

УТВЕРЖДАЮ

Президент
Инфокоммуникационного союза

А.Е. Крупнов

« ___ » _____ 2010 г.

СОГЛАСОВАНО

Первый заместитель начальника 8-го
Центра Федеральной службы
безопасности Российской Федерации



А.П. Баранов

« ___ » _____ 2010 г.

СОГЛАСОВАНО

Начальник 2-го управления Федеральной
службы по техническому и экспортному
контролю



А.В. Куц

« 30 » МАРТА 2010 г



**НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА
«РАЗРАБОТКА КОНЦЕПЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В
ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ
ОПЕРАТОРОВ СВЯЗИ»
(ШИФР «ТРИТОН»)**

**ОТРАСЛЕВАЯ МОДЕЛЬ УГРОЗ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В
ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ
ОПЕРАТОРОВ СВЯЗИ
(ICU-9/2009-ОМ1)**

Заместитель генерального директора
ЗАО «Рэйнвокс»

« 01 » МАРТА 2010 г.



ЛИСТ СОГЛАСОВАНИЙ

№ п/п	Должность	Фамилия, имя, отчество	Подпись	Дата
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

Инв. № подл	Подп. и дата	Инв. № дубл.	Взам. инв. №	Подп. и дата
-------------	--------------	--------------	--------------	--------------

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

ISU-9/2009-OM1

ЛИСТ ИЗМЕНЕНИЙ

Разрешение		Содержание изменений	Код	Примечание
Изм.	№ лис.			
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				

Инв. № подл	Подп. и дата	Инв. № дубл.	Взам. инв. №	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат

ICU-9/2009-OM1

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ	7
2. ОПИСАНИЕ ОБЪЕКТА ИНФОРМАТИЗАЦИИ	9
2.1 Общие характеристики корпоративной информационной системы.....	9
2.2 Состав.....	17
2.3 Структура	18
2.4 Состав информации	18
2.5 Формы представления информации.....	18
2.6 Объекты защиты.....	19
2.7 Характеристики безопасности	20
2.8 Информационные системы персональных данных	20
2.9 Контролируемая зона.....	22
3. КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ	23
3.1 Угрозы безопасности персональных данных	23
3.2 Классификация угроз безопасности персональных данных	26
3.3 Модель угроз верхнего уровня	28
3.4 Детализированная модель угроз	28
4. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПДн	32
4.1 Общие положения	32
4.2 Этапы разработки, производства, хранения, транспортировки, подготовки ввода в эксплуатацию	33
4.3 Этап эксплуатации.....	34
4.3.1 Типы нарушителей	35
4.3.2 Предположения об имеющейся у нарушителя информации.....	37
4.3.3 Предположения об имеющихся у нарушителей средствах атак	38
4.3.4 Возможности нарушителей.....	39
4.3.5 Каналы атак.....	44
4.4 Требуемый уровень криптографической защиты	45
5. МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ	46
5.1 Описание методики	46
5.2 Определение уровня исходной защищенности информационных систем персональных данных операторов связи	47
6. УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ	50
6.1 Угрозы утечки акустической (речевой) информации	51

Подп. и дата	
Взам. инв. №	
Инв. № дубл.	
Подп. и дата	
Инв. № подл.	

ICU-9/2009-OM1				
Ли	Изм.	№ докум.	Подп.	Дата
Разраб.		Романов В.В.		
Разраб.		Кочкин А.А.		
Разраб.		Черкас Ю.В.		
Н. контр.				
Утв.				
Отраслевая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных операторов связи				
		Лит	Лист	Листов
			5	79
Союз участников рынка инфокоммуникационных услуг				

6.2	Угрозы утечки видовой информации	52
6.3	Угрозы утечки информации по каналам ПЭМИН.....	55
7.	УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ	60
8.	ТИПОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРОВ СВЯЗИ	63
8.1	Общие положения	63
8.2	Типовая модель угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных операторов связи.....	64
9.	ЗАКЛЮЧЕНИЕ.....	69
Приложение 1. ИТ ИНФРАСТРУКТУРА ОПЕРАТОРА СВЯЗИ.....		71
Приложение 2. НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ		72
Приложение 3. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ.....		75
Приложение 4. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....		76

Име. № подл.						Подп. и дата				
Име. № дубл.						Взам. инв. №				
Подп. и дата						Подп. и дата				
ICU-9/2009-OM1										
Име. № подл.	Ли	Изм.	№ докум.	Подп.	Дата	Отраслевая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных операторов связи	Лит	Лист	Листов	
	Разраб.		Романов В.В.						6	79
	Разраб.		Кочкин А.А.							
	Разраб.		Черкас Ю.В.							
	Н. контр.									
Утв.										
							Союз участников рынка инфокоммуникационных услуг			

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Модель угроз содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) операторов связи. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, создающих условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз разработана с учетом требований нормативно-методических документов ФСТЭК России и ФСБ России.

Модель угроз содержит единые исходные данные по угрозам безопасности персональных данных (УБПДн), обрабатываемых в ИСПДн операторов связи, связанным:

- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Модель угроз является методическим документом и предназначена для операторов связи, заказчиков и разработчиков ИСПДн и их подсистем при решении следующих задач:

- разработка частных моделей угроз безопасности ПДн в конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования;
- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты, предусмотренных для соответствующего класса ИСПДн;

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата
-------------	--------------	--------------	--------------	--------------

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющих права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроль за обеспечением уровня защищенности персональных данных.

В Модели угроз дано обобщённое описание информационных систем операторов связи, объектов защиты, возможных источников УБПДн, основных классов уязвимостей ИСПДн, возможных видов неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн операторов связи, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться в процессе разработки частных моделей угроз, по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн.

Инв. № подл	Подп. и дата				Инв. № дубл.	Взам. инв. №				Подп. и дата
Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1					Лист
										8

2. ОПИСАНИЕ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

2.1 Общие характеристики корпоративной информационной системы

Корпоративная информационная система (КИС) является основой информационно-технологической инфраструктуры (ИТ - инфраструктура), поддерживающая решение актуальных задач и обеспечивающая достижение бизнес-целей оператора связи. Она представляет собой территориально распределенную совокупность программно-технических комплексов (ПТК), объединенных с помощью защищенных, в том числе доверенных каналов связи, расположенных на всех уровнях управления Оператора связи (Рисунок 2.1):

- 1 уровень – корпоративный центр;
- 2 уровень – филиалы;
- 3 уровень – зарубежные филиалы;
- 4 уровень – внешние информационные системы (дилеры оператора связи, другие внешние организации, имеющие доступ к ИСПДн Оператора связи на основании договора);
- 5 уровень – мобильные пользователи.

Для связи между ПТК используются:

- собственные оптоволоконные каналы связи;
- спутниковые каналы связи;
- радиоканалы (в т.ч. радиорелейные);
- проводные каналы связи;
- каналы связи Операторов связи;
- физические носители информации (съёмные носители информации, бумажные носители).

Инв. № подл.	Подп. и дата	Инв. № дубл.	Взам. инв. №	Подп. и дата	Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист
											9

При этом каналы связи по наличию контроля со стороны Оператора связи могут быть следующих типов:

- контролируемые – каналы связи, защищенные от НСД к информации режимными, организационно-техническими и техническими мерами, направленными на обеспечение заданных характеристик безопасности, использование которых контролируется оператором связи;
- неконтролируемые – каналы связи, использование которых контролируется сторонними организациями (сторонние организации гарантируют безопасность ПДн на основе договора);

По уровню защищенности каналы связи могут быть следующих типов:

- защищенные каналы:
 - доверенные каналы – каналы связи, которые обеспечивают конфиденциальность и (или) целостность информации, а также реализуют взаимную аутентификацию ПТК или их компонент;
 - защищенные волоконно-оптические линии связи, безопасность передаваемой информации в которых определяется физической средой распространения и значительной сложностью перехвата передаваемого в ней информационного сигнала;
- открытые каналы – сети связи общего пользования и (или) сети международного информационного обмена (Интернет), не обеспечивающие безопасность передаваемой информации.

В состав средств защиты ПДн при использовании доверенного канала, входят следующие механизмы:

- механизмы взаимной аутентификации компонент ПТК;
- механизмы обеспечения конфиденциальности передаваемой в рамках доверенного канала информации;
- механизмы обеспечения целостности передаваемой в рамках доверенного канала информации.

Инт. № подл.	
Подп. и дата	
Инт. № дубл.	
Взам. инв. №	
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист
						10

Взаимная аутентификация компонент ПТК при установлении доверенного канала достигается использованием механизмов аутентификации.

Обеспечение конфиденциальности передаваемых в рамках доверенного канала пользовательских данных и служебной информации достигается посредством применения механизма туннелирования и криптографических преобразований.

Обеспечение целостности передаваемых в рамках доверенного канала пользовательских данных и служебной информации, достигается посредством применения механизмов туннелирования и контроля целостности.

Каналы связи имеются между ПТК всех уровней управления.

КИС Операторов связи имеет топологию типа «звезда» и её логическим центром является «Корпоративный центр», к которому по каналам связи имеют подключение информационные системы, соответствующие представленным выше уровням управления.

Схема организации КИС Оператора связи представлена на Рисунке 2.1

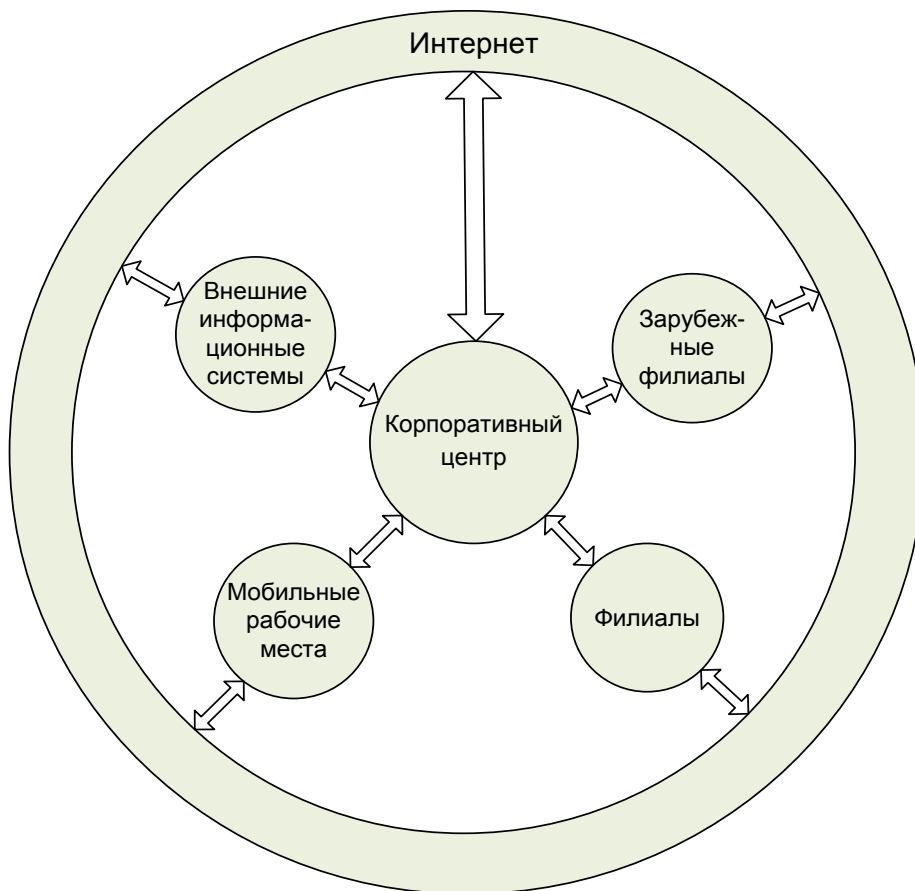


Рисунок 2.1 – Схема организации КИС Оператора связи

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Ине. № инв.	Подп. и дата
Ине. № инв.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

Корпоративный центр

Корпоративный центр является основной частью КИС Оператора связи и состоит в том числе из центра обработки данных (ЦОД), обеспечивающего консолидацию вычислительных ресурсов и хранилищ данных, а также автоматизированных рабочих мест пользователей.

Корпоративный центр находится в пределах РФ.

Филиалы

В состав КИС Оператора связи в рамках филиала входят в том числе рабочие места пользователей, а также может входить центр обработки данных филиала.

Филиалы находятся в пределах РФ.

Зарубежные филиалы

В состав КИС Оператора связи в рамках зарубежного филиала входят в том числе рабочие места пользователей, а также может входить центр обработки данных зарубежного филиала.

Зарубежные филиалы находятся за пределами РФ.

Филиалы Оператора связи, расположенные на территории Российской Федерации и за её пределами, функционируют в рамках единой корпоративной информационной системы, которая является доверенной средой эксплуатации ИСПДн.

Внешние информационные системы

К информационным системам внешнего взаимодействия относятся информационные системы, входящие в состав информационно-технологической инфраструктуры и обеспечивающие автоматизацию функций обмена информацией, с государственными и муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных.

Внешними операторами ПДн могут являться:

- бюро кредитных историй;

Подп. и дата
Взам. инв. №
Инв. № дубл.
Подп. и дата
Инв. № подл.

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1

- банки (системы типа «клиент-банк»);
- правоохранительные органы, осуществляющие оперативно-розыскные мероприятия (СОПМ);
- Федеральная налоговая служба РФ;
- пенсионные фонды;
- Федеральная миграционная служба РФ;
- военно-учетный стол;
- Федеральная служба государственной статистики;
- Федеральный фонд обязательного медицинского страхования;
- коллекторские агентства.

Внешний оператор ПДн определяет перечень передаваемых записей о субъектах (абонентах или сотрудниках) и форму представления ПДн в соответствии с действующим законодательством РФ или с пунктами договора, заключенного между оператором связи и внешним оператором ПДн.

Методы обеспечения безопасности ПДн также определяются внешними операторами ПДн, в том числе перечень используемых при взаимодействии технических средств защиты информации и порядок их эксплуатации. Требования, предъявляемые к системе защиты ИСПДн внешнего взаимодействия, формирует внешний оператор ПДн.

При взаимодействии Оператора связи с другим (внешним) оператором ПДн на основании договора, условиями которого предусмотрено использование СКЗИ и условия которого определяет внешний оператор ПДн, ответственность за классификацию ИСПДн, определение мер и средств защиты (в том числе определение класса применяемых криптосредств), реализуемых в ИСПДн внешнего взаимодействия, несет внешний оператор. В этом случае Оператор связи несет ответственность только за соблюдение правил эксплуатации ИСПДн.

Перед началом взаимодействия с внешними ИСПДн Оператор связи должен убедиться в адекватности защиты ПДн со стороны внешнего оператора ПДн.

Инт. № подл.	Подп. и дата
Инт. № дубл.	Взам. инв. №
Подп. и дата	
Инт. № подл.	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1

Разграничение ответственности за нарушение заданных характеристик безопасности ПДн между внешними операторами и оператором связи определяется соответствующими регламентами, двусторонними договорами, нормами законодательства.

Мобильное рабочее место

Мобильное рабочее место (МРМ) представляет собой АРМ, технические средства которого могут находиться за пределами контролируемой зоны.

Доверенная среда эксплуатации ИСПДн

Корпоративная информационная система Оператора связи является *доверенной средой* эксплуатации ИСПДн, в которой принят комплекс организационных и организационно-технических мер по защите информации.

Схема организации доверенной среды эксплуатации ИСПДн представлена на рисунке 2.

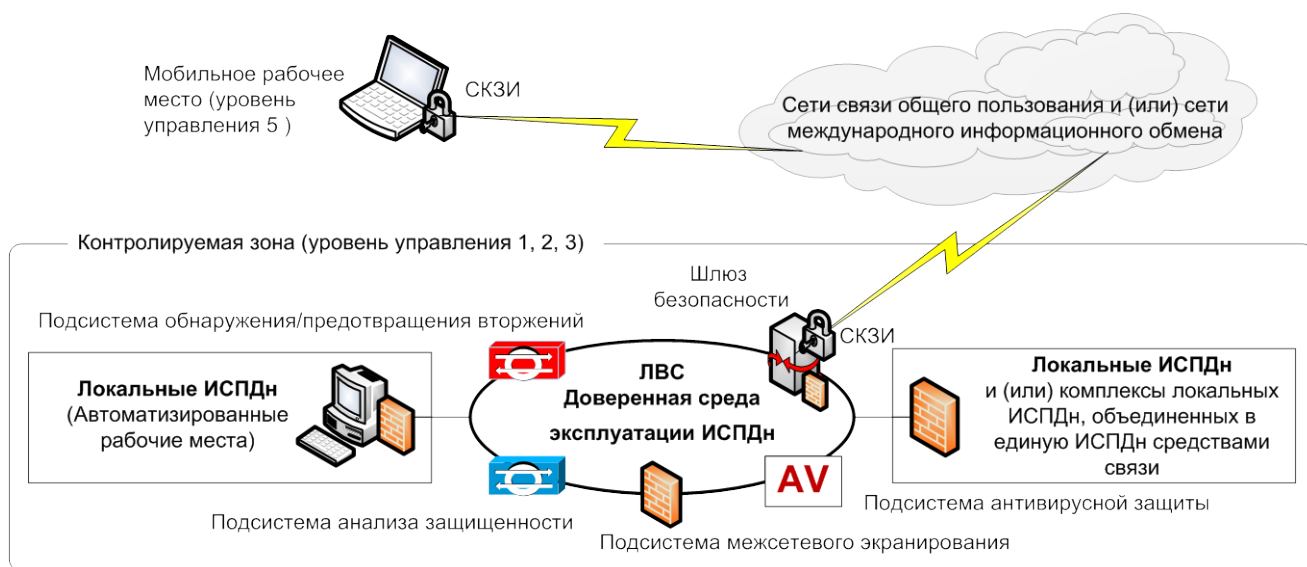


Рисунок 2.2 – Схема организации доверенной среды эксплуатации ИСПДн

Доверенная среда эксплуатации ИСПДн гарантируется выполнением комплекса организационных мер, включающих принятые политики информационной безопасности, правил подбора персонала и контроля его лояльности, технических мер, реализуемые в том числе в рамках подсистем межсетевого экранирования, обнаружения/предотвращения вторжений, анализа защищенности, антивирусной защиты в соответствии с разрешительными документами уполномоченных федеральных органов, включая ФСБ России и (или) ФСТЭК России.

Инт. № подл.	Подп. и дата
Инт. № дубл.	Взам. инв. №
Инт. № подл.	Подп. и дата
Инт. № подл.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

Доверенная среда эксплуатации ИСПДн позволяет:

- обеспечить требуемые характеристики безопасности ПДн при информационном обмене между ИСПДн;
- рассматривать структуру ИСПДн как локальную;
- обеспечить изоляцию ИСПДн от сетей связи общего пользования и (или) сетей международного информационного обмена (Интернет).

Подсистема межсетевого экранирования

Подсистема межсетевого экранирования представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в ИСПДн и выходящей из неё, и обеспечивает защиту ИСПДн посредством фильтрации информации, т.е. её анализа по совокупности критериев и принятия решения о её распространении в (из) ИСПДн.

Подсистема обнаружения вторжений

Подсистема обнаружения вторжений реализуется с использованием в составе КИС программных и (или) программно-аппаратных средств (систем) обнаружения вторжений, использующих комбинированные методы обнаружения атак, включающие в себя сигнатурные методы и методы выявления аномалий.

Подсистема анализа защищенности

Подсистема анализа защищенности реализуется на основе использования средств тестирования (анализа защищенности) и контроля (аудита) безопасности информации. 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 КИС, ищут незащищенные или несанкционированные сетевые подключения, проверяют настройки подсистемы межсетевого экранирования. Подобный анализ производится на основании детальных описаний уязвимостей настроек средств защиты (коммутаторов, маршрутизаторов, межсетевых экранов) или уязвимостей операционных систем или прикладного программного обеспечения.

Име. № подл	Подп. и дата	Име. № дубл.	Взам. инв. №	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-9/2009-ОМ1	Лист
						15

Подсистема антивирусной защиты

Подсистема антивирусной защиты реализуется с использованием в составе КИС специальных средств антивирусной защиты выполняющих следующие функции:

- обнаружение и (или) блокирование деструктивных вирусных воздействий на общесистемное и прикладное программное обеспечение, являющееся частью КИС;
- обнаружение и удаление неизвестных вирусов;
- обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске.

Средства антивирусной защиты КИС:

- являются совместимыми со штатным программным обеспечением КИС;
- включают в свой состав средства централизованного управления функционированием средств антивирусной защиты;
- обладают возможностью оперативного оповещения ответственных лиц обо всех событиях и фактах проявления программно-математических воздействий (ПМВ);
- обладают возможностью осуществления периодического тестирования или самотестирования средств антивирусной защиты;
- обладают возможностью наращивания состава средств защиты от ПМВ новыми дополнительными средствами без существенных ограничений работоспособности КИС и «конфликта» с другими типами средств защиты.

Взаимодействие ИСПДн с сетями связи общего пользования

Взаимодействие ИСПДн с сетями связи общего пользования и (или) сетями международного информационного обмена (Интернет) происходит по необходимости только со стороны ИСПДн через шлюз безопасности (Рисунок 2.2).

Шлюз безопасности установлен на границы ЛВС и выполняет необходимые функции на основе принятых правил политик безопасности, обеспечивающих безопасный доступ пользователей в том числе пользователей МРМ к информационным ресурсам сетей связи общего пользования и (или) сетям

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-9/2009-ОМ1	Лист
						16

международного информационного обмена (Интернет). В состав шлюза могут входить следующие подсистемы:

- прокси–сервер;
- межсетевой экран;
- система обнаружения/предотвращения вторжений;
- антивирусный контроль трафика;
- система мониторинга;
- СКЗИ.

2.2 Состав

Технические средства, обеспечивающие доступ пользователей к информационным ресурсам включают:

- АРМ. Автоматизированное рабочее место - программно-аппаратный комплекс, предназначенный для осуществления доступа пользователя к информационным ресурсам ИСПДн с произвольным набором системных и прикладных программных средств, имеющий возможность хранения информации после окончания сеанса работы пользователя.
- Терминальный клиент. Терминальный клиент – аппаратное средство, предназначенное для осуществления доступа пользователя к информационным ресурсам ИСПДн с фиксированным набором системных программных средств, не доступным для изменения пользователем ИСПДн, не имеющее возможности хранения информации после окончания сеанса работы пользователя и возможности печати.
- ЦОД. Центр обработки данных - это отказоустойчивая, масштабируемая, комплексная, централизованная ИТ система, обеспечивающая автоматизацию бизнес-процессов с высоким уровнем производительности и качеством предоставляемых инфраструктурных сервисов, в состав которой входят высоконадежное серверное оборудование, системы хранения и передачи данных, включая системы резервного копирования, системы энергообеспечения,

Инв. № подл	Подп. и дата				Лист		
						17	
Инв. № инв. №	Взам. инв. №				ICU-9/2009-ОМ1		
Инв. № дубл.	Инв. № дубл.				Лист		
						17	
Подп. и дата	Подп. и дата				ICU-9/2009-ОМ1		
Инв. № подл	Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист

кондиционирования и физического размещения, системы мониторинга и управления, системы безопасности, решения по виртуализации и консолидации ресурсов, основанная на кластерной технологии.

2.3 Структура

Обобщенная ИТ инфраструктура Оператора связи представлена в **Приложении 1**.

2.4 Состав информации

В ИСПДн обрабатываются персональные данные:

- абонентов – физических лиц;
- руководителей и главных бухгалтеров поставщиков, партнеров, абонентов – юридических лиц, других контрагентов;
- посетителей;
- соискателей;
- сотрудников оператора.

2.5 Формы представления информации

Средами обработки, хранения, передачи и вывода информации в ПТК ИСПДн являются:

- бумажные носители (представление данных – текстовая информация);
- проводные, оптоволоконные, радиоканалы связи (представление данных – записи баз данных, файлы специализированных форматов, видеоизображение, голосовая информация);
- стационарные средства хранения информации (представление данных – базы данных, файлы специализированных форматов, видеоизображение, голосовая информация);
- излучения в оптическом диапазоне (представление данных – изображение);

Ине. № подл	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1	Лист
						18

- излучения в акустическом диапазоне (представление данных – речь человека).

2.6 Объекты защиты

В качестве объектов защиты в ПТК выступают:

- персональные данные, циркулирующие по открытым каналам связи;
- информация, хранящаяся или обрабатываемая на серверах, дисковых массивах, ленточных библиотеках, АРМ, терминальных клиентах, других ТС ИСПДн;
- конфигурационная и управляющая информация;
- отчуждаемые носители информации;
- информация в электронных журналах регистрации;
- резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих файлов;
- остаточная информация на носителях информации;
- система защиты информации, в том числе ключевая и аутентифицирующая пользователей информация;
- общесистемное и прикладное программное обеспечение серверов, АРМ;
- аппаратные средства ПТК: оборудование серверов, АРМ, терминальных клиентов, коммуникационного оборудования;
- СКС внутри помещения, в котором функционирует ПТК;
- оборудование электропитания;
- внешние кабельные коммуникации;
- строительные конструкции и элементы инженерно-технических сооружений помещения, в котором функционирует ПТК;

Инв. № подл.	Подп. и дата			
	Взам. инв. №			
Инв. № дубл.	Подп. и дата			
	Инв. № инв.			
Инв. № подл.	Подп. и дата			
	Инв. № инв.			
Ли	Изм.	№ докум.	Подп.	Дат
ICU-9/2009-OM1				Лист
				19

- побочные сигналы, которые возникают в процессе функционирования ТС и в которых полностью или частично отражаются ПДн или другая защищаемая информация.

2.7 Характеристики безопасности

Для ПДн и объектов, которые могут выступать в качестве объектов угроз и требуют защиты, необходимо обеспечить выполнение следующих характеристик безопасности:

- конфиденциальность;
- целостность;
- достоверность (аутентичность);
- доступность.

В случае выделения в составе информационной системы оператора связи подсистем, каждая из которых является информационной системой персональных данных, информационной системе в целом задаются характеристики безопасности всех входящих в нее подсистем.

Обеспечение других характеристик безопасности (неотказуемость, учетность, адекватность) в ИСПДн не требуется, так как их нарушение не может привести к негативным последствиям для субъектов ПДн.

2.8 Информационные системы персональных данных

Информационные системы персональных данных операторов связи подразделяются на два типа¹:

- **к первому типу** относятся автоматизированные рабочие места (АРМ), являющиеся локальными информационными системами, не имеющими подключений к сетям связи общего пользования и (или) сетям международного информационного обмена и выделенные по функционально-технологическому принципу:

- АРМ пользователей;
- АРМ администраторов;

¹ Отраслевой классификатор. Информационные системы персональных данных операторов связи (ICU-4/2009-ОК)

Име. № подл.	Подп. и дата
Име. № дубл.	Взам. инв. №
Подп. и дата	
Име. № подл.	Подп. и дата

– **ко второму типу** относятся локальные информационные системы и (или) комплексы локальных информационных систем, объединенных в единую информационную систему средствами связи, не имеющими подключений к сетям связи общего пользования и (или) сетям международного информационного обмена.

Для осуществления разграничения доступа к ресурсам ИСПДн при межсетевом взаимодействии применяется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами. Межсетевой экран устанавливается между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран входит в состав защищаемой сети (состав ИСПДн). Для него путем настроек отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Положения настоящей Модели угроз распространяются на информационные системы персональных данных операторов связи, функционирующие в условиях доверенной среды (Рисунок 2.2).

ИСПДн операторов связи, рассматриваемые в настоящей Модели угроз, имеют следующие характеристики (исходные данные):

- по структуре ИСПДн являются локальными информационными системами, состоящими из комплекса технических и программных средств, предназначенных для обработки персональных данных, и функционирующих в доверенной среде;
- ИСПДн не имеют подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;
- ИСПДн являются многопользовательскими информационными системами;
- ИСПДн являются системами с разграничением прав доступа;
- все технические средства ИСПДн находятся в пределах Российской Федерации, за исключением технических средств ИСПДн зарубежных филиалов.

Инт. № подл.	
Подп. и дата	
Инт. № дубл.	
Взам. инв. №	
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1	Лист
						21

2.9 Контролируемая зона

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств².

Требования к порядку доступа на охраняемую территорию Оператора связи определены приказом Министерства информационных технологий и связи Российской Федерации от 09.01.2008 №1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации».

Стационарное оборудование размещается в изолированных помещениях.

Серверные и коммуникационные компоненты размещаются в серверных помещениях.

Каждое здание оператора находится под охраной. На входе функционируют системы контроля и управления доступом. Доступ возможен только при наличии пропуска. Также в каждом помещении с компонентами ИСПДн установлены замки.

Серверные помещения также оборудованы средствами контроля доступа. Доступ в эти помещения ограничен.

Организация и обеспечение функционирования СКЗИ осуществляется в соответствии с требованиями разрешительных документов ФСБ России.

² Базовая модель угроз безопасности персональных данных, при их обработке в информационных системах персональных данных

Инт. № подл.	Подп. и дата	Инт. № дубл.	Взам. инв. №	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист
						22

3. КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Угрозы безопасности персональных данных

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом:

- характеристик информационных систем персональных данных;
- свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию;
- возможностей источников угроз.

Характеристики ИСПДн

К характеристикам ИСПДн, обуславливающим возникновение УБПДн, относятся категория и объем обрабатываемых в информационной системе персональных данных, структура ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики безопасности ПДн, обрабатываемых в ИСПДн, режимы обработки персональных данных, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

При определении характеристик ИСПДн, учитываются положения отраслевого классификатора информационных систем персональных данных операторов связи (ICU-4/2009-ОК) определяющего категории и объем ПДн, характеристики безопасности ПДн, обрабатываемых в ИСПДн операторов связи.

Основными элементами ИСПДн являются:

- персональные данные, содержащиеся в базах данных, как совокупность информации и ее источников, используемых в ИСПДн;
- информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист
						23

– технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации);

– программные средства (операционные системы, системы управления базами данных и т.п.);

– средства защиты информации;

– вспомогательные технические средства и системы (ВТСС) – технические средства и системы, их коммуникации, не предназначенные для обработки ПД но размещенные в помещениях, в которых расположены ИСПДн, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной пожарной сигнализации, средства и системы оповещения и сигнализации контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофикации).

Свойства среды (пути) распространения информативных сигналов

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации канала УБПДн.

Возможности источников угроз

Возможности источников УБПДн обусловлены совокупностью методов и способов несанкционированного и (или) случайного доступа к ПДн в результате которого возможно нарушение характеристик безопасности ПДн:

– конфиденциальности (копирование, неправомерное распространение);

Ине. № подл	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Ине. № дубл.
Ине. № подл	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1	Лист
						24

- целостности (уничтожение, изменение);
- достоверности (аутентичности) (ложная информация);
- доступности (блокирование) .

Угроза безопасности ПДн реализуется в результате образования каналов реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает необходимые условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн (Рисунок 3.1) являются:

- источник УБПДн – субъект, материальный объект или физическое явление, создающие УБПДн;
- среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (характеристики безопасности) ПДн;
- носитель ПДн – физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

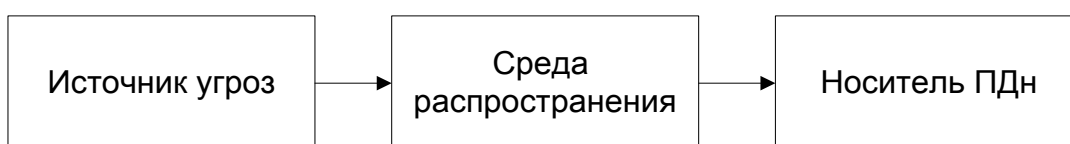


Рисунок 3.1 – Обобщенная схема канала реализации угроз безопасности персональных данных

Носители ПДн могут содержать информацию, представленную в следующих видах:

- акустическая (речевая) информация, содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, либо воспроизводимой акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

Ине. № подл.	Подп. и дата
Ине. № дубл.	
Взам. инв. №	
Подп. и дата	

- видовая информация, представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;
- информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;
- информация, обрабатываемая в ИСПДн, представленная в виде байт, IP-протоколов, файлов и других логических структур.

3.2 Классификация угроз безопасности персональных данных

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн операторов связи и разработки на их основе частных моделей применительно к конкретному виду ИСПДн угрозы классифицируются в соответствии со следующими признаками ([Рисунок 3.2](#)):

- по видам возможных источников УБПДн;
- по структуре ИСПДн, на которые направлена реализация УБПДн.
- по виду несанкционированных действий, осуществляемых с ПДн;
- по способам реализации УБПДн;
- по виду каналов, с использованием которых реализуется УБПДн.

По видам возможных источников УБПДн выделяются следующие классы угроз:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к КИС, включая пользователей ИСПДн, реализующих угрозы в КИС и (или) непосредственно в ИСПДн (внутренний нарушитель);
- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к КИС, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

Ине. № подл	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист
						26

По структуре ИСПДн, на которые направлена реализация УБПДн выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых в ИСПДн, на базе автоматизированных рабочих мест;
- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем и (или) комплексов локальных информационных систем, объединенных в единую информационную систему средствами связи.

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

- угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн.

По способам реализации УБПДн выделяются следующие классы угроз:

- угрозы, реализуемые в ИСПДн функционирующих в доверенной среде и не имеющих подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;
- угрозы, реализуемые в КИС при её подключении к сетям связи общего пользования и (или) сетям международного информационного обмена, реализация которых может привести к нарушению заданного уровня безопасности доверенной среды и как следствие – создать предпосылки для образования каналов реализации угроз в ИСПДн функционирующих в доверенной среде.

По виду каналов, с использованием которых реализуется УБПДн, выделяются следующие классы угроз:

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата
-------------	--------------	--------------	--------------	--------------

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

– угрозы, реализуемые через каналы, возникающие за счет использования технических средств съема (добывания) информации, обрабатываемой в технических средствах ИСПДн или ВТСС (технические каналы утечки информации);

– угрозы, реализуемые за счет несанкционированного доступа к ПДн в ИСПДн с использованием штатного программного обеспечения ИСПДн или специально разрабатываемого программного обеспечения.

3.3 Модель угроз верхнего уровня

Исходя из требуемых характеристик безопасности (раздел 2.7) ПДн и защищаемых объектов модель угроз верхнего уровня в ИСПДн содержит следующий перечень угроз:

- угроза нарушения конфиденциальности защищаемой информации;
- угроза нарушения целостности защищаемой информации.

3.4 Детализированная модель угроз

Детализированная модель угроз содержит совокупность условий и факторов, создающих опасность нарушения требуемых характеристик безопасности возможных объектов угроз.

Различают следующие угрозы безопасности объекта:

- угрозы, не являющиеся атакой;
- атаки.

К угрозам, которые не являются атаками, относятся:

- угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления (землетрясения, наводнения, ураганы и т.д.);
- угрозы социально–политического характера: забастовки, саботаж, локальные конфликты и т.д.;

Име. № дубл.	Име. № дубл.	Взам. инв. №	Подп. и дата
Име. № подл.	Подп. и дата		

Ли	Изм.	№ докум.	Подп.	Дат

– ошибочные действия и (или) нарушения тех или иных требований лицами, санкционировано взаимодействующими с возможными объектами угроз. К таким действиям и нарушениям относятся:

- непредумышленное искажение или удаление программных компонентов ИСПДн;
- внедрение и использование неучтенных программ;
- игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации:
 - нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации);
 - предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
 - настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;
 - несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

– угрозы техногенного характера, основными из которых являются:

- аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.);
- неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.;

Име. № подл	Подп. и дата	Име. № дубл.	Взам. инв. №	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат

- помехи и наводки, приводящие к сбоям в работе аппаратных средств.

Защита от угроз, не являющимися атаками, обеспечивается организационными и режимными мерами, принятыми у Оператора. Оператором разработаны и утверждены соответствующие должностные инструкции, положения и регламенты, а также периодически проводится повышение осведомленности персонала в части обеспечения режима информационной безопасности.

Реализация угроз, которые являются атаками, осуществляется нарушителем. Вероятность реализации таких угроз обуславливается возможностью нарушителя, поэтому перечень атак детализированной модели угроз определяется моделью нарушителя.

Инв. № подл	Подп. и дата				Инв. № дубл.	Взам. инв. №				Подп. и дата
Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1					Лист
										30

Инв № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Изм.	
Лист	
№ докум.	
Подп.	
Дата	

По видам возможных источников УБПДн

Угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к КИС, включая пользователей ИСПДн, реализующих угрозы в КИС и (или) непосредственно в ИСПДн (внутренний нарушитель)

Угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к КИС, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель)

По структуре ИСПДн, на которые направлена реализация УБПДн

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, на базе автоматизированных рабочих мест

Угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем и (или) комплексов локальных информационных систем, объединенных в единую информационную систему средствами связи

По виду несанкционированных действий, осуществляемых с ПДн

Угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации

Угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение

Угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн

По способам реализации УБПДн

Угрозы, реализуемые в ИСПДн функционирующих в доверенной среде и не имеющих подключений к сетям связи общего пользования и (или) сетям международного информационного обмена

Угрозы, реализуемые в КИС при её подключении к сетям связи общего пользования и (или) сетям международного информационного обмена, реализация которых может привести к нарушению заданного уровня безопасности доверенной среды и как следствие – создать предпосылки для образования каналов реализации угроз в ИСПДн функционирующих в доверенной среде

По виду каналов, с использованием которых реализуется УБПДн

Угрозы, реализуемые через каналы, возникающие за счет использования технических средств съема (добывания) информации, обрабатываемой в технических средствах ИСПДн или ВТСС (технические каналы утечки информации)

Угрозы, реализуемые за счет несанкционированного доступа к ПДн в ИСПДн с использованием штатного программного обеспечения ИСПДн или специально разрабатываемого программного обеспечения

Рисунок 3.2 – Классификация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных операторов связи

ИСУ-9/2009-ОМ1

4.2 Этапы разработки, производства, хранения, транспортировки, подготовки ввода в эксплуатацию

Объектами атак на этих этапах являются только технические и программные средства системы и документация на них.

Целями атак являются:

- получение сведений о средствах (об особенностях средств системы, об условиях их производства и эксплуатации);
- внесение негативных функциональных возможностей в технические и программные компоненты криптосредства и СФК, в том числе с использованием вредоносных программ (компьютерные вирусы, «троянские кони» и т.д.);
- внесение несанкционированных изменений в документацию на криптосредство и технические и программные компоненты СФК.
- неправильная конфигурация средств системы.

Для противодействия атакам, возможным на этих этапах, оператором связи предприняты соответствующие меры контроля:

– по соответствию технических и программных средств криптосредства, СФК и документации на эти средства, поступающих в зону ответственности оператора связи, эталонным образцам (защитные наклейки и пломбы на дистрибутивах программных и технических средств);

– целостности криптосредств, СФК и документации на эти средства, документации в процессе хранения и ввода в эксплуатацию:

- ограничение физического доступа к криптосредствам, СФК и документации на эти средства;
- хранение криптосредств и документации на них осуществляется в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение;

Ине. № подп	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата
-------------	--------------	--------------	--------------	--------------

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист 33

- транспортировка криптосредств осуществляется при соблюдении мер, исключающих бесконтрольный доступ к ним;
- использование механизмов контроля, описанных в документации на технические и программные средства криптосредства.

4.3 Этап эксплуатации

Атака характеризуется рядом существенных признаков. К этим существенным признакам на этапе эксплуатации технических и программных средств криптосредства и СФК можно отнести:

- нарушителя (субъекта атаки);
- объект атаки;
- цель атаки;
- имеющуюся у нарушителя информацию об объекте атаки;
- имеющиеся у нарушителя средства атаки;
- канал атаки.

Объектами атак в ИСПДн на этапе эксплуатации выступают:

- документация на криптосредство и на технические и программные компоненты СФК;
- защищаемые персональные данные;
- ключевая, аутентифицирующая и парольная информация;
- криптографически опасная информация (КОИ);
- криптосредство (программные и аппаратные компоненты криптосредства);
- технические и программные компоненты СФК;
- данные, передаваемые по каналам связи;
- помещение, в котором находятся защищаемые ресурсы ИСПДн.

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1

4.3.1 Типы нарушителей

Все физические лица, имеющие доступ к техническим и программным средствам ИСПДн разделяются на следующие категории:

- категория I – лица, не имеющие права доступа в контролируруемую зону ИСПДн;
- категория II – лица, имеющие право постоянного или разового доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны информационной системы;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны информационной системы.

Таким образом, внешними нарушителями могут быть как лица категория I, так и лица категория II, а внутренними нарушителями могут быть только лица категории II.

Типы нарушителей по возможностям доступа к различным компонентам ИСПДн представлены в таблице 4.1.

Таблица 4.1 – Типы нарушителей

Тип нарушителя	1	2	3	4	5	6	7	8
	Внешний нарушитель	Посетитель	Обслуживающий персонал	Сотрудник, не являющийся пользователем ИСПДн	Оператор ИСПДн	Администратор ИСПДн	Сотрудник обслуживающей ИСПДн организации	Дилер
Легальные права доступа:								
в контролируемую зону		✓	✓	✓	✓	✓	✓	
к ресурсам КИС				✓	✓	✓	✓	✓
к аппаратным средствам ИСПДн					✓	✓	✓	
к программным средствам ИСПДн					✓	✓	✓	✓
к подмножеству ПДн ИСПДн					✓	✓		✓
ко всему массиву ПДн ИСПДн						✓		
к настройкам СЗПДн						✓		
к настройкам СКЗИ						✓		

Ине. № подл. Подп. и дата

Ине. № дубл. Подп. и дата

Ине. № инв. №

Ине. № подл. Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

К внешним нарушителям категории I относятся:

- нарушители 1 типа:
 - физические лица, ведущие злоумышленную деятельность;
 - организованные преступные группы, сообщества.

К внутренним нарушителям категории II относятся:

- нарушители типа 2:
 - посетители, имеющий разовый доступ в КЗ;
 - определенные категории обсуживающего персонала и представителей ремонтных организаций, не имеющих доступ к компонентам ИСПДн;
- нарушители типа 3:
 - представители технических и обслуживающих служб, консультационных и других вспомогательных служб находящихся в пределах КЗ на постоянной основе или периодически;
- нарушители типа 4:
 - сотрудники, не являющиеся операторами или администраторами ИСПДн;
- нарушители типа 5:
 - оператором АРМ, терминального клиента ИСПДн;
- нарушители типа 6:
 - администраторы ИСПДн;
- нарушители типа 7:
 - сотрудники организаций, осуществляющих обслуживание ИСПДн на постоянной основе в соответствии с заключенными договорами (организации-разработчики ПО, ТС, организации, осуществляющие техническую поддержку);

Ине. № подп	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-9/2009-ОМ1	Лист
						36

- сведения о возможных для данного ИСПДн каналах атак;
- информацию о способах (методах) атак;
- данные о составе и маршрутах поставок технических и программных средств ИСПДн;
- данные о местах ремонта и обслуживания технических средств ИСПДн;
- данные об организациях осуществляющих поставку, ремонт, пусконаладочные и монтажные работы, обслуживание технических и программных средств ИСПДн;
- данные о составе пользователей ИСПДн;
- данные о реализованных в системе и средствах защиты принципах и алгоритмах.

Предполагается, что нарушитель не обладает сведениями о парольной и аутентифицирующей информации системы. При этом предполагается, что внутренний нарушитель обладает, в пределах своих полномочий, сведениями о собственной аутентифицирующей информации.

4.3.3 Предположения об имеющихся у нарушителей средствах атак

Имеющиеся у нарушителей средства атак являются, в том числе, следствием возможности сговора внешнего нарушителя (тип 1) с внутренними нарушителями. В общем случае нарушитель может использовать следующие средства атак:

- штатные средства, имеющиеся в ИСПДн;
- доступные в свободной продаже технические, программно-технические и программные средства;
- средства перехвата и обработки информации в кабельном и коммуникационном оборудовании, а также в каналах связи проходящих как в пределах контролируемой зоны, так и за ее пределами;
- общедоступные компьютерные вирусы;
- распределенные ресурсы различных сетей, в том числе сети Интернет;

Ине. № дубл.	Взам. инв. №	Подп. и дата
Ине. № подп	Подп. и дата	Ине. № дубл.

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1	Лист 38
----	------	----------	-------	-----	----------------	------------

- необходимые инструменты для работы с ТС и системами.

4.3.4 Возможности нарушителей

Потенциальный внешний нарушитель типа 1 имеет следующие возможности:

- действовать в интересах организованных преступных групп или отдельных лиц, действующих в своих интересах;
- реализовать угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ к ресурсам КИС через автоматизированные рабочие места КИС, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена, с целью нарушения заданного уровня безопасности доверенной среды, что, в свою очередь, может создать предпосылки для образования каналов реализации угроз в ИСПДн функционирующих в доверенной среде;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны;
- осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн, к которым относятся:
 - бюро кредитных историй – юридические лица, зарегистрированные в соответствии с законодательством Российской Федерации, являющиеся коммерческими организациями и оказывающие в

Ине. № подп	Подп. и дата				Лист
Ине. № дубл.	Взам. инв. №				ИСУ-9/2009-ОМ1
Ине. № инв.	Подп. и дата				Ли
Ине. № инв.	Подп. и дата				№ докум.
Ине. № подп	Подп. и дата				Дат

соответствии с Федеральным законом «О кредитных историях» услуги по формированию, обработке и хранению кредитных историй, а также по предоставлению кредитных отчетов и сопутствующих услуг⁴;

- уполномоченные государственные органы, осуществляющие оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации⁵.

Потенциальный внутренний нарушитель любого типа может действовать в интересах организованных преступных групп или отдельных лиц, действующих в своих интересах. Количество таких внутренних нарушителей на объектах не регламентируется.

Внутренний нарушитель (тип 5) скрывает свои несанкционированные действия от других сотрудников, самостоятельно осуществляет создание методов и средств реализации атак, а также самостоятельно реализует атаки. При этом внутренний нарушитель данного типа не имеет прямых возможностей доступа к средствам криптографической защиты информации других компонентов ИСПДн, так как доступ ограничен межсетевыми экранами, вследствие чего его возможности по доступу соответствуют возможностям нарушителя типа 4.

Нарушитель типа 6 не рассматривается в настоящей модели. Предполагается, что администраторы ИСПДн являются привилегированными пользователями и назначаются из числа особо доверенных лиц и осуществляют обслуживание технических и программных средств криптосредства и СФК, включая их настройку, конфигурирование и распределение ключевой документации. Их доверенность обеспечивается комплексом реализованных режимных, организационных, кадровых мер по подбору персонала и контролю их лояльности.

Нарушитель типа 7 не рассматривается в настоящей модели. Предполагается, что защита от данного типа нарушителя обеспечивается комплексом организационно-технических мер, кроме того, правила обращения с информацией, ставшей доступной вследствие проводимых мероприятий, условия конфиденциальности обозначены в договорах с организациями, осуществляющими техническую поддержку.

⁴ ст. 3, п. 6, №218-ФЗ «О кредитных историях»
⁵ ст. 64, п. 1, №126-ФЗ «О связи»

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата	Ли	Изм.	№ докум.	Подп.	Дат	Исх.	Лист
ICU-9/2009-OM1											40

Нарушитель типа 8 не рассматривается в настоящей модели. Предполагается, что защита от данного типа нарушителя обеспечивается комплексом организационно-технических мер предусматриваемых самими сторонними организациями, кроме того, правила обращения с информацией, ставшей доступной вследствие работы сторонних организаций, условия конфиденциальности обозначены в договорах с этими организациями.

В таблице 4.2 представлены возможности нарушителей по реализации угроз для ИСПДн, используемые при этом каналы атак и предположительные объекты атак, с учетом актуальности угроз определенных по результатам разработки Модели угроз.

При этом вводятся следующие ограничения:

- нарушитель 2 типа постоянно находится под контролем сотрудников, посещает контролируемую зону разово или редко, число помещений, в которых он может находиться – ограничено, доступ к компонентам ИСПДн отсутствует;
- нарушитель 3 типа постоянно находится под контролем сотрудников, при этом посещает контролируемую зону периодически или постоянно, число помещений в которых он может находиться – неограниченно, доступ к компонентам ИСПДн отсутствует;
- доступ в контролируемую зону подразделения, помещения регламентирован и контролируется соответствующим контрольно-пропускным режимом;
- в отношении контролируемых оператором каналов связи угроза перехвата информации потенциальным нарушителем не реализуется за счет отсутствия в них информационного взаимодействия с другими системами, отсутствия к таким каналам связи доступа посторонних лиц на законном основании, не соответствия ценности информации в таких каналах связи уровню возможных рисков при ее съеме;
- в пределах контролируемой зоны каналы связи и коммуникационное оборудование доступно только для администраторов, доступ пользователей и обслуживающего персонала ограничен, коробка СКС опечатаны;

Ине. № подп	Подп. и дата					Лист	
	Взам. инв. №						41
	Ине. № дубл.						
	Подп. и дата						
	Ине. № инв.						
Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1		

- обслуживающий персонал при работе в помещениях, где расположены компоненты системы, сотрудники, не являющиеся пользователями, находятся в помещениях с компонентами ИСПДн только в присутствии сотрудников оператора связи.

Таблица 4.2 – УБПДн ИСПДн

№ п/п	Угрозы безопасности ПДн	Тип нарушителя				
		1	2	3	4	5
		Внешний нарушитель	Посетитель	Обслуживающий персонал	Сотрудник, не являющийся пользователем ИСПДн	Оператор ИСПДн
1	Угрозы утечки информации по техническим каналам					
1.1	Угрозы утечки видовой информации:					
1.1.1	визуальный просмотр на экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн	-	+	+	+	-
2	Угрозы НСД, сбоев, ошибок, отказов в ИСПДн					
2.1	Угрозы использования уязвимостей ИСПДн:					
2.1.1	неверные настройки ПО, изменение режимов работы ТС и ПО (случайное либо преднамеренное)	-	-	-	+	+
2.1.2	сбои в работе ТС и ПО (сбои в электропитании, выход из строя аппаратных элементов, внешние воздействия электромагнитных полей)	-	-	-	+	+
2.2	Угрозы непосредственного доступа в операционную среду ИСПДн:					
2.2.1	доступ в операционную среду (локальную ОС отдельного ТС ИСПДн) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ	-	-	-	+	+
2.2.2	доступ в среду функционирования прикладных программ (локальная СУБД, например)	-	-	-	+	-
2.2.3	доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности	-	-	-	+	-
2.3	Угрозы, реализуемые с использованием протоколов межсетевое взаимодействия:					
2.3.1	сканирование сети для изучения логики работы ИСПДн, выявления протоколов, портов	+	-	-	+	+
2.3.2	анализ сетевого трафика для изучения логики работы ИСПДн, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены	+	-	-	-	-
2.3.3	применение специальных программ для выявления пароля (IP-спуфинг, разные виды перебора)	+	-	-	+	-
2.3.4	подмена доверенного объекта сети с присвоением его прав доступа, внедрение ложного объекта сети	+	-	-	+	-
2.3.5	реализация угрозы отказа в обслуживании	+	-	-	+	+
2.3.6	внедрение специализированных троянов, вредоносных программ	+	-	-	+	+

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	
Ине. № подл.	

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

№ п/п	Угрозы безопасности ПДн	Тип нарушителя				
		1	2	3	4	5
		Внешний нарушитель	Посетитель	Обслуживающий персонал	Сотрудник, не являющийся пользователем ИСПДн	Оператор ИСПДн
2.3.7	сетевые атаки	+	-	-	+	+
2.3.8	применение утилит администрирования сети	+	-	-	+	+
2.4	Угрозы программно-математических воздействий:					
2.4.1	внедрение программных закладок (непосредственное)	-	-	-	+	+
2.4.2	внедрение вредоносных программ (случайное или преднамеренное, непосредственное)	-	-	-	+	+
2.5	Угрозы несанкционированного физического доступа к съемным носителям информации:					
2.5.1	повреждение носителя информации	+	+	+	+	+
2.5.2	утрата носителя информации	-	-	-	-	+
2.5.3	хищение носителя информации	+	+	+	+	+
2.6	Угрозы доступа к ТС и системам обеспечения:					
2.6.1	подключение к ТС и системам	+	-	-	+	+
2.6.2	нарушение функционирования кабельных линий связи, оборудования	+	-	-	+	+
2.6.3	нарушение функционирования ТС обработки информации, НЖМД	-	-	-	+	+
2.6.4	доступ к системам обеспечения, их повреждение	+	-	-	+	+
2.6.5	доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные)	+	+	+	+	+
2.7	Угрозы разглашения информации:					
2.7.1	разглашение информации лицам, не имеющим права доступа к ней	-	-	-	-	+
2.7.2	копирование информации на незарегистрированный носитель информации, в том числе печать	-	-	-	-	+
2.7.3	передача носителя информации лицу, не имеющему права доступа к имеющейся на нем информации	-	-	-	-	+

Ине. № подп	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат

4.3.5 Каналы атак

Перечень каналов атак представлен в таблице 4.3

Таблица 4.3 – Каналы атак

№ п/п	Каналы атак	Тип нарушителя				
		1	2	3	4	5
		Внешний нарушитель	Посетитель	Обслуживающий персонал	Сотрудник, не являющийся пользователем ИСПДн	Оператор ИСПДн
1.	Каналы связи (внутри и вне КЗ), незащищенные от НСД к информации организационно-техническими мерами	+	+	+	+	+
2.	Штатные средства ИСПДн	-	-	-	+	+
3.	Уязвимости и недокументированные (недекларированные) возможности	+	-	-	+	+
4.	Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический)	-	+	+	+	+
5.	Съемные носители информации	-	-	-	-	+
6.	Носители информации, выведенные из употребления и ставшие после этого доступными нарушителю	+	+	+	+	-
7.	Носители информации, сданные в ремонт, на обслуживание, переданные для использования другим пользователям или для использования за пределами КЗ	+	-	-	-	-
8.	Неучтенные носители информации	+	+	+	+	+
9.	Технические каналы утечки	+	-	-	-	-
10.	Защищаемая информация в виде распечатанных документов	-	+	+	+	-
11.	Сигнальные цепи	+	-	-	-	-
12.	Цепи электропитания	+	-	-	-	-
13.	Цепи заземления	+	-	-	-	-
14.	Канал утечки за счет электронных устройств негласного получения информации	+	-	-	-	-
15.	Информационные и управляющие интерфейсы СВТ	-	-	-	+	-
16.	Использование методов социальной инженерии на пользователей ИСПДн	+	+	+	+	-

Ине. № подп. Подп. и дата

Ине. № дубл. Подп. и дата

Взам. инв. №

Ине. № инв. №

Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

5. МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ

5.1 Описание методики

Определение актуальных угроз безопасности ПДн в ИСПДн проведено в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», от 14.02.2008 г., утвержденной заместителем директора ФСТЭК России.

Данная методика предполагает выполнение следующих этапов определения актуальных угроз.

- определение уровня исходной защищенности ИСПДн;
- определение частоты (вероятности) реализации угрозы;
- определение коэффициента реализуемости угроз;
- оценка опасности угрозы;
- выбор актуальных угроз.

Выбор актуальных угроз

На данном этапе осуществляется выбор из общего перечня угроз безопасности ПДн тех, которые относятся к актуальным.

Таблица 5.1 – Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Ине. № дубл.	Подп. и дата	Взам. инв. №	Подп. и дата	Ине. № подл.	Лист
Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-9/2009-ОМ1

Таблица 5.2 – Технические и эксплуатационные характеристики ИСПДн операторов связи

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
По территориальному размещению			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом			
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)			
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий			
локальная ИСПДн, развернутая в пределах одного здания	✓		
По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть общего пользования			
ИСПДн, имеющая одноточечный выход в сеть общего пользования			
ИСПДн, физически отделенная от сети общего пользования	✓		
По встроенным (легальным) операциям с записями баз персональных данных			
чтение, поиск			
запись, удаление, сортировка			
модификация, передача			✓
По разграничению доступа к персональным данным			
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн		✓	
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн			
ИСПДн с открытым доступом			
По наличию соединений с другими базами ПДн иных ИСПДн			
Интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации-владельцу данной ИСПДн	✓		
По уровню обобщения (обезличивания) ПДн			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			✓
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки			
ИСПДн, предоставляющая всю БД с ПДн			
ИСПДн, предоставляющая часть ПДн		✓	
ИСПДн, не предоставляющие никакой информации			
	Количество решений	3	2
	Общее количество решений		7

Ине. № подл.	Подп. и дата
	Взам. инв. №
Ине. № дубл.	
Ине. № подл.	Подп. и дата
Ине. № подл.	

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

71,4% характеристик ИСПДн соответствуют уровню не ниже 'средний'.
Остальные 28,6% соответствуют уровню 'низкий'.

Информационные системы персональных данных операторов связи, с техническими и эксплуатационными характеристиками, приведенными в таблице 5.2, функционирующие в условиях доверенной среды (см. раздел 2.1), имеют средний уровень исходной защищенности с коэффициентом $Y_1=5$.

Ине. № подп	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата	Ине. № докум.	Подп.	Дат	Лист
ICU-9/2009-OM1								

Определение частоты (вероятности) реализации угроз утечки акустической (речевой) информации

Частота (вероятность) реализации угроз считается маловероятной ($Y_2=0$), т.к. стоимость применения специальных технических средств съема акустической информации несоизмерима с содержанием этой информации.

Расчет коэффициента реализуемости угроз утечки акустической (речевой) информации

$$Y=(Y_1+ Y_2)/20=(5+0)/20=0.25$$

При $Y=0.25$, возможность реализации угрозы считается **НИЗКОЙ**.

Оценка опасности угроз утечки акустической (речевой) информации

Реализация данного вида угроз может привести лишь к незначительным негативным последствиям для субъекта ПДн. Опасность считается **НИЗКОЙ**.

Оценка актуальности

В соответствии с таблицей 5.1, угрозы утечки акустической (речевой) информации для операторов связи являются неактуальными.

6.2 Угрозы утечки видовой информации

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Кроме этого просмотр (регистрация) ПДн возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Носителями ПДн являются, в основном, мониторы пользователей ИСПДн, относящихся ко второй группе потенциальных внутренних нарушителей (см. раздел

Ине. № подл.	Подп. и дата
Ине. № дубл.	Подп. и дата
Взам. инв. №	Подп. и дата
Ине. № инв.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1

4.2 настоящего документа). Кроме того, носителями ПДн могут являться документы на бумажной основе, содержащие защищаемую информацию.

Перехват ПДн может вестись:

– стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц. В данном случае, наиболее вероятным нарушителем, является внешний нарушитель;

– портативной возимой аппаратурой, размещаемой в транспортных средствах осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями. В данном случае, наиболее вероятным нарушителем, является внешний нарушитель;

– портативной носимой аппаратурой – физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них. В данном случае, наиболее вероятными нарушителями являются внутренние нарушители, имеющие возможность санкционированного доступа в контролируемую зону (см. таблицу).

Для наблюдения за объектами на значительном расстоянии (от нескольких сот метров до нескольких километров) используются, как правило, стационарные средства:

– крупногабаритные устройства с телескопическими объективами (телескопы), обладающие высоким коэффициентом усиления, сопряженные с различного рода устройствами регистрации изображений;

– телевизионные камеры, в том числе работающие при низких уровнях освещённости объекта наблюдения и обладающие высоким коэффициентом усиления и устойчивостью к засветкам от попавших в поле зрения ярких источников света;

– приборы ночного видения пассивного или активного (с подсветкой) типа.

К портативным средствам наблюдения (регистрации), используемым на дальностях до сотен метров относятся:

– портативные аналоговые и цифровые фото- и видеокамеры;

Ине. № дубл.	Ине. № инв. №	Подп. и дата
Ине. № подп	Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1

- цифровые видеокамеры, в том числе встроенные в сотовые телефоны;
- миниатюрные видеокамеры с пинхол-объективами⁶.

В качестве автономной автоматической аппаратуры используются миниатюрные оптические приборы с возможностью перехвата (просмотра) ПДн на расстояниях десятков метров.

Определение частоты (вероятности) реализации угроз утечки видовой информации

Частота (вероятность) реализации угроз считается низкой ($Y_2=2$), объективные предпосылки для реализации угроз существуют, но принимаемые меры существенно затрудняют их реализацию:

- исключение просмотра текстовой и графической видовой информации обеспечивается использованием штор или жалюзи в помещениях, в которых установлены устройства отображения информации;
- мониторы рабочих мест (АРМ.А и АРМ.П) располагаются в местах, исключающих возможность прямой видимости между средством наблюдения и носителем ПДн.

Наиболее вероятным источником угроз данного типа являются внутренние нарушители, относящиеся ко второй категории и имеющие доступ подмножеству ПДн ИСПДн (см. таблицу).

Наиболее вероятными средствами наблюдения являются цифровые видеокамеры, в том числе встроенные в сотовые телефоны.

Расчет коэффициента реализуемости угроз утечки видовой информации

$$Y=(Y_1+ Y_2)/20=(5+2)/20=0.35$$

При $Y=0.35$, возможность реализации угрозы считается **СРЕДНЕЙ**

Оценка опасности угроз утечки видовой информации

Учитывая незначительный объем отображаемых данных, реализация данного вида угроз может привести лишь к незначительным негативным последствиям для субъекта ПДн. Опасность считается **НИЗКОЙ**.

⁶ Роль объектива выполняет малое отверстие

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист
						54

Оценка актуальности

В соответствии с таблицей 5.1, угрозы утечки видовой информации для операторов связи являются неактуальными.

6.3 Угрозы утечки информации по каналам ПЭМИН

Возникновение угроз утечки ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанными с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПДн.

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях технических средств ИСПДн сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИСПДн.

Регистрации ПЭМИН осуществляется с целью перехвата информации циркулирующей в технических средствах, осуществляющих обработку ПДн (средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки ПДн, средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и других технических средствах обработки речевой, графической, видео- и буквенно-цифровой информации).

Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

Кроме этого перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн («аппаратурные закладки»).

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	
Ине. № подл.	

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист
						55

Основными каналами утечки ПДн за счет ПЭМИН являются:

- побочные электромагнитные излучения информативных сигналов технических средств и линий передачи информации;
- наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы служебных помещений;
- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств ИСПДн, или при наличии паразитной генерации в узлах элементов технических средств;
- радиоизлучения, формируемые в результате высокочастотного облучения технических средств ИСПДн, в которых проводится обработка информативных сигналов (параметрические каналы утечки информации).

Регистрация ПЭМИН может вестись с использованием аппаратуры следующих видов:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;
- портативной возимой аппаратуры, размещаемой в транспортных средствах осуществляющих движение вблизи служебных помещений или при парковке рядом с этими помещениями;
- портативной носимой аппаратурой – физическими лицами в непосредственной близости от ИСПДн;
- автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами в непосредственной близости от ИСПДн.

Перехват сигналов ПЭМИН может осуществляться:

- программно-аппаратными комплексами перехвата;
- портативными сканерными приёмниками;
- цифровыми анализаторами спектра, управляемыми компьютерами со специальным программным обеспечением;

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Ине. № дубл.
Ине. № подл.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ИСУ-9/2009-ОМ1	Лист
						56

- селективными микровольтметрами.

Кроме этого, для перехвата ПДн, могут использоваться параметрические каналы утечки информации, формируемые в результате высокочастотного облучения технических средств ИСПДн, в которых проводится обработка ПДн, и приема переизлученного сигнала средствами, аналогичными средствам перехвата ПЭМИН. При съеме информации по параметрическому каналу для исключения взаимного влияния облучающего и переизлученного сигналов используется временная или частотная развязка.

Каналы утечки информации, обусловленные наводками, образуются за счет соединительных линий технических средств ИСПДн и ВТСС и посторонних проводников (в том числе цепей электропитания и заземления).

Наводки электромагнитных излучений технических средств ИСПДн возникают при излучении элементами технических средств ИСПДн информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий технических средств ИСПДн, линий ВТСС и посторонних проводников. В результате на случайных антеннах (цепях ВТСС или посторонних проводниках) наводится информативный сигнал.

Прохождение информативных сигналов в цепи электропитания возможно при наличии емкостной, индуктивной или гальванической связей источника информативных сигналов в составе технических средств ИСПДн и цепей питания. Информативный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информативного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информативного сигнала.

Прохождение информативных сигналов в цепи заземления обусловлено наличием емкостной, индуктивной или гальванической связи источника информативных сигналов в составе технических средств ИСПДн и цепей заземления. При этом кроме заземляющих проводников, служащих для непосредственного соединения технических средств ИСПДн с контуром заземления, гальваническую связь с данным контуром могут иметь различные проводники, выходящие за пределы контролируемой зоны (нулевой провод сети электропитания, экраны соединительных

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Ине. № инв.	Подп. и дата
Ине. № инв.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист 57

кабелей, металлические трубы систем отопления и водоснабжения). Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, на которую могут наводиться информативные сигналы.

Для съема информации с проводных линий могут использоваться:

- средства съёма сигналов, содержащих защищаемую информацию, с цепей технических средств ИСПДн и ВТСС, линий связи и передачи данных, выходящих за пределы служебных помещений (эквиваленты сети, токовые трансформаторы, пробники);
- средства съёма наведённых информативных сигналов с цепей электропитания;
- средства съёма наведённых информативных сигналов с шин заземления;
- средства съёма наведённых информативных сигналов с проводящих инженерных коммуникаций.

Для волоконно-оптической системы передачи данных угрозой утечки информации является утечка оптического излучения, содержащего защищаемую информацию, с боковой поверхности оптического волокна за счет:

- физического процесса распространения оптического излучения с поверхности оптического волокна при его возбуждении внешними источниками излучения;
- релеевского, молекулярного и Ми-рассеяния, вызванных флуктуациями оптической плотности материалов;
- особенностей технологии изготовления оптического кабеля (на разъёмных и не разъёмных соединениях, на продольных изгибах, вызванных при изготовлении и прокладке оптического кабеля).

Появление новых каналов связи – сотовой связи, пейджинговых сообщений, спутниковых и беспроводных сетей передачи данных привело к развитию специализированных систем и средств контроля и перехвата информации, ориентированных на используемые в них информационные технологии, в том числе средств:

Ине. № подл.
Подп. и дата
Ине. № дубл.
Взам. инв. №
Подп. и дата
Ине. № инв.

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1

- перехвата пейджинговых сообщений и сотовой связи;
- перехвата информации в каналах передачи данных вычислительных сетей.

Определение частоты (вероятности) реализации угроз утечки информации по каналам ПЭМИН

Частота (вероятность) реализации угроз считается низкой ($Y_2=2$), объективные предпосылки для реализации угроз существуют, но принимаемые меры существенно затрудняют их реализацию:

- технические (аппаратные) средства ИСПДн, используемые для обработки ПДн, соответствуют требованиям стандартов Российской Федерации по электромагнитной совместимости, безопасности и санитарным нормам;
- технические (аппаратные) средства ИСПДн размещаются в специально оборудованных помещениях в пределах КЗ, что приводит к ослаблению побочных электромагнитных излучений (в том числе информативных сигналов) на границе КЗ до величин, обеспечивающих значительную сложность их выделения средством перехвата на фоне естественных шумов в условиях высокой энергонасыщенности.

Кроме того, стоимость реализации угроз утечки информации по каналам ПЭМИН, выраженная в стоимости специального оборудования и его эксплуатации, представляется значительной и несопоставимо превышающей возможный ущерб от нарушения конфиденциальности.

Расчет коэффициента реализуемости угроз утечки информации по каналам ПЭМИН

$$Y=(Y_1+ Y_2)/20=(5+2)/20=0.35$$

При $Y=0.35$, возможность реализации угрозы считается **СРЕДНЕЙ**.

Оценка опасности угроз утечки информации по каналам ПЭМИН

Реализация данного вида угроз может привести лишь к незначительным негативным последствиям для субъекта ПДн. Опасность считается **НИЗКОЙ**.

Оценка актуальности

В соответствии с таблицей 5.1 угрозы утечки информации по каналам ПЭМИН для операторов связи являются **НЕАКТУАЛЬНЫМИ**.

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Ине. № инв.	Подп. и дата
Ине. № инв.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист
						59

– встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессоры, микросхемы системных плат, видеоадаптеров, сетевых плат, звуковых плат, модемов, устройств ввода/вывода, магнитных жестких и оптических дисков, блоков питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода-вывода);

– микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.);

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

- пакеты передаваемых по сети сообщений;
- файлы (текстовые, графические, исполняемые и т.д.).

2) **Уязвимости программного и (или) аппаратного обеспечения**

Уязвимость ИСПДн - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении, которое может быть использовано для реализации угроз безопасности ПДн.

В ИСПДн рассматриваются следующие уязвимости:

- уязвимости программного обеспечения (наличие в ИСПДн вредоносной программы);
- уязвимости, вызванные наличием в ИСПДн программно-аппаратной закладки;
- уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных;
- уязвимости, вызванные недостатками организации технической защиты информации (ТЗИ) от НСД;
- уязвимости средств защиты информации (СЗИ);
- уязвимости программно-аппаратных средств ИСПДн в результате сбоев в работе, отказов этих средств.

Ине. № дубл.	Ине. № подп
Взам. инв. №	Подп. и дата
Подп. и дата	Подп. и дата

8. ТИПОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРОВ СВЯЗИ

8.1 Общие положения

В зависимости от целей и содержания обработки ПДн оператор связи может осуществлять обработку ПДн в ИСПДн различных типов.

В настоящем разделе приводится типовая модель угроз безопасности персональных данных, обрабатываемых в ИСПДн операторов связи имеющих характеристики (исходные данные) приведенные в разделе 2.2 настоящего документа.

Типовая модель угроз безопасности ПДн, характеризует наступление различных видов последствий в результате несанкционированного или случайного доступа и реализации УБПДн.

В типовой модели угроз, рассматриваются угрозы связанные с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в ней ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Угрозы, связанные с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения, в типовой модели угроз не рассматриваются в силу их неактуальности (см. раздел 6 настоящего документа).

Частные модели угроз безопасности ПДн, применительно к конкретным ИСПДн, составляются операторами связи на этапах их создания и (или) эксплуатации.

При разработке частных моделей угроз учитываются:

- требования нормативно-методических документов ФСТЭК России;
- требования к содержанию модели угроз и модели нарушителя, предъявляемые ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения;

Подп. и дата
Взам. инв. №
Инв. № дубл.
Подп. и дата
Инв. № подл.

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1

- положения настоящей Модели угроз.

Определение (оценка) актуальности угроз НСД к информации производится на этапе разработки частных моделей угроз в соответствии с методикой определения актуальных угроз (см. раздел 5.1 настоящего документа).

При определении (оценке) актуальности угроз НСД, учитываются положения «Низкоуровневого анализа рисков нарушения безопасности персональных данных в информационных системах персональных данных операторов связи с определением каналов реализации угроз безопасности персональных данных» (ICU-6/2009-AP2).

8.2 Типовая модель угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных операторов связи

При обработке ПДн в информационных системах персональных данных, имеющих характеристики (исходные данные) приведенные в разделе 2.2 настоящего документа и функционирующие в условиях доверенной среды, возможна реализация следующих угроз несанкционированного доступа к информации:

1) Угрозы непосредственного доступа

Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода ИСПДн.

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн.

Угрозы, реализуемые в ходе загрузки операционной системы

Эти угрозы направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода-вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИСПДн. Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации.

Угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем

Эти угрозы направлены на выполнение непосредственно несанкционированного доступа к информации. При получении доступа в

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Ине. № инв.	Подп. и дата
Ине. № инв.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1

операционную среду нарушитель может воспользоваться как стандартными функциями операционной системы или какой-либо прикладной программы общего пользования (например, СУБД), так и специально созданными для выполнения несанкционированного доступа программами.

Угрозы, реализуемые после загрузки операционной среды зависящие от того, какая из прикладных программ запускается пользователем или уже запущена

Большая часть таких угроз – это угрозы внедрения вредоносных программ.

2) Угрозы удаленного доступа

Угрозы удаленного доступа реализуются с использованием протоколов межсетевого взаимодействия.

Анализ сетевого трафика

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль.

Сканирование сети

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них.

Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Угроза выявления пароля

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей.

Ине. № подп	Подп. и дата
Ине. № дубл.	Взам. инв. №
Подп. и дата	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1

Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа

Под доверенным объектом понимается объект сети (компьютер межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

В результате возможно изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных, несанкционированный доступ к сетевым ресурсам, навязывание ложной информации.

Навязывание ложного маршрута сети

Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации и управления сетью для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае, если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска, заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

Отказ в обслуживании

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается или не в состоянии обрабатывать поступающие пакеты.

Удаленный запуск приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы,

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Ине. № подл.	Подп. и дата
Ине. № подл.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1	Лист 66

«сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста.

3) **Угрозы создания нештатных режимов работы**

Угрозы создания нештатных режимов работы программных (программно - аппаратных) средств - это угрозы «Отказа в обслуживании».

Их реализация обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

- содержания служебной информации в пакетах сообщений, передаваемых по сети;
- условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);
- форматов представления данных (с несоответствием измененных форматов установленных для обработки по протоколам сетевого взаимодействия);
- программного обеспечения обработки данных.

В результате реализации угроз «Отказа в обслуживании» происходит переполнение буферов и блокирование процедур обработки, «зацикливание» процедур обработки и «зависание», отбрасывание пакетов сообщений и др.

4) **Угрозы внедрения по сети вредоносных программ (программ математического воздействия)**

Основными видами вредоносных программ являются:

- программные закладки;
- классические программные вирусы;
- вредоносные программы, распространяющиеся по сети (сетевые черви);
- другие вредоносные программы, предназначенные для осуществления НСД.

Подп. и дата
Взам. инв. №
Инв. № дубл.
Подп. и дата
Инв. № подл.

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИСПДн, в процессе его разработки, сопровождения, модификации и настройки.

5) **Комбинированные угрозы**

Комбинированные угрозы представляют собой комбинацию всевозможных УБПДн. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду ИСПДн, в том числе путем формирования нетрадиционных информационных каналов доступа.

Нетрадиционный информационный канал - это канал скрытной передачи информации с использованием традиционных каналов связи и специальных преобразований передаваемой информации, не относящихся к криптографическим.

Для формирования нетрадиционных каналов могут использоваться методы:

- компьютерной стеганографии;
- основанные на манипуляции различных характеристик ИСПДн, которые можно получать санкционировано (например, времени обработки различных запросов, объемов доступной памяти или доступных для чтения идентификаторов файлов или процессов и т.п.).

Ине. № подп					Подп. и дата
Ине. № дубл.					Взам. инв. №
Подп. и дата					Подп. и дата
					Лист
ICU-9/2009-OM1					68
Ли	Изм.	№ докум.	Подп.	Дат	

9. ЗАКЛЮЧЕНИЕ

С использованием данных о классе информационной системы персональных данных⁷ и составленного перечня актуальных угроз⁸, на основе:

- нормативно-методических документов ФСТЭК России;
- профилей защиты:
 - специальная информационная система персональных данных Оператора связи класса «Автоматизированное рабочее место». Профиль защиты. (ICU-12/2009-ПЗ1);
 - специальная информационная система персональных Данных Оператора связи второго класса. Профиль защиты. (ICU-13/2009-ПЗ2);
 - специальная информационная система персональных данных Оператора связи третьего класса. Профиль защиты. (ICU-14/2009-ПЗ3),

формулируются конкретные организационно-технические требования по защите информационных систем персональных данных, и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

На основе методических документов ФСТЭК России, ФСБ России, с использованием данных о типе нарушителя и предположениях о его возможностях, средствах и каналах атак (раздел 4), определяется необходимость использования СКЗИ:

- ИСПДн в пределах КЗ – СКЗИ не требуется, если безопасность ПДн обеспечивается другими методами и способами;
- контролируемые каналы связи – СКЗИ не требуется;
- открытые каналы связи - необходимо применять СКЗИ;

⁷ Классификация информационных систем персональных данных операторов связи производится с учетом положений Отраслевого классификатора (ICU-4/2009-ОК).

⁸ Составление перечня актуальных угроз безопасности персональных данных, производится на этапе разработки частных моделей угроз безопасности персональных данных.

Ине. № подл	Подп. и дата					Лист	
	Взам. инв. №						ICU-9/2009-ОМ1
	Ине. № дубл.						
	Подп. и дата						
					69		
	Ли	Изм.	№ докум.	Подп.	Дат		

- неконтролируемые каналы связи – в случае отсутствия гарантии безопасности ПДн со стороны организаций, предоставляющих каналы связи, необходимо применять СКЗИ;
- мобильное рабочее место (МРМ) – необходимо применять СКЗИ как в канале связи с МРМ, так и на МРМ (шифрование информации на накопителях во время обработки и хранения).

В связи с тем, что информационные системы персональных данных операторов связи по своим характеристикам и номенклатуре угроз безопасности персональных данных близки к наиболее распространенным информационным системам, целесообразно при их защите максимально использовать традиционные подходы к технической защите информации в автоматизированных системах.

При выборе криптографических средств защиты персональных данных необходимо использовать сертифицированные в системе сертификации ФСБ России криптографические средства защиты информации.

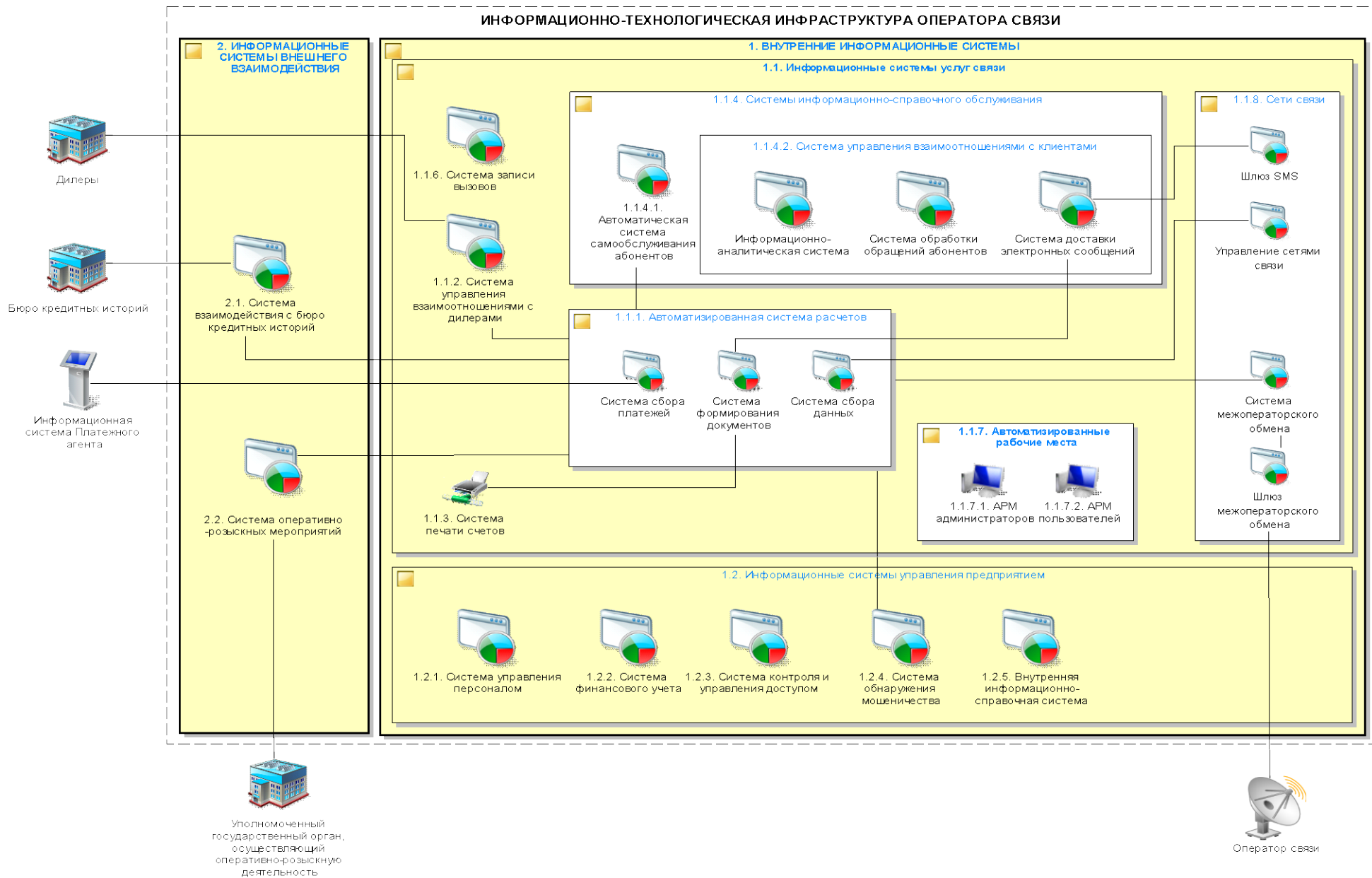
При выборе программных и технических средств защиты (некриптографических средств) рекомендуется использовать сертифицированные средства защиты информации.

Ине. № подл	Подп. и дата				Ине. № дубл.	Взам. инв. №	Подп. и дата	Ине. № подл	Лист
	Подп. и дата								
Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-OM1				70

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Изм.	
Лист	
№ докум.	
Подп.	
Дата	
ISU-9/2009-ОМ1	
Лист	71

Приложение 1. ИТ ИНФРАСТРУКТУРА ОПЕРАТОРА СВЯЗИ



10. Отраслевой классификатор. Информационные системы персональных данных операторов связи. (ICU-4/2009-ОК).

11. Специальная информационная система персональных данных Оператора связи класса «Автоматизированное рабочее место». Профиль защиты. (ICU-12/2009-ПЗ1).

12. Специальная информационная система персональных Данных Оператора связи второго класса. Профиль защиты. (ICU-13/2009-ПЗ2).

13. Специальная информационная система персональных данных Оператора связи третьего класса. Профиль защиты. (ICU-14/2009-ПЗ3).

14. Низкоуровневый анализ рисков нарушения безопасности персональных данных в информационных системах персональных данных операторов связи с определением каналов реализации угроз безопасности персональных данных. (ICU-6/2009-AP2).

15. Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Введена в действие приказом от 13 июня 2001 года № 152 (ФАПСИ).

16. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), введено приказом ФСБ РФ от 9 февраля 2005 г. № 66.

17. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622.

18. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные руководством 8 центра ФСБ РФ 21 февраля 2008 года № 149/54-144.

Подп. и дата
Взам. инв. №
Инв. № дубл.
Подп. и дата
Инв. № подл.

Ли	Изм.	№ докум.	Подп.	Дат	ICU-9/2009-ОМ1	Лист
						73

Приложение 3. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
АРМ.А	Автоматизированное рабочее место администратора
АРМ.П	Автоматизированное рабочее место пользователя
ВТСС	Вспомогательные технические средства и системы
ИС	Информационная система
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
КИС	Корпоративная информационная система
КОИ	Криптографически опасная информация
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПМВ	Программно-математическое воздействие
ПО	Программное обеспечение
ПТК	Программно-технический комплекс
ПЭМИН	Побочные электромагнитные излучения и наводки
СВТ	Средства вычислительной техники
СКЗИ	Система криптографической защиты информации
СФК	Среда функционирования криптосредства
УБПДн	Угрозы безопасности персональных данных
ФЗ	Федеральный закон
ФСБ России	Федеральная служба безопасности России
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Ине. № дубл.	Взам. инв. №	Подп. и дата
Ине. № подл.	Подп. и дата	Ине. № подл.
Ли	Изм.	№ докум.
Подп.	Дат	

Приложение 4. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Автоматизированная система (АС)	Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
Атака	Целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности
Доверенная среда эксплуатации ИСПДн	Среда эксплуатации ИСПДн, обеспечение требуемых характеристик безопасности (необходимого уровня безопасности) в которой гарантируется выполнением требований разрешительных документов уполномоченных федеральных органов, включая ФСБ России и (или) ФСТЭК России.
Доверие	Основание для уверенности в том, что сущность отвечает своим целям безопасности.
Достоверность (аутентичность)	Свойство обеспечения идентичности субъекта или ресурса заявленной идентичности
Доступ к информации	Возможность получения информации и ее использования
Доступность информации	Состояние информации, характеризующееся способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия
Защита информации	Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
Защита информации от несанкционированного доступа	Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.
Защита конфиденциальности ПДн	Способность ИСПДн обеспечить санкционированный доступ на чтение (копирование) информации субъекту доступа, в соответствии с его правами, предусмотренными политикой информационной безопасности
Защита целостности ПДн	Способность ИСПДн обеспечить санкционированный доступ на изменение (уничтожение) информации субъекту доступа, в соответствии с его правами, предусмотренными политикой информационной безопасности
Идентификация	Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных

Ине. № подл.	Подп. и дата
	Взам. инв. №
Ине. № дубл.	Подп. и дата
	Ине. № инв.
Ине. № подл.	Подп. и дата
	Ине. № инв.
Ине. № подл.	Подп. и дата
	Ине. № инв.

Термин	Определение
	идентификаторов
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 средств автоматизации или без использования таких средств
Информационно-телекоммуникационная сеть общего пользования	Информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано
Информация	Сведения (сообщения, данные) независимо от формы их представления
Канал атаки	Среда переноса от субъекта атаки (а, возможно, и о объекта к субъекту атаки) действий, осуществляемых при проведении атаки
Контролируемая зона (КЗ)	Пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств
Конфиденциальная информация (КИ)	Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации
Конфиденциальность информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
Криптографически опасная информация (КОИ)	Информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения
Криптосредство	Шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну
Локальная вычислительная сеть (ЛВС)	Совокупность основных технических средств и систем, осуществляющих обмен информацией между собой и с другими информационными системами, в том числе с ЛВС, через определенные точки входа/выхода информации, которые являются границей ЛВС
Межсетевой экран (МЭ)	Локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и (или) выходящей из АС
Модель нарушителя	Предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности».
Модель угроз	Перечень возможных угроз

Ине. № подл.	Подп. и дата
Ине. № дубл.	Взам. инв. №
Ине. № инв.	Подп. и дата
Ине. № подл.	Подп. и дата

Ли	Изм.	№ докум.	Подп.	Дат
----	------	----------	-------	-----

Термин	Определение
Нарушитель безопасности ПДн	Физическое лицо случайно или преднамеренно совершающее действия, следствием которого является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных
Носитель информации	Физическое лицо, или материальный объект, в том числе, физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов
Обеспечение доступности информации	Способность СЗИ безошибочно (ошибки второго рода) аутентифицировать субъект, запросивший доступ к информации, и предоставлять ему права, предусмотренные политикой информационной безопасности
Объект доступа	Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа
Объект защиты	Информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации
Персональные данные (ПДн)	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
Пользователь	Сотрудник организации, обладающий учетной записью АС, полученной в установленном порядке
Система защиты информации (СЗИ)	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
Средство криптографической защиты информации (СКЗИ)	Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности
Социальная инженерия	Метод несанкционированного доступа к информации или системам хранения информации без использования технических средств
Субъект атаки	Лицо (или иницируемый им процесс), проводящее (проводящий) атаку
Уровень криптографической защиты информации	Совокупность требований, предъявляемых к криптосредству
Целостность информации	Состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и

Ине. № дубл.	Подп. и дата			
	Взам. инв. №			
Ине. № подл.	Подп. и дата			
	Ине. № подл.			
Ли	Изм.	№ докум.	Подп.	Дат

Термин	Определение
	неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения

Ине. № подл	Подп. и дата	Ине. № дубл.	Взам. инв. №	Подп. и дата
-------------	--------------	--------------	--------------	--------------

Ли	Изм.	№ докум.	Подп.	Дат