с проектной документацией;

– обоснование и закупка совокупности используемых в ИСПДн серийно выпускаемых технических средств обработки, передачи и хранения информации;

– разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

– обоснование и закупка совокупности используемых в ИСПДн сертифицированных технических, программных и программно-технических СрЗИ и их установка;

– проведение сертификации по требованиям безопасности информации технических, программных и программно-технических СрЗИ, в случае когда на рынке отсутствуют требуемые сертифицированные СрЗИ;

– разработка и реализация разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации;

– определение подразделений и назначение лиц, ответственных за эксплуатацию СрЗИ, с их обучением по направлению обеспечения безопасности ПДн;

– разработка эксплуатационной документации на ИСПДн и СрЗИ, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);

– выполнение других мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности ПДн.

8.6.8. На стадии ввода в действие АС (ИСПДн, СЗПДн) осуществляются:

– выполнение генерации пакета прикладных программ в комплексе с программными СрЗИ;

– опытная эксплуатация СрЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

– приемо-сдаточные испытания СрЗИ по результатам опытной эксплуатации;

– организация охраны и физической защиты помещений ИСПДн, исключающих несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;

– оценка соответствия ИСПДн требованиям безопасности ПДн.

9. Ответственность должностных лиц организации за обеспечение защиты информации, содержащей ПДн, на объекте информатизации

9.1. Лицами, ответственными за организацию, обеспечение и выполнение мероприятий по защите ПДн в Организации, являются:

– начальник Организации;

– начальник отдела безопасности;

– начальник отдела информационных технологий;

– системный администратор;

– администратор информационной безопасности;

– начальники отделов Организации;

– работники, допущенные к обработке ПДн в ИСПДн.

Они обязаны:

– не допускать проведения в Организации работ и мероприятий, связанных с использованием ПДн без принятия необходимых мер по защите ПДн;

– определять объекты информатизации, предназначенные для работы с ПДн, организовывать их защиту;

– контролировать работу структурных подразделений Организации и должностных лиц при обработке ПДн.

9.2. Начальник Организации несет ответственность за общую организацию работ по защите информации на объекте информатизации и созданию эффективной СЗПДн этих объектов.

9.3. Начальник отдела безопасности или администратор информационной безопасности несет ответственность за:

– руководство и координацию работ по защите информации на объекте информатизации;

– организацию выполнения требований по защите информации на объекте информатизации;

– обоснованность необходимости создания СЗПДн объекта информатизации;

– разработку организационно-распорядительных документов по защите информации на объекте информатизации;

– организацию разработки технического задания на создание СЗПДн, подготовку проектов договоров со сторонними организациями на выполнение работ по защите информации на объекте информатизации;

– организацию контроля состояния СЗПДн объекта информатизации, соблюдения работниками установленных норм и требований по защите информации;

– организацию контроля охраны помещений объекта;

– совершенствование СЗПДн.

Он имеет право:

– контролировать деятельность структурных подразделений Организации, должностных лиц по выполнению ими требований по защите ПДн;

– участвовать в работе различного рода заседаний, комиссий, экспертных групп Организации при рассмотрении вопросов защиты ПДн;

– вносить предложения начальнику Организации о приостановке работ с ПДн в случае нарушения требований по защите ПДн;

– готовить предложения о привлечении к проведению работ по защите ПДн сторонних организаций, имеющих лицензию на соответствующий вид деятельности.

9.4. Администратор информационной безопасности объекта информатизации Организации несет ответственность за:

сопровождение СрЗИ от несанкционированного доступа;

– непосредственное управление режимами работы и административную поддержку функционирования применяемых специальных программных и программно-аппаратных СрЗИ от несанкционированного доступа;

– настройку и сопровождение в процессе эксплуатации подсистемы управления доступом;

– проверку состояния используемых СрЗИ от несанкционированного доступа, правильности их настройки;

– организацию разграничения доступа;

– учет и контроль состава и полномочий пользователей;

– выполнение требований по обеспечению безопасности при организации технического обслуживания и отправке в ремонт СВТ;

– учет, хранение, прием и выдачу персональных идентификаторов и ключевых дискет ответственным исполнителям;

– контроль учета, создания, хранения и использования резервных и архивных копий массивов данных.

Он обязан:

– разрабатывать проекты годовых планов работ по защите ПДн в Организации, предусматривающих задачи структурным подразделениям по решению конкретных вопросов защиты ПДн, организацию их выполнения, а также контроль за их эффективностью;

– организовывать разработку и согласование методической документации по защите ПДн;

– согласовывать мероприятия по защите ПДн в ИСПДн с начальником Организации;

– определять степень опасности технических каналов утечки информации, различных способов НСД к ПДн, их разрушения (уничтожения) или искажения;

– определять необходимые меры по защите ПДн, организовывать их разработку и реализацию;

– организовывать аттестацию ИСПДн;

– организовывать проведение периодического контроля эффективности мер защиты ПДн, учет и анализ результатов контроля;

– организовывать расследования нарушений в области защиты ПДн и разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений;

– анализировать состояние работ по защите ПДн и разрабатывать предложения по совершенствованию системы защиты ПДн в Организации;

– организовывать проведение занятий с работниками Организации по вопросам защиты информации.

9.5. Системный администратор объекта информатизации несет ответственность за:

– выбор типа и версии серверных и клиентских операционных систем, установку, настройку, сопровождение операционных систем серверов;

– обновление справочного и антивирусного программного обеспечения;

– реализацию совместно с администратором информационной безопасности сетевой политики безопасности;

– настройку аппаратной и программной составляющей серверного, коммутационного, телекоммуникационного оборудования, средств аппаратной безопасности сегментов, сетевого периферийного оборудования;

– регистрацию пользователей и предоставление им прав доступа к сетевым информационным ресурсам, регистрацию компьютеров в сети;

– реализацию адресной и маршрутной политики сети;

– реализацию политики антивирусной защиты;

– обеспечение работоспособности структурированной кабельной сети;

– архивирование, резервное копирование информации;

– ведение аудита системных событий и безопасности;

– оперативное управление работой сети;

– контроль физической сохранности средств и оборудования сети.

9.6. Начальники отделов, эксплуатирующих объект информатизации, несут ответственность за:

– выполнение требований по защите информации на объекте информатизации;

– осуществлять постоянный контроль за подчиненными, разъяснять и требовать от подчиненных выполнения требований нормативных правовых актов по вопросам защиты ПДн;

– ведение необходимой документации объекта информатизации;

– правильность определения пользователям своего подразделения необходимости и прав доступа к защищаемым информационным ресурсам.

9.7. Пользователи АС объекта информатизации несут ответственность за:

– соблюдение мер по защите информации и правил эксплуатации СВТ;

– обеспечение сохранности СВТ, машинных носителей информации и целостность установленного программного обеспечения;

– соблюдение установленных требований по обращению с машинными носителями информации.

9.8. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, привлекаются к дисциплинарной, гражданско-правовой, административной, уголовной и иной предусмотренной законодательством РФ ответственности.

9.9. В случае замеченных нарушений требований данного положения работником, последний обязан немедленно сообщить об этом своему непосредственному руководителю, администратору информационной безопасностилибо начальнику отдела безопасности.

9.10. Отдел информационных технологий при эксплуатации и развертывании ИСПДн проводит следующие работы:

– по согласованию с начальниками отделов проводит анализ возможности решения определенных задач на ИСПДн и уточнение содержания необходимых для этого изменений в конфигурации аппаратных и программных средств;

– установку (развертывание, обновление версий) программных средств, необходимых для решения в ИСПДн конкретных задач;

– удаление (затирание) программных пакетов, необходимость в использовании которых отпала;

– установку (развертывание) новых ИСПДн или подключение дополнительных устройств (узлов, блоков), необходимых для решения конкретных задач.

9.11. Отдел безопасности при эксплуатации и развертывании ИСПДн проводит следующие работы:

– организовывает аттестацию и контрольные проверки ИСПДн;

– устанавливает и вводит в эксплуатацию средства защиты ПДн в соответствии с эксплуатационной и технической документацией к ним;

– организовывает в установленном порядке расследования причин и условий появления нарушений по вопросам технической защиты ПДн и разрабатывает предложения по устранению недостатков и предупреждению подобного рода нарушений;

– проводит анализ возможности решения (а также совмещения) указанных задач в конкретных ИСПДн (с точки зрения обеспечения безопасности) и принимает решение об отнесении их к той или иной группе по степени защищенности;

9.12. Любые планируемые изменения в составе основных или вспомогательных технических средств, изменения в системе электропитания, связи, заземления или конструкции ИСПДн должны быть в обязательном порядке согласовываться с отделом безопасности.

9.13. Иные права и обязанности работников Организации приведены в соответствующих положениях об отделах и должностных регламентах работников.

9.14 Права субъекта ПДн определяются гл. 3 Федерального закона «О персональных данных «от 27.07.2006 N 152-ФЗ.

9.15. Эксплуатация ИСПДн осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, предписанием на эксплуатацию технических средств, а также требованиями соответствующих документов по вопросам защиты ПДн.

10. Планирование работ по защите персональных данных

10.1. Основные мероприятия и работы по защите ПДн в ИСПДн Организации являются составной частью плана основных мероприятий по защите информации в Организации, разрабатываемого на очередной календарный год.

10.2. План основных мероприятий по защите информации определяет перечень основных проводимых организационно-технических мероприятий по защите информации (в том числе ПДн) в Организации с указанием:

– сроков выполнения мероприятий;

– ответственных работников за исполнением соответствующих пунктов плана основных мероприятий по защите информации.

10.3. В план основных мероприятий по защите информации включаются:

– мероприятия по категорированию и аттестации объектов информатизации;

– работы по защите объектов информатизации от утечки информации по техническим каналам и НСД (созданию СЗСИ);

– мероприятия по контролю состояния защиты информации;

– мероприятия по обучению и повышению квалификации работников, допущенных к обработке ПДн,

10.4. План основных мероприятий по защите информации на очередной календарный год разрабатывается отделом информатизации и ввода данных.

10.5. Согласованный с заинтересованными лицами план основных мероприятий по защите информации утверждается распоряжением начальника Организации не позднее 25 декабря текущего года.

11. Контроль состояния защиты персональных данных

11.2. Контроль состояния защиты ПДн в Организации осуществляется с целью своевременного выявления и предотвращения утечки информации, содержащей ПДн по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на ПДн и оценки защиты ПДн от технических средств разведки (далее – контроль).

11.3. Контроль заключается в проверке выполнения требований действующего законодательства по вопросам защиты ПДн, в оценке обоснованности и эффективности принятых мер по защите ПДн и осуществляется отделом информатизации и ввода данных, в том числе с применением контрольно-измерительной аппаратуры и сертифицированных программных средств контроля.

11.4. Контроль эффективности внедренных мер и средств защиты ПДн должен проводиться в соответствии с требованиями предписаний на эксплуатацию технических средств, требований эксплуатационной документации на сертифицированные средства ПДн, требований других нормативных документов не реже одного раза в год.

11.5. Обязательным является контроль средств защиты ПДн при вводе их в эксплуатацию после проведения ремонта средств защиты ПДн при изменениях условий и расположения или эксплуатации.

11.6. Контроль защиты информации организуется начальником Организации.

11.7. К проведению контрольных мероприятий могут привлекаться ответственные работники за эксплуатацию ИСПДн.

11.8. Для проведения некоторых мероприятий контроля (измерение сопротивления защитного заземления, выявление опасных каналов утечки информации, проверка исправности и работоспособности средств защиты информации, оценка эффективности защищенности информации и т.п.) в случае невозможности или экономической нецелесообразности их выполнения силами работников Организации могут привлекаться лицензированные сторонние организации.

11.9. Контроль состояния и эффективности защиты ПДн может осуществляться в соответствии с планом основных мероприятий по защите

информации на текущий год или носить внеплановый (внезапный) характер и может проводиться как с использованием контрольно-измерительной аппаратуры (оценка эффективности защищенности ИСПДн, контроль работоспособности средств защиты и т.п.), так и без ее применения (контроль соответствия условий эксплуатации ИСПДн, контроль соответствия требованиям организационнораспорядительной документации и т.п.).

11.10. Результаты периодического контроля оформляются отдельными протоколами или актами.

11.11. По всем выявленным нарушениям требований по защите ПДн администратор информационной безопасности в пределах предоставленных ему прав и своих функциональных обязанностей обязан добиваться их немедленного устранения.

11.12. Начальники отделов, в чьем ведении находятся ИСПДн, и ответственные за их эксплуатацию, обязаны принять все необходимые меры по немедленному устранению выяв-

ленных нарушений. При невозможности их немедленного устранения они обязаны прекратить работы с ПДн и организовать работы по устранению выявленных нарушений.

11.13. Исполнители, проводящие обработку ПДн в ИСПДн, обязаны выполнять требования по защите ПДн и ответственного за эксплуатацию ИСПДн по устранению допущенных ими нарушений норм и требований по защите ПДн и несут персональную ответственность за соблюдение требований по защите ПДн в ходе проведения работ.

11.14. Сопровождение системы защиты информации от НСД на стадии эксплуатации ИСПДн, включая ведение служебной информации (генерацию и смену паролей, ключей, сопровождение правил разграничения доступа), оперативный контроль за функционированием системы защиты ПДн от НСД, контроль соответствия общесистемной программной среды эталону (контроль целостности программного обеспечения) и приемку включаемых в ИСПДн новых программных средств, а также контроль за ходом технологического процесса обработки ПДн путем регистрации и анализа действий работников (пользователей) по системному журналу, осуществляется администратором безопасности ИСПДн.

11.15. Администратором безопасности ИСПДн назначается работник отдела безопасности.

11.16. Учет, хранение и выдача работникам паролей и ключей для системы защиты ПДн от НСД, оперативный контроль за действиями работников, использующих ИСПДн, осуществляют работники отдела безопасности.

11.17. Общий контроль, внеплановый контроль и методическое обеспечение работников, допущенных к обработке ПДн, осуществляется отделом безопасности.

11.18. Защита ПДн считается эффективной, если принимаемые меры защиты соответствуют установленным требованиям или нормам руководящих документов по защите ПДн.

11.19. Несоответствие мер установленным требованиям или нормам по защите ПДн является нарушением.

11.20..Нарушения по степени важности делятся по трем категориям:

– первая – невыполнение требований или норм по защите ПДн, в результате чего имелась или имеется реальная возможность их утечки по техническим каналам;

– вторая – невыполнение требований по защите ПДн, в результате чего создаются предпосылки к их утечке по техническим каналам;

– третья – невыполнение других требований по защите ПДн.

11.21. При обнаружении нарушений первой категории в ИСПДн необходимо:

– немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения, и принять меры;

– организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц;

– сообщить в отдел безопасности о вскрытых нарушениях и принятых мерах.

11.22. Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер отделом информационных технологий.

11.23. При обнаружении нарушений второй и третьей категорий начальники отделов обязаны принять необходимые меры по их устранению в сроки, согласованные с отделом информационных технологий и отделом безопасности.

12. Аттестование информационных систем персональных данных

12.1. Под аттестацией ИСПДн по требованиям безопасности информации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – Аттестата соответствия подтверждается, что объект (ИСПДн) соответствует требованиям стандартов или иных нормативных документов по защите ПДн, утвер-

жденных ФСТЭК России, ФСБ России или другими органами государственного управления в пределах их компетенции.

12.1. Наличие действующего Аттестата соответствия дает право обработки ПДн соответствующей категории и объема в ИСПДн и на период времени, установленный в Аттестате соответствия.

12.2. ИСПДн классифицированные по 1 и 2 классу подлежат обязательной аттестации.

12.3. Аттестация по требованиям безопасности информации предшествует началу обработки ПДн и вызвана необходимостью официального подтверждения эффективности комплекса используемых в ИСПДн мер и средств защиты ПДн.

12.4. При аттестации ИСПДн подтверждается ее соответствие требованиям по защите информации от утечки по возможным физическим каналам и НСД к ней, за исключением проведения специальных проверок технических средств на отсутствие электронных «закладок».

12.5. Аттестация предусматривает комплексную проверку (аттестационные испытания) ИСПДн в реальных условиях эксплуатации с целью оценки соответствия Использованного комплекса мер и средств защиты ПДн требуемому уровню безопасности ПДн.

12.6. Аттестационные испытания осуществляются аттестационной комиссией, формируемой аккредитованным органом по аттестации из компетентных специалистов в необходимых для конкретной ИСПДн, по согласованной с заявителем программе испытаний.

12.7. Программа испытаний разрабатывается на основе анализа исходных данных об ИСПДн, представляемых отделом безопасности, моделью актуальных угроз ИСПДн «и должна включать необходимые виды испытаний, определенные методическими рекомендациями для соответствующих видов объектов

информатизации, а также определять сроки, условия и методики проведения испытаний.

12.8. Программа испытаний может уточняться и корректироваться в процессе испытаний по согласованию с заявителем и руководителем аттестационной комиссии.

12.9. Для проведения испытаний Организация представляет аттестационной комиссии следующие исходные данные и документацию:

– техническое задание на ИСПДн;

– технический паспорт на ИСПДн;

– приемо-сдаточную документацию на ИСПДн;

– акт классификации ИСПДн;

– состав технических и программных средств, входящих в ИСПДн;

– планы размещения технических средств и систем;

– состав и схемы размещения средств защиты ПДн;

– план контролируемой зоны;

– схемы прокладки линий передачи данных;

– схемы и характеристики систем электропитания и заземления технических средств;

– перечень защищаемых в ИСПДн ресурсов;

– организационно-распорядительная документация разрешительной системы доступа работников к защищаемым ресурсам ИСПДн;

– описание технологического процесса обработки ПДн в ИСПДн;

– технологические инструкции работникам (пользователям) ИСПДн и администратору безопасности ИСПДн;

– инструкции по эксплуатации средств защиты ПДн;

– предписания на эксплуатацию технических средств;

– протоколы специальных исследований технических средств;

– сертификаты соответствия требованиям безопасности ПДн на средства и системы обработки и передачи ПДн, используемые средства защиты ПДн

– данные по уровню подготовки кадров, обеспечивающих защиту ПДн;

– данные о техническом обеспечении средствами контроля эффективности защиты ПДн и их метрологической поверке;

– нормативную и методическую документацию по защите ПДн и контролю эффективности защиты ПДн.

12.10. Приведенный общий перечень исходных данных и документации может уточняться Организацией в зависимости от особенностей аттестуемой ИСПДн по согласованию с аттестационной комиссией.

12.11. Аттестационные испытания ИСПДн проводятся до полного их завершения в соответствии с программой испытаний вне зависимости от промежуточных результатов испытаний.

12.12. Аттестат соответствия выдается на период, в течение которого обеспечивается неизменность условий функционирования ИСПДн и технологии обработки ПДн, могущих повлиять на характеристики, определяющие безопасность ПДн (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки ПДн, средства и меры защиты), на срок, устанавливаемый нормативными правовыми документами ФСТЭК России.

12.13. В случае изменений условий и технологии обработки ПДн ответственные за эксплуатацию ИСПДн лица обязаны известить об этом начальника отдела безопасности, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты ИСПДн.

13. Взаимодействие с другими организациями

13.1. Взаимодействие по вопросам защиты ПДн Организации со сторонними организациями (при необходимости) организуется начальником отдела безопасности с целью:

– обеспечения Организации недостающими и вновь разработанными руководящими, нормативно-методическими и иными материалами по вопросам защиты ПДн;

– обеспечения средствами защиты ПДн;

– выполнения организационных и технических мероприятий в области защиты ПДн, на проведение которых у Организации отсутствует соответствующее разрешение либо отсутствуют технические средства и подготовленные работники (специалисты);

– выполнения организационных и технических мероприятий в области защиты ПДн, выполнение которых силами Организации экономически невыгодно;

– контроля эффективности проводимых мероприятий по защите ПДн.

13.2. Привлекаемая для оказания услуг в области защиты ПДн сторонняя организация должна иметь лицензию на соответствующий вид деятельности.

13.3. Перечень совместно выполняемых организационных и технических мероприятий в области защиты ПДн определяется с учетом планируемых работ по созданию (реконструкции) ИСПДн и включается в себя план основных мероприятий по защите ПДн.

13.4. С привлекаемой организацией Организация заключает двусторонний договор (соглашение, контракт).

Заместитель начальника

отдела безопасности А. А. Злой

Лист ознакомления сотрудников

с Положением о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в Администрации президента России по г. Москва

в Администрации президента России по г. Москва

_____

(наименование структурного подразделения)

№ п/п Фамилия, имя, отчество работника Дата ознакомления с Положением Подпись работника

1 Литарова Ольга Николаевна 15.09.2016

2 Созинова Елена Георгиевна 15.09.2016
3 Павличенко Анна Анатольевна 15.09.2016
4 Артамонова Ляля Саматовна 15.09.2016
5 Быкова Надежда Евгеньевна 15.09.2016
6 Шишаева Елена Гуновна 15.09.2016
7 Шарапова Елена Александровна 15.09.2016
8 Родина Татьяна Николаевна 15.09.2016
9 Дюк Марина Алексеевна 15.09.2016
10 Богачев Артем алексеевич 15.09.2016
11 Злой Андрей Андреевич 15.09.2016
12 Тереньтев Александр Павлович 15.09.2016
13 Поздеев Николай Борисович 15.09.2016
14 Усиков Андрей Владимирович 15.09.2016
15 Костина Наталья Витальевна 15.09.2016
16 Черный Никита Сергеевич 15.09.2016

4.Положение обработке ПДн

Приложение №2
УТВЕРЖДЕНО
Приказом ППО «Администрация президента»
по г. Москва
от «15» сентября 2017 г.
№ _____
ПОЛОЖЕНИЕ
о персональных данных в первичной профсоюзной организации «Администрация президента» по г. Москва
Комсомольск-на-Амуре
2017
Оглавление

1. Термины и определения

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Персональные данные работников организации – информация, которая необходима работодателю в связи с трудовыми отношениями и касается конкретного работника; сведения о фактах, событиях и обстоятельствах жизни гражданского служащего, позволяющие идентифицировать его личность и содержащиеся в личном деле гражданского служащего либо подлежащие включению в его личное дело (если работники организации являются государственными гражданскими служащими).

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-теле-

коммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием или без использования таких средств.

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Конец ознакомительного фрагмента.