МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Прикладной информатики

БАКАЛАВРСКАЯ РАБОТА

На тему

РАЗРАБОТКА СИСТЕМЫ АВТОМАТИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ЗАЩИТЫ ИНФОРМАЦИИ

Исполнитель
Смольников Сергей Александрович

Руководитель
доктор технических наук
профессор Истомин Евгений Петрович

«К защите допускаю»
Заведующий кафедрой

кандидат технических наук
Слесарева Людмила Сергеевна

«27» 06 2016 г.

Санкт–Петербург
2016

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Прикладной информатики

БАКАЛАВРСКАЯ РАБОТА

На тему

РАЗРАБОТКА СИСТЕМЫ АВТОМАТИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ЗАЩИТЫ ИНФОРМАЦИИ

Исполнитель
Смольников Сергей Александрович

Руководитель
доктор технических наук
профессор Истомин Евгений Петрович

«К защите допускаю»
Заведующий кафедрой

кандидат технических наук
Слесарева Людмила Сергеевна

«___»_____20__г.

Санкт–Петербург
2016

Содержание

Введение

Что такое информация? Информацией являются сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы в процессе жизнедеятельности и работы.

Информационная среда уже давно стала неотъемлемой частью нашей повседневной жизни, каждый день мы так или иначе имеем дело со средствами сбора, обработки, хранения и распространения информации.

По этой причине на современном «цифровом» этапе развития общества, защита информации как никогда актуальна. Зачастую, злоумышленникам нужны сведения, которые хранятся в базах данных крупных организаций. Всё чаще и чаще в средствах массой информации публикуются статьи, на тему популярных видах махинаций, связанных с рассылкой сообщений на мобильный телефон и электронную почту. А ведь получив доступ к БД с данными о пользователях, преступники могут шантажировать любого человека, его близких, или же испортить ему репутацию, выложив конфиденциальную информацию.

Защищенность персональных данных актуальна в России, поскольку Федеральные Законы, касающиеся этой области, существуют не так давно. По этой причине, нередко люди, ответственные за обработку персональных данных не знаю самых очевидных правил безопасности, доверенных им сведений. В связи с этим, на специалистов по информационной безопасности ложиться не только ответственность за безопасность информационной системы в организации, но и система обучения персонала этой фирмы.

Персональными данными являются такие сведения о человеке, как фамилия, имя, отчество, число, месяц, год и место рождения, адрес жительства, семейное и социальное положение, образование, имущество, вид профессии, уровень доходов и многое другое, то есть такие сведения относятся к информации

ограниченного доступа и должны быть защищены в соответствии с законодательством Российской Федерации.

В случае не соблюдения положений, организация может быть привлечена к судебному разбирательству (вплоть до приостановления действий, аннулирования соответствующих лицензий), а виновные люди – к гражданской, уголовной, административной, дисциплинарной ответственности.

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

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

1. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 План предпроектного обследования

Предпроектное обследование состоит из алгоритма, который состоит из ниже перечисленных действий.

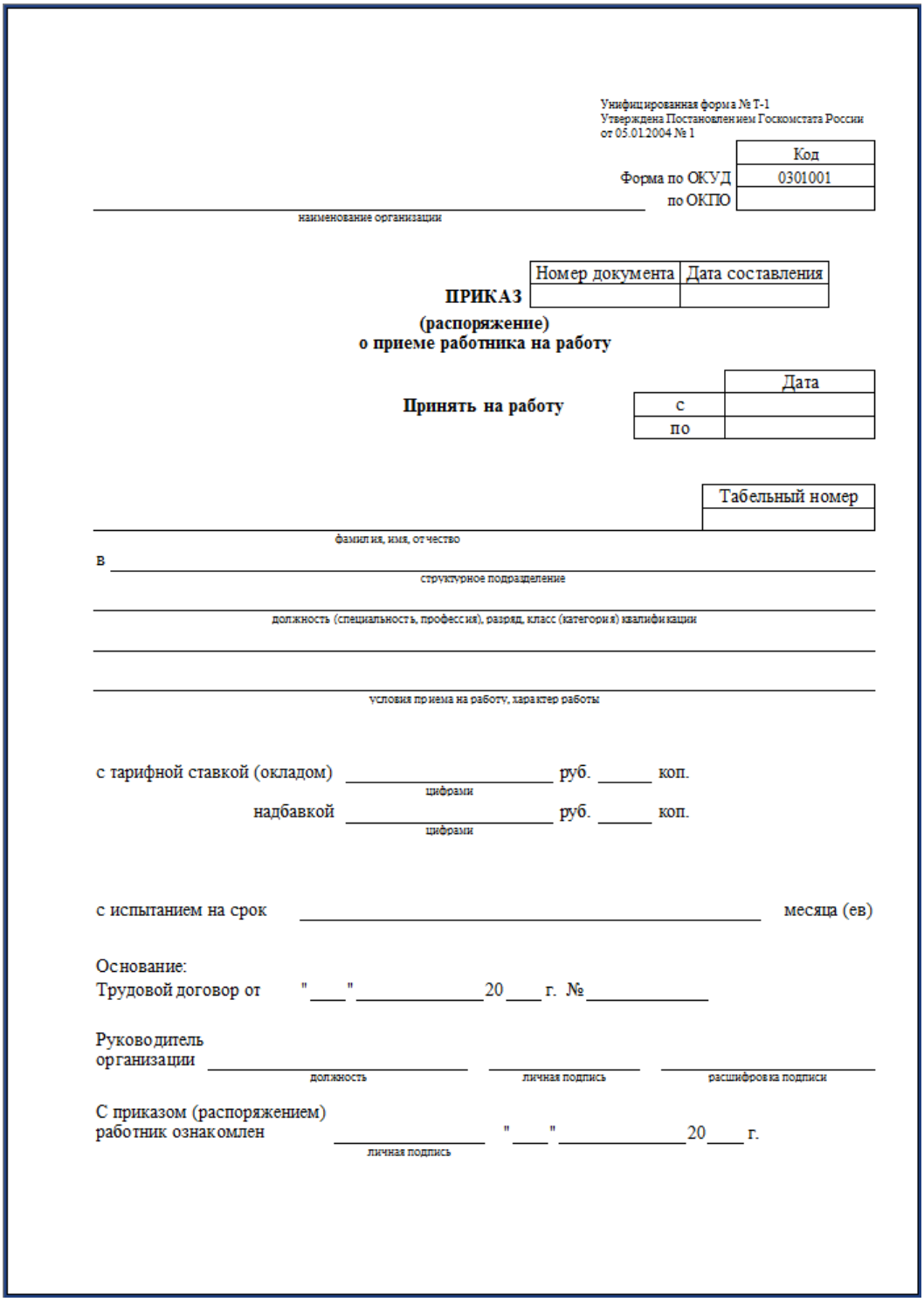
1. Необходимо посчитать сколько информационных систем персональных данных, узнать их состав, предназначение и определить какие границы имеет каждая система.
2. Определить какие именно персональные данные использует информационная система.
3. Необходимо определить законна ли обработка персональных данных, наличие согласия от субъектов на обработку персональных данных, знает ли Регулятор о осуществлении процедуры обработки.
4. С какой целью создаётся информационная система персональных данных и какими способами будет происходить обработка персональных данных в каждой информационной системе защиты персональных данных.
5. Определить какие технические, программные средства и системы будут использоваться в информационной системе персональных данных и их количество.
6. Разработать частную модель угроз безопасности персональных данных – для каждой информационной системы персональных данных.
7. Определить необходимые класс информационной системы персональных данных – для каждой информационной системы персональных данных.
8. Определить степень участия сотрудников в обработке персональных данных, распределить роли и обязанности.
9. Разработать организационно-распорядительный и регламентную документацию (приказы, инструкции, журналы учета, положения и др.).

Первоначальные документы в организации:

В отделе кадров:

№Т-1 «Распоряжение (или приказ) о приёме рабочего на работу в штат»,

№Т-1а «Распоряжение (или приказ) о приёме рабочих на работу в штат».



Унифицированная форма № Т-1
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

	Код
Форма по ОКУД	0301001
по ОКПО	

_____
наименование организации

Номер документа	Дата составления

ПРИКАЗ
(распоряжение)
о приеме работника на работу

	Дата
с	
по	

Принять на работу

Табельный номер

_____
фамилия, имя, отчество

в _____
структурное подразделение

_____
должность (специальность, профессия), разряд, класс (категория) квалификации

_____

_____
условия приема на работу, характер работы

с тарифной ставкой (окладом) _____ руб. _____ коп.
цифрами

надбавкой _____ руб. _____ коп.
цифрами

с испытанием на срок _____ месяца (ев)

Основание:
Трудовой договор от "___" _____ 20___ г. №_____

Руководитель
организации _____ _____ _____
должность личная подпись расшифровка подписи

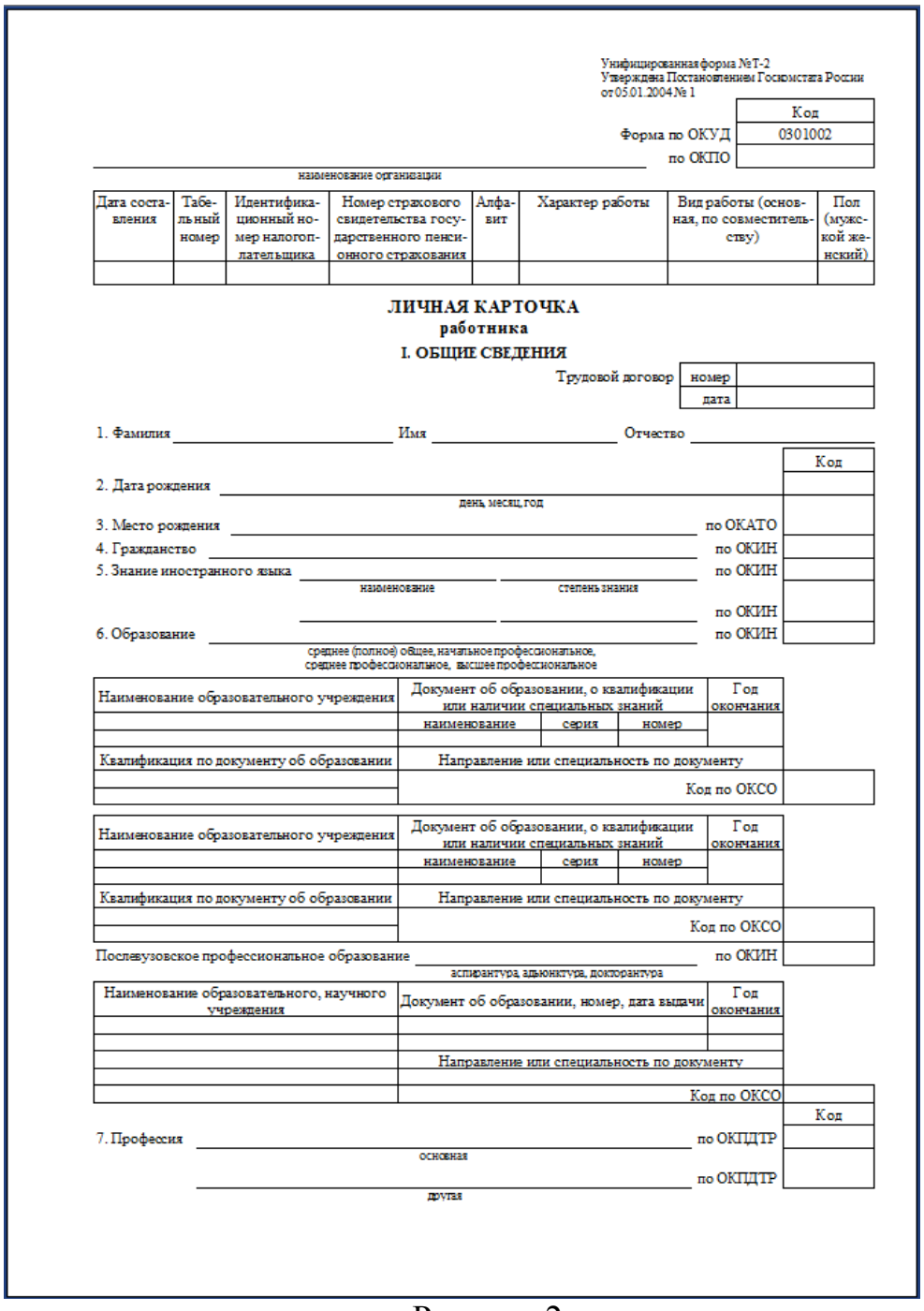
С приказом (распоряжением)
работник ознакомлен _____ "___" _____ 20___ г.
личная подпись

Рисунок 1

Вышеперечисленные документы применяются при оформлении сотрудника или сотрудников на штатную работу. Такие документы хранятся 75 лет.

Бланк формы №Т-2 «Личная карточка работника» (Рисунок 2).

Бланк формы №Т-2ГС(МС) «Личная карточка государственного (муниципального) служащего».



Унифицированная форма №Т-2
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

	Код
Форма по ОКУД	0301002
по ОКПО	

наименование организации

Дата составления	Табельный номер	Идентификационный номер налогоплательщика	Номер страхового свидетельства государственного пенсионного страхования	Алфавит	Характер работы	Вид работы (основная, по совместительству)	Пол (мужской женский)

ЛИЧНАЯ КАРТОЧКА
работника
I. ОБЩИЕ СВЕДЕНИЯ

Трудовой договор	номер	
	дата	

1. Фамилия _____ Имя _____ Отчество _____

	Код
2. Дата рождения _____ (день, месяц, год)	
3. Место рождения _____ по ОКАТО	
4. Гражданство _____ по ОКИН	
5. Знание иностранного языка _____ (наименование) _____ (степень знания) по ОКИН	
_____ _____ по ОКИН	
6. Образование _____ по ОКИН	

(среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное)

Наименование образовательного учреждения	Документ об образовании, о квалификации или наличии специальных знаний			Год окончания
	наименование	серия	номер	
Квалификация по документу об образовании	Направление или специальность по документу			
	Код по ОКСО			

Наименование образовательного учреждения	Документ об образовании, о квалификации или наличии специальных знаний			Год окончания
	наименование	серия	номер	
Квалификация по документу об образовании	Направление или специальность по документу			
	Код по ОКСО			
Послевузовское профессиональное образование _____ (аспирантура, адъюнктура, докторантура) по ОКИН				

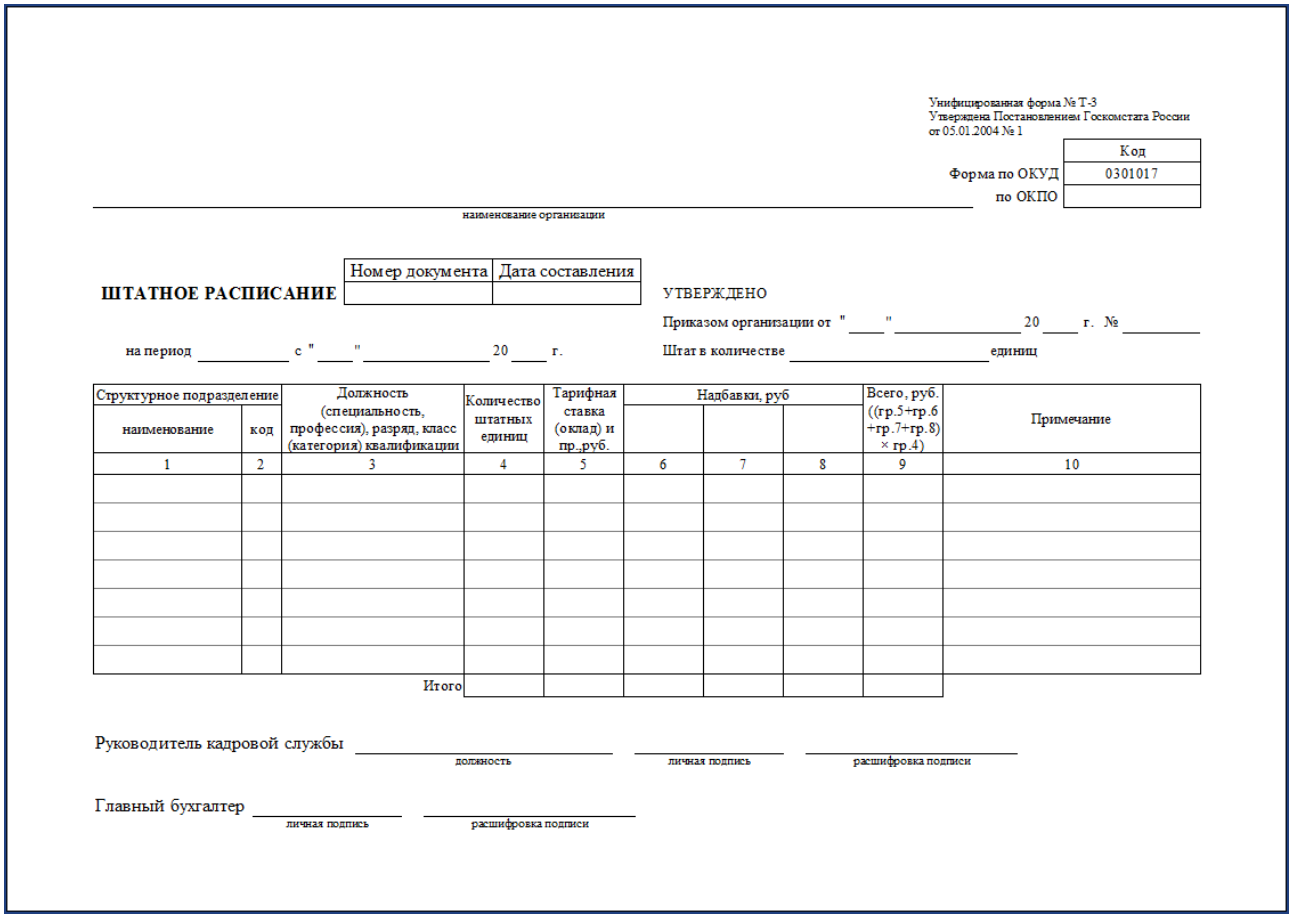
Наименование образовательного, научного учреждения	Документ об образовании, номер, дата выдачи	Год окончания
	Направление или специальность по документу	
	Код по ОКСО	

	Код
7. Профессия _____ (основная) по ОКПДТР	
_____ (другая) по ОКПДТР	

Рисунок 2

Каждый работник организации, без исключения, после заключения договора о приёме на работу, должен иметь личную карточку (бланк формы №Т-2), что позволяет учитывать данные о сотрудниках. Срок хранения таких документов - 75 лет.

Бланк формы №Т-3 «Штатное расписание» (Рисунок 3).



Унифицированная форма № Т-3
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

	Код
Форма по ОКУД	0301017
по ОКПО	

_____
наименование организации

ШТАТНОЕ РАСПИСАНИЕ

Номер документа	Дата составления

УТВЕРЖДЕНО
Приказом организации от "____" _____ 20____ г. № _____

на период _____ с "____" _____ 20____ г.
Штат в количестве _____ единиц

Структурное подразделение		Должность (специальность, профессия), разряд, класс (категория) квалификации	Количество штатных единиц	Тарифная ставка (оклад) и пр.,руб.	Надбавки, руб			Всего, руб. ((гр.5+гр.6 +гр.7+гр.8) × гр.4)	Примечание
наименование	код								
1	2	3	4	5	6	7	8	9	10
		Итого							

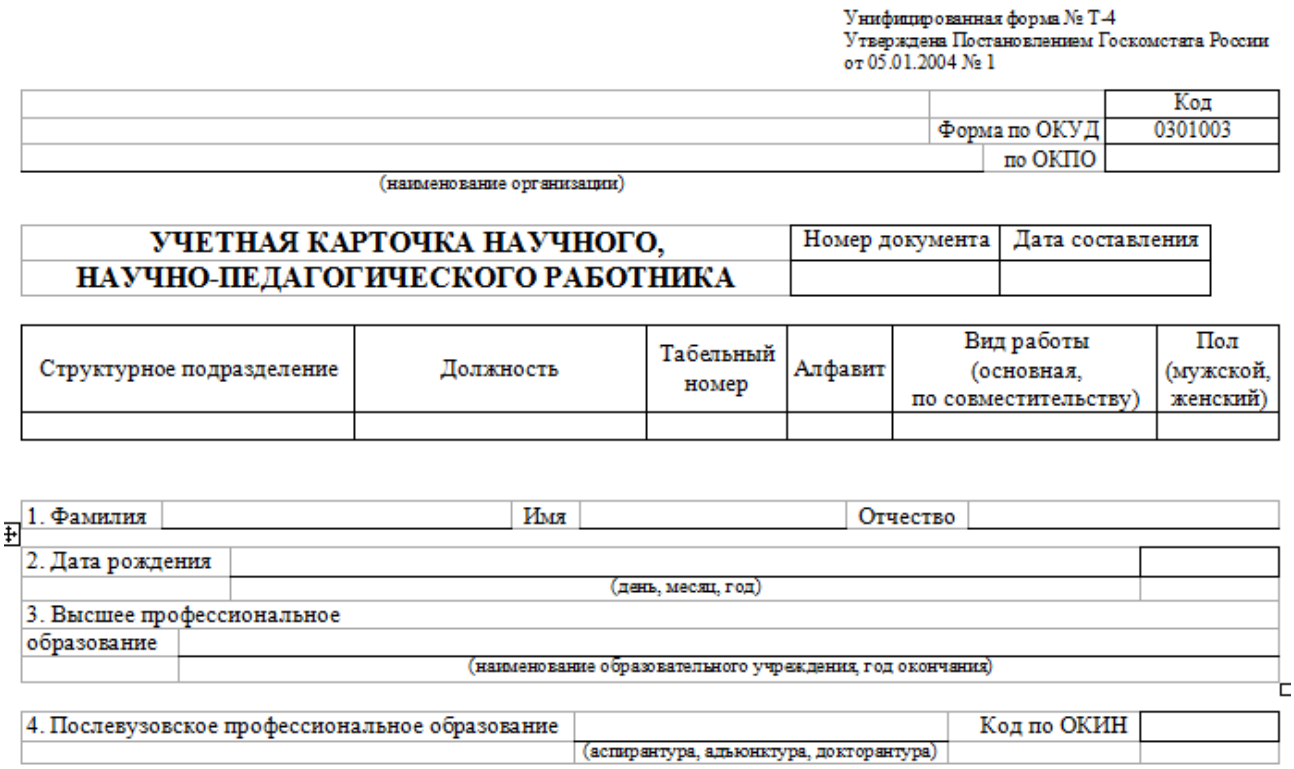
Руководитель кадровой службы _____ _____ _____
должность личная подпись расшифровка подписи

Главный бухгалтер _____ _____
личная подпись расшифровка подписи

Рисунок 3

Данная форма является важным и неотъемлемым документом, который отражает структуру и штатную численность организации и содержит список подразделений, должностей, данные о количестве должностных окладов, надбавок и сумме месячной заработной платы, соответственно перед составлением документа, необходимо разобраться со структурой организации. Такой документ хранится 3 года.

Бланк формы №Т-4 «Учетная карточка научного, научно-педагогического работника» (Рисунок 4).



Унифицированная форма № Т-4
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

		Код
	Форма по ОКУД	0301003
	по ОКПО	

(наименование организации)

УЧЕТНАЯ КАРТОЧКА НАУЧНОГО, НАУЧНО-ПЕДАГОГИЧЕСКОГО РАБОТНИКА	Номер документа	Дата составления

Структурное подразделение	Должность	Табельный номер	Алфавит	Вид работы (основная, по совместительству)	Пол (мужской, женский)

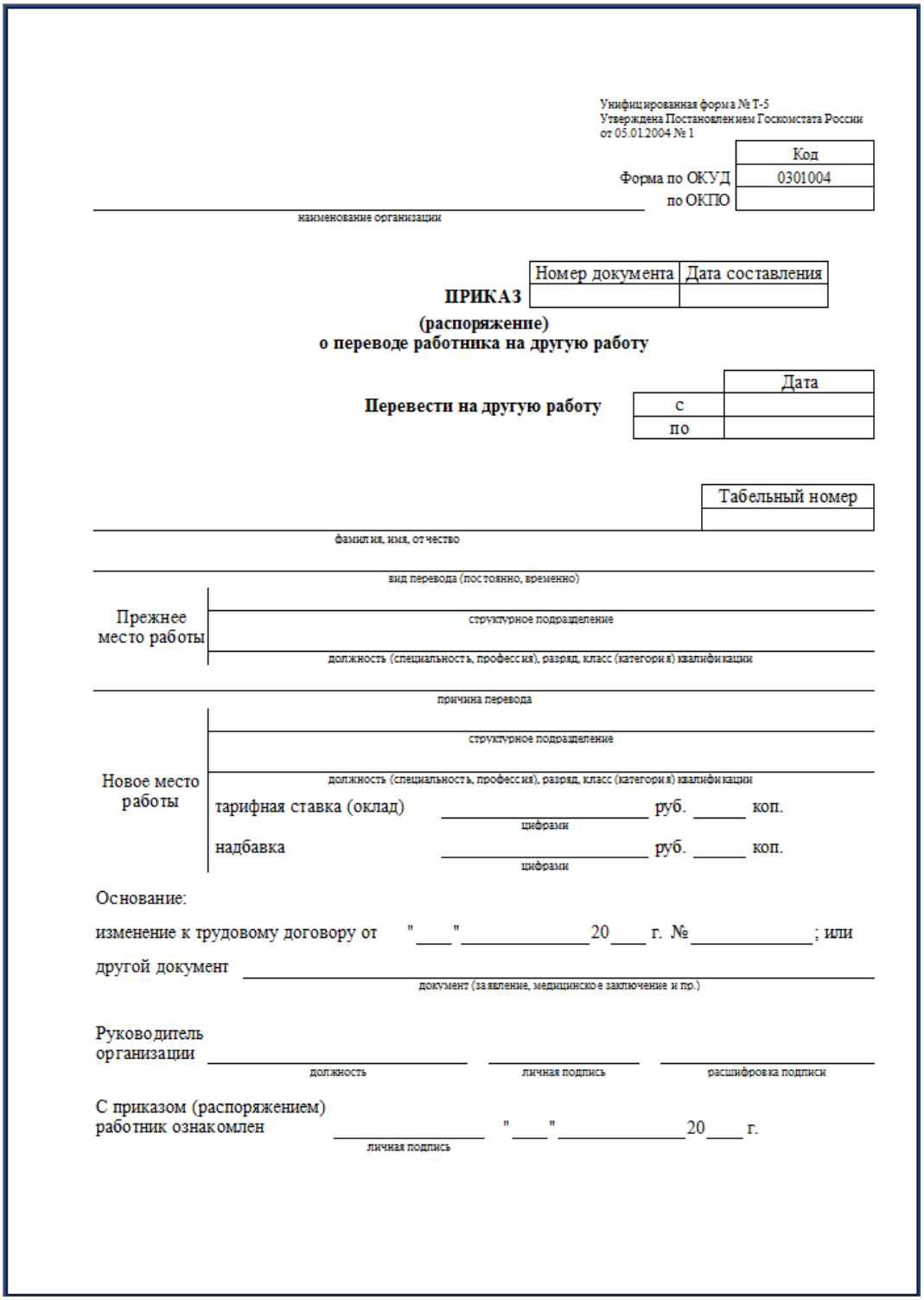
1. Фамилия		Имя		Отчество	
2. Дата рождения					
	(день, месяц, год)				
3. Высшее профессиональное образование					
	(наименование образовательного учреждения, год окончания)				
4. Послевузовское профессиональное образование				Код по ОКИН	
	(аспирантура, адъюнктура, докторантура)				

Рисунок 4

Документ предназначен только для научных и образовательных учреждениях и подразумевает учет научных сотрудников. Содержит в себе информацию о дипломе доктора наук и кандидата наук, об аттестате доцента и профессора, либо о других документах похожих по содержанию, подтверждающих о том, что работник имеет ученую степень.

Бланк формы №Т-5 «Распоряжение (приказ) о переводе работника на другую работу» (Рисунок 5).

Бланк формы №Т-5а «Распоряжение (приказ) о переводе работников на другую работу».



Унифицированная форма № Т-5
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

	Код
Форма по ОКУД	0301004
по ОКПО	

наименование организации

Номер документа	Дата составления

ПРИКАЗ
(распоряжение)
о переводе работника на другую работу

	Дата
с	
по	

Перевести на другую работу

Табельный номер

фамилия, имя, отчество

вид перевода (постоянно, временно)

Прежнее место работы
структурное подразделение
должность (специальность, профессия), разряд, класс (категория) квалификации

причина перевода

Новое место работы
структурное подразделение
должность (специальность, профессия), разряд, класс (категория) квалификации
тарифная ставка (оклад) _____ руб. _____ коп.
цифрами
надбавка _____ руб. _____ коп.
цифрами

Основание:
изменение к трудовому договору от "___" _____ 20___ г. № _____; или
другой документ _____
документ (заявление, медицинское заключение и пр.)

Руководитель организации _____ _____ _____
должность личная подпись расшифровка подписи

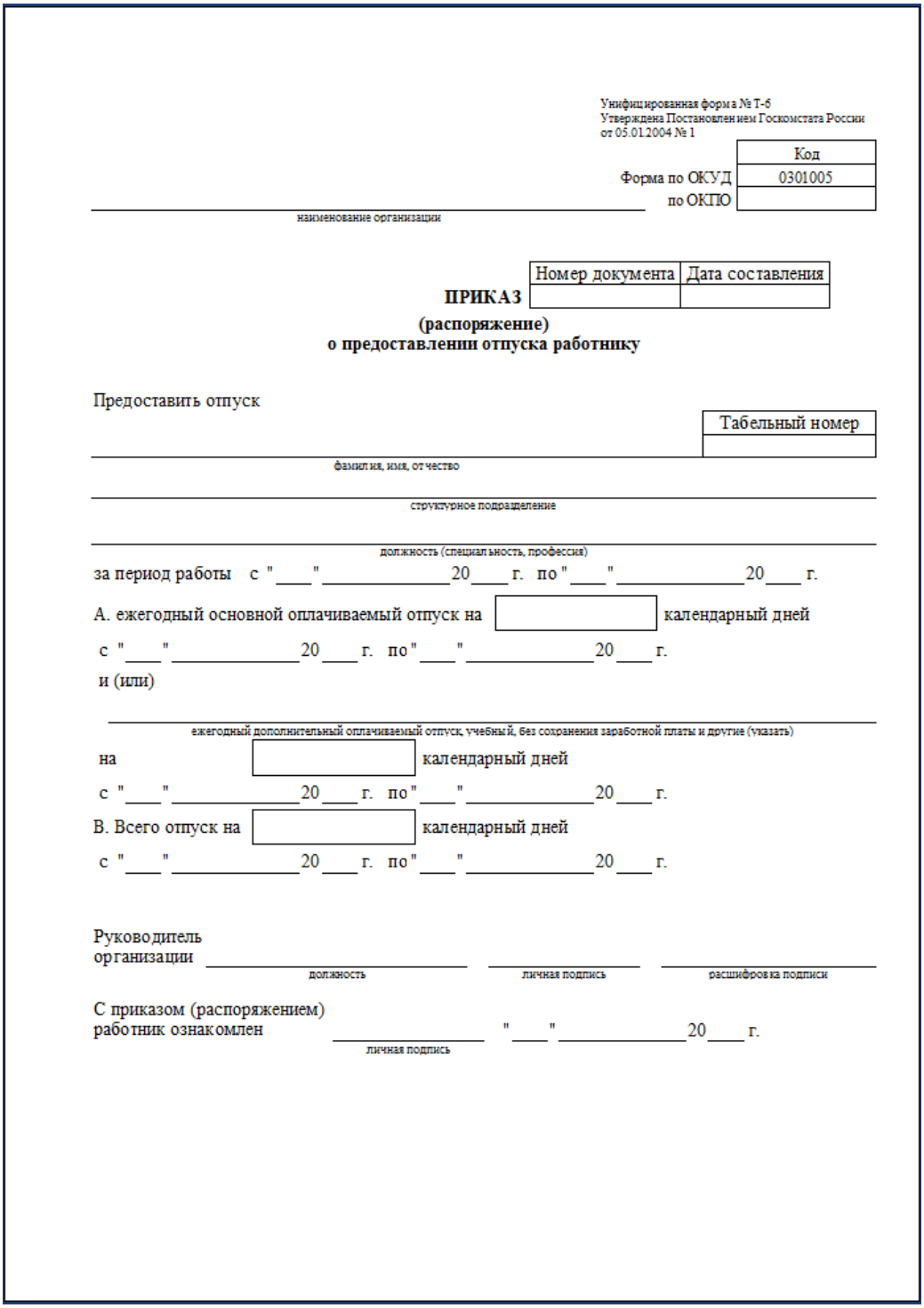
С приказом (распоряжением) работник ознакомлен _____ "___" _____ 20___ г.
личная подпись

Рисунок 5

При переводе работников на другие должности внутри организации, к этим документам должно прилагаться согласие работника в письменной форме. Хранить такие бланки в течении 75-ти лет.

Бланк формы №Т-6 «Распоряжение (приказ) о предоставлении отпуска работнику» (Рисунок 6).

Бланк формы №Т-6а «Распоряжение (приказ) о предоставлении отпуска работникам».



Унифицированная форма № Т-6
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

	Код
Форма по ОКУД	0301005
по ОКПО	

_____
наименование организации

Номер документа	Дата составления

ПРИКАЗ
(распоряжение)
о предоставлении отпуска работнику

Предоставить отпуск

Табельный номер

_____
фамилия, имя, отчество

_____
структурное подразделение

_____
должность (специальность, профессия)

за период работы с "___" _____ 20___ г. по "___" _____ 20___ г.

А. ежегодный основной оплачиваемый отпуск на _____ календарный дней

с "___" _____ 20___ г. по "___" _____ 20___ г.

и (или)

_____
ежегодный дополнительный оплачиваемый отпуск, учебный, без сохранения заработной платы и другие (указать)

на _____ календарный дней

с "___" _____ 20___ г. по "___" _____ 20___ г.

В. Всего отпуск на _____ календарный дней

с "___" _____ 20___ г. по "___" _____ 20___ г.

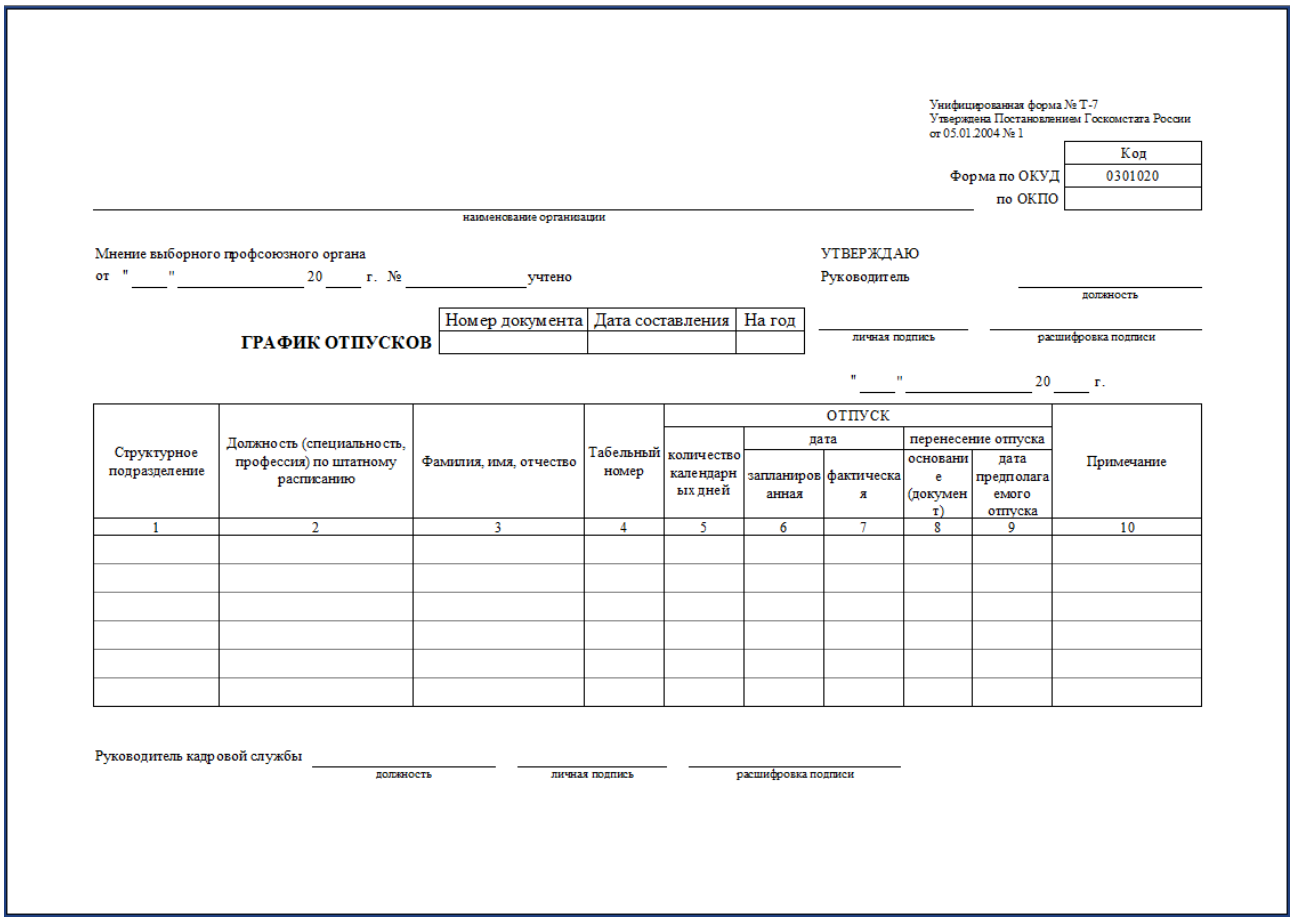
Руководитель организации _____ _____ _____
должность личная подпись расшифровка подписи

С приказом (распоряжением) работник ознакомлен _____ "___" _____ 20___ г.
личная подпись

Рисунок 6

Используется для того, чтобы оформить отпуск штатному сотруднику. Такой документ хранится 5 лет.

Бланк формы №Т-7 «График отпусков» (Рисунок 7).



Унифицированная форма № Т-7
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

	Код
Форма по ОКУД	0301020
по ОКПО	

_____
наименование организации

Мнение выборного профсоюзного органа
от "____" _____ 20____ г. № _____ учтено

УТВЕРЖДАЮ
Руководитель _____ _____
должность личная подпись расшифровка подписи
"____" _____ 20____ г.

ГРАФИК ОТПУСКОВ

Номер документа	Дата составления	На год

Структурное подразделение	Должность (специальность, профессия) по штатному расписанию	Фамилия, имя, отчество	Табельный номер	ОТПУСК					Примечание
				количество календарных дней	дата		перенесение отпуска		
					запланированная	фактическая	основание (документ)	дата предполагаемого отпуска	
1	2	3	4	5	6	7	8	9	10

Руководитель кадровой службы _____ _____ _____
должность личная подпись расшифровка подписи

Рисунок 7

Наличие такого нормативного акта позволяет определить ежегодную очередь предоставления отпусков работникам за счёт предприятия, т.е. график отпусков является обязательным не только для работодателя, но и для работников (Трудовой Кодекс Российской Федерации, статья 123 «Очередность предоставления ежегодных оплачиваемых отпусков»).

Работодателю требуется утвердить данный акт, не позже, чем за 14 дней до 1 января каждого года.

Правила о порядке составления графика отпусков могут быть прописаны в трудовом распорядке или же в положении коллективного договора, либо в других документах предприятия.

Сотрудник должен письменно подтвердит о том, что он знает когда наступает его отпуск, не позднее чем за 14 календарных дней до того как начнётся отпуск данного работника.

Работодателю рекомендуется хранить график отпусков до конца проверки Инспекции Федеральной Налоговой Службы или Государственной инспекции труда, в любом другом случае хранение 1 год.

Бланк формы №Т-8 «Распоряжение (приказ) о прекращении (расторжении) трудового договора с работником (увольнении)» (Рисунок 8).

Бланк формы №Т-8а «Приказ (распоряжение) о прекращении (расторжении) трудового договора с работниками (увольнении)».

Унифицированная форма № Т-8
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

	Код
Форма по ОКУД	0301006
по ОКПО	

_____
наименование организации

Номер документа	Дата составления

ПРИКАЗ
(распоряжение)
о прекращении (расторжении) трудового договора с работником (увольнении)

Прекратить действие трудового договора от "____" _____ 20____ г. № _____ ,
уволить "____" _____ 20____ г.
ненужное зачеркнуть

Табельный номер

_____
фамилия, имя, отчество

_____
структурное подразделение

_____
должность (специальность, профессия), разряд, класс (категория) квалификации

_____
основание прекращения (расторжения) трудового договора (увольнения)

Основание (документ, номер, дата): _____
заявление работника, служебная записка, медицинское заключение и т.д.

Руководитель организации _____ _____ _____
должность личная подпись расшифровка подписи

С приказом (распоряжением) работник ознакомлен _____ "____" _____ 20____ г.
личная подпись

Мотивированное мнение выборного профсоюзного органа в письменной форме
(от "____" _____ 20____ г. № _____) рассмотрено

Рисунок 8

Приказ о прекращении трудового(-вых) договора(-ров), между работником или работниками и работодателем составляет отдел кадров, подписывает руководитель предприятия или уполномоченное лицо, объявляется сотруднику или сотрудникам под расписку. Хранятся 75 лет.

Бланк формы №Т-9 «Приказ (распоряжение) о направлении работника в командировку» (Рисунок 9).

Бланк формы №Т-9а «Приказ (распоряжение) о направлении работников в командировку».

www.buhsol.ru

Унифицированная форма № Т-9
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

	Код
Форма по ОКУД	0301022
по ОКПО	

_____
(наименование организации)

Номер документа	Дата составления

ПРИКАЗ
(распоряжение)
о направлении работника в командировку

Направить в командировку:

Табельный номер

_____
(фамилия, имя, отчество)

_____
(структурное подразделение)

_____
(должность (специальность, профессия))

_____
(место назначения (страна, город, организация))

_____

_____

сроком на _____ календарных дней

с "___" _____ 20___ г. по "___" _____ 20 ___ г.

с целью _____

_____

Командировка за счет средств _____
(указать источник финансирования)

_____

Основание (документ, номер, дата): _____
(служебное задание, другое основание (указать))

Руководитель организации _____ _____ _____
(должность) (личная подпись) (расшифровка подписи)

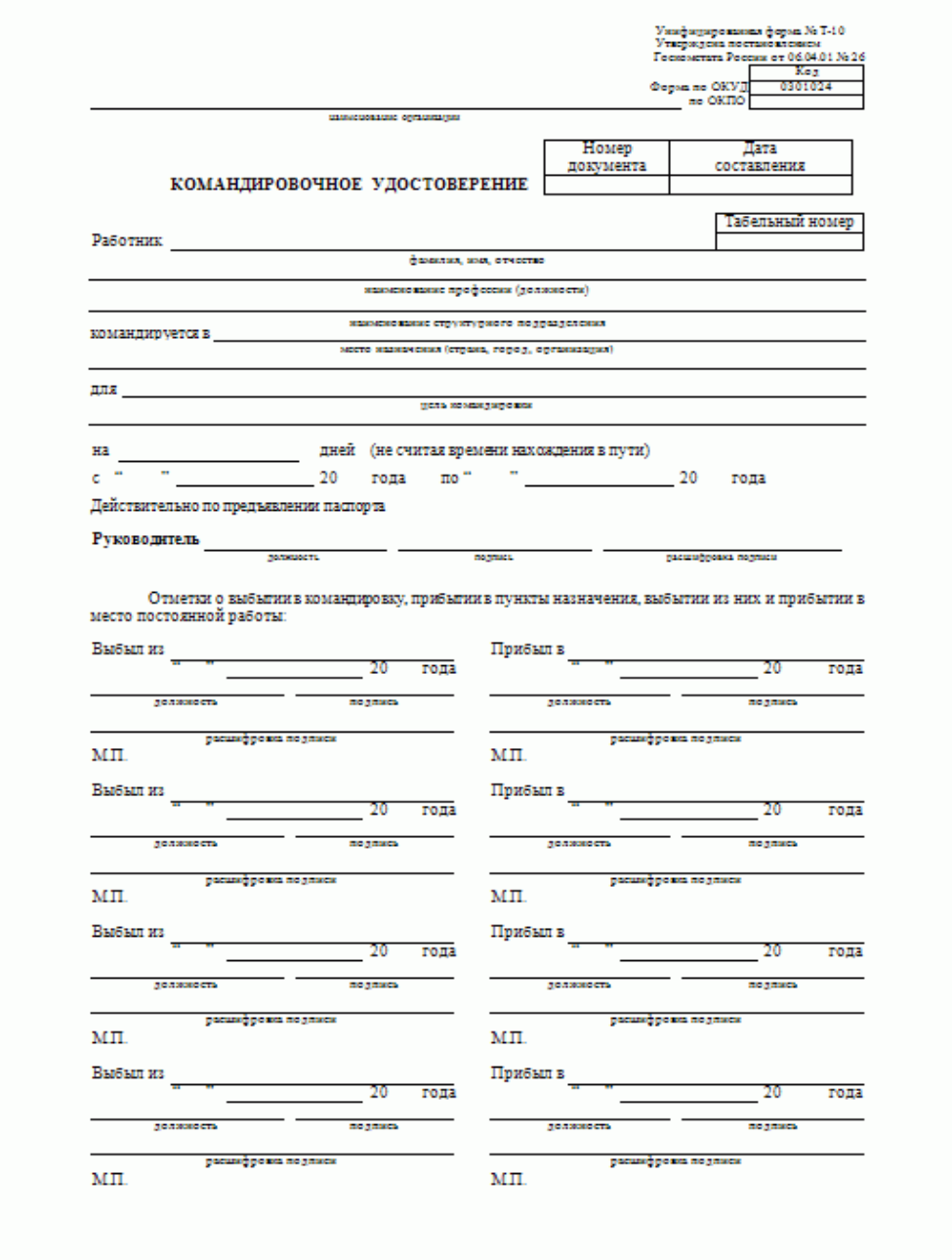
С приказом (распоряжением) работник ознакомлен _____ "___" _____ 20 ___ г.
(личная подпись)

Рисунок 9

Прежде чем отправлять сотрудника или сотрудников в командировку, необходимо составить приказ на командировку, это очень просто сделать, т.е. заполнить бланк формы Т-9 или же Т9а.

Если работники отправляются на долгосрочную командировку в зарубежные страны, то срок хранение таких приказов – 10 лет, в любом другом случае – 5 лет.

Бланк формы №Т-10 «Командировочное удостоверение» (Рисунок 10).



Унифицированная форма № Т-10
Утверждена постановлением
Госкомстата России от 05.01.04 № 1

	Код
Форма по ОКУД	0301024
по ОКПО	

наименование организации

КОМАНДИРОВОЧНОЕ УДОСТОВЕРЕНИЕ

Номер документа	Дата составления

Табельный номер

Работник _____
фамилия, имя, отчество

_____
наименование профессии (должности)

_____
наименование структурного подразделения

командируется в _____
место назначения (страна, город, организация)

для _____
цель командировки

на _____ дней (не считая времени нахождения в пути)

с "__" _____ 20 года по "__" _____ 20 года

Действительно по предъявлении паспорта

Руководитель _____ _____ _____
должность подпись расшифровка подписи

Отметки о выбытии в командировку, прибытии в пункты назначения, выбытии из них и прибытии в место постоянной работы:

Выбыл из _____ "__" _____ 20 года
должность подпись
расшифровка подписи
М.П.

Прибыл в _____ "__" _____ 20 года
должность подпись
расшифровка подписи
М.П.

Выбыл из _____ "__" _____ 20 года
должность подпись
расшифровка подписи
М.П.

Прибыл в _____ "__" _____ 20 года
должность подпись
расшифровка подписи
М.П.

Выбыл из _____ "__" _____ 20 года
должность подпись
расшифровка подписи
М.П.

Прибыл в _____ "__" _____ 20 года
должность подпись
расшифровка подписи
М.П.

Выбыл из _____ "__" _____ 20 года
должность подпись
расшифровка подписи
М.П.

Прибыл в _____ "__" _____ 20 года
должность подпись
расшифровка подписи
М.П.

Рисунок 10

Служит для подтверждения времени пребывания в служебной командировке.

Необходимость заполнение бланка формы Т-10 наступает тогда, когда организация направляет работника в командировку и свидетельствует о том, сколько времени работник пребывает в командировке. Заполняется удостоверение отделом кадров или бухгалтерией в одном экземпляре, содержит сведения о прибытии работника и выбытии в каждом месте назначения, удостоверение подписывает руководитель организации. Командировочное удостоверение хранится 5 лет, но есть исключения, когда сотрудник отправляется в районы Крайнего Севера, в этом случае срок продлевается до 75 лет.

Бланк формы №Т-10а «Служебное задание для направления в командировку и отчет о его выполнении».

Прописывается сама цель отправки работника в командировку и о результате выполнения. В ходе заполнения бланка по форме Т-9 учитывается бланк Т-10а, т.е. экономическая обоснованность трат на поездку работника. Срок хранения 5 лет (при долгосрочных зарубежных командировках – 10 лет). Хранится столько же, сколько и форма Т-9 и Т-9а.

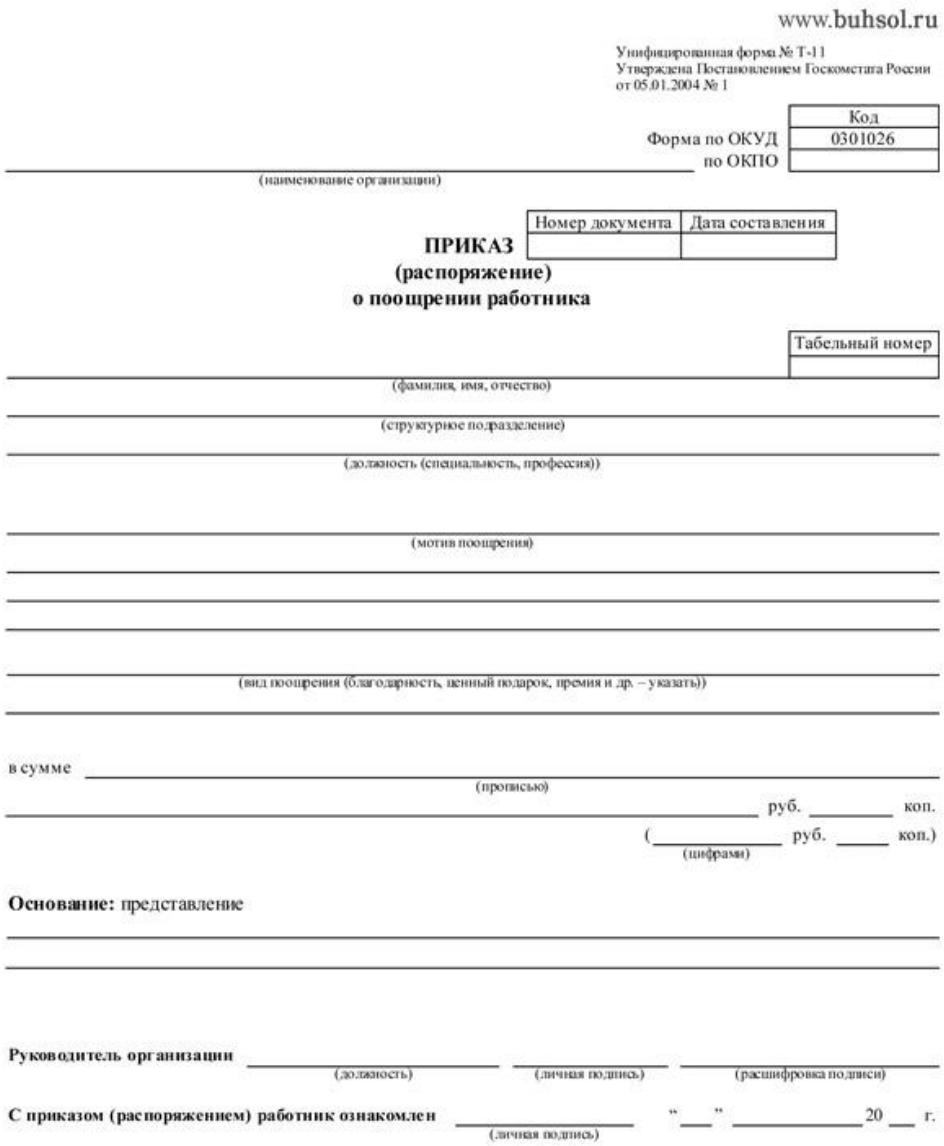
Бланк формы №Т-11 «Распоряжение (приказ) о поощрении работника» (Рисунок 11).

Бланк формы №Т-11а «Распоряжение (приказ) о поощрении работников».

В том случае, когда работник заслуживает поощрение за свою работу, на его имя заполняется данный документ и затем делается пометка в личной карточке и трудовой этого сотрудника. Такие формы хранятся 75 лет.

Все эти документы заполняются с использованием персональных данных, но где же начала обработки персональных данных?

Обработка персональных данных начинается с заполнения субъектом персональных данных согласия на обработку персональных данных (пункт 1 часть 1 статья 6 Федерального Закона №152).



www.buhsol.ru

Унифицированная форма № Т-11
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

	Код
Форма по ОКУД	0301026
по ОКПО	

_____
(наименование организации)

Номер документа	Дата составления

ПРИКАЗ
(распоряжение)
о поощрении работника

Табельный номер

_____
(фамилия, имя, отчество)

_____
(структурное подразделение)

_____
(должность (специальность, профессия))

_____
(мотив поощрения)

_____
_____
_____

_____
(вид поощрения (благодарность, ценный подарок, премия и др. – указать))

_____

в сумме _____
(прописью)

_____ руб. _____ коп.
(_____ руб. _____ коп.)
(цифрами)

Основание: представление

_____
_____

Руководитель организации _____ _____ _____
(должность) (личная подпись) (расшифровка подписи)

С приказом (распоряжением) работник ознакомлен _____ "___" _____ 20___ г.
(личная подпись)

Рисунок 11

Вот так выглядит согласие на обработку персональных данных. (Рисунок 12)

С помощью данного согласия осуществляется дальнейшая законная обработка персональных данных.

Данный бланк может быть на бумаге в письменном виде или же являться электронным документом с электронной подписью субъекта персональных данных.

Разработкой данного согласия занимается отдел кадров данной организации.

Каждый работник данного предприятия, иными словами субъект персональных данных ставит свою подпись на данном согласии, т.е. даёт свое согласие на обработку своих персональных данных.

Когда подписывает: при приеме на работу, при заключении договора т.е. с момента факт. начала обработки персональных данных .

Согласие на обработку персональных данных должно включать в себя (часть 4 статья 9 Федерального Закона 152):

1. фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2. наименование или фамилию, имя, отчество и адрес (юридический) оператора, получающего согласие субъекта персональных данных;
3. цель обработки персональных данных;
4. перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
5. перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
6. срок, в течение которого действует согласие, а также способ его отзыва, если иное не установлено федеральным законом;
7. подпись субъекта персональных данных.

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

г._____ «____»_____20___г.

Субъект персональных данных,

_____

(Фамилия, Имя, Отчество полностью)

_____серия_____№_____выдан_____

вид основного документа, удостоверяющий личность

_____

(кем и когда)

проживающий(ая) по адресу_____

_____,

В лице представителя субъекта персональных данных (заполняется в случае получения согласия от представителя субъекта персональных данных),

_____,

(Фамилия, Имя, Отчество полностью)

_____серия_____№_____выдан_____

вид основного документа, удостоверяющий личность

_____

(кем и когда)

проживающий(ая) по адресу_____

_____,

действующий от имени субъекта персональных данных на основании_____

_____

(реквизиты доверенности или иного документа, подтверждающего полномочия представителя),

принимаю решение о предоставлении моих персональных данных и даю согласие на их обработку свободно, своей волей и в своем интересе -

Наименование и адрес оператора, получающего согласие субъекта персональных данных:
ООО «Интерштамп», ИНН 7707604465, 115598, г. Москва, ул. Загорьевская, д. 10, корп. 4.

Со следующей целью обработки персональных данных:
выполнения поручения физических лиц (субъектов персональных данных), основанного на заключенном в простой письменной форме агентском договоре с оператором персональных данных, обращающихся за въездной визой в иностранные государства таких стран, как (включая, но не ограничиваясь - **нужное подчеркнуть**): Франция, Испания, Финляндия, Греция, Болгария, Литва, Эстония, Бельгия, Нидерланды, Мальта, Дания, Чешская Республика, Швеция, Австрия, по передаче пакетов документов в дипломатические представительства указанных иностранных государств для получения данными лицам и виз.

Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных:

фамилия, имя, отчество; дата рождения; место рождения; адрес; гражданство; семейное положение; данные о детях; образование; сведения трудовой деятельности; доходы; фотография; пол; номер контактного телефона; адрес электронной почты; паспортные данные: а) вид документа; б) серия и номер документа; в) орган, выдавший документ; наименование; код; г) дата выдачи документа.

Наименование и адрес лица, осуществляющего обработку персональных данных по поручению оператора (если обработка будет поручена такому лицу):_____

_____

Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных:

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной обработки персональных данных (сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение использования, распространение), в том числе передачу), обезличивание, блокирование, уничтожение персональных данных).

Срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом:

Персональные данные субъекта подлежат хранению в течение сроков, установленных законодательством РФ. По достижению целей обработки персональные данные уничтожаются. Согласие может быть отозвано субъектом путем направления письменного уведомления оператору. На основании письменного обращения субъекта персональных данных с требованием о прекращении обработки его персональных данных оператор прекратит обработку таких персональных данных в течение 3 (трех) рабочих дней, о чем будет направлено письменное уведомление субъекту персональных данных в течение 10 (десяти) рабочих дней; ликвидация или реорганизация ООО «Интерштамп».

Подпись субъекта персональных данных:

_____

(Ф.И.О. полностью, подпись)

Рисунок 12

В том случае, когда согласие субъекта персональных данных предоставляется через законного представителя, в бланке согласия нужно прописать имя, фамилию, отчество, место жительства этого представителя, серию, номер паспорта, каким органом он выдан, дату выдачи, код подразделения и реквизиты документа, который подтверждает возможность этого представителя отвечать от лица субъекта персональных данных.

Оператор персональных данных может возложить некоторые аспекты обработки персональных данных на другого человека или компанию, но только с письменного согласия субъекта персональных данных, чьи данные передаются на обработку.

Далее, человек или целая компания, которым переданы полномочия на обработку, обязаны соблюдать принципы и правила ведения своей деятельности, т.е. какую-то часть обработки персональных данных, в соответствии с нынешним Федеральным Законом.

Должны быть чётко прописаны операции с персональными данными, которые берёт на себя лицо, реализующее обработку персональных данных, цели этих операция, указывается обязанность соблюдения конфиденциальности персональных данных и необходимые требования к защите персональных данных, предусмотренные Федеральным Законом.

Бланк согласия должен содержать данные предусмотренные частью 4 статьей 9 Федерального Закона №152, в случае несоответствия, согласие является не действительным, а обработка персональных данных является незаконной деятельностью, что может повлечь неблагоприятные последствия для организации.

Подписанное электронной цифровой подписью и не нарушающее Федеральный Закон №152, согласие на обработку персональных данных на электронном носителе имеет ту же силу, что и согласие, подписанное собственноручно.

Лицо, являющееся оператором персональных данных, должно уведомить орган Роскомнадзора, который отвечает за территорию на которой зарегистрирован Оператор персональных данных:

1. Фамилию, имя, отчество индивидуального предпринимателя, адрес оператора;
2. С какой целью происходит обработка персональных данных;
3. Какие категории персональных данных подвергаются обработке;
4. Какие категории субъектов, персональные данные которых обрабатываются;
5. На каком основании с точки зрения права происходит обработка персональных данных;
6. Перечень операций с персональными данными, подробное или общее пояснение способов, которые использует оператор в ходе обработки персональных данных;
7. Описание мер, предусмотренных статьёй 18.1 и 19 упомянутого Федерального Закона №152;
8. Фамилия, имя, отчество физ. лица или наименование юр. лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
9. Число, месяц, год начала обработки персональных данных;
10. На какой срок происходит обработка персональных данных и условия прекращения обработки персональных данных;
11. Сведения о наличии или об отсутствии трансграничной передачи персональных данных;
12. Информация об обеспечении безопасности персональных данных в соответствии с требованиями Правительства РФ.

Т.е. тем, кто уже подал Уведомление необходимо сообщить уполномоченному органу по защите прав субъектов персональных данных дополнительную информацию:

правовое основание обработки персональных данных;

фамилия, имя, отчество физического лица или наименование юр. лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

Роскомнадзор в течение 30 дней с даты поступления уведомления об обработке персональных данных вносит сведения в Реестр Операторов.

Сведения, содержащиеся в Реестре Операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

Непредставление или несвоевременное предоставление Уведомления об обработке персональных данных влечет адм. ответственность в соответствии со статьёй 13.11 и 19.7 Кодекса Российской Федерации об административных правонарушениях: предупреждение или наложение адм. штрафа на юридических лиц - от 3000 до 5000 руб.

1.2 Законодательные основы защиты персональных данных

На данный момент в Российской Федерации в сфере обеспечения защиты персональных данных осуществляется регулирование на государственном уровне. Правовое регулирование вопросов обработки персональных данных осуществляется в соответствии с Конституцией Российской Федерации и международными договорами Российской Федерации, на основании вступившего в силу с 2007 года Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятых во исполнение его положений, нормативно-правовых актов и методических документов.

Также нормативными актами, оказывающие правовое регулирование в области защиты персональных данных являются:

Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Трудовой кодекс Российской Федерации (глава 14).

Федеральный закон Российской Федерации от 28 марта 1998 №53-ФЗ «О воинской обязанности».

Постановление Правительства РФ от 17 ноября 2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Постановление Правительства РФ от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Необходимо рассмотреть главные понятия, используемые в нормативно-правовых актах.

К персональными данным относят сведения, о субъекту персональных данных (человеку), самыми простыми примерами являются его полное имя, дата рождения, место жительства, положение в семье и обществе, имущество, которым он владеет, уровень образования, наименование профессии, заработок и т. д.

Обработка персональных данных – совокупность действий, таких, как сбор, систематизация, накопление сведений, хранение, внесение изменений, использование, распространение, блокировка, удаление персональных данных.

Действия над такими данными, находящимися в автоматизированной информационной системе персональных данных либо извлеченных из такой системы считается, если такие действия с персональными данными, как использование, внесение изменений, распространение, удаление персональных данных в отношении каждого человека, осуществляются при непосредственном участии человека.

Обработка персональных данных осуществляется с помощью средств вычислительной техники, информационно-вычислительных комплексов и сетей, средств и систем приема, передачи и обработки персональных данных (систем и средств с помощью которых происходит звукозапись, звукоусиление, звуковоспроизведение, переговоры, изготовление, тиражирование документов и прочие средства обрабатывающие речевую, графическую, видео- и буквенно-цифровую информацию), программного обеспечения обеспечивающего защиту информации, применяемого в информационных системах.

Информационная система – комплекс сведений содержащихся в базах данных и осуществляющих её обработку технических средств и информационных технологий.

Под безопасностью персональных данных имеют ввиду защищенности персональных данных, которая характеризуется способностью пользователей, технических средств и информационных технологий обеспечивать целостность, доступность и конфиденциальность сведений, относящихся к персональным данным при их сборе, хранении, распространении, изменении в автоматизированной информационной системе и т.д.

Данные характеризующие физиологические особенности человека, основе которых устанавливают его личность, в том числе фото человека, снимки отпечатков пальцев, отличительные черты на теле и модель сетчатки глаза, называются биометрическими персональными данными.

При осуществлении безопасности персональных данных во время их обработки в автоматизированной информационной системе используются системы защиты персональных сведений, криптографические средства защиты персональных данных, средства против несанкционированного доступа, изъятия информации по каналам связи, воздействий с помощью технических и программных средств хранения, распространения, использования, и внесения изменений в персональные данные и соответственно информационные технологии используемые в информационных системах. Все используемые средства обязательно должны соответствовать законодательству Российской Федерации, в сфере защиты информации.

Во время обработки персональных данных в автоматизированных информационных системах происходит защита голосовой информации и данных подверженных обработке техническими средствами, в том числе бумажных, магнитных и магнитно-оптических носителей информации.

1.3 Анализ технического и программного обеспечения предприятия

В организации хранение персональных данных производится без информационной системы защиты персональных данных, в обычной картотеке. Процесс обработки персональных данных осуществляется следующим путём:

1. Отдел кадров разрабатывает соглашение на обработку персональных данных;
2. Работник предоставляет свои персональные данные отделу кадров;
3. Он же подписывает соглашение на обработку персональных данных;
4. Работник отдела кадров формирует новое дело, в которое вкладывает документы с персональными данными;
5. Относит в картотеку, где данные хранятся, пока не понадобятся;

Всё это показано на SADT-модели (IDEF0) «как-есть». (Рисунок 13 -14)

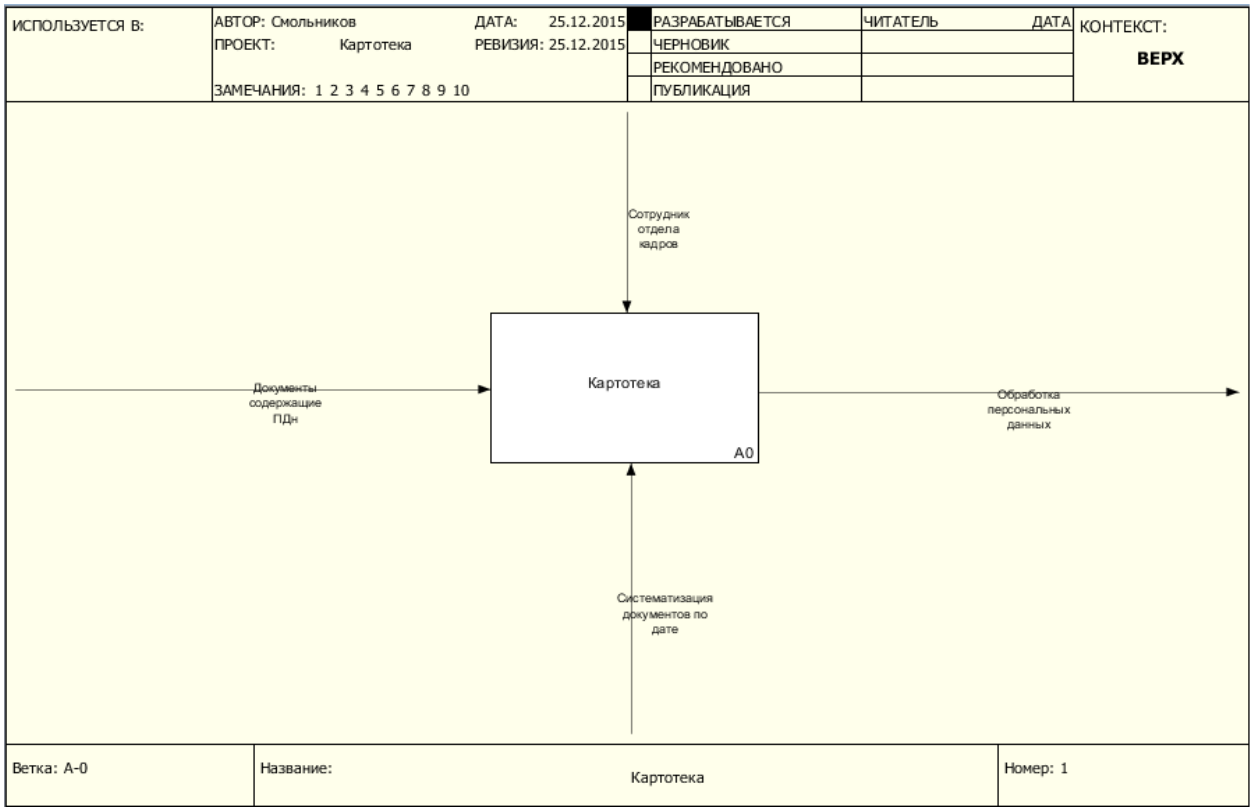


Рисунок 13.

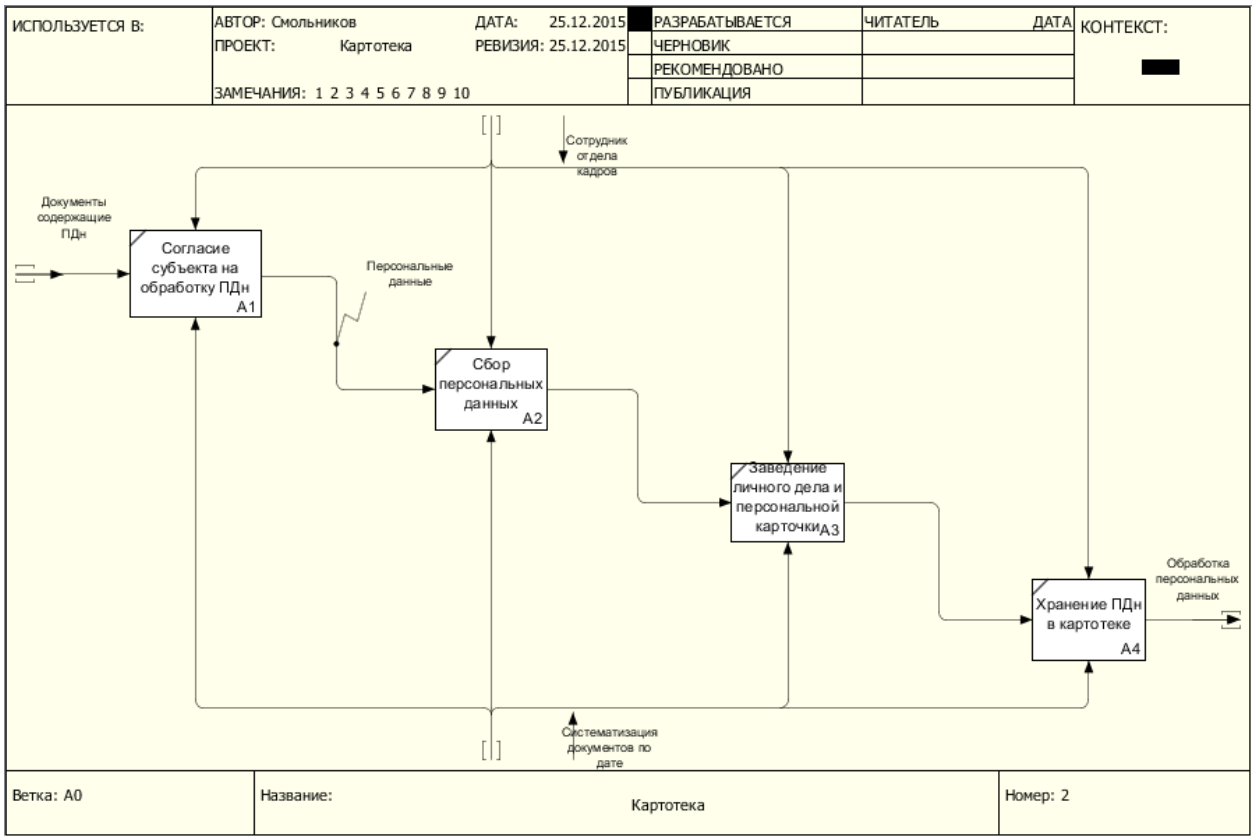


Рисунок 14.

С каждым годом растёт штат сотрудников, технологии развиваются и появляется необходимость в информационной системе персональных данных. В ходе дипломной работы на этапе проведения анализа была разработана SADT-модель(IDEF0) «как-должно-быть». На этой модели примерно показаны процессы, которые будут происходить в автоматизированной системе персональных данных системе. (Рисунок 15-16)

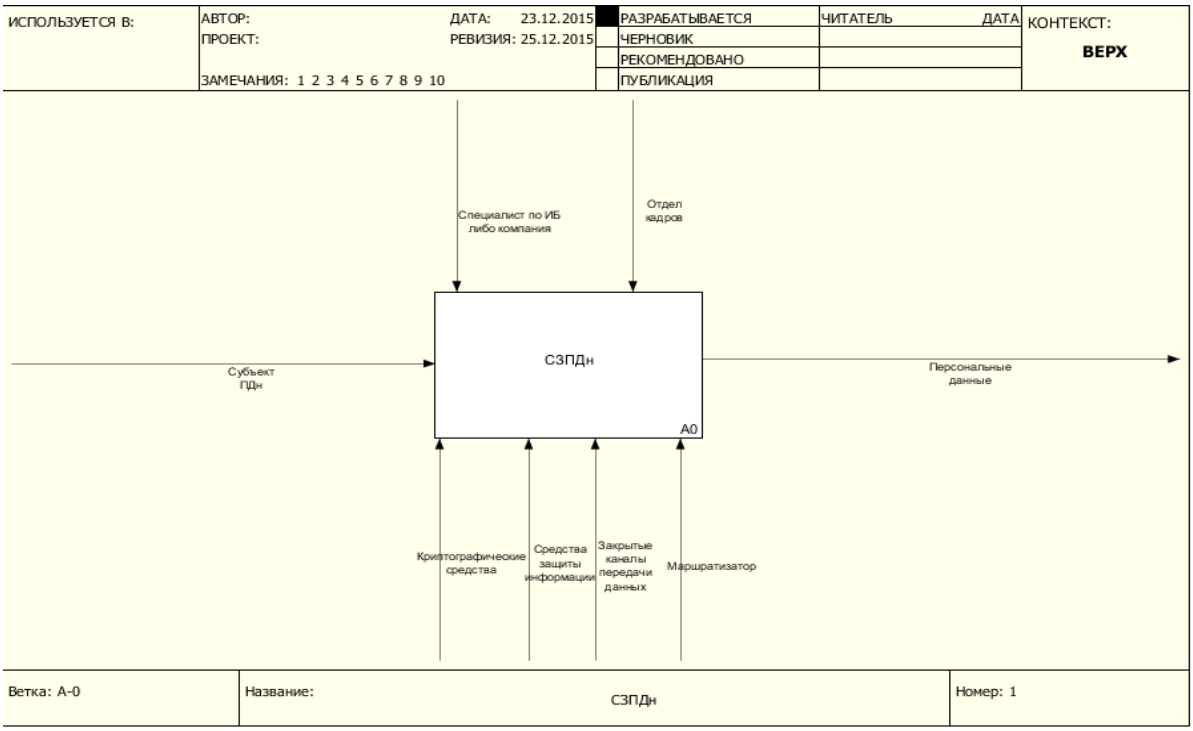


Рисунок 15

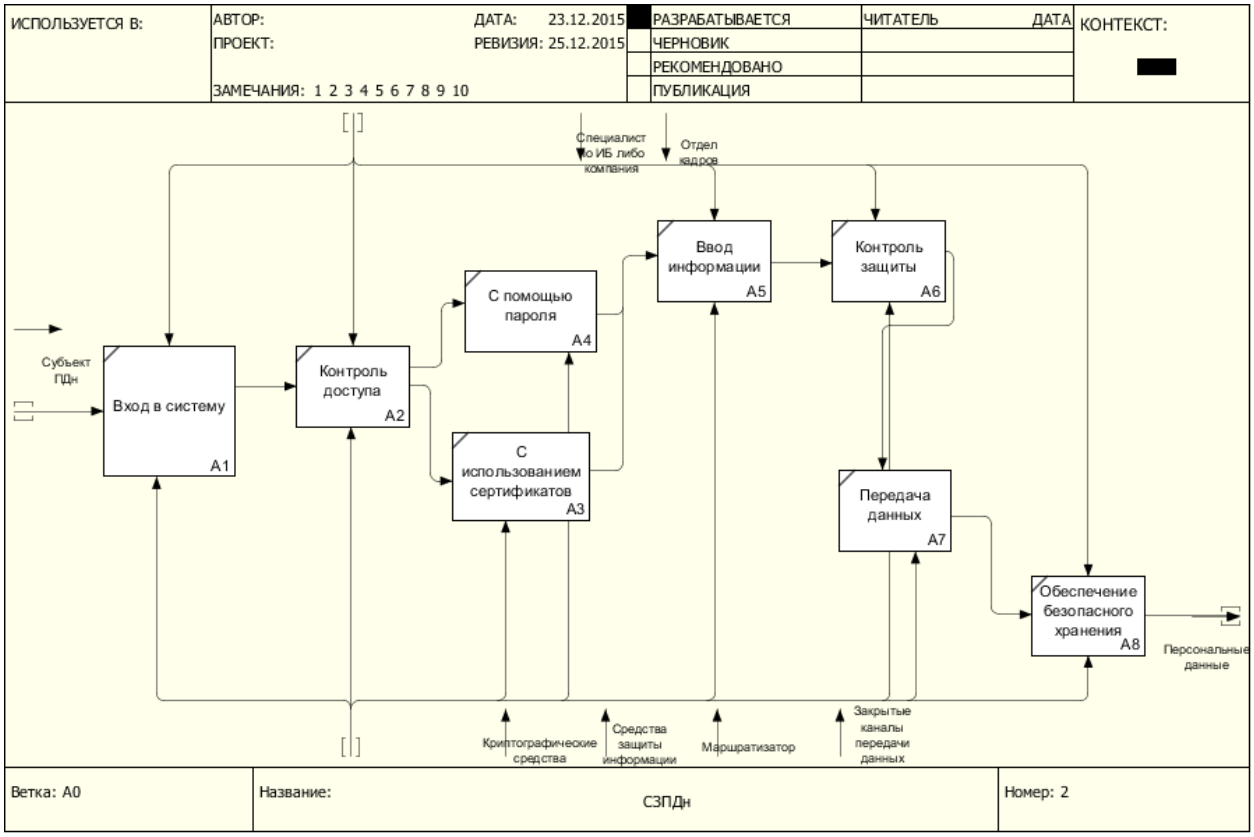


Рисунок 16

В системе обработка будет происходить по пунктам:

1. Субъект ставит свою подпись на бланке согласия на обработку персональных данных, тем самым подтверждая, что он согласен с обработкой своих персональных сведений;
2. Сотрудник отдела кадров производит входи в систему с помощью пароля или с использованием сертификатов;
3. Осуществляет ввод персональных данных;
4. Все выполняемые операции происходят под строгим мониторингом (контролем) со стороны ответственного специалиста;
5. Затем сотрудник отдела кадров производит передачу персональных данных на сервер;
6. В ходе передачи данных происходит криптографическая обработка информации, что позволяет защитить сведения во время передачи;
7. В конечном итоге информация находится на сервере, за безопасность информации несёт ответственность уполномоченное лицо, которому предоставили право на обработку и защиту персональных данных.

2.ВЕРОЯТНЫЕ ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ

2.1 Классификация угроз информационной безопасности

Угроза – так обычно называют любой процесс, если он может принести вред чьим-то интересам. Конкретнее, под угрозой безопасности автоматизированной системы обработки персональных данных имеется ввиду воздействие на автоматизированную систему, если есть вероятность косвенного или прямого причинения ущерба её безопасности.

Злоумышленникам получить и использовать в своих целях сведения из информационной системы персональных данных гораздо проще, чем из баз данных, которых хранятся в бумажном виде.

Список вероятных угроз и оценка вероятностей их осуществления позволяют провести анализ риска их осуществления и опираясь на анализ выдвигать требования к системе защиты автоматизированной системы.

Каждую угрозу можно классифицировать по определенному признаку, а классификация признаков позволяет обобщенно сформулировать требования.

Информация, которая содержится и обрабатывается в сегодняшних автоматизированной системе подвергается опасности воздействия огромного количества факторов, поэтому становится нереализуемым формализация задачи описания полного множества угроз.

В этом случае описывается не подробный список угроз, а список их классификаций.

Разделение на классы вероятных угроз информационной безопасности автоматизированной системы может быть проведено по таким общим признакам, как:

Природа влияния:

Естественные угрозы, вызванные воздействиями на автоматизированную систему объективных физических процессов или стихийных природных явлений;

Искусственные угрозы безопасности автоматизированной системы, вызванные деятельностью человека.

По степени преднамеренности проявления:

Угрозы, вызванные по вине работников, например, ввод неверных данных;

Угрозы преднамеренного действия, например хищение, использование или уничтожение данных злоумышленниками.

По непосредственному источнику угроз:

Природные явления;

Угрозой является челок: например сотрудник, которого подкупили;

Санкционированные программно-аппаратные средства, например удаление данных;

Несанкционированные программно-аппаратные средства, например заражение вычислительного устройства с помощью вредоносных программ.

По месту нахождения источника угроз:

Вне контролируемой зоны автоматизированной системы, например утечка сведений, передаваемых по каналам связи;

В пределах контролируемой зоны автоматизированной системы, например применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т.п.;

Непосредственно в автоматизированной системы, например некорректное использование ресурсов автоматизированной системы.

По степени зависимости от активности автоматизированной системы:

Независимо от активности автоматизированной системы, например вскрытие шифров криптозащиты информации;

Только в процессе обработки данных, например угрозы выполнения и распространения программных вирусов.

По степени воздействия на автоматизированной системы:

пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС, например угроза копирования секретных данных;

активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС, например внедрение троянских коней и вирусов.

По этапам доступа пользователей или программ к ресурсам:

угрозы, проявляющиеся на этапе доступа к ресурсам автоматизированной системы, например: угрозы несанкционированного доступа в автоматизированную систему;

угрозы, проявляющиеся после разрешения доступа к ресурсам автоматизированной системы, например угрозы несанкционированного или некорректного использования ресурсов автоматизированной системы.

По способу доступа к ресурсам автоматизированной системы:

угрозы, осуществляемые с использованием стандартного пути доступа к ресурсам автоматизированной системы

угрозы, осуществляемые с использованием скрытого нестандартного пути доступа к ресурсам автоматизированной системы, например: доступ из вне к ресурсам автоматизированной системы с помощью недокументированных возможностей операционной системы.

По текущему месту расположения информации, хранимой и обрабатываемой в автоматизированной системе:

угрозы доступа к информации, которая находится на внешних запоминающих устройствах;

угрозы доступа к информации, которая находится в оперативной памяти, например: доступ к системной области оперативной памяти со стороны программных средств;

угрозы доступа к информации, передающейся в каналах связи;

угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере.

Опасные воздействия на автоматизированную систему подразделяются на случайные и преднамеренные.

Причинами первых воздействий при эксплуатации автоматизированной системы могут быть:

аварии по причине стихийных бедствий или перебоев с электропитанием;

отказы и сбои аппаратных средств;

ошибки в программных средствах;

ошибки в работе сотрудников и пользователей;

помехи в каналах связи из-за действий из вне.

Самыми распространенными компьютерными нарушениями считаются баги в программном обеспечении.

Программное обеспечение всех технических средств, которые используются в автоматизированной системе, написано человеком, в связи с этим нарушения в работе программ случается достаточно часто.

Чем сложнее программное обеспечение, тем выше процент вероятности того, что оно содержит ошибки.

Чаще всего в таких нарушениях нет серьёзной опасности, но некоторые возможно приведут к неблагоприятным последствиям, например, выход сервера из строя.

Такие нарушения в работе исправляются пакетами обновлений, которые выпускает разработчик программного обеспечения.

Специально спланированные угрозы исходят от нарушителей.

Нарушителем может оказаться любой человек, возможно даже он сотрудник этой организации.

У нарушителя могут быть совершенно разные мотивы, исходя из которых он предпринимает данные действия.

Деньги, нездоровый интерес, конкурентная борьба, стремление показать себя и т.д.

И это далеко не полный список целей преступников.

Угрозы направленные на распространение конфиденциальной информации, нарушение работоспособности автоматизированной системы и угрозы направленные на изменение или искажение информации относятся к непосредственным, т.к. действия направлены непосредственно на информацию, которая находится под защитой. Рассмотрев угрозы и классификацию

автоматизированных систем, можно перейти к анализу угроз и классификации самой информационной системы персональных данных.

Информационная система персональных данных означает совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Совокупность условий и факторов, создающих опасность несанкционированного доступа не формируется с учетом характеристик информационных систем персональных данных, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

К характеристикам информационной системы персональных данных, обусловливающим возникновение угроз безопасности персональных данных, можно отнести категории и объемы обрабатываемых в информационных системах персональных данных, структуру информационных систем персональных данных, наличие подключений информационных систем персональных данных к сетям общего пользования, режимы обработки персональных данных, режимы разграничения прав доступа к информации пользователей информационной системы персональных данных, местонахождение и условия размещения технических средств информационной системы персональных данных.

Информационные системы персональных данных являются комплексом информационных и программно-аппаратных средств, а также информационных технологий, применяемых при сборе, хранении, изменении, распространении и уничтожении персональных данных.

Основными звеньями информационной системы персональных данных являются:

персональные данные, которые находятся в базах данных;

информационные технологии, которые применяются в ходе обработки персональных данных;

технические средства, осуществляющие сбор, хранение, использование, изменение или распространение персональных данных;

программы;

средства защиты информации;

вспомогательные технические средства и системы – технические средства и системы, их коммуникации, которые не предназначены для обработки персональных данных, но размещаются в тех служебных помещениях, в которых расположены информационные системы персональных данных или их технические составляющие.

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются персональных данных, и определяются при оценке возможности реализации угроз безопасности персональных данных.

Возможности источников угроз безопасности персональных данных обусловлены совокупностью способов несанкционированного и (или) случайного доступа к персональным данным, в результате которого возможно нарушение конфиденциальности, целостности и блокировки персональных данных.

Угроза безопасности персональных данных реализуется в результате образования канала реализации угрозы безопасности персональных данных между источником угрозы и источником персональных данных, что создает условия для несанкционированного доступа к персональным данным.

Основными составляющими канала реализации угроз безопасности персональных данных (приложение 1) являются:

источник угроз безопасности персональных данных;

среда (путь) распространения персональных данных или воздействий, в которой физическое поле, сигнал, данные или программы могут

распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) персональных данных;
источник персональных данных.

Носители персональных данных могут содержать информацию, представленную в следующих видах:

речевые данные, которые, естественно, содержатся в устной речи пользователя информационной системы персональных данных при осуществлении им функции голосового ввода персональных данных в информационную систему персональных данных, а также содержащаяся в электромагнитных полях и сигналах, получающиеся после преобразований речевой информации;

видовая информация, представленная в виде текста и картинок различных устройств отображения информации средств вычислительной техники;

информация, которая обрабатывается в информационной системе персональных данных, в виде электрических, электромагнитных и оптических сигналов;

информация, которая обрабатывается в информационной системе персональных данных, представленная в виде логических структур.

В целях классификации и создания перечня угроз безопасности персональных данных при их использовании в информационной системе персональных данных и разработке на их основе частных моделей применительно к конкретному виду информационных систем персональных данных угрозы разделяются на классы и подклассы в соответствии со следующими признаками (приложение 1):

по виду защищаемых от угроз безопасности персональных данных сведений, содержащих персональные данные;

по видам вероятных источников угроз безопасности персональных данных;

по типу информационных систем персональных данных, на которые направлены попытки угроз безопасности персональных данных;

по способу осуществления угроз безопасности персональных данных;

по виду нарушаемого свойства информации;

по используемой уязвимости;

по объекту воздействия.

По видам возможных источников угроз безопасности персональных данных выделяются следующие классы угроз:

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к информационной системе персональных данных, включая сотрудников организации, реализующих угрозы непосредственно в информационной системе персональных данных;

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к информационной системе персональных данных, реализующих угрозы из внешней среды, т.е. из связи общего пользования и сетей международного информационного обмена.

Кроме того, угрозы могут появляться в результате внедрения аппаратных закладок и вредоносных программ.

Классифицировать угрозы безопасности персональных данных можно по типу информационных систем персональных данных, к которым направленны эти угрозы:

угрозы безопасности персональных данных, которые обрабатываются в информационной системе персональных данных на базе автономного автоматизированного рабочего места;

угрозы безопасности персональных данных, которые обрабатываются в информационной системе персональных данных на базе автоматизированного рабочего места, подключенного к глобальной сети интернет;

угрозы безопасности персональных данных, которые обрабатываются в информационной системе персональных данных на базе локальных информационных систем, т.е. без подключения к глобальной сети интернет;

угрозы безопасности персональных данных, которые обрабатываются в информационной системе персональных данных на базе локальных

информационных систем с подключением к глобальной сети обмена информацией;

угрозы безопасности персональных данных, обрабатываемых в информационной системе персональных данных на базе автоматизированной информационных систем без доступа к сетям общего пользования;

угрозы безопасности персональных данных, обрабатываемых в информационной системе персональных данных на базе распределенных информационных систем с подключением к сети общего пользования.

По методам осуществления угрозы безопасности персональных данных можно разделить на следующие подклассы:

угрозы, связанные с несанкционированным доступом к персональным данным;

угрозы утечки персональных данных по техническим каналам утечки информации;

угрозы специальных воздействий на информационная система персональных данных.

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

угрозы, которые приводят к неконтролируемому распространению или незаконному обороту данных, при осуществлении которых информация не подвергается изменениям;

угрозы, которые приводят к случайному воздействию на содержание информации, в результате которого хранящиеся данные меняются или уничтожаются;

угрозы, которые приводят к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы информационной системы персональных данных, в таком случае происходит блокировка персональных данных.

По типу уязвимостей можно выделить следующие подклассы угроз:

угрозы, которые осуществляются с использованием уязвимости системного программного обеспечения;

угрозы, возникшие с помощью слабых мест прикладного программного обеспечения;

угрозы, всплывающие в результате использования уязвимости, которую вызвала аппаратная закладка в автоматизированной системе;

угрозы, осуществляемые благодаря уязвимостям протоколов сетевого взаимодействия и каналов передачи данных;

угрозы, появляющиеся в результате использования уязвимостей, вызванных недостатками организации ТЗИ от несанкционированного доступа;

угрозы, которые реализуются с использованием слабых мест, обусловливающих о наличие технических каналов утечки информации;

угрозы, возникшие в результате использования слабых мест в средствах защиты информации.

По объекту воздействия выделяются следующие подклассы вероятных угроз:

угрозы безопасности персональных данных, которые обрабатываются на автоматизированных рабочих местах;

угрозы безопасности персональных данных, которые обрабатываются в выделенных средствах обработки (принтерах, плоттерах и т.д.)

угрозы безопасности персональных данных, передача которых осуществляется с помощью каналов связи;

угрозы прикладным программам, с помощью которых происходит обработка информации;

угрозы системному программному обеспечению, благодаря которому функционирует информационная система персональных данных.

Реализация одной из угроз безопасности персональных данных перечисленных классов или их совокупности может привести к следующим типам последствий для субъектов персональных данных:

значительным негативным последствиям для субъектов персональных данных;

негативным последствиям для субъектов персональных данных;

незначительным негативным последствиям для субъектов персональных данных.

Угрозы утечки персональных данных по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки персональных данных.

Угрозы, связанные с несанкционированным доступом, приведены в приложении и представляются в виде совокупности обобщенных классов возможных источников угроз несанкционированного доступа, уязвимостей программного и аппаратного обеспечения информационной системы персональных данных, способов реализации угроз, объектов воздействия и возможных деструктивных действий.

2.2 Изучение подходов к защите персональных данных

Для изучения были взяты следующие системы:

- Dallas Lock 8.0-К
- Secret Net
- UserGate Proxy & Firewall 5.2.F
- Антивирусная программа Касперского для Windows Workstations
- Антивирусная программа Касперского Business Space Security

Dallas Lock 8.0-К

Средство предназначено для обеспечения защиты компьютера, подключенного к локальной вычислительной сети, от несанкционированного или случайного доступа. Поддерживает только 32-х битные версии операционных систем семейства Windows.

Система представляет программное средство, обеспечивающее защиту от несанкционированного доступа к информационным ресурсам компьютеров с возможностью подключения аппаратных идентификаторов и осуществляет:

• Препятствие для несанкционированного доступа на персональной электронно-вычислительной машине в локальной вычислительной сети через локальный, сетевой и терминальный входы;

• Разграничение полномочий и аудит действий пользователей по доступу к файловой системе и другим ресурсам компьютера. Разграничения касаются всех пользователей – локальных, сетевых, доменных, терминальных;

• Контроль целостности защищаемых данных и программных средств;

• Защита компьютера от загрузки с внешних носителей;

• Замкнутая программная среда;

• Контроль каналов распространения конфиденциальной информации;

• Контроль устройств;

• Централизованное управление, мониторинг и сетевой аудит;

• Масштабируемая система защиты.

SECRET NET

Создано для защиты сведений, относящихся к коммерческой, гос. тайне или являющимися персональными данными. Является средством защиты от инсайдерских угроз, возможно применение, как на автономных станциях, так и в информационных сетях, есть возможность подключения аппаратных идентификаторов. Работает под управлением операционных систем компании Windows как 32х битных, так и64х, основные возможности аналогичны «Dallas Lock 7.7», но имеются дополнительные:

• Защита терминальных сессий – защита инфраструктуры основанной на терминальных сессиях для платформ Citrix и Microsoft;

• Замкнутая программная среда.

АНТИВИРУСНАЯ ПРОГРАММА КАСПЕРСКОГО ДЛЯ WINDOWS WORKSTATIONS

Является решением для проблем связанных с комплексной антивирусной защитой рабочих станций, находящихся в корпоративной сети и за неё границами, от разных различных видов вредоносных и потенциально опасных программных средств, и атак через сеть.

Основные возможности:

• Комплексная защита рабочих мест;

• Защита файловых систем;

• Защита средств электронных коммуникаций;

• Защита работы в интернете;

• Пресечение атак со стороны хакеров;

• Контроль использования внешних устройств.

АНТИВИРУС КАСПЕРСКОГО BUSINESS SPACE SECURITY

Это система для антивирусной защиты файлов, находящихся на сервере, электронно-вычислительных машин, персональных компьютеров, портативных вычислительных устройств, т.е. система обеспечивает безопасность корпоративной сети.

Основные возможности:

• Защита рабочих мест и серверов;

• Защита файловой системы;

• Защита электронных коммуникаций;

• Защита во время сёрфинга в интернете;

• Предотвращение хакерских атак;

• Мониторинг использования внешних устройств;

• Защита от фишинга;

• Межсетевой экран и система обнаружения вторжений;

• Мониторинг активности программ и поиск слабых мест;

• Веб-Мониторинг.

USERGATE PROXY & FIREWALL 5.2.F

Данный комплекс существует для организации доступа в Интернет из локальной сети, учёта трафика и защиты корпоративной сети от внешних угроз. User Gate является эффективным программным обеспечением и существует для использования в небольших организациях.

• Информационная безопасность;

• Мониторинг и статистика;

• Организация доступа в Интернет;

• Администрирование сети;

• Повышение уровня безопасность использования Интернета;

• Понижение нецелевого трафика (в том числе снижение затрат компании);

• Увеличение коэффициента полезного действия работников (запрет соц. сетей, форумов и сёрфинга в интернете т.д.).

Автор отдаёт предпочтение системе защиты Secret Net.

Secret Net – средство предназначенное для защиты сведений коммерческой или гос. тайны, исключающее несанкционированный и случайный доступ на автоматизированных рабочих местах и сервере.

Является эффективным средством защиты от угроз внутри самой организации.

Преимущества средства защиты информации от несанкционированного доступа Secret Net:

1) Средство защиты Secret Net, имеющее соответствующие сертификаты и позволяющее привести автоматизированные системы в соответствие с требованиями регулирующих документов: Федеральный закон №98, Федеральный закон №152, Федеральный закон №5485-1. Сертификаты Федеральной службы по техническому и экспортному контролю Российской Федерации дают возможность использовать Secret Net для защиты: сертной информации и гос. тайны в автоматизированных системах до класса 1Б включительно;

информационных систем обработки персональных данных до класса К1 включительно.

2) Надежность и масштабируемость.

Secret Net осуществляет защиту отдельных рабочих станций в небольших организациях и вычислительных инфраструктур класса Enterprise. Сетевой вариант Secret Net может быть успешно развернут в сложной доменной сети с большим количеством филиалов.

3) Доступная цена.

Комплектность поставки зависит от размеров защищаемой системы и требований, касающихся безопасности.

4) Удобное администрирование.

Что позволяет централизованно управлять политикой безопасности и аудитом.

Ключевые возможности средств защиты информации от несанкционированного доступа Secret Net:

1)Разграничение доступа - усиление аутентификации пользователей, полномочное управление доступом на основе категорий конфиденциальности ресурсов и прав допуска пользователей, разграничение доступа к устройствам компьютера. В качестве персональных идентификаторов могут быть использованы: iButton, eToken, Rutoken.

2)Доверенная информационная среда - защита компьютера от загрузки с внешних носителей либо программным, либо аппаратным способом; замкнутая

программная среда; контроль целостности программ и данных.
3)Контроль над каналами распространения конфиденциальной информации - регистрация событий безопасности, контроль печати и отчуждения конфиденциальной информации, гарантированное удаление данных.
4)Контроль устройств - контроль неизменности аппаратной конфигурации компьютера и доступа пользователей к устройствам компьютеров, централизованные политики использования отчуждаемых носителей в организации.
5)Центральное управление, мониторинг и аудит (сетевой вариант) – управление на расстоянии и оперативный мониторинг в режиме реального времени, централизованные политики безопасности, аудит событий информационной безопасности. Возможность развертывания серверов безопасности с подчинением в филиалах организации.
6)Защита терминальных сессий - защита инфраструктуры основанной на терминальных сессиях для платформ Citrix и Microsoft.
7)Масштабируемая система защиты - Secret Net поставляется справляться с защитой как в автономном режиме, предназначенном для защиты отдельных компьютеров, так и в сетевом.
Варианты Secret Net:
- автономный вариант – предназначен для защиты серверов и рабочих станций
- сетевой вариант – дополнен средствами центрального управления безопасностью для работы в больших сетях с большим количеством рабочих мест.

3.ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Системная архитектура проекта

Разработка физической модели данных и состава функций системы, уточнение требований к системе (диаграммы UML).

Диаграмма прецедентов в UML — диаграмма, которая отражает отношения между актёрами и прецедентами и являющаяся основной частью модели прецедентов, позволяющей подробно описать систему на концептуальном уровне.

Прецедент - возможность моделируемой системы (часть её функциональности), которая позволяет пользователю получить конкретный, измеримый и нужный ему результат. Прецедент соответствует отдельному сервису системы, определяет один из вариантов её использования и описывает типичный способ взаимодействия пользователя с системой. Варианты использования обычно применяются для спецификации внешних требований к системе.

На первой диаграмме показано следующее (Рисунок 18):

- Для контроля и мониторинга функционирования системы защиты назначается ответственное лицо, имеющее должные зная в области информационной безопасности и защите персональных данных;
- Администрация назначает специалиста по информационной безопасности;
- Специалист проводит обучение сотрудников, которые непосредственно учувствуют в обработке персональных данных.

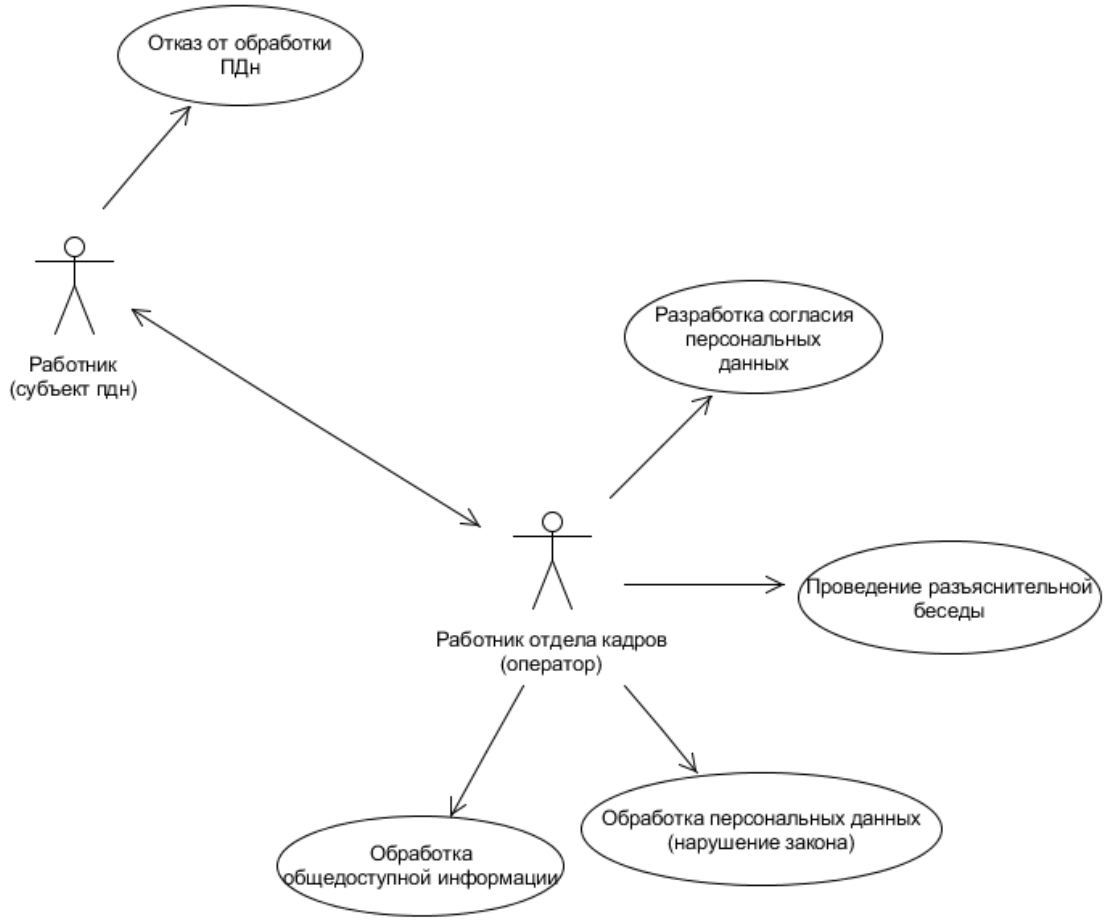

Отказ от обработки ПДн
Работник (субъект пдн)
Разработка согласия персональных данных
Работник отдела кадров (оператор)
Проведение разъяснительной беседы
Обработка общедоступной информации
Обработка персональных данных (нарушение закона)

Рисунок 18

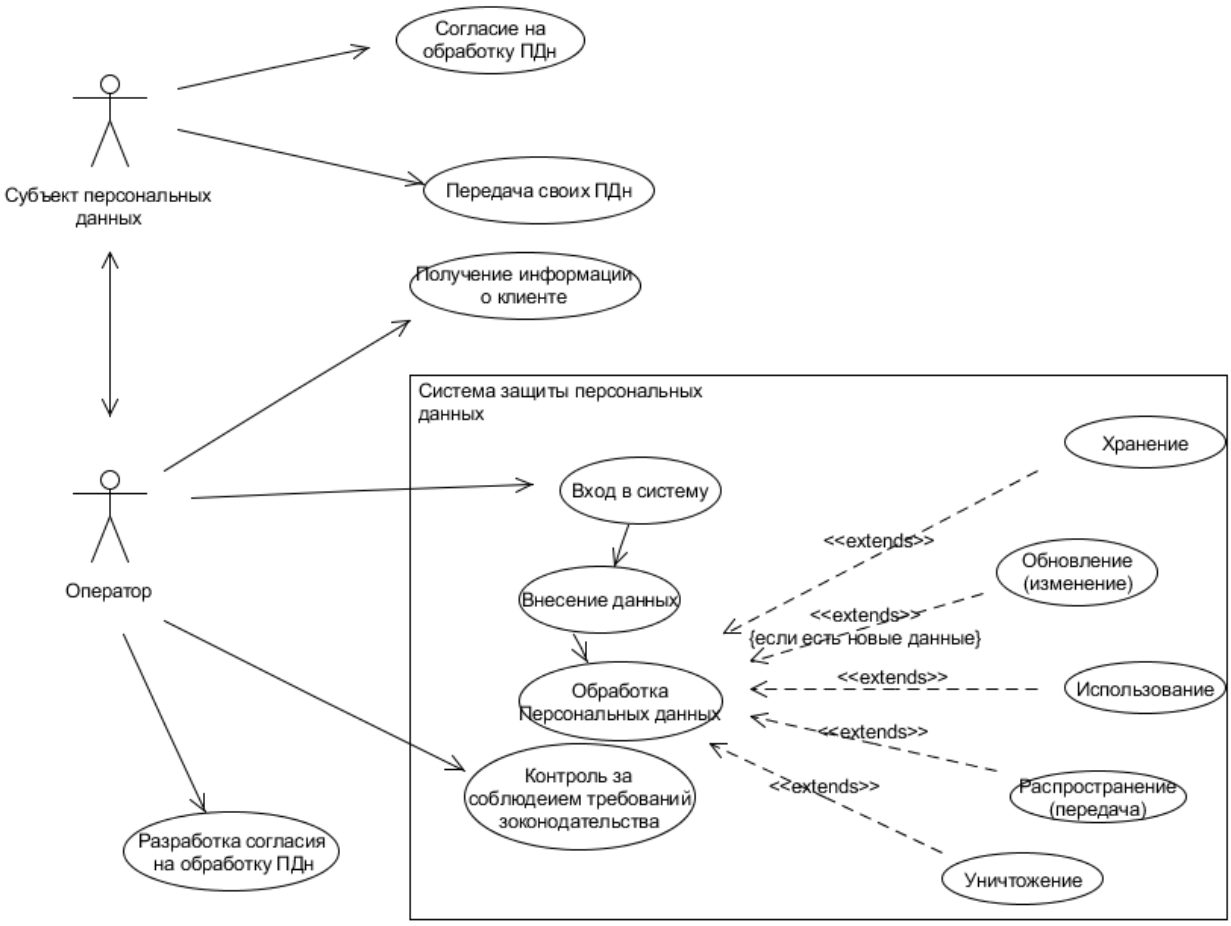


Рисунок 19

Диаграмма №2 показывает следующее (Рисунок 19):

- Оператор (работник отдела кадров) занимается разработкой согласия на обработку персональных данных;
- Субъект подписывает согласие и таким образом соглашается с обработкой своих персональных сведений;
- Оператор имеет доступ к системе и производит вход с помощью ЕТокена;
- Вносит необходимую информацию в информационную систему персональных данных;
- Информация на сервере обрабатывается;
- Оператор следует нормам законодательства.

Диаграмма прецедентов №3 чётко отражает обязанности специалиста по информационной безопасности, администратора и сотрудника организации, который будет участвовать в мероприятиях по обработке персональных данных (Рисунок 20).

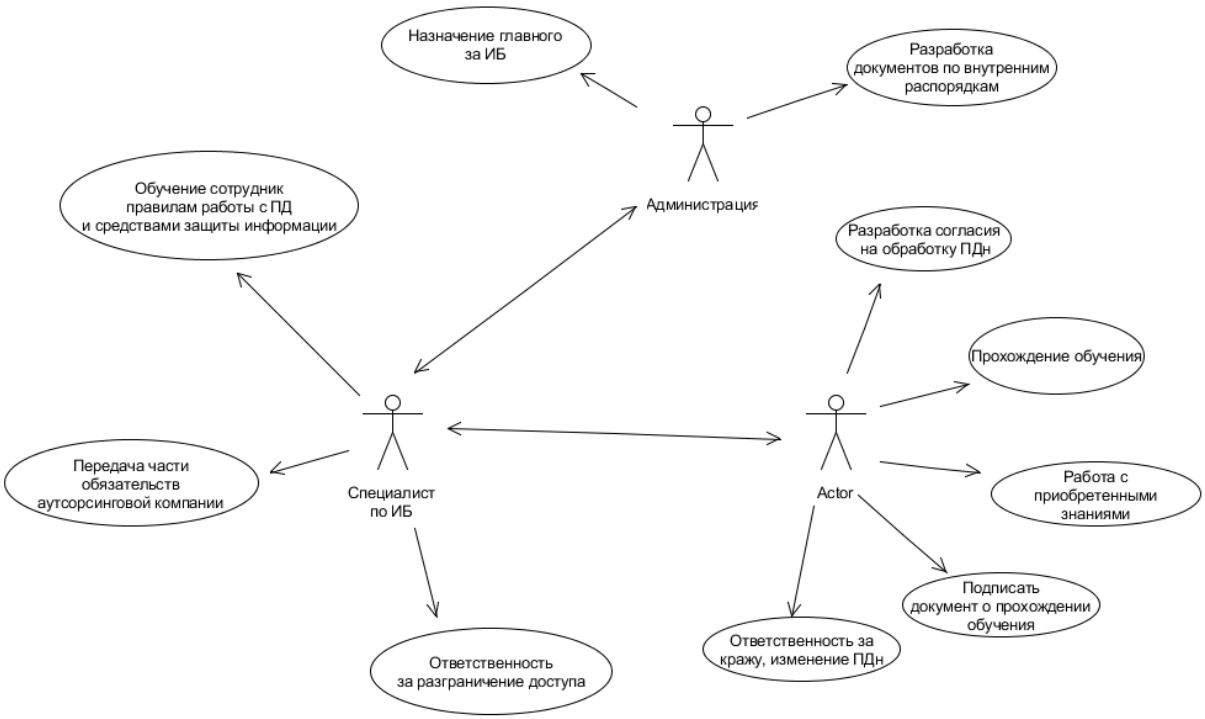


Рисунок 20

Диаграмма последовательности показывает взаимодействие и моделирует процессы взаимодейсвия между объектами системы с учетом времени, а также обмен сообщениями между объектами (Рисунок 21).

На данной диаграмме показаны поочерёдные действия, происходящие с персональными данными в информационной системе персональных данных.

Действия Оператора:

- Перед началом работы, Оператор, имеющих доступ в систему, выпоняет вход через свой рабочий компьютер;
- Если у Опертора есть солгасие на обработку персональных данных субъекта, то он производит ввод персональных данных;

- Данные шифруются;
- Сведения подвергаются фильтрации и передаются через межсетевой экран на сервер организации, где хранятся персональные данные;
- На сервера данные обрабатываются;
- После всех действий Оператор персональных данных получает ответ от сервера о том, что данные переданы на севрер.

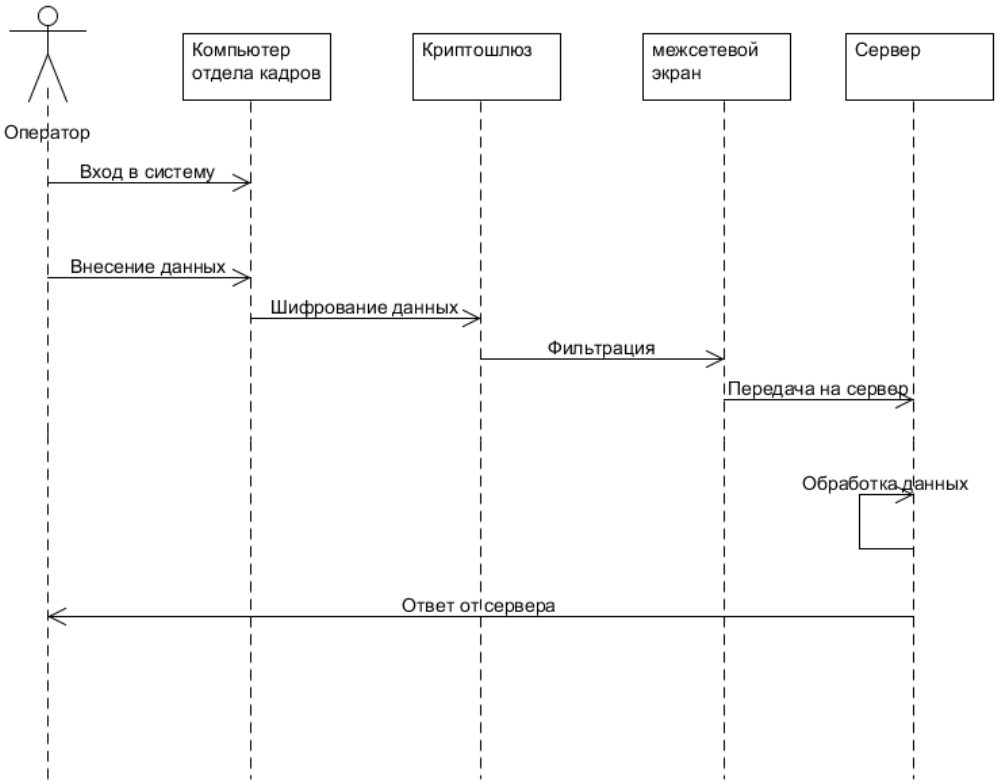


Рисунок 21

Диаграмма отражает физическим представление системы, таким образом она позволяет определить архитектуру создаемой системы, путём установления зависимостей между программами (Рисунок 22).

Диаграмма развертывания применяются для создания визуальной модели представления системы, визуализируя элементы и компоненты программ. Таким образом данная диаграмма графически показывает взаимодействие процессоров, устройств и их связи (Рисунок 23).

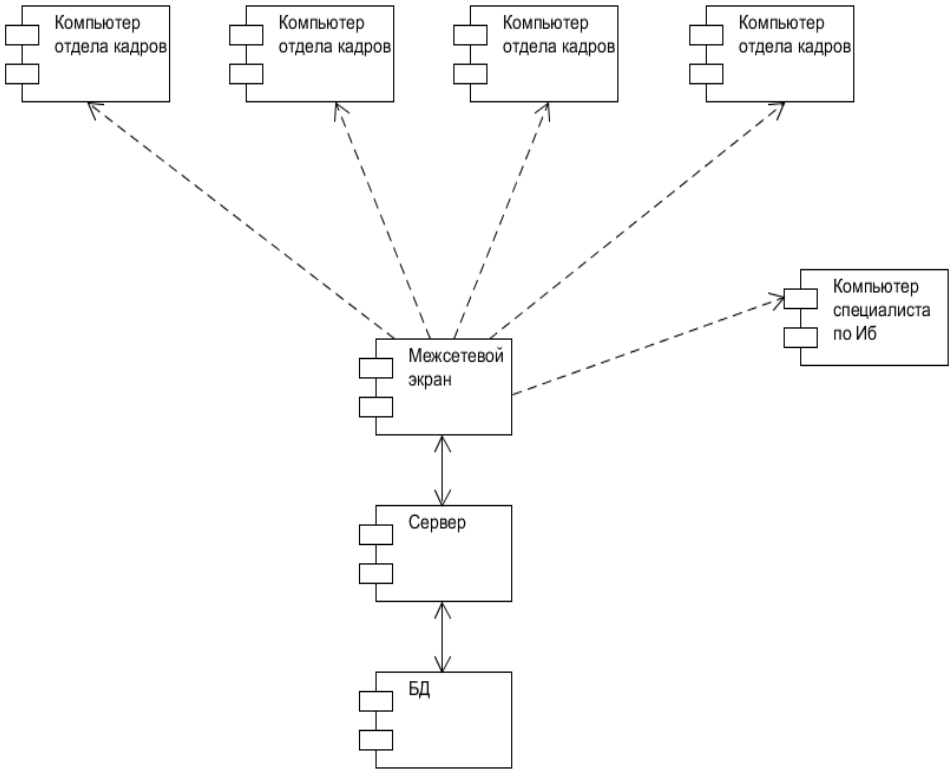


Рисунок 22

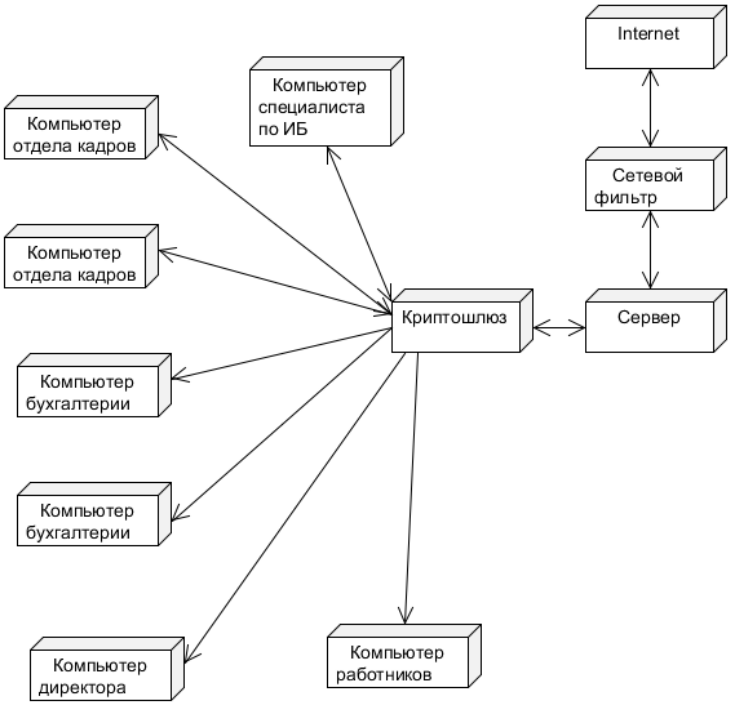


Рисунок 23

3.2 Анализ размещения и функционирования средств защиты информационной системы персональных данных

Средства защиты от несанкционированного доступа представлены следующими создаваемыми компонентами:

– набор драйверов «eToken PKI Client»;

– ПО «eToken Network Logon»;

– USB-ключи «eToken PRO (Java) / 72K»;

– eToken TMS 2.

Размещение компонент подсистемы защиты от НСД представлено в таблице 1.

Таблица 1 – Расположение элементов подсистемы защиты от НСД

Компонент	Расположение
Набор драйверов «eToken PKI Client 5.1».	В виде программного обеспечения на серверах и рабочих местах информационной системы персональных данных под управлением операционной системы семейства Windows.
USB-ключи «eToken PRO (Java) / 72K».	Пользователи информационной системы персональных данных.
eToken TMS 2.	В виде программного обеспечения на создаваемом сервере, который размещается в зоне управления системы защиты персональных данных.
Программное обеспечение «eToken Network Logon».	В виде программного обеспечения на серверах и рабочих местах системы персональных данных под управлением операционной системой Windows.

Взаимодействие между компонентами подсистемы защиты информационной системы персональных данных от несанкционированного доступа приведено на рисунке 24.

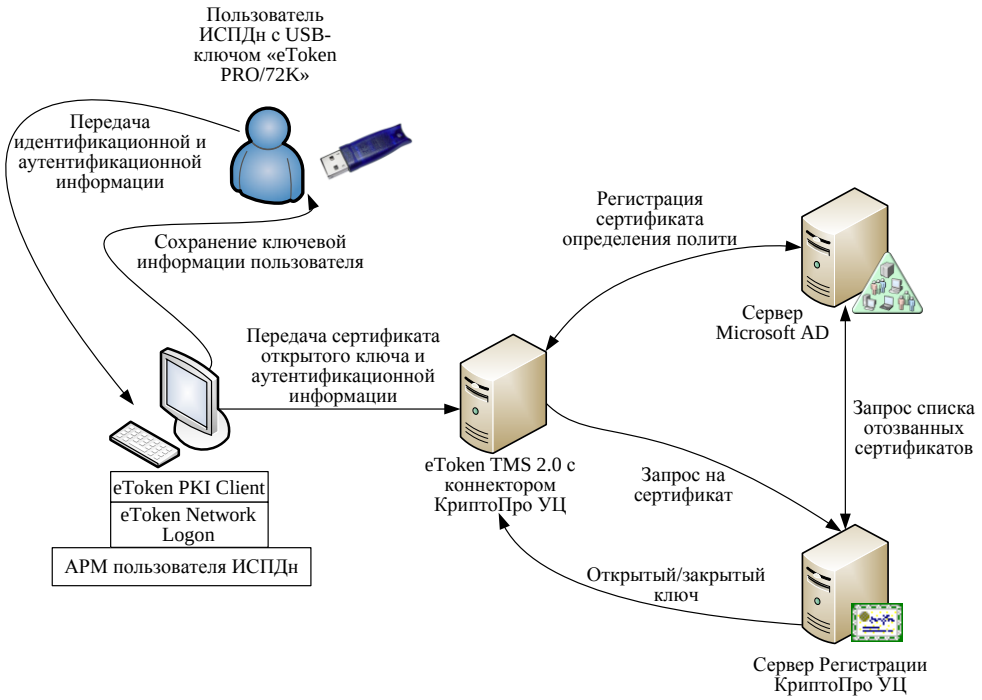


Рисунок 24 – Схема работы и местоположения компонентов подсистемы защиты от несанкционированного доступа

Компоненты подсистемы защиты от НСД должны работать в режимах, приведенных в таблице 2.

Таблица 2 – Режимы функционирования компонент средств защиты от НСД

Компонент	Режим функционирования
Набор драйверов «eToken PKI Client».	В рабочие часы пользователей.
ПО «eToken Network Logon».	В рабочие часы пользователей.
USB-ключи «eToken PRO (Java) / 72K».	В рабочие часы пользователей.

eToken TMS 2.0.	24/7.
Центр Сертификации «КриптоПро УЦ».	24/7.
Центр Регистрации «КриптоПро УЦ».	24/7.
Рабочее место администратора Центра Регистрации.	В рабочие часы администраторов.
Рабочее место разбора конфликтных ситуаций.	В рабочие часы администраторов.

Средства компании «Secret Net», созданные для защиты от несанкционированного доступа:

– защищенное хранение открытых и закрытых ключей в памяти аппаратного идентификатора «eToken»;

– идентификацию и двухфакторную аутентификацию работников информационной системы персональных данных при входе/выходе в операционную систему или программу;

– блокирование автоматизированных рабочих мест и принудительный выход сотрудника при отключении аппаратного идентификатора пользователя.

Комплекс по защите узлов – «Symantec Endpoint Protection», производства компании Symantec является средством антивирусной защиты, средством персонального межсетевого экранирования, средством управления съемными носителями.

«Symantec Endpoint Protection» обеспечивает интегрированную защиту от вирусов и шпионских программ на базе технологии Symantec Antivirus с полной защитой в реальном времени и автоматическими средствами локализации и дезактивации угроз.

Решение на базе «Symantec Endpoint Protection» состоит из следующих компонентов:

– комплексное интегрированное средство антивирусной защиты (САВЗ) средства управления съемными носителями (СУСН), персонального межсетевого экранирования «Symantec Endpoint Protection Client»;

– сервер обеспечивающий управление «Symantec Endpoint Protection Manage»;

– консоль для управления сервером «Symantec Endpoint Protection Manager Console».

Размещение компонент «Symantec Endpoint Protection» представлено в таблице 3. Взаимодействие между элементами «Symantec Endpoint Protection» представлено на рисунке 25.

Таблица 3 – Размещение компонент «Symantec Endpoint Protection»

Компонент	Расположение
«Symantec Endpoint Protection Client».	В виде программного обеспечения на автоматизированных рабочих местах пользователей информационной системы персональных данных.
«Symantec Endpoint Protection Manage».	В виде программного обеспечения на создаваемом сервере, который размещается в зоне управления системы защиты персональных данных.
«Symantec Endpoint Protection Manager Console».	В виде программного обеспечения на существующем автоматизированном рабочем месте администратора САВЗ.

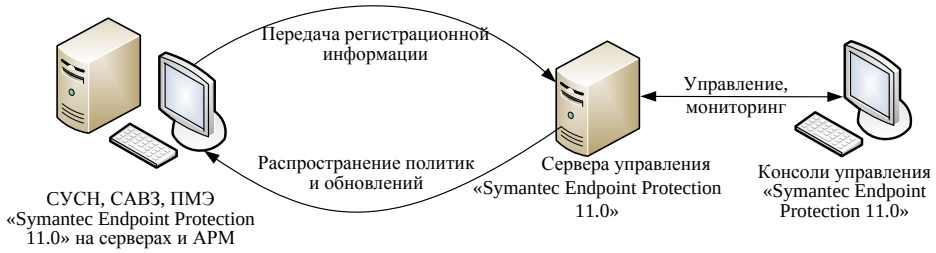


Рисунок 25 – Схема работы и местоположение элементов «Symantec Endpoint Protection»

Элементы «Symantec Endpoint Protection» должны функционировать в режимах, приведенных в таблице 4.

Таблица 4 – Режимы функционирования средств «Symantec Endpoint Protection»

Компонент	Режим функционирования
СУСН «Symantec Endpoint Protection Client».	В рабочие часы пользователей.
САВЗ «Symantec Endpoint Protection Client».	В рабочие часы пользователей.
Персональный межсетевой экран «Symantec Endpoint Protection Client».	В рабочие часы пользователей.
Сервер управления «Symantec Endpoint Protection Manage».	Круглосуточно и ежедневно.
Консоль управления «Symantec Endpoint Protection Manager Console».	В рабочие часы администраторов.

Средства антивирусной защиты «Symantec Endpoint Protection Client» осуществляют:

– автоматическую проверку на наличие вирусов и других вредоносных программ по типовым шаблонам или сигнатурам;

– автоматическую антивирусную проверку и проверку наличия других вредоносных программ с помощью эвристического анализа;

– автоматическая блокировка вредоносных программ и возможность удаления этих программ;

– возможность выполнения проверок по расписанию;

– проверку всех файлов на наличие вирусов непосредственно в момент их запуска;

– контроль выполнения макросов в документах формата Microsoft Office, с блокировкой опасных макрокоманд;

– проверку на вирусы исполняемых скриптов;

– возможность исключеать из антивирусной проверки файлы доверенных приложений.

– возможность получения информации о состоянии и работе программы, используя различные варианты отчетов с разным уровнем детализации.

– обновление шаблонов популярных вредоносных программ по расписанию;

– регистрацию обнаружения, блокированием, удалением вредоносных программ.

СУСН «Symantec Endpoint Protection Client» осуществляет управление подключением периферийных средств, а так режимами его работы.

«Symantec Endpoint Protection Client» является персональным межсетевым экраном, обеспечивающим персональную защиту автоматизированных рабочих мест и серверов на базе Microsoft Windows.

Средства межсетевого экранирования представлены межсетевыми экранами Cisco ASA 5500 Series и «Symantec Endpoint Protection». Кроме того в процессах защиты межсетевого взаимодействия принимают участие существующие на предприятии средства сетевой инфраструктуры.

Размещение компонент подсистемы представлено в таблице 5.

Таблица 5 – Размещение компонент межсетевого экранирования

Компонент	Расположение
Cisco ASA 5500 Series.	Выделенное программно-аппаратное средство между зоной серверов информационной системы персональных данных и остальными зонами.

Взаимодействие защищенных зон информационной системы персональных данных возможно только при участии средств межсетевого экранирования. Оно может быть реализовано путём:

– ПМЭ (Symantec Endpoint Protection);

– МСЭ Cisco 5500 Series (размещение представлено на рисунке 26).

На рисунке 26 представлена схема расположения элементов межсетевого экранирования.

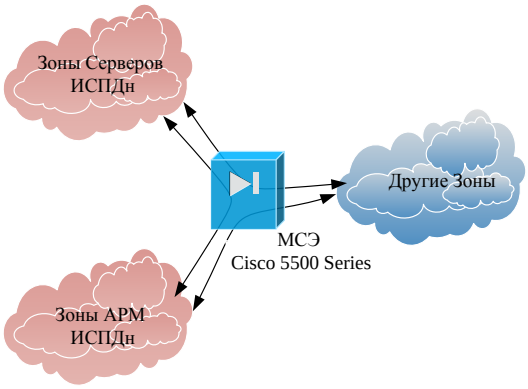


Рисунок 26 – Схема расположения элементов межсетевого экранирования

Элементы подсистемы межсетевого экранирования функционируют в следующих режимах, приведенных в таблице 6.

Таблица 6 – Режимы функционирования средств межсетевого экранирования

Компонент	Режим функционирования
МСЭ «Cisco ASA 5500 Series».	Круглосуточно и ежедневно.
Консоль управлений.	В рабочие часы администраторов безопасности.

Подсистема защиты межсетевого взаимодействия обеспечивает:

– разделение всех узлов информационной системы персональных данных и системы защиты персональных данных на защищенные зоны, которые обеспечиваются организацией виртуальных локальных сетей;

– запрет взаимодействия узлов защищенных зон 10 и 30 в обход средств межсетевого экранирования;

– маршрутизацию сетевого трафика между защищаемыми зонами;

– фильтрацию трафика между зонами на основе параметров протоколов 3-4 уровня модели OSI;

– регистрацию и учет пакетов, которые подвергаются фильтрации. В функции регистрации включаются адрес, время и результат фильтрации;

– регистрацию запуска внутренних процессов;

– регистрацию сессии администратора межсетевого экрана в систему либо загрузки и инициализации системы.

Средства криптографической защиты представлены следующими создаваемыми компонентами:

– криптошлюз «S-terra CSP VPN Gate»;

– S-terra VPN клиент «CSP VPN Client».

Принцип расположения элементов подсистемы расписан в таблице 7.

Таблица 7 – Расположение средств криптографической защиты

Компонент	Расположение
Криптошлюз «S-terra CSP VPN Gate».	В виде ПАК, который размещается на границе зоны серверов информационной системы персональных данных.
S-terra VPN клиент «CSP VPN Client».	В виде программного обеспечения установленного на АРМ удаленного пользователя информационной системы персональных данных.

Взаимодействие между компонентами подсистемы приведено на рисунке 27.

Компоненты подсистемы криптографической защиты работают в следующих режимах, приведенных в таблице 8.

Таблица 8 – Режимы функционирования средств криптографической защиты

Компонент	Режим функционирования
Криптошлюз «S-terra CSP VPN Gate».	Круглосуточно и ежедневно.
S-terra VPN клиент «CSP VPN Client».	В рабочие часы пользователей.

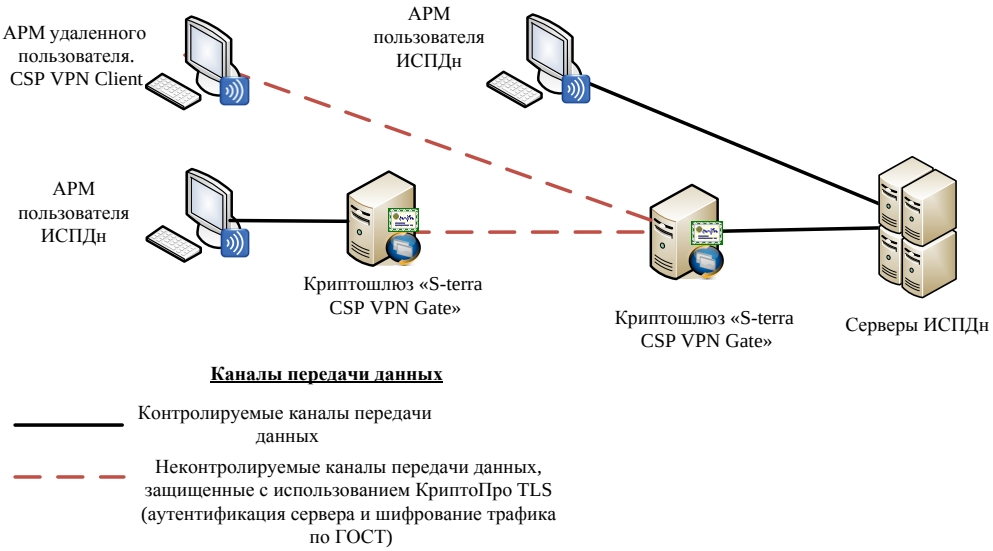


Рисунок 27 – Принцип размещения компонентов криптографической защиты

Подсистема криптографической защиты обеспечивает:

– шифрование защищаемой информации при ее передаче по неконтролируемым каналам связи;

– шифрование команд управления при их передаче по неконтролируемым каналам связи;

– управление криптографическими ключами.

– изготовление сертификатов ключей подписи.

– изготовление списков отозванных (аннулированных и приостановленных) сертификатов ключей подписи.

– регистрацию событий, связанных с безопасностью информационной системы персональных данных (использование ключей подписи; создание, завершение защищенного соединения; проверка ключей подписи).

Подсистема криптографической защиты данных обеспечивает:

– шифрование защищаемой информации;

– изготовление криптографических ключей;

– управление криптографическими ключами.

Средства обнаружения вторжений является программно-аппаратным продуктом IBM – «Proventia Intrusion Prevention Appliance».

Размещение компонент представлено в таблице 9.

Таблица 9 – Размещение компонент средств обнаружения вторжений

Компонент	Расположение
«IBM Proventia Prevention Appliance».	Программно-аппаратное средство, которое размещается в зоне подключения к сети Интернет.
Консоль управления.	В рабочие часы администратора безопасности.

Взаимодействие элементов подсистемы и информационной системы персональных данных приведено на рисунке 28.

Средство обнаружения вторжений «IBM Proventia IPS» обеспечивает:

– обнаружение трафика известной сетевой атаки из потока данных;

– обнаружение аномальной или запрещенной политикой безопасности сетевой активности;

– возможность автоматического реагирования на обнаруженное вторжение;

– периодическое обновление обнаруживаемых сигнатур атак;

– регистрацию событий, связанных с безопасностью ИСПДн.

Средства анализа защищенности представлены компонентом – «MaxPatrol».

Размещение компонент подсистемы представлено в таблице 10.

Таблица 10 – Размещение компонент подсистемы обнаружения вторжений

Компонент	Расположение
MaxPatrol Server Audit.	В виде программного обеспечения на создаваемом автоматизированном рабочем месте аудитора информационной безопасности.

Взаимодействие средств анализа защищенности с элементами информационной системы персональных данных приведено на рисунке 29.

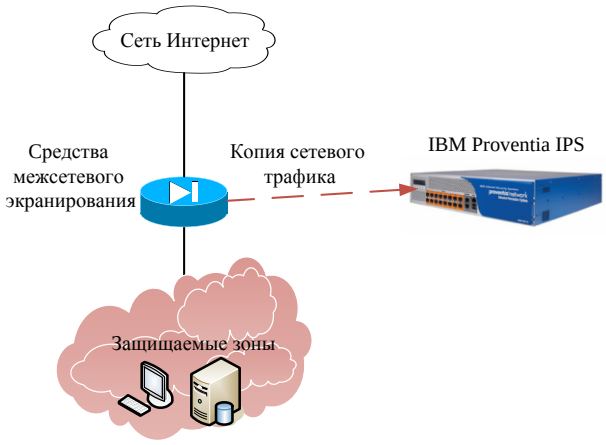


Рисунок 28 – Принцип функционирования и размещения компонентов подсистемы обнаружения вторжений

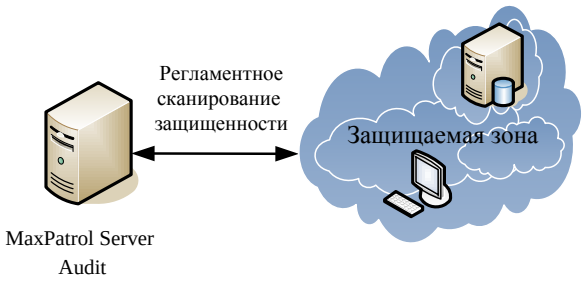


Рисунок 29 – Принцип функционирования и размещения составляющих элементов подсистемы анализа защищенности

Средство анализа защищенности «MaxPatrol» осуществляет:

– проверка сетевых узлов и сервисов и обнаружение изменений;

– поиск и обнаружение слабых мест программно-аппаратного обеспечения информационной системы персональных данных и системы защиты информации;

– выполнение тестов, показывающих эффективность функционирования системы защиты персональных данных:

– мониторинг соблюдений политик безопасности;

– обновление базы уязвимостей выполняется каждый день;

– ведение отчетной документации о обнаруженных уязвимостях и способах их предотвращения.

4.ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ПРОЕКТА

За основу расчета были взяты: затраты на мероприятия по разработке системы защиты персональных данных, затраты на закупку средств защиты и ввод в эксплуатацию, сумма, необходимая для поддержки системы защиты персональных данных.

Сумма расходов по разработке системы зашиты персональных данных и ввода в эксплуатацию средств защиты информации в большей степени зависят от того, какая схема работ выбрана.

С экономической точки зрения, более рациональным будет воспользоваться услугами системных интеграторов, выполняющих работы, в области информационной безопасности, имеющих лицензии и сертификаты Федеральной службы технического и экспортного контроля и Федеральной службы безопасности Российской Федерации.

В таком случае не придётся содержать целый отдел специалистов и платить им зарплату, что уже снижает затраты на создание и поддержание системы защиты персональных данных и повышает её качество.

Для расчета экономической эффективности внедрения разработанной системы защиты персональных данных необходимо суммарную ее стоимость разработки, внедрения и поддержки за три года сравнить со стоимостью возможного ущерба со стороны регуляторных рисков за такой же период.

Экономическая эффективность создания и поддержки спроектированной системы защиты персональных данных будет равна:

$$Э = \frac{П \cdot 100\%}{З} = \frac{269100{,}00}{172942{,}50} = 1{,}56,$$

где $П$ – вероятные финансовые потери за период 3 года за счет регуляторных рисков;

З – сумма на создание и поддержку системы защиты персональных данных в течении 3 лет.

С помощью анализа было выявлено, что каждый рубль, который будет потрачен на реализацию проекта системы защиты персональных данных и поддержку её функционирования в течении 36 месяцев, позволяет сократить риски на 1,56 рублей.

Заключение

Пожалуй самым актуальным на сегодняшний день вопросом в области защиты информации в Российской Федерации является защита персональных данных в соответствии с законами Российской Федерации и вероятными угрозами безопасности информационных систем персональных данных.

Особенно актуальна проблема, связанная с обеспечением безопасности персональных данных в государственных организациях и просто, информационных системах, которых можно назвать крупными, по количеству обрабатываемых персональных данных и единицам аппаратных средств и систем.

Отличительной чертой автоматизированной информационной системы персональных данных является метод передачи информации. Информация передаётся по неконтролируемому каналу, который представляет собой связи общего пользования или глобальную сеть интернет.

В большинстве случаев обработке подвергаются персональные данные второй категории, т.е. имя, фамилия, год, месяц, дата и место, где родился, образование и т.д.

Автоматизированная информационная система персональных данных всегда является специальной, так как для неё кроме обеспечения конфиденциальности необходимо так же обеспечить целостность и доступность.

Опираясь на модель угроз, информационная система персональных данных характеризуется низким уровнем исходной защищённости и радом угроз, имеющих высокую вероятность реализации.

К средствам криптографической защиты в рамках системы защиты персональных данных должны предъявляться требования по сертификации Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации не ниже класс КС2.

Специалист по защите информации в ходе экспертной оценке присваивает определённый класс специальной информационной системы персональных данных. Информационной системе персональных данных присваивается класс К2, так как в случае нарушения характеристики безопасности персональных данных, субъекты персональных данных пострадают не значительно.

Для того чтобы свести к нулю вероятности угроз на протяжении всего жизненного цикла информационной системы персональных данных, реализуется следующий комплекс мер и средств защиты:

– проведение тестов, наглядно показывающих эффективность системы защиты персональных данных;

– организационных и организационно-технических;

– инженерных и инженерно-технических;

– технических;

– программных, аппаратных и программно-аппаратных.

Разрабатываемая система защиты персональных данных согласно анализу должна состоять из следующих подсистем:

– подсистема защиты от несанкционированного доступа или случайного доступа;

– подсистема антивирусной защиты;

– подсистема межсетевого экранирования;

– подсистема криптографической защиты;

– подсистема обнаружения вторжений;

– подсистема анализа защищенности.

Согласно факторному анализу имеющихся сегодня на рынке средств защиты, которые можно использовать в рамках системы защиты персональных данных, наилучшие показатели у следующих:

– ПО Symantec Endpoint Protection – СУСН, ПМЭ, САВЗ;

– ПО eToken Network Logon, применяемый совместно с идентификаторами eToken PRO (Java)/72K/CERT-1883 – средство обеспечения усиленной аутентификации;

– Cisco ASA 5500 Series – программно-аппаратные межсетевые экраны;

– S-Terra CSP VPN – программные и программно-аппаратные средства криптографической защиты;

– IBM Proventia IPS – программно-аппаратная система, исключающая вторжения;

– MaxPatrol – программное средство обнаружения вторжений.

Перечисленные средства защиты обладают необходимыми сертификатами Федеральной службы безопасности и Федеральной службы по техническому и экспортному контролю Российской Федерации и образуют в совокупности комплексную систему защиты персональных данных, осуществляющую соблюдение всех требований законов, а так же требований, выявленных на основе модели угроз и нарушителя информационная система персональных данных. Разработанная на основе такого решения система защиты персональных данных имеет наиболее лучшие технико-экономические показатели эффективности.

Главные функции «eToken Network Logon» – надёжное хранение открытых и закрытых ключей в памяти идентификатора eToken PRO, идентификация и двухфакторная аутентификация пользователей информационной системы персональных данных при входе/выходе в операционную систему или программу, блокировка рабочей зоны и принудительный выход пользователя при изъятии аппаратного идентификатора пользователя.

Решение «Symantec Endpoint Protection» включает в себя следующие элементы:

– «Symantec Endpoint Protection Client» – САВЗ, СУСН, ПМЭ;

– «Symantec Endpoint Protection Manage» – сервер управления;

– «Symantec Endpoint Protection Manager Console» – консоль управления.

САВЗ «Symantec Endpoint Protection Client» обеспечивает антивирусную защиту автоматизированных рабочих мест и серверов на базе Microsoft Windows.

СУСН «Symantec Endpoint Protection Client» позволяется управлять подключением периферийных устройств, а также режимами их функционирования.

ПМЭ «Symantec Endpoint Protection Client» представляет собой персональный межсетевой экран, обеспечивающий персональную защиту автоматизированных рабочих мест и серверов на базе Microsoft Windows.

Для межсетевого экранирования требуется разделение всех узлов информационной системы персональных данных и системы защиты персональных данных на защищенные зоны, обеспечивающихся организацией виртуальных локальных сетей, запрет взаимодействия узлов защищенных зон в обход средств межсетевого экранирования Cisco ASA 5500 Series.

Cisco ASA 5500 Series должен выполнять:

– маршрутизацию сетевого трафика между защищаемыми зонами;

– подвергать фильтрации трафик между зонами на основе параметров протоколов 3-4 уровня модели OSI;

– регистрацию и учет фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.

Подсистема криптографической защиты, в составе «S-terra CSP VPN Gate» и «CSP VPN Client» реализует зашифровку конфиденциальных данных и её передачу по неконтролируемым каналам, управления криптографическими ключами.

Средство обнаружения вторжений «IBM Proventia Prevention Appliance» реализует обнаружение трафика известной сетевой атаки, аномальной или запрещенной политикой безопасности сетевой активности.

Средство анализа защиты «MaxPatrol» показывает слабые места программно-аппаратного обеспечения информационной системы персональных

данных и системы защиты персональных данных, а так же проводит тестирование эффективности работы системы защиты персональных данных.

В совокупности, средства защиты составляют комплексную систему защиты персональных данных для информационной системы.

Список использованных источников

1. Российская Федерация. Законы. О персональных данных [Электронный ресурс]: Федеральный закон N 152-ФЗ: [принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 года] // СПС Консультант Плюс.

2. Российская Федерация. Постановления. Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 17 ноября 2007 г. N 781. // СПС Консультант Плюс.

3. Российская Федерация. Приказы. Порядок проведения классификации информационных систем персональных данных [Электронный ресурс]: приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. N 55/86/20 // СПС Консультант Плюс.

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: утв. Федеральной службой по техническому и экспортному контролю 15 февраля 2008 г // СПС Консультант Плюс.

5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: утв. Федеральной службой по техническому и экспортному контролю 14 февраля 2008 г // СПС Консультант Плюс.

6. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г. N 114 // СПС Консультант Плюс.

7. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 25 июля 1997 г // СПС Консультант Плюс.
8. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г // СПС Консультант Плюс.
9. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г // СПС Консультант Плюс.
10. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г // СПС Консультант Плюс.
11. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации [Электронный ресурс]: утв. ФСБ РФ 21 февраля 2008 г. N 149/54-144 // СПС Консультант Плюс.
12. 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

[Электронный ресурс]: утв. ФСБ РФ 21 февраля 2008 г. N 149/6/6-622 // СПС Консультант Плюс.

13. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федер. закон: [принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 г.] // СПС Консультант Плюс.

14. Российская Федерация. Приказы. Положение о сертификации средств защиты информации по требованиям безопасности информации [Электронный ресурс]: приказ Гостехкомиссии РФ от 27.10.1995 N 199 // СПС Консультант Плюс.

15. Российская Федерация. Законы Трудовой кодекс Российской Федерации [Электронный ресурс]: фед. закон: [принят Гос. Думой 21 дек. 2001 г.; одобр. Советом Федерации 26 дек. 2001 г.: по сост. на 1 марта 2009 г.] // СПС Консультант Плюс.

16. Российская Федерация. Законы. Гражданский кодекс Российской Федерации [Электронный ресурс]: офиц. текст. – М. : Экзамен, 2001. – 304 с..

17. Комментарий к Кодексу Российской Федерации об административных правонарушениях" (постатейный): [Электронный ресурс] / под ред. Н.Г. Салищевой; 6-е издание, переработанное и дополненное – Проспект, 2009 // СПС Консультант Плюс.

18. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации [Текст]: федер. закон: [принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 г.]. – М.: Омега-Л, 2007. – 24 с. – 500 экз. – ISBN 5-370-00202-9, 978-5-370-00202-1.

19. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс]. – Введ. 2007–01–01. // СПС Консультант Плюс.

20. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. – Введ. 2006–12–27. // СПС Консультант Плюс.

21. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения [Электронный ресурс]. – Введ. 2000–06–30. // СПС Консультант Плюс.

Приложение 1

Классификация угроз безопасности персональных данных