Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2017 г.

Разработка комплексной системы защиты информации на предприятии ООО "Диджитер"

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Автор проекта,
студент группы КЭ- 520
_____ Федосеев, Е. А.
_____ 2017 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

ЗИ – защита информации;

СЗИ – средство защиты информации;

ИС – информационная система;

НСД – несанкционированный доступ;

КСЗИ – комплексная система защиты информации;

КТ – коммерческая тайна;

ООО – общество с ограниченной ответственностью;

АРМ – автоматизированное рабочие место;

ВКР – выпускная квалификационная работа;

ПО – программное обеспечение;

РД – руководящие документы;

РФ – Российская Федерация;

ФЗ – Федеральный закон;

ФСБ – Федеральная служба безопасности;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании;

Ресурс – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер). Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса;

Угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза;

Уязвимость – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость;

Критичность ресурса – степень значимости ресурса для информационной системы, т.е. как сильно реализация угроз информационной безопасности на ресурс повлияет на работу информационной системы. Единица измерения рубли;

Критичность реализации угрозы – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Единица измерения проценты(%);

Вероятность реализации угрозы через данную уязвимость в течение года – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Единица измерения проценты(%).

ВВЕДЕНИЕ

Потребность в защите информации в современном Российском обществе существует не только у предприятий крупного и среднего бизнеса, но и у малого бизнеса. Регулярное появление новых угроз требует постоянного совершенствования защищённости любой организации, ведь в противном случае при реализации угрозы предприятию может быть нанесён непоправимый ущерб. Возможности малого бизнеса зачастую не позволяют организовать работу специальных служб, обеспечивающих информационную безопасность организации, осуществляющих выявление, предупреждение и устранение возникающих в ней угроз.

Малый бизнес является одним из наименее защищенных от угроз информационной безопасности в силу ряда причин:

1.Высокая стоимость средств защиты информации;

2.Потребность в привлечении сторонних квалифицированных специалистов в области ЗИ;

3.Недостаточное методическое обеспечение деятельности по разработке КСЗИ.

Актуальность данной работы заключается в создании комплексной системы защиты информации в ООО “Диджитер”.

Объектом выпускной квалификационной работы является компьютерная фирма ООО “Диджитер”, занимающаяся продажей компьютеров и оргтехники для корпоративных клиентов и государственных структур.

Предметом выпускной квалификационной работы является КСЗИ.

Целью ВКР является создание комплексной системы мер по защите информации, составляющей коммерческую тайну ООО “Диджитер”.

В соответствии с поставленной целью необходимо решить следующие задачи:

1.Проанализировать информационную систему ООО “Диджитер” с точки зрения информационной безопасности;

2.Определить объекты защиты и привести теоретическое обоснование рекомендуемых средств защиты информации;

3.Разработать проект комплексной системы защиты информации ООО “Диджитер”;

4.Дать оценку экономической целесообразности реализации проекта КСЗИ в ООО “Диджитер”.

1. ПРОВЕДЕНИЕ ПРЕДПРОЕКТНОГО ОБСЛЕДОВАНИЯ В ООО «ДИДЖИТЕР»

1.1. Разработка паспорта предприятия с точки зрения информационной безопасности

При разработке комплекса мер по защите информации необходимо определить общие сведения об объекте защиты. Паспорт предприятия с точки зрения информационной безопасности необходим для выявления общей информации об организации, определения контролируемой зоны защищаемого помещения и объектов защиты информации, на которых обрабатывается информация ограниченного доступа. Компьютерная фирма ООО «Диджитер» занимается продажей и обслуживанием компьютеров и оргтехники для корпоративных клиентов и государственных структур.

В паспорте предприятия представлены реквизиты организации, перечислены основные виды деятельности предприятия, виды защищаемой информации, программно - аппаратные средства, показана общая структура организации, описана строительная инфраструктура здания, информационная среда предприятия, представлена общая схема помещения (Приложение А).

Данная информация была получена в результате устного опроса генерального директора предприятия и непосредственного ознакомления с информационной системой компании.

В качестве объекта защиты была выбрана вся организация ООО «Диджитер», так как предприятие расположено в одном помещении и имеет 10 сотрудников, 6 защищаемых АРМ и 1 сервер.

1.2. Разработка модели деятельности ООО “Диджитер”

Модель деятельности представляет собой описание базовых бизнес – процессов, которые представляют совокупность простых мероприятий, служащих для создания конечной услуги. Данная модель необходима для выявления информа-

ционных потоков и информации ограниченного доступа циркулирующей на предприятии.

В результате анализа организации ООО “Диджитер” была разработана модель деятельности, описывающая базовые бизнес – процессы предприятия (Приложение Б). В данной схеме отражены входные и выходные параметры, ресурсы, внешнее воздействие.

1.3. Выявление защищаемой информации

В ходе анализа деятельности ООО “Диджитер” была выявлена информация ограниченного доступа, которая представляет собой сведения, составляющие коммерческую тайну (на основании Федерального закона от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне")[6].

На предприятии отсутствует режим коммерческой тайны, соответственно для установления режима необходима разработка и реализация комплекса мер:

1. Определение перечня информации, составляющей коммерческую тайну;
2. Ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
3. Учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
4. Регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
5. Нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации.

Основываясь на данных полученных в результате выявления защищаемой информации, в рамках данного пункта был разработан перечень сведений составляющих КТ (Приложение Г), положения о режиме КТ (Приложение В) и подготовлены соответствующие приказы об их утверждении (Приложение Е).

1.4. Описание информационной системы предприятия ООО “Диджитер”

Для разработки комплексной системы защиты информации необходимо проанализировать информационную систему ООО “Диджитер”. Данный анализ позволит выявить характеристики АРМ, сервера и программного обеспечения установленного на них, а так же ответить на вопросы касающиеся обновления ПО и готовности к установке новых программных средств.

Таблица 1 – Аппаратное обеспечение

№	Наименование	Характеристики	Год выпуска	Количество
1	2	3	4	5
АРМ				
1	Системный блок: HP ProDesk 490 G3	Core i5-6500, 4x 3200 Гц, 4 Гб, 500 ГБ, NVIDIA AMD Radeon R5 310, Ethernet, DVD±RW	2015	6
2	Монитор: Acer V226HQLAb	LED 21.5", 1920x1080	2015	6
3	Клавиатура: Genius KM-122	Тип — проводная; Интерфейс — USB; Количество клавиш — 116;	2015	6
4	Мышь: Genius KM-122	Оптическая светодиодная, 1200 dpi;	2015	6
5	ИБП: Источник питания	APC Back-Up CS 500VA	2015	7
6	МФУ: лазерное Samsung SL-M2070	A4 2400x600 dpi 18 стр/мин (A4) , 14 сек.	2015	2

Продолжение таблицы 1

1	2	3	4	5
Дополнительные оборудование				
1	Телефон: Nokia 1100	Монохромный дисплей, 96 x 65 px, телефонная книга на 50 номеров.	2003	1
2	Сервер: Intel	Intel Xeon E 5410 x64, 4x2.33 ГГц, , 24 Гб, 2 ТБ	2015	1
3	MikroTik RB951G-2HnD	802.11n, частота 2.4 ГГц, 5 портов, 1000 Мбит/сек	2015	1
4	Внешний жесткий диск	500ГБ	2015	1
5	Маршрутизатор D-Link DIR-640L/A2A	Количество LAN портов - 5; базовая скорость передачи данных 1000 Мб/с	2015	1

Таблица 2 – Программное обеспечение

№	Наименование	Описание	Версия
АРМ 1-6			
1	Windows 7 Professional	Операционная система установленная на АРМ сотрудников.	6.1.7601.22616
2	Microsoft Office 2013	Офисный пакет для работы с документами	15.0.4771.1001 SP1
3	1С Предприятие 8.3	Ведение бухгалтерского и налогового учёта	8.3.4.437
4	КриптоПро CSP v.4.0 R2	Генерация электронной подписи, работа с сертификатами.	9842
5	Skype	Служит для обмена текстовыми , голосовыми сообщениями и видеозвонками.	7.34.66.103
6	ICQ	Служит для мгновенного обмена сообщениями.	10.0.12161
7	WinRAR	Предназначен для открытия, сжатия файлов и папок.	5.40
8	Adobe Acrobat	Предназначен для создания и просмотра электронных документов в формате PDF	11.0.00
9	ESET NOD32 Smart Security	Антивирусное программное обеспечение установленное на АРМ.	10.0.369.1

1.5. Выявление объектов защиты ООО “Диджитер”

Объект защиты информации – это информация или носитель информации, или информационный процесс, которую(ый) необходимо защищать в соответствии с целью защиты информации.

На основании предпроектного обследования ООО “Диджитер” составим перечень объектов, которые нуждаются в защите:

1. Помещение для работы с защищаемой информацией;
2. Сервер;
3. Автоматизированные рабочие места сотрудников;
4. Линии и средства связи;
5. Устройства ввода-вывода и отображения информации;
6. Системы дублирования и хранения информации;
7. Носители информации;
8. Информационная инфраструктура;
9. Персонал.

Подробный перечень объектов защиты представлен в (Приложение Д).

1.6. Разработка модели угроз и уязвимостей выявленных объектов защиты ООО “Диджитер”

Модель угроз и уязвимостей представляет собой описание существующих угроз информационной безопасности и уязвимостей, через которые реализуется данная угроза.

Перед тем, как выявить наиболее важные угрозы информационной безопасности, стоит выделить наиболее важные объекты, к которым относятся:

1. Персонал;
2. Сервер;
3. Автоматизированные рабочие места сотрудников, на которых обрабатывается защищаемая информация.

Так как утверждённой ФСТЭК модели угроз для внедрения режима коммерческой тайны нет, мы будем руководствоваться «Базовая модель угроз безопасности персональных данных при их обработки в информационных системах персональных данных» (утв. ФСТЭК РФ от 15 февраля 2008г)[1].

Таблица 3 – Модель угроз

Объект	Угроза	Уязвимость	Вероятность
1	2	3	4
Персонал	Угрозы связанные с нарушением свойства информации		
	Разглашение, копирование, хищение информации составляющей коммерческую тайну	Нарушение соглашения о неразглашении коммерческой тайны	Высокая вероятность
		Несанкционированное проникновение в помещение	
		Отсутствие режима коммерческой тайны	
	Уничтожение, модификация, блокировка носителей информации содержащих коммерческую тайну, АРМ сотрудников, серверного оборудования	Несанкционированное проникновение в помещение	Средняя вероятность
		Отсутствие мероприятий по повышению информационной грамотности	
		Отсутствие инструкции по работе с АРМ и серверным оборудованием обрабатывающим коммерческую тайну	
		Отсутствие пломбирования корпуса АРМ	

Продолжение таблицы 3

1	2	3	4
	Утечка, хищение носителей информации содержащих коммерческую тайну	Отсутствие учета носителей содержащих коммерческую тайну	Высокая вероятность
		Отсутствие пропускного режима	
		Отсутствие пломбирования корпуса АРМ	
Автоматизированные рабочие места сотрудников, на которых обрабатывается защищаемая информация	Угрозы несанкционированного доступа		
	Несанкционированный доступ к АРМ сотрудников	Отсутствие регламента доступа к АРМ	Высокая вероятность
		Отсутствие средств защиты от НСД	
		Отсутствие пломбирования корпуса АРМ	
		Отсутствие видеонаблюдения	
	Угрозы несанкционированного доступа по каналам связи		
	Анализ сетевого трафика с перехватом передаваемой по сети информации	Отсутствие СЗИ	Низкая вероятность
	Сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений	Отсутствие системы обнаружения вторжений	Маловероятно
	Выявление паролей	Отсутствие использования одноразовых паролей	Средняя вероятность
	Получение НСД путем подмены доверенного объекта	Отсутствие СЗИ от НСД	Низкая вероятность
	Отказ в обслуживании	Отсутствие VPN	Средняя вероятность

Продолжение таблицы 3

1	2	3	4
Сервер	Угрозы несанкционированного доступа		
	Проникновение нарушителя в помещение с сервером	Отсутствие видеонаблюдения	Средняя вероятность
		Отсутствие пропускного режима	
	Угрозы несанкционированного доступа по каналам связи		
	Несанкционированный доступ к базам данных хранящимся на сервере	Установка программного обеспечения, которое может создать условия для НСД	Средняя вероятность
		Отсутствие регламента эксплуатации средств антивирусной защиты	
	Анализ сетевого трафика	Отсутствие СЗИ	Низкая вероятность
	Сканирование сети	Отсутствие системы обнаружения вторжений	Маловероятно
	Подмена доверенного объекта сети и присвоение прав доступа	Отсутствие СЗИ от НСД	Низкая вероятность
	Отказ в обслуживании	Отсутствие VPN	Средняя вероятность

1.7. Расчет рисков важных объектов защиты ООО “Диджитер”

Одним из важных этапов в создании комплексной системы защиты информации является расчет рисков. Данный расчет рисков служит для выявления наиболее вероятных угроз, связанных с объектами информации, а также, уязвимостей, через которые данные угрозы могут быть реализованы.

Для расчета рисков важных объектов была использована «Методика определения актуальных угроз безопасности персональных данных при их обработки в информационных системах персональных данных» (утв. ФСТЭК РФ от 14 февраля 2008г)[5], так как утверждённой методики для коммерческой тайны нет.

Перед оценкой возможности реализации угрозы необходимо установить уровень исходной защищенности ИС. Для этого составим таблицу (Таблица 4).

Таблица 4 – Исходный уровень защищенности ИС

Технические и эксплуатационные характеристики информационной системы	Уровень защищенности ИС
По территориальному размещению: локальная ИС	Высокий
По наличию соединения с сетями общего пользования: имеющая одноточечный выход в сеть общего пользования	Средний
По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка	Средний
По разграничению доступа к информации: ИС, к которой имеют доступ определенные перечнем сотрудники организации	Средний
По наличию соединений с другими базами данных и другими ИС: в которой используется одна база данных, принадлежащая организации – владельцу данной ИС	Высокий
По объему данных, которые предоставляются сторонним пользователям системы без предварительной обработки: предоставляющая часть	Средний

На основании составленной таблицы можно сделать вывод, что исходный уровень защищенности информационной системы является «средним», так как 4 показателя из 6 имеют средний уровень защищенности. В связи с этим, числовой коэффициент Y_1 равен 5 ($Y_1 = 5$).

Далее необходимо определить вероятность реализации угрозы Y2. В зависимости от вероятности реализации угрозы (маловероятно, низкая вероятность, средняя вероятность и высокая вероятность), каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2, а именно: 0, 2, 5 и 10 соответственно.

Составим таблицу вероятности для актуальных угроз в соответствии с числовыми коэффициентам (Таблица 5).

Таблица 5 - Вероятность реализации угроз

Объект	Угроза	Уровень вероятности реализации угрозы	Вероятность реализации угрозы, Y2
1	2	3	4
Персонал	Угрозы связанные с нарушением свойства информации		
	Разглашение, копирование, хищение информации составляющей коммерческую тайну	Высокая вероятность	10
	Уничтожение, модификация, блокировка носителей информации содержащих коммерческую тайну, АРМ сотрудников, серверного оборудования	Средняя вероятность	5
	Утечка, хищение носителей информации содержащих коммерческую тайну	Высокая вероятность	10
Автоматизированные рабочие места сотрудников, на которых обрабатывается защищаемая информация	Угрозы несанкционированного доступа		
	Несанкционированный доступ к АРМ сотрудников	Высокая вероятность	10
	Угрозы несанкционированного доступа по каналам связи		
	Анализ сетевого трафика с перехватом передаваемой по сети информации	Маловероятно	0
	Сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений	Маловероятно	0
	Выявление паролей	Средняя вероятность	5
	Получение НСД путем подмены доверенного объекта	Низкая вероятность	2
	Отказ в обслуживании	Средняя вероятность	5

Продолжение таблицы 5

1	2	3	4
Сервер	Угрозы несанкционированного доступа		
	Проникновение нарушителя в помещение с сервером	Средняя вероятность	5
	Угрозы несанкционированного доступа по каналам связи		
	Несанкционированный доступ к базам данных хранящимся на сервере	Средняя вероятность	5
	Анализ сетевого трафика	Маловероятно	0
	Сканирование сети	Маловероятно	0
	Подмена доверенного объекта сети и присвоение прав доступа	Низкая вероятность	2
	Отказ в обслуживании	Средняя вероятность	5

Полученные значения Y_1 и Y_2, необходимы для расчёта коэффициента реализуемости угрозы Y. Данный коэффициент рассчитывается по формуле:

$$Y = {(Y_1 + Y_2)}/{20}$$

Рассчитаем коэффициент реализуемости угроз и внесём результаты в таблицу (Таблица 6).

Таблица 6 - Коэффициент реализуемости угроз

Объект	Угроза	Коэффициент реализации угрозы, Y	Возможность реализации угрозы
1	2	3	4
Персонал	Угрозы связанные с нарушением свойства информации		
	Разглашение, копирование, хищение информации составляющей коммерческую тайну	0,75	Высокая

Продолжение таблицы 6

1	2	3	4
	Уничтожение, модификация, блокировка носителей информации содержащих коммерческую тайну, АРМ сотрудников, серверного оборудования	0,5	Средняя
	Утечка, хищение носителей информации содержащих коммерческую тайну	0,75	Высокая
Автоматизированные рабочие места сотрудников, на которых обрабатывается защищаемая информация	Угрозы несанкционированного доступа		
	Несанкционированный доступ к АРМ сотрудников	0,75	Высокая
	Угрозы несанкционированного доступа по каналам связи		
	Анализ сетевого трафика с перехватом передаваемой по сети информации	0,25	Низкая
	Сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений	0,25	Низкая
	Выявление паролей	0,5	Средняя
	Получение НСД путем подмены доверенного объекта	0,35	Средняя
	Отказ в обслуживании	0,5	Средняя
Сервер	Угрозы несанкционированного доступа		
	Проникновение нарушителя в помещение с сервером	0,5	Средняя
	Угрозы несанкционированного доступа по каналам связи		
	Несанкционированный доступ к базам данных хранящимся на сервере	0,5	Средняя
	Анализ сетевого трафика	0,25	Низкая
	Сканирование сети	0,25	Низкая
	Подмена доверенного объекта сети и присвоение прав доступа	0,35	Средняя

Продолжение таблицы 6

1	2	3	4
	Отказ в обслуживании	0,5	Средняя

В данном пункте мы установили исходный уровень защищенности ИС предприятия ООО “Диджитер”, а так же рассчитали коэффициент реализуемости угроз выявленных в пункте 1.6. Возможность реализации угрозы позволяет выявить приоритетные направления для устранения установленных угроз.

1.8. Разработка технического задания для создания КСЗИ

На основании проведённого анализа были получены сведения, необходимые для разработки технического задания на создание комплексной системы защиты информации (Приложение Д).

Техническое задание разрабатывалось на основании ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы»[3] и включает в себя следующие разделы:

1. Общие сведения;
2. Основные назначения и цели создания системы;
3. Характеристика объектов защиты;
4. Требования к КСЗИ;
5. Состав и содержание работ по созданию системы;
6. Порядок контроля и приемки системы;
7. Требования к составу и содержанию работ по подготовке объекта защиты к вводу КСЗИ в действие;
8. Требования к документации.

ВЫВОД ПО ПЕРВОЙ ГЛАВЕ

В процессе проведения предпроектного обследования информационной системы ООО “Диджитер”, был разработан паспорт предприятия с точки зрения информационной безопасности, в котором представлены общие сведения об организации. Разработана модель деятельности ООО “Диджитер”. Выявлены объекты защиты информации, разработана модель угроз и рассчитаны риски для важных объектов защиты.

Руководствуясь разработанной нами моделью деятельности ООО “Диджитер” и результатами анализа ИС предприятия была выявлена информация ограниченного доступа – сведения, составляющие коммерческую тайну. В организации ООО “Диджитер” отсутствует режим коммерческой тайны. Руководством компании была поставлена задача о введении режима коммерческой тайны. Для этого в рамках ВКР был разработан комплекс организационно – распорядительных документов и сформулированы рекомендации по реализации, требуемых законодательством, мер по защите информации.

Для выявленных объектов защиты ООО “Диджитер”, руководствуясь методикой ФСТЭК была разработана модель угроз. Проведен расчет рисков для выявленных объектов защиты, согласно которому определен исходный уровень защищенности информационной системы – “средний”. Выявлено, что наивысшую степень реализации угроз имеют угрозы связанные с: разглашением, копированием, хищением информации составляющей коммерческую тайну; утечкой, хищением носителей информации содержащих коммерческую тайну; несанкционированным доступом к АРМ сотрудников.

Результатом первой главы является разработанное техническое задание на внедрение КСЗИ в ООО “Диджитер”, основой которого явились результаты описанных выше мероприятий.

2. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Обзор возможных методов устранения уязвимостей

Важным этапом работы по созданию комплексной системы защиты информации является определение и анализ имеющихся мер, методов и средств, направленных на устранение выявленных у объектов защиты угроз и уязвимостей. На данном этапе работы необходимо определить наиболее эффективные пути решения поставленных задач.

2.2. Угрозы связанные с нарушением свойства информации

2.2.1. Разглашение, копирование, хищение информации ограниченного доступа

Данный тип угрозы реализуется посредством акустического, оптического и материального каналов утечки информации. Уязвимости, приводящие к возможной реализации данной угрозы:

1. Нарушение соглашения о неразглашении коммерческой тайны;
2. Несанкционированное проникновение в помещение;
3. Отсутствие режима коммерческой тайны.

Установленные уязвимости возможно устранить благодаря разработке организационно-распорядительной документации, включающей в себя: положение о режиме коммерческой тайны, перечень сведений составляющих коммерческую тайну, приказы об их утверждении. Для наилучшей эффективности устранения данных уязвимостей, необходимо провести беседу с сотрудниками организации, работающими с информацией ограниченного доступа с целью доведения требований по работе с ней и ответственности за её разглашение.

2.2.2. Уничтожение, модификация, блокировка носителей информации, АРМ сотрудников, серверного оборудования

К данному типу угроз относятся следующие уязвимости:

1.Несанкционированное проникновение в помещение;

2.Отсутствие мероприятий по повышению информационной грамотности;

3.Отсутствие инструкции по работе с АРМ и серверным оборудованием обрабатывающим коммерческую тайну;

4.Отсутствие учета носителей содержащих коммерческую тайну;

5.Отсутствие пломбирования корпуса АРМ.

В качестве решения по устранению данных уязвимостей, необходимо выполнение ряда мероприятий. Во первых, необходимо установить средство контроля и управления доступом. Данное средство позволит организовать пропускной режим, благодаря которому ограничим доступ сотрудникам не имеющим доступ к защищаемой информации. Во вторых, необходимо через определённый промежуток времени проводить мероприятия по повышению информационной грамотности. Проводимые мероприятия позволят улучшить владение приемами поиска, сбора, обработки, анализа и синтеза необходимой информации. В третьих, необходима инструкция по работе с АРМ и серверным оборудованием. В рамках данной дипломной работы, разработка данной инструкции не требуется. В четвёртых, нанести на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя такой информации. Учет носителей позволит в любое время определить, у кого находиться тот или иной документ, содержащий информацию ограниченного доступа. В пятых, произвести опломбировку системных блоков АРМ сотрудников и сервера, а так же назначение ответственного за сохранность пломб. Данный способ позволит исключить физическое несанкционированное взаимодействие с носителями, содержащими коммерческую тайну.

2.3. Угрозы, связанные с НСД

В связи со стремительным развитием информационных технологий, большое количество организаций занимается обработкой информации ограниченного доступа в рамках своей информационной системы. В результате, в условиях высокой конкурентности, возрастает интерес сторонних компаний к информации ограниченного доступа своих конкурентов.

Несанкционированный доступ, служит одним из методов для получения сторонними организациями информации ограниченного доступа.

Несанкционированный доступ представляет собой противоправное действие, в результате которого злоумышленник получает доступ к защищаемой информации для сторонних лиц. На основании предпроектного обследования, в рамках данной ВКР были установлены следующие угрозы связанные с несанкционированным доступом:

1. Несанкционированный доступ к АРМ сотрудников;
2. Угрозы несанкционированного доступа по каналам связи.

2.3.1. Несанкционированный доступ к АРМ сотрудников

Угроза несанкционированного доступа к АРМ сотрудников может быть реализована посредством следующих уязвимостей:

1. Отсутствие пломбирования корпуса АРМ;
2. Отсутствие регламента доступа к АРМ;
3. Отсутствие видеонаблюдения;
4. Отсутствие средств защиты от НСД.

Способ устранения первой уязвимости представлен в пункте 2.3. В качестве решения второй проблемы можно разработать матрицу доступа, в которой будет содержаться список лиц, допущенных к АРМ на которых обрабатывается информация ограниченного доступа. В рамках данной ВКР, разработка матрицы доступа не требуется. Третью уязвимость можно устранить посредством внедрения на

объекте видеонаблюдения. Видеонаблюдение предназначено для контроля сотрудников, имеющих доступ к информации ограниченного доступа, а так же для выявления несанкционированного проникновения в помещение с конфиденциальной информацией. Для устранения четвёртой проблемы необходимо установить специальное программно-аппаратное средство защиты информации. Для этого необходимо сравнить сертифицированные СЗИ от НСД. Сравнение средств защиты представлено в таблице (Таблица 7).

Таблица 7 – Сравнение средств защиты от НСД

Критерии сравнения	Secret Net 7	Dallas Lock 8.0 – K	Страж NT 4.0	СЗИ Аура 1.2.4
Класс защищенности	По 3 классу защищенности	По 5 классу защищенности	По 3 классу защищенности	По 5 классу защищенности
Уровень контроля НДВ	По 2 уровню контроля	По 4 уровню контроля	По 2 уровню контроля	По 4 уровню контроля
Класс автоматизированных систем	До класса 1Б включительно	До класса 1Г включительно	До класса 1 Б включительно	До класса 1Г включительно
Совместимость с Windows 7 Professional	Да	Да	Да	Да
Наличие сертификата ФСТЭК (дата окончания)	07.09.2018	25.09.2018	20.04.2019	26.12.2017
Стоимость (руб.)	7425	7500	7500	4000
Стоимость технической поддержки в год (руб.)	1485	0	0	0

Таким образом, на основании данного анализа СЗИ от НСД было выбрано СЗИ "Аура 1.2.4". Данный выбор был связан с низкой стоимостью продукта и удовлетворением функциональными возможностями продукта. СЗИ "Аура 1.2.4" позволяет обеспечить идентификацию и аутентификацию автоматизированных рабочих мест сотрудников, а также разграничить доступ к устройствам и защищаемой информации, путем применения политики доступа. Скриншоты настроек представлены в приложении (Приложение И).

2.3.2. Угрозы несанкционированного доступа по каналам связи

У данного вида угрозы выявлены следующие уязвимости:

1. Анализ сетевого трафика;
2. Сканирование сети;
3. Выявление паролей;
4. Получение НСД путем подмены доверенного объекта;
5. Отказ в обслуживании.

Первые две проблемы связанными с анализом сетевого трафика и сканированием сети имеют малую вероятность реализации. Это связано с тем что в организации установлен антивирус включающий в себя защиту от данных уязвимостей. Таким образом, в рамках ВКР устранение данных уязвимостей не требуется. Проблему связанной с выявлением паролей можно устранить путем реализации одноразовых паролей. Данный способ является эффективным от подсматривания паролей другими сотрудниками. Четвёртая уязвимость может быть ликвидирована путём грамотной настройки управлением доступа. Уязвимость типа отказа в обслуживании могут сделать сеть организации недоступной. Таким образом во избежание этого необходимо настроить виртуальную внутреннюю сеть, позволяющей ликвидировать выявленную уязвимость.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

На основании выявленных угроз информационной безопасности в организации ООО “Диджитер”, в рамках ВКР, был разработан комплекс мероприятий, направленных на минимизацию вероятности реализации выявленных угроз:

1.От угрозы, связанной с разглашением, копированием, хищением информации ограниченного доступа: разработка организационно-распорядительной документации по защите информации, составляющей коммерческую тайну в организации; проведение беседы с сотрудниками организации для ознакомления под расписку с требованиями по работе с защищаемой информации.

2.От угрозы, связанной с уничтожением, модификацией, блокировкой, хищением носителей информации, АРМ сотрудников, серверного оборудования: установка средства контроля управлением доступа; проведение мероприятий по повышению информационной грамотности персонала; разработка инструкции по работе с АРМ и серверным оборудованием; нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна"; опломбировка системных блоков автоматизированных рабочих мест сотрудников и сервера, а так же назначение ответственного за их сохранность.

3.От угрозы, связанной с несанкционированным доступом к АРМ сотрудников: разработка матрицы доступа; внедрение в организации видеонаблюдения; установка СЗИ от НСД " Аура 1.2.4";

4.От угрозы, связанной с несанкционированным доступом по каналам связи: использование одноразовых паролей; настройка управления доступом; настройка виртуальной внутренней сети организации.

Результаты теоретического обоснования выбора средств защиты для реализации КСЗИ ООО “Диджитер”, легли в основу разработки проекта.

3. РАЗРАБОТКА ПРОЕКТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Описание объекта

Компания ООО «Диджитер» является поставщиком компьютеров и оргтехники для корпоративных клиентов и государственных структур. Таким образом, в организации циркулирует большое число потоков защищаемой информации. Потоки защищаемой информации (Таблица 8).

Таблица 8 – Потоки защищаемой информации

Входящие	Исходящие
Документооборот с клиентами	
Заявки от контрагентов; Информация о контрагентах; Информация о закупках; Информация от дистрибьютеров;	Отчёты о продажах; Договора поставки; Отчёты о задолженностях покупателей; Отчёты о прибылях/убытках;

3.2. Резюме проекта

Проект системы защиты информации разработан согласно утвержденному техническому заданию на создание КСЗИ ООО “Диджитер” (Приложение Д).

Для реализации поставленных задач, необходима разработка комплекса организационных, инженерно – технических и программно – аппаратных мер. Построенная матрица ответственности решает задачи по установлению ответственных лиц за выполнение определённого этапа работы. Результатом данного проекта будет являться созданная КСЗИ, включающая в себя внедрение программных и инженерно – технических средств, разработку необходимых документов, соответствующих требованиям нормативно-правовых актов и удовлетворяющих поставленным задачам.

3.3. Цели и задачи проекта

Целями создания КСЗИ ООО “Диджитер” являются:

1.Предотвращение разглашения, копирования, хищения, уничтожения, модификации, искажения информации ограниченного доступа;

2.Защита информации составляющей коммерческую тайну в соответствии с законодательством.

3.4. Объект и поставки

3.4.1. Организационно – распорядительная документация

В данном проекте предусмотрено создание необходимых документов в области информационной безопасности:

1.Перечень сведений, составляющих коммерческую тайну ООО “Диджитер” (Приложение Г);

2.Положение о коммерческой тайне (Приложение В);

3.Приказ об утверждении перечня сведений, составляющих коммерческую тайну (Приложение Е);

4.Приказ об утверждении положения о коммерческой тайне (Приложение Е).

3.4.2. Программно – аппаратные и инженерно – технические меры

При создании КСЗИ необходимо приобрести и внедрить следующие программно – аппаратные и инженерно – технические средства, представленные в таблице (Таблица 9).

Таблица 9 – Средства защиты информации

Наименование СЗИ	Предприятие – поставщик
СЗИ от НСД « Аура 1.2.4»	СПИИРАН
Комплект видеонаблюдения «ЭкоЛайн Dome-204» включающий в себя: 1. 4 внутренние AHD видеокамеры 2 Мп (Berger BVD-2036R-MF); 2. Видеорегистратор CTV-HD924A Lite; 3. Блок питания 3 А; 4. Кабель КВК-П-2 2х0,5; 5. Коннекторы BNC под винт; 6. Коннектор питания с клеммной колодкой "мама"; 7. Коннектор с клеммной колодкой "папа".	ООО «Системы видеонаблюдения»
Средство контроля управления доступом включающее в себя: 1. Считыватель Matrix-II; 2. Автономный контроллер Z-5R; 3. Кнопка выхода Optimus; 4. Электромагнитный замок Optimus EM-180.	

3.4.3. Обучение персонала

Необходимые тренинги сотрудников по обучению новым требованиям к защите информации с разъяснением важности введения организационно-распорядительных документов, предусмотренных проектом, а так же программно-аппаратных решений.

3.5. Риски реализации проекта

Важным условием для внедрения проекта по созданию комплексной системы защиты информации ООО “Диджитер”, является расчёт рисков. Для расчётов уровня рисков воспользуемся формулой:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th)$$

где величина Th означает уровень угрозы, рассчитывается по следующей формуле:

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}$$

где ER – критичность реализации угрозы (%);

P(V) – вероятность реализации угрозы (%).

Таблица 10 – Потоки защищаемой информации

Риски / пути их реализации	Критичность ER	Вероятность P(V)	Th	CTh
1	2	3	4	5
1. Риски изменений в стране, обществе				
1.1. Изменение политических и экономических характеристик и факторов:				0,054
– политические и экономические изменения	25	10	0,025	
– изменение законодательства	30	10	0,03	
1.2. Влияние непредвиденных ситуаций:				0,0007
– стихийные бедствия и природные катаклизмы	7	1	0,0007	
2. Риски окружения проекта в составе организации				
2.1. Изменение финансовой обстановки проекта:				0,636
– приостановка финансирования	90	20	0,018	
– отсутствие резервных средств для реагирования на события рисков (в т.ч. для ликвидации отставания от графика)	90	70	0,63	
2.2. Низкая организованность работ				0,116
– отставание от графика работ, срыв сроков	20	10	0,02	
– недостаток рабочей силы	40	20	0,08	
– преуменьшение стоимости работ и расход финансовых средств для других задач	40	5	0,02	

Продолжение таблицы 10

1	2	3	4	5
2.3. Риски персонала				0,151
– влияние индивидуальных личностных качеств сотрудников (переоценка собственных возможностей, преувеличение роли технологической стороны в ущерб менеджменту)	30	10	0,03	
– риск отсутствия персонала, которому сложно подобрать замену (болезнь, увольнение, отпуск и другие непредвиденные обстоятельства)	50	25	0,125	

В данном пункте были рассчитаны риски проекта по созданию КСЗИ ООО “Диджитер. Максимальный риск связан с изменением финансовой обстановки проекта. Минимальный риск связан с влиянием непредвиденных обстоятельств.

3.6. Структура разбиения работ

Структура разбиения работ представляет собой детальное описание каждого этапа по созданию КСЗИ в ООО “Диджитер”, и помогает оптимизировать план проекта и требования заказчика. Структура разбиения работ представлена на рисунке 1.

Структура декомпозиции работ по совершенствованию КСЗИ:

КСЗИ 1. Проектирование

КСЗИ 1.1. Определение главных показателей имеющихся бизнес-процессов с точки зрения информационной безопасности;

КСЗИ 1.2. Выявление и анализ проблем, слабых мест имеющихся бизнес-процессов;

КСЗИ 1.3. Разработка значений главных показателей новых бизнес – процессов;

КСЗИ 1.4. Анализ и отбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;

КСЗИ 1.5. Разработка и согласование структуры новых бизнес – процессов.

КСЗИ 2. Создание новой организационно – распорядительной документации

КСЗИ 2.1. Положение «О коммерческой тайне»;

КСЗИ 2.2. Перечень сведений, составляющих коммерческую тайну;

КСЗИ 2.3. Приказы об утверждении положения режима коммерческой тайны и перечня сведений, составляющих коммерческую тайну;

КСЗИ 2.4. Внесение изменений в должностные инструкции;

КСЗИ 2.5. Согласование и утверждение организационно – распорядительных документов.

КСЗИ 3. Подготовка реализации проекта созданию КСЗИ

КСЗИ 3.1. Определение ответственных лиц и исполнителей проекта;

КСЗИ 3.2. Приобретение программно – аппаратного средства защиты от НСД;

КСЗИ 3.3. Приобретение средства контроля и управления доступом;

КСЗИ 3.4. Приобретение средств видеонаблюдения;

КСЗИ 4. Внедрение

КСЗИ 4.1. Установка и настройка программно – аппаратного средства защиты от НСД;

КСЗИ 4.2. Установка средства контроля и управления доступом;

КСЗИ 4.3. Установка средств видеонаблюдения;

КСЗИ 4.4. Контроль защищенности;

КСЗИ 4.5. Обучение персонала.

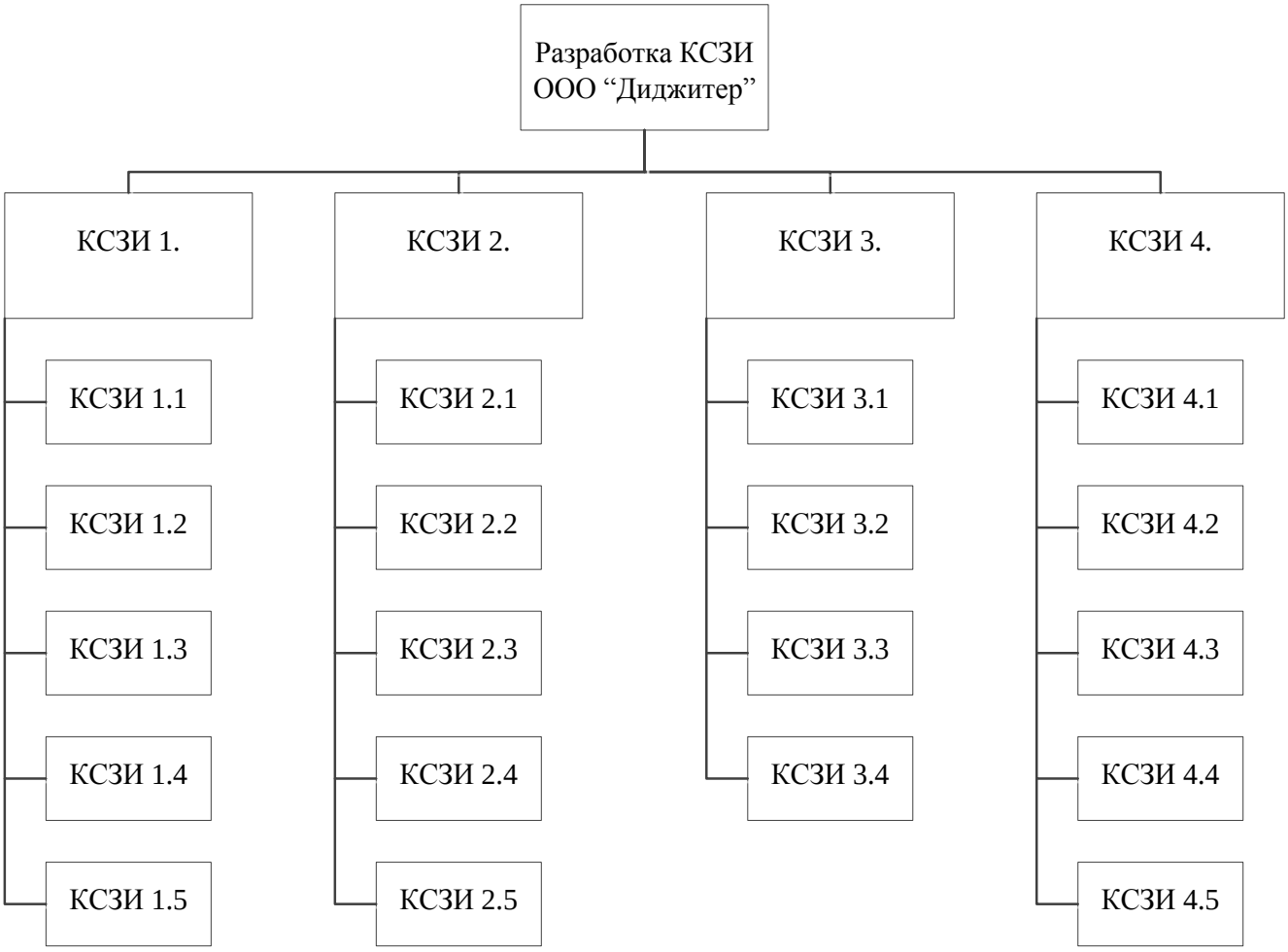

Рисунок 1 – Структурная схема разбиения работ

3.7. Структурная схема реализации проекта

Для точного и своевременного выполнения данного проекта, необходима совместная работа указанных сотрудников организации. В связи с этим, была разработана структурная схема организации проекта. Структурная схема организации представлена на рисунке 2.

Рисунок 2 – Структурная схема реализации проекта

3.8. Матрица ответственности

Все действия исполнителей по работам делятся на условные группы:

1. Управление (У);
2. Исполнение (И);
3. Контроль (К).

Матрица ответственности представлена в таблице (Таблица 11).

Таблица 11 – Матрица ответственности

Исполнитель/Работа	1	2	3	4
КСЗИ 1.	К			
КСЗИ 1.1.	К/У		И	
КСЗИ 1.2.	И		К	
КСЗИ 1.3.	И		К	
КСЗИ 1.4.	К/У		И	
КСЗИ 1.5.	И		К	
КСЗИ 2.	К	У/И		
КСЗИ 2.1.	К	У/И		
КСЗИ 2.2.	К	У/И		
КСЗИ 2.3.	К	У/И		
КСЗИ 2.4.	К	У/И		
КСЗИ 2.5	К	У/И		
КСЗИ 3.	К			
КСЗИ 3.1.	К		И	
КСЗИ 3.2.	К			
КСЗИ 3.3	К			
КСЗИ 3.4.	К			
КСЗИ 4.	К			И
КСЗИ 4.1.	И		К	
КСЗИ 4.2.	К			И
КСЗИ 4.3.	К			И
КСЗИ 4.4.	К	И		
КСЗИ 4.5.	И	К	К	

3.9. Диаграмма Ганта

Диаграмма Ганта представляет собой столбчатые гистограммы, которые используются для иллюстрации плана и графика работ.

Разработка диаграммы Ганта необходима для наглядного показа плана и графика работ данного проекта. Так же данная диаграмма является одним из методов планирования проектов и используется в приложениях по управлению проектами. Диаграмма Ганта для проекта по созданию КСЗИ ООО «Диджитер» представлена в (Приложение Ж).

Сетевой график – это динамическая модель производственного процесса, отражающая технологическую зависимость и последовательность выполнения комплекса работ, связывающая их свершение во времени с учётом затрат ресурсов и стоимости работ с выделением при этом узких (критических) мест.

Сетевой график представляет собой наглядное представление всех работ проекта, а так же их выполнение по временному интервалу. Сетевой график для проекта по созданию КСЗИ ООО «Диджитер» представлен в (Приложение З).

Готовая диаграмма Ганта и сетевой график позволяют четко определить точные сроки выполнения проекта, которые составляют 26 дней.

3.10. Оценка экономической эффективности проекта

В результате предпроектного обследования были выявлены уязвимости, которые подлежат устранению. Данные проблемы возможно устранить с помощью создания комплексной системы защиты информации. Для этого необходимо произвести расчёт экономической эффективности проекта, который ответит на вопрос о целесообразности реализации мер по созданию комплексной системы защиты информации. Стоимость программных и технических средств представлена в таблице 12. Стоимость услуг по реализации проекта представлена в таблице 13. Поток денежных платежей представлен в таблице 14.

Таблица 12 – Стоимость обеспечения

№ п/п	Наименование	Количество	Цена за шт. (руб.)	Сумма (руб.)
1	СЗИ НСД «Аура 1.2.4»	6	4000	24000
2	комплект видеонаблюдения «ЭкоЛайн Dome-204»	1	13880	13880
3	Считыватель карт Matrix-II	1	1585	1585
4	Карта Optimus EM-marine	10	23	230
5	Кнопка выхода Optimus	1	99	99
6	Автономный контроллер Z – 5R	1	580	580
7	Электромагнитный замок Optimus EM – 180	1	1700	1700
Итог				42074

Таблица 13 – Стоимость услуг по обеспечению проекта

№ п/п	Наименование	Стоимость (руб.)
1	Разработка и описание бизнес-процессов компании с точки зрения ИБ	9600
2	Разработка организационно-распорядительной документации	4600
3	Установка и настройка средства защиты от НСД «Аура 1.2.4»	8000
4	Установка и настройка комплекта видеонаблюдения «ЭкоЛайн Dome-204»	7000
5	Установка средства контроля управления доступом	5000
6	Обучение пользователей	2400
Итог		36600

Стоимость внедрения КСЗИ в ООО “Диджитер” составляет 78674 рублей.

Таблица 14 – Поток денежных платежей по проекту

Периоды	0	1	2	3
Первоначальные инвестиции (руб.)	-78674			
Выгоды (размеры риска) (руб.)		3000000	3000000	3000000
Стоимость годовой поддержки (руб.)		-5000	-5000	-5000
Затраты на администрирование и инфраструктуру (руб.)		-10000	-10000	-10000
Итого	-78674	2985000	2985000	2985000

Денежные вложения в реализацию проекта комплексной системы защиты информации составляют 78605 рублей. Ежегодно для поддержания системы необходимо выделять по 15000 рублей, на протяжении трех лет.

Для наглядного показа отличия вложений средств в проект от дохода хранения денег в банке воспользуемся методом Net Present Value (NPV). Рассчитаем NPV по формуле:

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+r)^t} - \sum_{t=0}^{n} \frac{I_t}{(1+r)^t}$$

где CF – денежный поток;

I — сумма инвестиционных вложений в проект в t-ом периоде;

r — ставка дисконтирования;

n — количество периодов.

Значение финансовых поступлений будем считать равным размеру ставки Центробанка России. Ставка центрального банка составляет 9,25 %

$$NPV = -78674 + 2985000/1{,}0925 + 2985000/(1{,}0925)^2 + 2985000/(1{,}0925)^3 =$$
$$= -78674 + 2732265 + 2500929 + 2289180 = 7443700$$

Из произведенного расчета видно, что значение NPV больше 0. Таким образом, в данной организации будет целесообразным проект внедрения КСЗИ. На основании вышесказанного можно сделать вывод, что создание КСЗИ в данной организации будет эффективным, так как величина потерь при отсутствии реализованных мер будет превышать затраты на ее реализацию и обслуживание.

ВЫВОД ПО ТРЕТЕЙ ГЛАВЕ

Итогом выполненных работ служит проект по созданию комплексной системы защиты информации в организации ООО “Диджитер”. В рамках разработки проекта КСЗИ были выявлены потоки защищаемой информации. Составлено резюме проекта. Целью создания КСЗИ является: предотвращение разглашения, копирования, хищения, уничтожения, модификации, искажения информации ограниченного доступа; защита информации составляющей коммерческую тайну в соответствии с законодательством. Были определены необходимые организационно – распорядительные документы, программно – аппаратные и инженерно – технические меры. Рассчитаны риски реализации проекта. Выполняемые работы были разделены и упорядоченно структурированы. Представлены структурные схемы разбиения работ и реализации проекта. Для каждого вида работ был назначен ответственный, в связи с этим была разработана матрица ответственности. Разработаны графики которые наглядно показывают сроки и объемы выполнения работ.

Результатом выполнения проекта, является исполнение разработанных мер по комплексной защите информации.

По результатам расчета стоимости создания КСЗИ в ООО “Диджитер”, и ее обслуживания была произведена оценка эффективности. По данным оценки суммарные затраты на реализацию проекта составляют 78674 рублей, проект займёт 26 дней. С точки зрения экономической целесообразности проект признан эффективным, о чем свидетельствуют результаты расчета по методу Net Present Value. Реализация данного проекта позволит сэкономить организации, ликвидировать угрозы и тем самым предприятие получит дополнительную выгоду.

4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1. Введение

В связи с тем фактом, что работа с информационной системой производится с использованием средств вычислительной техники, необходимо обеспечить соответствие рабочих мест сотрудников ООО “Диджитер” действующим нормам стандартов по безопасности жизнедеятельности.

Целью проекта является создание КСЗИ в ООО “Диджитер”. Организация ООО “Диджитер” представляет собой информационную инфраструктуру включающую в себя: 1 сервер и 6 рабочих станций.

4.2. Рекомендации по организации рабочего места пользователя

4.2.1. Требования к помещениям для размещения рабочего места

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное помещениев котором будут располагаться рабочие места, оборудование ЭВМ с ВДТ.

По требованиям СанПиН 2.2.2/2.4.1340-03[8] помещения для эксплуатации ПЭВМ должны отвечать следующим требованиям:

1.Помещения для эксплуатации ПЭВМ должны иметь естественное и искусственное освещение;

2.Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации;

3.Не допускается размещение мест пользователей ПЭВМ во всех образовательных и культурно-развлекательных учреждениях для детей и подростков в цокольных и подвальных помещениях;

4.Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные), должна составлять не менее 4,5 $м^2$;

5.Для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка - 0,7 - 0,8; для стен - 0,5 - 0,6; для пола - 0,3 - 0,5;

6.Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации;

7.Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

4.2.2. Требования к уровням шума на рабочих местах

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03[8] предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16[9] для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах. Источниками шума в данной организации являются рабочие станции и сервер. На основании СанПиН 2.2.4.3359-16[9], нормативным эквивалентным уровнем звука на рабочих местах является 80 дБА. В соответствии с нормами, ограничивающими предельно допустимое звуковое давление для рабочих мест, оснащенных ПЭВМ: шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений ПЭВМ.

4.2.3. Требования к освещению на рабочих местах

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное освещение, не вызывающее раннего переутомления.

Согласно СанПиН 2.2.2/2.4.1340-03[8], есть следующие требования к освещению на рабочих местах:

1.Рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева;

2.Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами, следует применять системы комбинированного освещения;

3.Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 - 500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк;

4.Для освещения помещений с ПЭВМ следует применять светильники с зеркальными параболическими решетками, укомплектованными электронными пуско-регулирующими аппаратами (ЭПРА) ;

5.Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении видеодисплейных терминалов. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору;

6.Коэффициент пульсации не должен превышать 5%;

7.Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

4.2.4. Общие требования к организации рабочих мест пользователей

Рабочее место оператора ЭВМ проектируется согласно СанПиН 2.2.2/2.4.1340-03[8] «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

1.При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м;

2.Рабочие места с ПЭВМ в помещениях с источниками вредных производственных факторов должны размещаться в изолированных кабинах с организованным воздухообменом;

3.Рабочие места с ПЭВМ при выполнении творческой работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5 - 2,0 м;

4.Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600 - 700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов;

5.Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы;

6.При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5 - 0,7;

7.Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ;

8.Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию;

9.Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений;

10. Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680 - 800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм;

11. Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, равной 725 мм;

12. Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной - не менее 500 мм, глубиной на уровне колен - не менее 450 мм и на уровне вытянутых ног - не менее 650 мм;

13. Конструкция рабочего стула должна обеспечивать:

13.1.Ширину и глубину поверхности сиденья не менее 400 мм;

13.2.Поверхность сиденья с закругленным передним краем;

13.3.Регулировку высоты поверхности сиденья в пределах 400 - 550 мм и углам наклона вперед до 15 град, и назад до 5 град.;

13.4.Высоту опорной поверхности спинки 300 +-20 мм, ширину - не менее 380 мм и радиус кривизны горизонтальной плоскости - 400 мм;

13.5. Угол наклона спинки в вертикальной плоскости в пределах +-30 градусов;

13.6. Регулировку расстояния спинки от переднего края сиденья в пределах 260 - 400 мм;

13.7. Стационарные или съемные подлокотники длиной не менее 250 мм и шириной - 50 - 70 мм;

13.8. Регулировку подлокотников по высоте над сиденьем в пределах 230 +-30 мм и внутреннего расстояния между подлокотниками в пределах 350 - 500 мм;

14. Рабочее место пользователя ПЭВМ следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм;

15. Клавиатуру следует располагать на поверхности стола на расстоянии 100 - 300 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

4.2.5. Требования к электробезопасности

По степени опасности поражения электрическим током согласно Правилам Устройства Электроустановок (ПУЭ) рабочее помещение относится к классу помещений с повышенной опасностью, так как имеется возможность одновременного прикосновения человека к имеющим соединения с землей металлоконструкциям здания с одной стороны и металлическим корпусам электрооборудования с другой.

Если физический доступ к токоведущим частям оборудования затруднен, то основной причиной возникновения данного опасного фактора может являться прикосновение к металлическим нетоковедущим частям (например, корпусу ПЭВМ), которые могут оказаться под напряжением в результате повреждения

изоляции. В соответствии с правилами электробезопасности, должен осуществляться постоянный контроль состояния электропроводки, предохранительных щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

Для предотвращения образования и защиты от статического электричества в помещениях с ПЭВМ необходимо использовать аэроионизаторы и увлажнители воздуха. В отделке помещений следует отдавать предпочтение антистатическим материалам. Полы должны иметь антистатическое покрытие.

Согласно документу «Правила устройства электроустановок (ПУЭ) электробезопасность работающих обеспечивается конструкцией электроустановок; техническими способностями и средствами защиты, организационными средствами защиты. Предусмотрены следующие технические способы и средства защиты от поражения электрическим током:

1. Обеспечение недоступности токоведущих частей, находящихся под напряжением для случайного прикосновения;
2. Устранение опасности поражения при появлении напряжения на нетоковедущих частях электрооборудования посредством заземления (зануления).

4.2.6. Рекомендации по организации режима труда и отдыха пользователя

Режимы труда и отдыха при работе с ПЭВМ и ВДТ должны организовываться в зависимости от вида и категории трудовой деятельности согласно СанПиН 2.2.2/2.4.1340-03[8].

По виду трудовой деятельности работу оператора можно отнести к группе «А» – работа по считыванию информации с экрана ВДТ или ПЭВМ с предварительным запросом.

Для видов трудовой деятельности устанавливается три категории тяжести и напряженности работы с ВДТ и ПЭВМ.

Для группы А категории определяются по суммарному числу считываемых знаков за рабочую смену, но не более 60 000 знаков за смену:

1. Категория – до 20 000 знаков;

2. Категория – до 40 000 знаков;

3. Категория – до 60 000 знаков.

Продолжительность обеденного перерыва определяется действующим законодательством о труде и правилами внутреннего распорядка предприятия.

Для обеспечения оптимальной работоспособности и сохранения здоровья профессиональных пользователей, на протяжении рабочей смены должны устанавливаться регламентированные перерывы. Время регламентированных перерывов в течении рабочей смены следует устанавливать в зависимости от ее продолжительности, вида и категории трудовой деятельности. Продолжительность непрерывной работы без регламентированного перерыва не должна превышать двух часов. При восьмичасовой рабочей смене и работе на ВДТ и ПЭВМ регламентированные перерывы следует устанавливать:

1. Для 1 категории работ через 2 ч. от начала рабочей смены и через 2 ч. после обеденного перерыва продолжительностью 15 мин. каждый;

2. Для 2 категории работ через 2 ч. от начала рабочей смены и через 1,5–2 ч. после обеденного перерыва продолжительностью 15 мин. каждый или продолжительностью 10 мин. через каждый час работы;

3. Для 3 категории работ через 2 ч. от начала рабочей смены и через 1,5−2,0 ч. после обеденного перерыва продолжительностью 20 мин. каждый или продолжительностью 15 мин. через каждый час работы.

Во время регламентированных перерывов с целью снижения нервно эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления целесообразно выполнять комплексы упражнений для глаз, для улучшения мозгового кровообращения, для снятия утомления с плечевого пояса и рук, а также общего воздействия.

В случаях возникновения у пользователя зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических, эргономических требований, режимов труда и отдыха следует

применять индивидуальный подход в ограничении времени работ с ВДТ и ПЭВМ. Коррекцию длительности перерывов для отдыха или проводить смену деятельности на другую, не связанную с использованием ВДТ и ПЭВМ.

Организационные мероприятия, устраняющие причины возникновения пожаров: обучение рабочих и служащих противопожарным правилам, проведение лекций, инструкций и т.п. Технические мероприятия: соблюдение противопожарных правил и норм при устройстве оборудования отопления, вентиляции и т.д.

4.3. Пожарная безопасность

Постановление Правительства РФ от 25.04.2012 N 390 (ред. от 21.03.2017) "О противопожарном режиме"[7] устанавливают следующие правила:

1.В отношении каждого объекта (за исключением индивидуальных жилых домов) руководителем (иным уполномоченным должностным лицом) организации (индивидуальным предпринимателем), в пользовании которой на праве собственности или на ином законном основании находятся объекты (далее - руководитель организации), утверждается инструкция о мерах пожарной безопасности в соответствии с требованиями;

2.Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности;

3.Обучение лиц мерам пожарной безопасности осуществляется путем проведения противопожарного инструктажа и прохождения пожарно-технического минимума;

4.Порядок и сроки проведения противопожарного инструктажа и прохождения пожарно-технического минимума определяются руководителем организации. Обучение мерам пожарной безопасности осуществляется в соответствии с нормативными документами по пожарной безопасности;

5.Руководитель организации назначает лицо, ответственное за пожарную безопасность, которое обеспечивает соблюдение требований пожарной безопасности на объекте;

6.В складских, производственных, административных и общественных помещениях, местах открытого хранения веществ и материалов, а также размещения технологических установок руководитель организации обеспечивает наличие табличек с номером телефона для вызова пожарной охраны;

7.На объекте с массовым пребыванием людей (кроме жилых домов), а также на объекте с рабочими местами на этаже для 10 и более человек руководитель организации обеспечивает наличие планов эвакуации людей при пожаре;

8.На объекте с массовым пребыванием людей руководитель организации обеспечивает наличие инструкции о действиях персонала по эвакуации людей при пожаре, а также проведение не реже 1 раза в полугодие практических тренировок лиц, осуществляющих свою деятельность на объекте;

9. Хранение огнетушителя осуществляется в соответствии с требованиями инструкции по его эксплуатации;

10. Запрещается на территориях, прилегающих к объектам, в том числе к жилым домам, а также к объектам садоводческих, огороднических и дачных некоммерческих объединений граждан, оставлять емкости с легковоспламеняющимися и горючими жидкостями, горючими газами;

11. Руководитель организации обеспечивает наличие на дверях помещений производственного и складского назначения и наружных установках обозначение их категорий по взрывопожарной и пожарной опасности;

12. Руководитель организации обеспечивает устранение повреждений толстослойных напыляемых составов, огнезащитных обмазок, штукатурки, облицовки плитными, листовыми и другими огнезащитными материалами, в том числе на каркасе, комбинации этих материалов, в том числе с тонкослойными вспучивающимися покрытиями строительных конструкций, горючих отделочных и теплоизоляционных материалов, воздуховодов, металлических опор оборудования и эстакад, а также осуществляет проверку состояния огнезащитной обработки (пропитки) в соответствии с инструкцией завода-изготовителя с составлением протокола проверки состояния огнезащитной обработки (пропитки). Проверка состоя-

ния огнезащитной обработки (пропитки) при отсутствии в инструкции сроков периодичности проводится не реже 1 раза в год;

13. Руководитель организации организует проведение работ по заделке негорючими материалами, обеспечивающими требуемый предел огнестойкости и дымогазонепроницаемость, образовавшихся отверстий и зазоров в местах пересечения противопожарных преград различными инженерными (в том числе электрическими проводами, кабелями) и технологическими коммуникациями;

14. На объектах запрещается:

14.1. Хранить и применять на чердаках, в подвалах и цокольных этажах легковоспламеняющиеся и горючие жидкости, порох, взрывчатые вещества, пиротехнические изделия, баллоны с горючими газами, товары в аэрозольной упаковке, целлулоид и другие пожаровзрывоопасные вещества и материалы, кроме случаев, предусмотренных иными нормативными документами по пожарной безопасности;

14.2. Использовать чердаки, технические этажи, вентиляционные камеры и другие технические помещения для организации производственных участков, мастерских, а также для хранения продукции, оборудования, мебели и других предметов;

14.3. Размещать в лифтовых холлах кладовые, киоски, ларьки и другие подобные помещения;

14.4. Устраивать в подвалах и цокольных этажах мастерские, а также размещать иные хозяйственные помещения, размещение которых не допускается нормативными документами по пожарной безопасности, если нет самостоятельного выхода или выход из них не изолирован противопожарными преградами от общих лестничных клеток;

14.5. Снимать предусмотренные проектной документацией двери эвакуационных выходов из поэтажных коридоров, холлов, фойе, тамбуров и лестничных клеток, другие двери, препятствующие распространению опасных факторов пожара на путях эвакуации;

14.6.Производить изменение объемно-планировочных решений и размещение инженерных коммуникаций и оборудования, в результате которых ограничивается доступ к огнетушителям, пожарным кранам и другим системам обеспечения пожарной безопасности или уменьшается зона действия автоматических систем противопожарной защиты (автоматической пожарной сигнализации, стационарной автоматической установки пожаротушения, системы дымоудаления, системы оповещения и управления эвакуацией);

14.7.Проводить уборку помещений и стирку одежды с применением бензина, керосина и других легковоспламеняющихся и горючих жидкостей, а также производить отогревание замерзших труб паяльными лампами и другими способами с применением открытого огня;

14.8.Устраивать в лестничных клетках и поэтажных коридорах кладовые и другие подсобные помещения, а также хранить под лестничными маршами и на лестничных площадках вещи, мебель и другие горючие материалы;

14.9.Устраивать в производственных и складских помещениях зданий (кроме зданий V степени огнестойкости) антресоли, конторки и другие встроенные помещения из горючих материалов и листового металла;

14.10.Устанавливать в лестничных клетках внешние блоки кондиционеров;

14.11.Загромождать и закрывать проходы к местам крепления спасательных устройств;

15. Приямки у оконных проемов подвальных и цокольных этажей зданий (сооружений) должны быть очищены от мусора и посторонних предметов;

16. Руководитель организации обеспечивает сбор использованных обтирочных материалов в контейнеры из негорючего материала с закрывающейся крышкой и удаление по окончании рабочей смены содержимого указанных контейнеров.

17. В зданиях с витражами высотой более одного этажа не допускается нарушение конструкций дымонепроницаемых негорючих диафрагм, установленных в витражах на уровне каждого этажа.

18. Руководителем организации, на объекте которой возник пожар, обеспечивается доступ пожарным подразделениям в закрытые помещения для целей локализации и тушения пожара.

19. Руководитель организации при расстановке в помещениях технологического, выставочного и другого оборудования обеспечивает наличие проходов к путям эвакуации и эвакуационным выходам.

20. Запрещается оставлять по окончании рабочего времени не обесточенными электроустановки и бытовые электроприборы в помещениях, в которых отсутствует дежурный персонал, за исключением дежурного освещения, систем противопожарной защиты, а также других электроустановок и электротехнических приборов, если это обусловлено их функциональным назначением и (или) предусмотрено требованиями инструкции по эксплуатации.

21. Запрещается:

21.1.Эксплуатировать электропровода и кабели с видимыми нарушениями изоляции;

21.2.Пользоваться розетками, рубильниками, другими электроустановочными изделиями с повреждениями;

21.3.Обертывать электролампы и светильники бумагой, тканью и другими горючими материалами, а также эксплуатировать светильники со снятыми колпаками (рассеивателями), предусмотренными конструкцией светильника;

21.4.Пользоваться электроутюгами, электроплитками, электрочайниками и другими электронагревательными приборами, не имеющими устройств тепловой защиты, а также при отсутствии или неисправности терморегуляторов, предусмотренных конструкцией;

21.5.Применять нестандартные (самодельные) электронагревательные приборы;

22. Руководитель организации обеспечивает исправное состояние знаков пожарной безопасности, в том числе обозначающих пути эвакуации и эвакуационные выходы;

23. Запрещается пользоваться неисправными газовыми приборами, а также устанавливать (размещать) мебель и другие горючие предметы и материалы на расстоянии менее 0,2 метра от бытовых газовых приборов по горизонтали и менее 0,7 метра - по вертикали (при нависании указанных предметов и материалов над бытовыми газовыми приборами);

24. В соответствии с инструкцией завода-изготовителя руководитель организации обеспечивает проверку огнезадерживающих устройств (заслонок, шиберов, клапанов и др.) в воздуховодах, устройств блокировки вентиляционных систем с автоматическими установками пожарной сигнализации или пожаротушения, автоматических устройств отключения вентиляции при пожаре;

25. При эксплуатации систем вентиляции и кондиционирования воздуха запрещается:

25.1.Оставлять двери вентиляционных камер открытыми;

25.2.Закрывать вытяжные каналы, отверстия и решетки;

25.3.Подключать к воздуховодам газовые отопительные приборы

25.4.Выжигать скопившиеся в воздуховодах жировые отложения, пыль и другие горючие вещества;

26. Руководитель организации определяет порядок и сроки проведения работ по очистке вентиляционных камер, циклонов, фильтров и воздуховодов от горючих отходов с составлением соответствующего акта, при этом такие работы проводятся не реже 1 раза в год;

27. Руководитель организации обеспечивает укомплектованность пожарных кранов внутреннего противопожарного водопровода пожарными рукавами, ручными пожарными стволами и вентилями, организует перекатку пожарных рукавов (не реже 1 раза в год);

28. Руководитель организации обеспечивает исправное состояние систем и средств противопожарной защиты объекта (автоматических (автономных) установок пожаротушения, автоматических установок пожарной сигнализации , установок систем противодымной защиты, системы оповещения людей о пожаре, средств пожарной сигнализации, противопожарных дверей, противопожарных и

дымовых клапанов, защитных устройств в противопожарных преградах) и организует не реже 1 раза в квартал проведение проверки работоспособности указанных систем и средств противопожарной защиты объекта с оформлением соответствующего акта проверки.

29. Выбор типа и расчет необходимого количества огнетушителей следует производить в зависимости от огнетушащей способности, предельной площади, класса пожара горючих веществ и материалов защищаемом помещении или на объекте согласно СП 9.13130.2009[10].

Для ООО “Диджитер” актуальны следующие классы пожаров:

Класс А - пожары твердых веществ, основном органического происхождения, горение которых сопровождается тлением (древесина, текстиль, бумага).

Класс Е - пожары, связанные с горением электроустановок.

Для данных классов пожаров, исходя из рекомендация СП 9.13130.2009[10], следует применять порошковые огнетушители.

Огнетушители следует располагать на защищаемом объекте в соответствии с требованиями ГОСТ 12.4.009[4] таким образом, чтобы они были защищены от воздействия прямых солнечных лучей, тепловых потоков, механических воздействий и других неблагоприятных факторов (вибрация, агрессивная среда, повышенная влажность и т.д.). Они должны быть хорошо видны и легкодоступны в случае пожара. Предпочтительно размещать огнетушители вблизи мест наиболее вероятного возникновения пожара, вдоль путей прохода, а также около выхода из помещения. Огнетушители не должны препятствовать эвакуации людей во время пожара.

Огнетушители, введенные в эксплуатацию, должны подвергаться техническому обслуживанию, которое обеспечивает поддержание огнетушителей в постоянной готовности к использованию и надежную работу всех узлов огнетушителя в течение всего срока эксплуатации. Техническое обслуживание включает в себя периодические проверки, осмотры, ремонт, испытания и перезарядку огнетушителей.

ВЫВОД ПО ЧЕТВЕРТОЙ ГЛАВЕ

В данной главе были установлены требования и рекомендации к работе в организации. Были установлены требования к помещениям, в которых располагаются рабочие места. Данные помещения должны соответствовать требованиям СанПиН 2.2.2/2.4.1340-03[8]. Установлены требования к уровням шума на рабочих местах. Для этого была представлена таблица из СанПиНа 2.2.4.3359-16[9].

Выявлены основные требования к освещению на рабочих местах. Так же указаны общие требования к организации рабочих мест пользователей. Указаны требования к электробезапасности. Даны рекомендации по организации режима труда и отдыха пользователя, который работает с рабочей станцией.

На основании постановления правительства РФ от 25.04.2012 N 390 (ред. от 21.03.2017) "О противопожарном режиме"[7], были установлены требования к пожарной безопасности предприятия.

ЗАКЛЮЧЕНИЕ

В ходе выполнения ВКР был произведен анализ существующих мер по защите информации на предприятии ООО “Диджитер”. В результате этого были выявлены угрозы, которые требуют устранения. На основании этого был разработан проект КСЗИ ООО “Диджитер”. Данный проект, включает в себя мероприятия, благодаря которым возможно устранение угроз и уязвимостей в данной организации.

В процессе выполнения данной ВКР, было произведено предпроектное обследование, которое включает в себя:

1.Разработку паспорта предприятия с точки зрения информационной безопасности – выявлена общая структура организации, информационная среда предприятия, программно - аппаратные средства, виды деятельности, виды защищаемой информации, конкуренты, описана строительная инфраструктура здания, определена контролируемая зона защищаемого помещения и объектов защиты информации, на которых обрабатывается информация ограниченного доступа.

2.Разработку модели деятельности предприятия – выявлены базовые бизнес – процессы, определены информационные потоки и информация ограниченного доступа циркулирующая на предприятии.

3.Описание информационной системы предприятия – выявлены характеристики АРМ, сервера и программное обеспечение установленное на них, а так же периферийные устройства.

4.Выявление объектов защиты – были выявлены объекты защиты, в которых обрабатывается и циркулирует информация ограниченного доступа.

5.Разработку модели угроз и уязвимостей для важных объектов защиты и расчет рисков для них – установлены угрозы и уязвимости для важных объектов защиты и вероятность их реализации, а так же рассчитаны риски по выбранной методике ФСТЭК.

В результате установленной информации было разработано техническое задание на создание КСЗИ ООО “Диджитер”.

Были выявлены угрозы и уязвимости, с помощью которых может быть разглашена информация ограниченного доступа. В связи с этим, разработаны мероприятия затрудняющие или полностью исключающие реализацию угроз через уязвимости.

Была рассчитана экономическая целесообразность внедрения данного проекта, по итогу которой было установлено, что создание КСЗИ в ООО “Диджитер” экономически целесообразно.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативно-правовые документы

1. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15.02.2008) // КонсультантПлюс [Электронный ресурс]. – http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=99662&fld=134&dst=1000000001,0&rnd=0.8630855495122507#0

2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 27.12.2006 N 373-ст) // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?base=EXP&n=418509&req=doc#0

3. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. – М.: Стандартинформ, 2009. – 12 с.

4. ГОСТ 12.4.009-83. Межгосударственный стандарт. Система стандартов безопасности труда. Пожарная техника для защиты объектов. Основные виды. Размещение и обслуживание // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ESU&n=9134#0

5. «Методика определения актуальных угроз безопасности персональных данных при их обработки в информационных системах персональных данных» (утв. ФСТЭК РФ от 14 февраля 2008г) // КонсультантПлюс [Электронный ресурс]. –

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=77814&fld=134&dst=1000000001,0&rnd=0.7356947169060526#0

6. «О коммерческой тайне»: федеральный закон Российской Федерации от 29 июля 2004 №98-ФЗ: (в ред. от 12.03.14) // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=160225&fld=134&dst=1000000001,0&rnd=0.7837671849669785#0

7. Постановление Правительства РФ от 25.04.2012 N 390 (ред. от 21.03.2017) «О противопожарном режиме» (вместе с «Правилами противопожарного режима в Российской Федерации») // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=214359&fld=134&dst=1000000001,0&rnd=0.02918617286551339 3#0

8. СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы — М.: Изд-во стандартов, 2003. — 32 с.

9. СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические требования к физическим факторам на рабочих местах // Информационная система МЕГАНОРМ [Электронный ресурс]. – Режим доступа: http://meganorm.ru/Index2/1/4293753/4293753139.htm

10. СП 9.13130.2009. Свод правил. Техника пожарная. Огнетушители. Требования к эксплуатации" (утв. Приказом МЧС РФ от 25.03.2009 N 179) // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=91587&fld=134&dst=100001,0&rnd=0.26064711048474565#0

11. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017) // КонсультантПлюс [Электронный ресурс]. – http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=201079&fld=134&dst=1000000001,0&rnd=0.7021406734602476#0

Основная литература

12. Безопасность жизнедеятельности. /Под ред. Н.А. Белова - М.: Знание, 2000 – 364 с.

13. Борьба с шумом на производстве: Справочник / Е.Я. Юдин, Л.А. Борисов; Под общ. ред. Е.Я. Юдина – М.: Машиностроение, 1985. – 400 с.

14. Дубовцев, В.А. Безопасность жизнедеятельности. / Учеб. пособие для дипломников. - Киров: изд. КирПИ, 1992. – 213 с.

15. Репин В., Елиферов В. Процессный подход к управлению. Моделирование бизнес-процессов. - М: РИА Стандарты и качество, 2006. - 405 с.

ПРИЛОЖЕНИЕ А

ООО «Диджитер»
Общество с ограниченной ответственностью «Диджитер»
Юридический адрес: 454126, г. Челябинск, ул. Татьяничевой, 9, пом. 51
Фактический адрес: 454126, г. Челябинск, ул. Татьяничевой, 9
Тел.: 8(351)7512749, e-mail: info@digiter74.ru
ИНН 7453281507, КПП 745301001, ОГРН 1157453003960, ОКПО 34555531
БИК 047501779, р/с 40702810590000020773 в ПАО "Челябинвестбанк"
кор/счет 30101810400000000779
Компьютеры / Комплектующие / Оргтехника / Программное обеспечение

УТВЕРЖДАЮ
Генеральный Директор
ООО «Диджитер»
_____С.А. Сабельников
Дата_____

ПАСПОРТ
ПРЕДПРИЯТИЯ

С точки зрения
обеспечения информационной
безопасности

«___»_____2017 № ___
г. Челябинск

Паспорт предприятия ООО «Диджитер»

Содержание паспорта предприятия:

1. Организационно - правовая форма предприятия (организации, учреждения) и его реквизиты:

1.1. Название предприятия: Общество с ограниченной ответственностью «Диджитер».

1.2. Численность сотрудников: 10.

1.3. Банковские реквизиты:

1.4. ИНН 7453281507

1.5. КПП 745301001

1.6. р/сч. № 40702810590000020773

1.7. к/сч. № 30101810400000000779

1.8. в ф-ле ПАО «Челябинвестбанк» г. Челябинск

1.9. БИК 047501779

2. Виды деятельности предприятия.

2.1. Торговля оптовая прочей офисной техникой и оборудованием;

2.2. Торговля оптовая электрической бытовой техникой;

2.3. Торговля оптовая радио-, теле- и видеоаппаратурой и аппаратурой для цифровых видеодисков (dvd);

2.4. Торговля оптовая грампластинками, аудио- и видеомагнитными лентами, компакт-дисками (cd) и цифровыми видеодисками (dvd) (кроме носителей без записей);

2.5. Торговля оптовая компьютерами, периферийными устройствами к компьютерам и программным обеспечением;

2.6. Торговля оптовая прочими машинами, приборами, аппаратурой и оборудованием общепромышленного и специального назначения;

2.7. Торговля оптовая неспециализированная;

2.8. Торговля розничная компьютерами, периферийными устройствами к ним и программным обеспечением в специализированных магазинах;

2.9. Торговля розничная офисными машинами и оборудованием в специализированных магазинах;

2.10. Торговля розничная аудио- и видеотехникой в специализированных магазинах;

2.11. Торговля розничная бытовыми электротоварами в специализированных магазинах;

2.12. Торговля розничная мебелью в специализированных магазинах;

2.13. Торговля розничная музыкальными записями, аудиолентами, компакт-дисками и кассетами в специализированных магазинах;

2.14. Торговля розничная лентами и дисками без записей в специализированных магазинах;

2.15. Торговля розничная прочими товарами в специализированных магазинах;

2.16. Торговля розничная фотоаппаратурой, оптическими приборами и средствами измерений, кроме очков, в специализированных магазинах;

2.17. Торговля розничная очками, включая сборку и ремонт очков в специализированных магазинах;

2.18. Торговля розничная по почте;

2.19. Торговля розничная, осуществляемая непосредственно при помощи информационно - коммуникационной сети интернет;

2.20. Торговля розничная через интернет-аукционы;

2.21. Торговля розничная, осуществляемая непосредственно при помощи телевидения, радио, телефона;

2.22. Торговля розничная прочая вне магазинов, палаток, рынков;

2.23. Перевозка грузов неспециализированными автотранспортными средствами;

2.24. Хранение и складирование прочих грузов;

2.25. Транспортная обработка прочих грузов;

2.26. Разработка компьютерного программного обеспечения;

2.27. Деятельность консультативная и работы в области компьютерных технологий;

2.28. Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая;

2.29. Деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность;

2.30. Деятельность по созданию и использованию баз данных и информационных ресурсов;

2.31. Ремонт компьютеров и периферийного компьютерного оборудования;

2.32. Ремонт электронной бытовой техники;

2.33. Ремонт бытовой техники.

3. Предполагаемые виды защищаемой информации.

3.1. Коммерческая тайна.

4. Перечень предприятий поставщиков, клиентов и конкурентов

4.1. Клиентами ООО " Диджитер " являются как физические, так и юридические лица.

4.2. Конкуренты ООО " Диджитер ":

4.2.1. ИНФОРМАЦИОННЫЕ РЕШЕНИЯ;

4.2.2. ЮКАС КОМ;

4.2.3. ИНФОТЕХ.

5. Описание организационной структуры предприятия.

Организационная структура ООО " Диджитер " так же включает в себя:

Рисунок А.1 – Организационная структура ООО " Диджитер "

6. Описание строительной инфраструктуры здания.

Организация располагается по адресу Татьяничевой 9, помещение 51:

6.1. 5 этажное здание;

6.2. Ничем не ограждено;

6.3. Система центрального водяного отопления;

6.4. Система пожаротушения.

7. Программно – аппаратные средства:

7.1. Пакет Microsoft Office 2013 , необходим при оформлении (дополнении и изменении) договоров, приказов, распоряжений.

7.2. ESET NOD32 – антивирусное программное обеспечение установленное на АРМ.

7.3. 1С Предприятие 8.3 –необходима для автоматизации бухгалтерского и налогового учета.

8. Описание информационной среды предприятия.

Таблица А 1– Информационная среда предприятия

Программа	Назначение
Windows 7 Professional	Операционная система установленная на АРМ сотрудников.
Microsoft Office 2013	Офисный пакет для работы с документами.
1С Предприятие 8.3	Ведение бухгалтерского и налогового учёта.
КриптоПро CSP v.4.0	Генерация электронной подписи, работа с сертификатами.
ESET NOD32	Антивирусное программное обеспечение установленное на АРМ.
Skype	Служит для обмена текстовыми , голосовыми сообщениями и видеозвонками.
ICQ	Служит для мгновенного обмена сообщениями.
WinRAR	Предназначен для открытия, сжатия файлов и папок.
Adobe Acrobat	Предназначен для создания и просмотра электронных документов в формате PDF
Skype	Служит для обмена текстовыми , голосовыми сообщениями и видеозвонками.

9. Схема помещения предприятия.

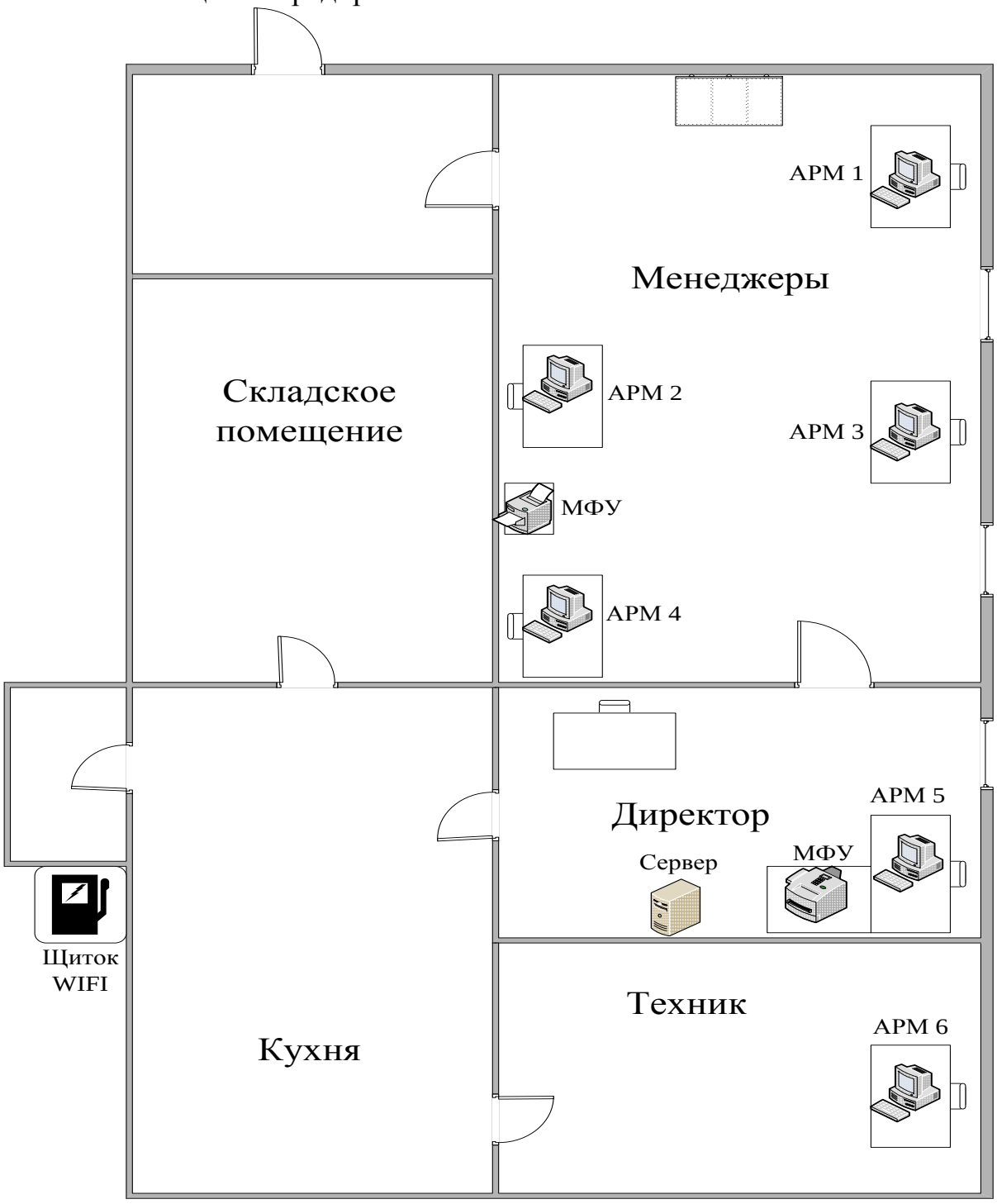

Рисунок А 2 – Схема помещения

ПРИЛОЖЕНИЕ Б

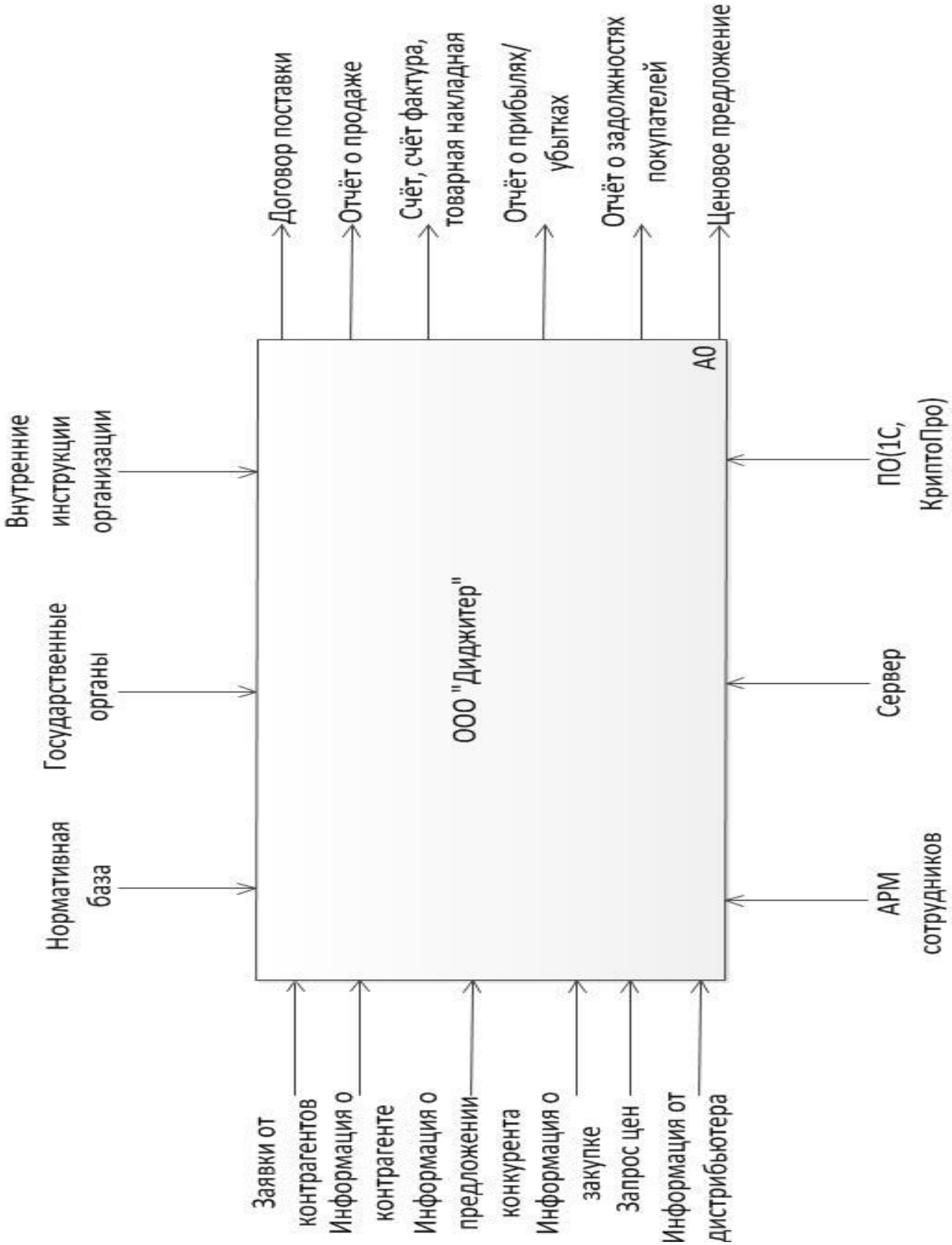

Рисунок Б 1 - Общая модель деятельности

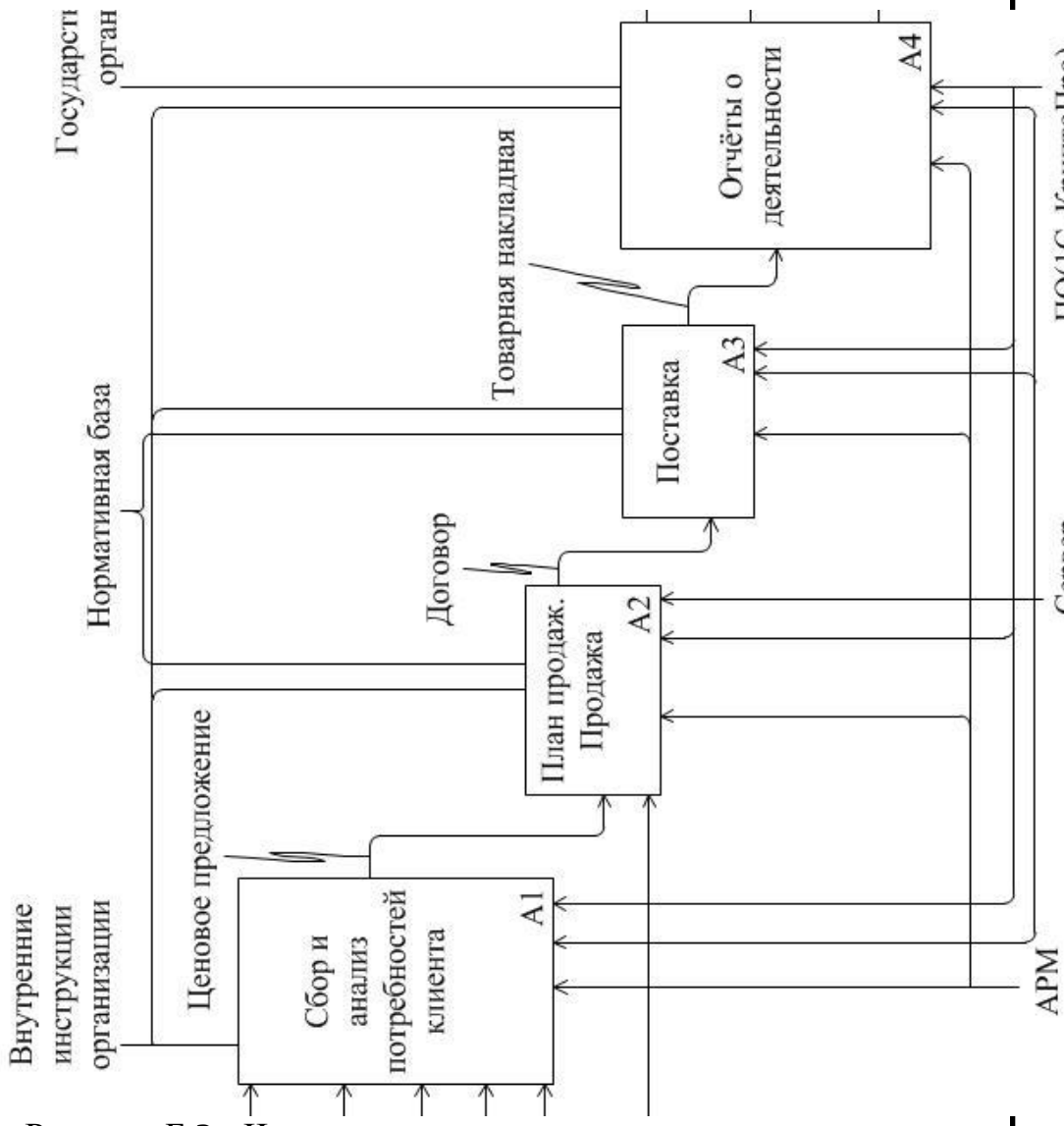

Рисунок Б 2 - Частная модель деятельности

ПРИЛОЖЕНИЕ В

УТВЕРЖДАЮ
Генеральный Директор

ООО «Диджитер»
_____С.А. Сабельников
Дата_____

ПОЛОЖЕНИЕ

О коммерческой тайне

«___»_____2017 № ___

г. Челябинск

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение разработано на основании Гражданского кодекса, ФЗ «О коммерческой тайне» от 29.07.2004г. №98-ФЗ, других федеральных законов РФ;

1.2. Настоящее положение регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателя информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну;

Продолжение приложения В

1.3. Настоящее Положение распространяется на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована;

1.4. Настоящее Положение не распространяется на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне;

1.5. Законодательство Российской Федерации о коммерческой тайне состоит из Гражданского кодекса Российской Федерации, Федерального закона «О коммерческой тайне» № 98-ФЗ от 29.07.2004г., других федеральных законов.

II. ПОРЯДОК ОПРЕДЕЛЕНИЯ ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

2.1. Право на отнесение информации к сведениям, составляющим коммерческую тайну, и на определение Перечня и состава таких сведений принадлежит обладателю такой информации в рамках действующего законодательства Российской Федерации и настоящего Положения;

2.2. Непосредственное отнесение сведений к коммерческой тайне и присвоение грифа "Коммерческая тайна" является обязанностью исполнителя и должностного лица, изготовившего, подписавшего (утвердившего) документ, на основании Перечня сведений, составляющих коммерческую тайну ООО «Диджитер»;

2.3. Перечень сведений, составляющих коммерческую тайну (далее – Перечень) создается на основе предложений генерального директора с учетом настоящего Положения и действующего законодательства Российской Федерации;

Перечень, изменения и дополнения в него принимаются и утверждаются в соответствии с Уставом ООО «Диджитер»;

Продолжение приложения В

2.4. Информация, самостоятельно полученная лицом при осуществлении исследований, систематических наблюдений или иной деятельности, считается полученной законным способом несмотря на то, что содержание указанной информации может совпадать с содержанием информации, составляющей коммерческую тайну, обладателем которой является другое лицо;

2.5. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом;

2.6. Ограничения на распространение сведений, составляющих коммерческую тайну, возникающие в результате совместной деятельности ООО «Диджитер», его партнеров или клиентов, должны быть оговорены в договоре о сотруд-

ничестве (взаимной деятельности, обслуживании), в котором также отражаются взаимные обязательства и ответственность сторон за сохранность этих сведений;

2.7. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также, если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

III. ПРАВА ОБЛАДАТЕЛЯ ИНФОРМАЦИЕЙ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

3.1. Обладатель информации, составляющей коммерческую тайну вправе:

3.1.1. Использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

Продолжение приложения В

3.1.2. Вводить в гражданский оборот информацию, составляющую коммерческую тайну, на основании договоров, предусматривающих включение в них условий об охране конфиденциальности этой информации;

3.1.3. Требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

3.1.4. Требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;

3.1.5. Защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

IV. КРУГ ЛИЦ ИМЕЮЩИХ ДОСТУП К ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

4.1. Должностные лица и сотрудники ООО «Диджитер» могут иметь доступ к коммерческой тайне (к сведениям, составляющим коммерческую тайну Общества, материальным или электронным носителях которые непосредственно создаются, контролируются или используются в работе в процессе исполнения трудовых обязанностей лицом, имеющим доступ);

4.2. Доступ к сведениям, составляющим коммерческую тайну ООО «Диджитер», имеют лица, получившие допуск, о чем свидетельствует запись в журналах учета лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

Продолжение приложения В

4.3. Предоставление сведений, составляющих коммерческую тайну ООО «Диджитер», иным работникам, не имеющим доступ в соответствии с журналами лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана, не допускается.

V. ОХРАНА ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

5.1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

5.1.1. Определение перечня информации, составляющей коммерческую тайну;

5.1.2. Ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

5.1.3. Учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

5.1.4. Регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5.1.5. Нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Продолжение приложения В

5.2. Наряду с мерами, указанными в части 1 настоящего раздела, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры;

5.3. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

5.3.1. Исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

5.3.1. Обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

5.4. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

VI. ПРАВИЛА ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

6.1. Информация, составляющая коммерческую тайну Общества, не может быть сообщена сотрудником Общества третьим лицам, не имеющим допуска с данной информации;

6.2. Сотрудник ООО «Диджитер» имеет право передавать информацию, составляющую коммерческую тайну ООО «Диджитер» только лицам, имеющим допуск к данной информации, в объемах, предварительно согласованных в журналах учета лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

Продолжение приложения В

6.3. В тех случаях, когда сотрудник ООО «Диджитер» выполняет свои непосредственные должностные обязанности, информация, составляющая коммерческую тайну ООО, может разглашаться сотрудником ООО только в рамках вопросов, входящих в компетенцию данного сотрудника и при условии соблюдения требований, предусмотренных п.6.2. настоящего Положения;

6.4. Сотрудник должен знать также, кому из сотрудников ООО «Диджитер» разрешено работать с информацией, составляющей коммерческую тайну, к которой он сам допущен, и в каком объеме эта информация может быть доведена до этих сотрудников;

6.5. При участии в работе сторонних организаций сотрудник может знакомить их представителей с информацией, составляющей коммерческую тайну, только с разрешения генерального директора. При этом руководитель должен определить конкретные вопросы, подлежащие рассмотрению, и указать, кому и в каком объеме может быть сообщена информация, подлежащая защите;

6.6. Запрещается помещать без необходимости информацию, составляющую коммерческую тайну Общества, в документы открытого характера. Такое нарушение порядка обращения с информацией, составляющей коммерческую тайну Общества, рассматривается как их разглашение и влечет ответственность в соответствии с установленным порядком;

6.7. В целях защиты информации, составляющей коммерческую тайну, для распечатки документов, содержащих такую информацию, может применяться специальная бумага (не позволяющая делать аутентичные копии), а также различные специальные средства и методы, позволяющие однозначно выявить источник и способ утечки информации, содержащей коммерческую тайну;

6.8. Об утрате или недостаче документов, изделий, содержащих информацию, составляющую коммерческую тайну Общества, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов, металлических шкафов, личных печатей, а также о причинах и условиях возможной утечки такой

Продолжение приложения В

информации сотрудник обязан немедленно сообщить непосредственному генеральному директору Общества;

6.9. При увольнении, перед уходом в отпуск, отъездом в командировку или предполагаемым отсутствием на рабочем месте в течение более или менее длительного срока сотрудник обязан сдать директору Общества все носители информации, составляющие коммерческую тайну (рукописи, черновики, документы, чертежи, магнитные ленты, дискеты, распечатки на принтерах и т.д.), которые находились в распоряжении сотрудника в связи с выполнением им служебных обязанностей;

6.10. Сотрудник обязан по первому требованию уполномоченного лица предъявлять для проверки все числящиеся за ним материалы, содержащие информацию, составляющую коммерческую тайну Общества, представлять устные или письменные объяснения о нарушениях установленных правил выполнения работ, учета и хранения документов и т.д., фактов разглашения коммерческой тайны, утраты документов, содержащих коммерческую тайну Общества;

6.11. В случае попытки посторонних лиц получить информацию, составляющую коммерческую тайну, сотрудник обязан сообщить об этом директору ООО «Диджитер»;

6.12. Общество по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им информацию, содержащую коммерческую тайну, на безвозмездной основе. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами;

6.13. Общество, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие информацию обязаны предоставить эту информацию по запросу судов, органов прокуратуры,

Продолжение приложения В

органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

VII. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИИ СОСТАВЛЯЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

7.1. Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государствен-

ного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами;

7.2. В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке;

7.3. Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию в соответствии с пунктом 7.1 настоящего раздела, обязаны предоставить эту информацию по запросу судов, органов прокуратуры, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации;

7.4. На документах, предоставляемых указанным в пунктах 7.1 и 7.3 настоящего раздела органам и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф "Коммерческая тайна".

Продолжение приложения В

VIII. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ

8.1.Нарушение настоящего Положения влечет за собой дисциплинарную гражданско-правовую, административную или угол ответственность в соответствии с гражданским законодательством РФ;

8.2. Работник, который в связи с исполнением должностных обязанностей получил доступ к информации, составляющей коммерческую тайну обладателем которой является ООО «Диджитер» и его контрагенты, в случае умышленного

или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии законодательством РФ;

8.3. Лицо, которое использовало информацию, составляющую коммерческую тайну и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайной ошибки, не может в соответствии с законодательством РФ быть привлечено к ответственности;

8.4. По требованию ООО «Диджитер» лицо, указанное в пункте 9.2 настоящей статьи, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять меры ООО «Диджитер» вправе требовать в судебном порядке защиты своих прав;

8.5. Работники общества подписывают обязательство о неразглашении коммерческой тайны и несут ответственность за допуск на территорию предприятия третьих лиц, проведения этими лицами осмотров, фото-, видеосъемок, объектов находящихся на территории ООО «Диджитер».

Окончание приложения В

IX. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Настоящее Положение утверждается приказом генерального директора ООО «Диджитер». Изменения и дополнения в настоящее Положение вносятся по решению генерального директора ООО «Диджитер» ;

9.2. Если в результате изменения законодательства Российской Федерации отдельные статьи настоящего Положения вступают в противоречие с Законом, указанные статьи утрачивают силу и до момента внесения изменений и дополне-

ний в настоящее Положение применяются нормы законодательства Российской Федерации;

9.3. Все приложения к настоящему Положению являются его неотъемлемой частью и имеют юридическую силу наравне с Положением.

Генеральный директор С.А. Сабельников

СОГЛАСОВАНО

Заместитель генерального директора В.В. Уфимцев

ПРИЛОЖЕНИЕ Г

ООО «Диджитер»

Общество с ограниченной ответственностью «Диджитер»
Юридический адрес: 454126, г. Челябинск, ул. Татьяничевой, 9, пом. 51
Фактический адрес: 454126, г. Челябинск, ул. Татьяничевой, 9
Тел.: 8(351)7512749, e-mail: info@digiter74.ru
ИНН 7453281507, КПП 745301001, ОГРН 1157453003960, ОКПО 34555531
БИК 047501779, р/с 40702810590000020773 в ПАО "Челябинвестбанк"
кор/счет 30101810400000000779

Компьютеры / Комплектующие / Оргтехника / Программное обеспечение

УТВЕРЖДАЮ
Генеральный Директор

ООО «Диджитер»
_____С.А. Сабельников
Дата_____

ПЕРЕЧЕНЬ

Сведений, составляющих

коммерческую тайну

«___»_____2017 № ___

г. Челябинск

Таблица Г1 – Перечень сведений, составляющих коммерческую тайну

№ п.п.	Характер сведений	Срок действия ограничений на доступ к сведениям
1	**2**	**3**
1. Управление и кадры		
1.1.	Сведения, содержащие анализ количественного и качественного состава кадров Компании и его структурных подразделений.	До принятия решения об их раскрытии

Продолжение приложения Г

Продолжение таблицы Г 1

1	2	3
1.2.	Сведения о подготовке, принятии и исполнении отдельных решений руководства Компании по коммерческим, организационным, научно-техническим и иным вопросам, содержащим информацию, которая позволяет увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, услуг или получить иную коммерческую выгоду.	До принятия решения об их раскрытии
1.3.	Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления Компанией по вопросам, содержащим информацию, которая позволяет увеличить доходы, избежать неоправданных расходов.	До принятия решения об их раскрытии

2. Планы		
2.1.	Сведения о стратегии развития Компании, о перспективных планах изменения, расширения или свертывания отдельных видов деятельности, услуг и их технико-экономических обоснованиях.	5 лет
3. Финансовая информация		
3.1.	Сведения о результатах внутреннего аудита деятельности Компании.	До принятия решения об их раскрытии
3.2.	Сведения, содержащие анализ финансовой устойчивости Компании, оценку факторов, оказывающих влияние на финансовое состояние Компании и результаты финансовых операций.	До принятия решения об их раскрытии
4. Маркетинговая деятельность		
4.1.	Сведения о результатах изучения рынка, содержащие оценку состояния и перспектив развития рыночной конъюнктуры.	3 года
4.2.	Сведения о рыночной стратегии Компании.	До принятия решения об их раскрытии
5. Партнеры и конкуренты		
5.1.	Систематизированные сведения (в том числе базы данных) о компаньонах, поставщиках, подрядчиках, заказчиках, потребителях, покупателях, клиентах, спонсорах, посредниках и других деловых партнерах Компании.	Постоянно
5.2.	Сведения о конкурентах и деловых партнерах Компании, которые не содержатся в открытых источниках информации, а также сведения, раскрывающие источники или способы получения этой информации.	Постоянно

Окончание приложения Г

Продолжение таблицы Г 1

1	2	3
6. Переговоры и контракты		
6.1.	Сведения о подготовке и результатах проведения переговоров с деловыми партнерами.	5 лет
6.2.	Сведения о содержании и фактах заключения сделок.	До принятия решения об их раскрытии
6.3.	Сведения, условия конфиденциальности которых установлены в договорах, контрактах, соглашениях и других обязательствах Компании.	До принятия решения об их раскрытии
7. Производство и технология		
7.1.	Сведения о структуре бизнес-процессов Компании.	5 лет
7.2.	Сведения, содержащие оценку технической оснащен-	До принятия

	ности, состояния программного и компьютерного обеспечения Компании.	решения об их раскрытии
8. Обеспечение безопасности		
8.1.	Сведения о состоянии и порядке организации в Компании системы обеспечения защиты коммерческой тайны.	Постоянно
8.2.	Сведения о состоянии и порядке организации системы охраны, пропускного режима, инженерно-технической безопасности и сигнализации на объектах Компании.	Постоянно
8.3.	Сведения о состоянии и порядке организации системы обеспечения информационной безопасности Компании.	Постоянно
8.4.	Сведения о настройках и паролях доступа, используемых в средствах защиты информационных ресурсов и автоматизированных систем управления Компании.	Постоянно
8.5.	Сведения о результатах аудита защищенности информационных ресурсов и автоматизированных систем управления Компании.	5 лет
8.6.	Сведения, содержащие анализ состояния безопасности финансовых, материальных и кадровых ресурсов Компании.	До принятия решения об их раскрытии
8.7.	Сведения, раскрывающие содержание и методы проведения конкретных мероприятий, направленных на обеспечение безопасности Компании.	Постоянно

Генеральный директор С.А. Сабельников

ПРИЛОЖЕНИЕ Д

ООО «Диджитер»

Общество с ограниченной ответственностью «Диджитер»
Юридический адрес: 454126, г. Челябинск, ул. Татьяничевой, 9, пом. 51
Фактический адрес: 454126, г. Челябинск, ул. Татьяничевой, 9
Тел.: 8(351)7512749, e-mail: info@digiter74.ru
ИНН 7453281507, КПП 745301001, ОГРН 1157453003960, ОКПО 34555531
БИК 047501779, р/с 40702810590000020773 в ПАО "Челябинвестбанк"
кор/счет 30101810400000000779

Компьютеры / Комплектующие / Оргтехника / Программное обеспечение

УТВЕРЖДАЮ

Генеральный Директор
ООО «Диджитер»
_____С.А. Сабельников
Дата_____

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

по созданию КСЗИ в ООО «Диджитер»

СОГЛАСОВАНО

Заместитель ген. директора

ООО «Диджитер»

_____ В.В. Уфимцев

Дата_____

Продолжение приложения Д

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование и условное обозначение системы

Полное наименование системы: Комплексная система защиты информации в обществе с ограниченной ответственностью “Диджитер”

Условное обозначение: КСЗИ в ООО “Диджитер”.

1.2. Наименования заказчика и исполнителя

Заказчик системы защиты: ООО “Диджитер”, в лице генерального директора предприятия.

Разработчик системы защиты: ООО “Диджитер”, в лице генерального директора предприятия.

1.3. Перечень документов, на основании которых создается КСЗИ:

1.3.1. Конституция Российской Федерации;

1.3.2. Федеральный закон от 29 июля 2004 года N 98-ФЗ «О коммерческой тайне»;

1.3.3. Трудовой кодекс РФ от 30.12.2001 N 197-ФЗ;

1.3.4. Федеральный закон от 08.02.1998 N 14 «Об обществах с ограниченной ответственностью»;

1.3.5. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ;

1.3.6. Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 N 44;

1.3.7. Федеральный закон "О закупках товаров, работ, услуг отдельными видами юридических лиц" от 18.07.2011 N 223;

1.3.8. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. N 149;

1.3.9. Гражданский кодекс Российской Федерации часть 4 от 18 декабря 2006 года N 230-ФЗ.

Продолжение приложения Д

1.4. Порядок оформления и предъявления заказчику результатов работ по созданию КСЗИ, по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы.

Результаты работы оформляются и предъявляются генеральному директору по мере исполнения в виде предварительных проектов. Окончательный вариант проекта согласуется и предоставляется на рассмотрение заказчику в лице генерального директора предприятия.

1.5. Изменения в техническом задании на КСЗИ оформляются дополнением или согласованы и подписаны сторонами протоколом. Дополнение или протокол являются в будущем неотъемлемой частью технического задания.

2. НАЗНАЧЕНИЕ И ЦЕЛИ РАЗРАБОТКИ КСЗИ

2.1. Назначение и цели

Цель – обеспечить безопасность информационных активов ООО “Диджитер”.

3. ХАРАКТЕРИСТИКА ОБЪЕКТОВ ЗАЩИТЫ

3.1. Краткие сведения об объектах защиты

3.1.1. Автоматизированные рабочие места:

3.1.1.1. АРМ генерального директора;

3.1.1.2. АРМ сотрудников организации.

3.1.2. Сервер:

3.1.2.1. Intel Xeon E 5410 x64, 4x2.33 ГГц, 24 Гб, 2 ТБ.

3.1.3. Персонал:

3.1.3.1. Генеральный директор;

3.1.3.2. Сотрудники организации (9 человек).

Продолжение приложения Д

4. ТРЕБОВАНИЯ К КСЗИ

4.1. Требования организации-заказчика КСЗИ:

4.1.1. Определить перечень информации, составляющей коммерческую тайну;

4.1.2. Ограничить доступ к информации, составляющей коммерческую тайну;

4.1.3. Произвести учёт лиц, получивших доступ к информации, составляющей коммерческую тайну;

4.1.4. Урегулировать отношения по использованию информации, составляющей коммерческую тайну;

4.1.5. Нанести на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна".

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО РАЗРАБОТКЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. КСЗИ 1. Проектирование

5.2. КСЗИ 1.1. Определение главных показателей имеющихся бизнес-процессов с точки зрения информационной безопасности;

5.3. КСЗИ 1.2. Выявление и анализ проблем, слабых мест имеющихся бизнес-процессов;

5.4. КСЗИ 1.3. Разработка значений главных показателей новых бизнес-процессов;

5.5. КСЗИ 1.4. Анализ и отбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;

5.6. КСЗИ 1.5. Разработка и согласование структуры новых бизнес-процессов;

5.7. КСЗИ 2. Создание новой организационно-распорядительной документации

5.8. КСЗИ 2.1. Положение «О коммерческой тайне»;

Продолжение приложения Д

5.9. КСЗИ 2.2. Перечень сведений, составляющих коммерческую тайну;

5.10. КСЗИ 2.3. Приказы об утверждении положения режима коммерческой тайны и перечня сведений, составляющих коммерческую тайну;

5.11. КСЗИ 2.4. Внесение изменений в должностные инструкции;

5.12. КСЗИ 2.5. Согласование и утверждение организационно-распорядительных документов.

5.13. КСЗИ 3. Подготовка реализации проекта созданию КСЗИ

5.14. КСЗИ 3.1. Определение ответственных лиц и исполнителей проекта;

5.15. КСЗИ 3.2. Приобретение программно-аппаратного средства защиты от НСД;

5.16. КСЗИ 3.3. Приобретение средства контроля и управления доступом;

5.17. КСЗИ 3.4. Приобретение средств видеонаблюдения;

5.18. КСЗИ 4. Внедрение

5.19. КСЗИ 4.1. Установка и настройка программно-аппаратного средства защиты от НСД;

5.20. КСЗИ 4.2. Установка средства контроля и управления доступом;

5.21. КСЗИ 4.3. Установка средств видеонаблюдения;

5.22. КСЗИ 4.4. Контроль защищенности;

5.23. КСЗИ 4.5. Обучение персонала.

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

6.1. Критериями для приёмки работ является полное выполнение требований, установленных в пункте 4 данного технического задания;

6.2. Порядок приёмки осуществляется единовременно;

6.3. Порядок оформления замечаний в письменном виде.

7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ВВОДУ КСЗИ В ЭКСПЛУАТАЦИЮ

Продолжение приложения Д

7.1. Требованиями к составу и содержанию работ является выполнение всех разработанных мероприятий по вводу КСЗИ в ООО «Диджитер».

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

8.1. Перечень документов которые должны быть разработаны и соответствовать требованиям технического задания:

8.1.1. Перечень сведений, составляющих коммерческую тайну;

8.1.2. Положение о режиме коммерческой тайны;

8.1.3. Приказы об утверждении документов.

8.2. Порядок предоставления документов в письменном виде.

9. ИСТОЧНИКИ РАЗРАБОТКИ КСЗИ

9.1. Источники финансирования и бюджет.

Таблица Д 1 – Стоимость обеспечения

№ п/п	Наименование	Количество	Цена за шт. (руб.)	Сумма (руб.)
1	СЗИ НСД «Аура 1.2.4»	6	4000	24000
2	комплект видеонаблюдения «ЭкоЛайн Dome-204»	1	13880	13880
3	Считыватель карт Matrix-II	1	1585	1585
4	Карта Optimus EM-marine	10	23	230
5	Кнопка выхода Optimus	1	99	99
6	Автономный контроллер Z – 5R	1	580	580
7	Электромагнитный замок Optimus EM – 180	1	1700	1700
Итог				42074

Продолжение приложения Д

Таблица Д 2 – Стоимость услуг по обеспечению проекта

№ п/п	Наименование	Стоимость (руб.)
1	Разработка и описание бизнес-процессов компании с точки зрения ИБ	9600
2	Разработка организационно-распорядительной документации	4800
3	Установка и настройка средства защиты от НСД «Аура 1.2.4»	8000
4	Установка и настройка комплекта видеонаблюдения «ЭкоЛайн Dome-204»	7000
5	Установка средства контроля управления доступом	5000

6	Обучение пользователей	2400
Итог		36600

ПРИЛОЖЕНИЕ Е

ООО «Диджитер»

Общество с ограниченной ответственностью «Диджитер»
Юридический адрес: 454126, г. Челябинск, ул. Татьяничевой, 9, пом. 51
Фактический адрес: 454126, г. Челябинск, ул. Татьяничевой, 9
Тел.: 8(351)7512749, e-mail: info@digiter74.ru
ИНН 7453281507, КПП 745301001, ОГРН 1157453003960, ОКПО 34555531
БИК 047501779, р/с 40702810590000020773 в ПАО "Челябинвестбанк"
кор/счет 30101810400000000779

ПРИКАЗ

«___»_____2017 № ___

Об утверждении перечня сведений, составляющих коммерческую тайну

В соответствии с Федеральным законом Российской Федерации от 02.02.2006 № 98-ФЗ «О коммерческой тайне».

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый Перечень сведений, составляющих коммерческую тайну, обрабатываемых в ООО «Диджитер» составленный на 4 (четырех) листах, прошитых и пронумерованных.

2. За поддержанием перечня в актуальном состоянии назначить ответственного:

2.1. Заместителя генерального директора – Владимира Викторовича Уфимцева.

3. Обновление перечня производить один раз в квартал.

3.1. Ознакомить с данным Перечнем начальников отделов ООО «Диджитер». Ответственного за ознакомление назначить заместителя генерального директора – Владимира Викторовича Уфимцева.

Продолжение приложения Е

4. С приказом ознакомить:

4.1. Начальника тендерного отдела – Михаила Васильевича Румянцева.

4.2. Начальника отдела продаж – Сергея Дмитриевича Замятина.

4.3. Начальника технического отдела – Антона Павловича Воронцова.

4.4. Бухгалтера – Кристину Юрьевну Толкачеву.

Контроль исполнения приказа возложить на заместителя генерального директора – Владимира Викторовича Уфимцева.

Генеральный директор С.А. Сабельников

С приказом ознакомлен(а):

Начальник тендерного отдела М.В. Румянцев

Начальник отдела продаж С.Д. Зымятин

Начальник технического отдела А.П. Воронцов

Бухгалтер К.Ю. Толкачев

Продолжение приложения Е

ООО «Диджитер»
Общество с ограниченной ответственностью «Диджитер»
Юридический адрес: 454126, г. Челябинск, ул. Татьяничевой, 9, пом. 51
Фактический адрес: 454126, г. Челябинск, ул. Татьяничевой, 9
Тел.: 8(351)7512749, e-mail: info@digiter74.ru
ИНН 7453281507, КПП 745301001, ОГРН 1157453003960, ОКПО 34555531
БИК 047501779, р/с 40702810590000020773 в ПАО "Челябинвестбанк"
кор/счет 30101810400000000779
Компьютеры / Комплектующие / Оргтехника / Программное обеспечение

ПРИКАЗ

«___»_____2017 № ___

Об утверждении положения о коммерческой тайне

В соответствии с Федеральным законом Российской Федерации от 02.02.2006 № 98-ФЗ «О коммерческой тайне».

ПРИКАЗЫВАЮ:

4.Утвердить прилагаемое Положение о коммерческой тайне ООО «Диджитер» составленный на 11 (одиннадцати) листах, прошитых и пронумерованных.

5. За поддержанием перечня в актуальном состоянии назначить ответственного:

2.1. Заместителя генерального директора – Владимира Викторовича Уфимцева.

6.Обновление перечня производить один раз в квартал.

1.1. Ознакомить с данным Положением начальников отделов ООО «Диджитер». Ответственный за ознакомление заместитель генерального директора – Владимира Викторовича Уфимцева.

2. С приказом ознакомить:

Окончание приложения Е

2.1. Начальника тендерного отдела – Михаила Васильевича Румянцева.

2.2. Начальника отдела продаж – Сергея Дмитриевича Замятина.

2.3. Начальника технического отдела – Антона Павловича Воронцова.

2.4. Бухгалтера – Кристину Юрьевну Толкачеву.

Контроль исполнения приказа возложить на заместителя генерального директора – Владимира Викторовича Уфимцева.

Генеральный директор С.А. Сабельников

С приказом ознакомлен(а):

Начальник тендерного отдела М.В. Румянцев

Начальник отдела продаж С.Д. Зымятин

Начальник технического отдела А.П. Воронцов

Бухгалтер К.Ю. Толкачев

ПРИЛОЖЕНИЕ Ж

При построении диаграммы Ганта, для начала необходимо определить перечень работ и их сроков.

Таблице Ж 1 – Перечень задач и сроков

Работа	Название работы	Длительность	Начало	Окончание
1	2	3	4	5
1	Проектирование	13	06.03.2017	20.03.2017

Работа	Название работы	Длитель-ность	Начало	Окончание
1	2	3	4	5
1.1	Определение главных показателей имеющихся бизнес-процессов с точки зрения информационной безопасности;	3	06.03.2017	9.03.2017
1.2	Выявление и анализ проблем, слабых мест имеющихся бизнес-процессов;	2	9.03.2017	11.03.2017
1.3	Разработка значений главных показателей новых бизнес – процессов;	2	11.03.2017	13.03.2017
1.4	Анализ и отбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;	3	13.03.2017	16.03.2017
1.5	Разработка и согласование структуры новых бизнес – процессов;	3	16.03.2017	19.03.2017
2	Создание новой организационно – распорядительной документации	8	20.03.2017	28.03.2017
2.1	Положение «О коммерческой тайне»;	3	20.03.2017	23.03.2017
2.2	Перечень сведений, составляющих коммерческую тайну;	2	23.03.2017	25.03.2017
2.3	Приказы об утверждении положения режима коммерческой тайны и перечня сведений, составляющих коммерческую тайну;	1	25.03.2017	26.03.2017
2.4	Внесение изменений в должностные инструкции.	2	25.03.2017	27.03.2017

Продолжение приложения Е

Продолжение таблицы Ж 1

1	2	3	4	5
2.5	Согласование и утверждение организационно – распорядительных документов	1	27.03.2017	28.03.2017

3	Подготовка реализации проекта созданию КСЗИ	2	28.03.2017	30.03.2017
3.1	Определение ответственных лиц и исполнителей проекта;	1	28.03.2017	29.03.2017
3.2	Приобретение программно – аппаратного средства защиты от НСД;	1	28.03.2017	29.03.2017
3.3	Приобретение средства контроля и управления доступом;	1	29.03.2017	30.03.2017
3.4	Приобретение средств видеонаблюдения	1	29.03.2017	30.03.2017
4	Внедрение	3	30.03.2017	2.04.2017
4.1	Установка и настройка программно – аппаратного средства защиты от НСД;	1	30.03.2017	31.03.2017
4.2	Установка средства контроля и управления доступом;	1	31.03.2017	1.04.2017
4.3	Установка средств видеонаблюдения.	1	31.03.2017	1.04.2017
4.4	Контроль защищенности	1	01.04.2017	02.04.2017
4.5	Обучение персонала	1	01.04.2017	02.04.2017
Проект создания КСЗИ		26	06.03.2017	2.04.2017

Окончание приложения Ж

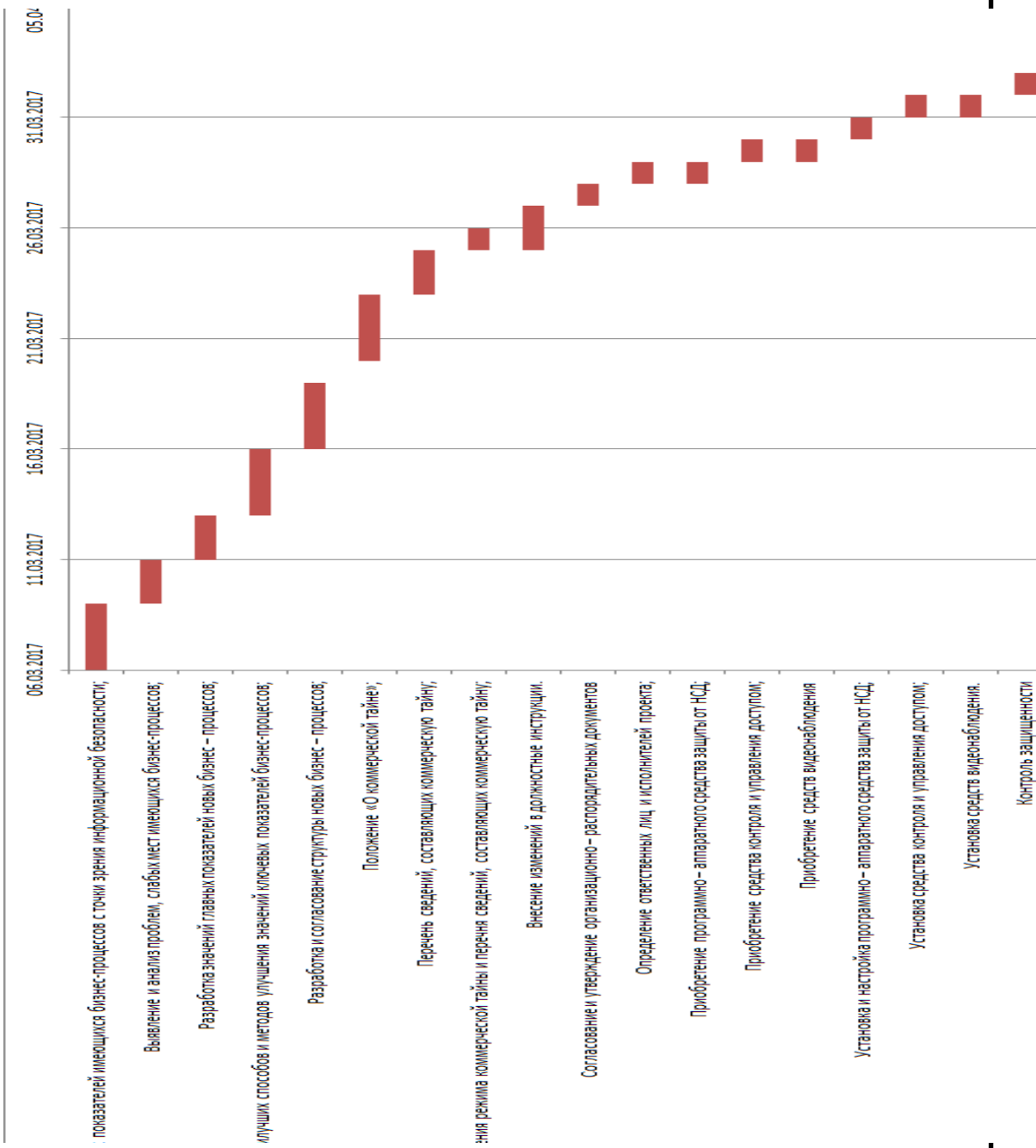

Рисунок Ж 2 - Диаграмма Ганта

ПРИЛОЖЕНИЕ З

Для определения соответствия плану работ определим необходимые сроки выполнения работ. Составим сетевой график (Таблица 3.1).

Т – длительность работы, дней

$\mathbf{Т_{рн}}$ – ранний срок начала работы

$\mathbf{Т_{пн}}$ – поздний срок начала работы

$\mathbf{Т_{ро}}$ – ранний срок окончания работы

$\mathbf{Т_{по}}$ – поздний срок окончания работы

Таблица 3.1 – Расписание выполнения работ

Работа	Название работы	Т	$Т_{рн}$	$Т_{пн}$	$Т_{ро}$	$Т_{по}$
1	2	3	4	5	6	7
1	Проектирование	13	06.03. 2017	06.03. 2017	19.03. 2017	24.03. 2017
1.1	Определение главных показателей имеющихся бизнес-процессов с точки зрения информационной безопасности;	3	06.03. 2017	06.03. 2017	08.03. 2017	10.03. 2017
1.2	Выявление и анализ проблем, слабых мест имеющихся бизнес-процессов;	2	08.03. 2017	10.03. 2017	10.03. 2017	13.03. 2017
1.3	Разработка значений главных показателей новых бизнес – процессов;	2	10.03. 2017	13.03. 2017	12.03. 2017	16.03. 2017
1.4	Анализ и отбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;	3	12.03. 2017	16.03. 2017	15.03. 2017	20.03. 2017
1.5	Разработка и согласование структуры новых бизнес – процессов;	3	15.03. 2017	20.03. 2017	17.03. 2017	24.03. 2017
2	Создание новой организационно – распорядительной документации	8	17.03. 2017	24.03. 2017	26.03. 2017	02.04. 2017
2.1	Положение «О коммерческой тайне»;	3	17.03. 2017	24.03. 2017	19.03. 2017	27.03. 2017

Продолжение приложения З

Продолжение таблицы З 1

2.2	Перечень сведений, составляющих коммерческую тайну;	2	19.03. 2017	27.03. 2017	21.03. 2017	29.03. 2017
2.3	Приказы об утверждении положения режима коммерческой тайны и перечня сведений, составляющих коммерческую тайну;	1	21.03. 2017	29.03. 2017	22.03. 2017	30.03. 2017
2.4	Внесение изменений в должностные инструкции.	2	22.03. 2017	30.03. 2017	24.03. 2017	1.04.2 017
2.5	Согласование и утверждение организационно – распоряди-	1	24.03. 2017	1.04.2 017	25.03. 2017	02.04. 2017

	тельных документов					
3	Подготовка реализации проекта созданию КСЗИ	2	25.03.2017	02.04.2017	27.03.2017	04.04.2017
3.1	Определение ответственных лиц и исполнителей проекта;	1	25.03.2017	02.04.2017	26.03.2017	03.04.2017
3.2	Приобретение программно – аппаратного средства защиты от НСД;	1	25.03.2017	02.04.2017	26.03.2017	03.04.2017
3.3	Приобретение средства контроля и управления доступом;	1	26.03.2017	03.04.2017	27.03.2017	04.04.2017
3.4	Приобретение средств видеонаблюдения	1	26.03.2017	03.04.2017	27.03.2017	04.04.2017
4	Внедрение	3	27.03.2017	04.04.2017	30.03.2017	07.04.2017
4.1	Установка и настройка программно – аппаратного средства защиты от НСД;	1	27.03.2017	04.04.2017	28.03.2017	05.04.2017
4.2	Установка средства контроля и управления доступом;	1	28.03.2017	05.04.2017	29.03.2017	06.04.2017
4.3	Установка средств видеонаблюдения.	1	28.03.2017	05.04.2017	29.03.2017	06.04.2017
4.4	Контроль защищенности	1	29.03.2017	06.04.2017	30.03.2017	07.04.2017
4.5	Обучение персонала	1	29.03.2017	06.04.2017	30.03.2017	07.04.2017

ПРИЛОЖЕНИЕ И

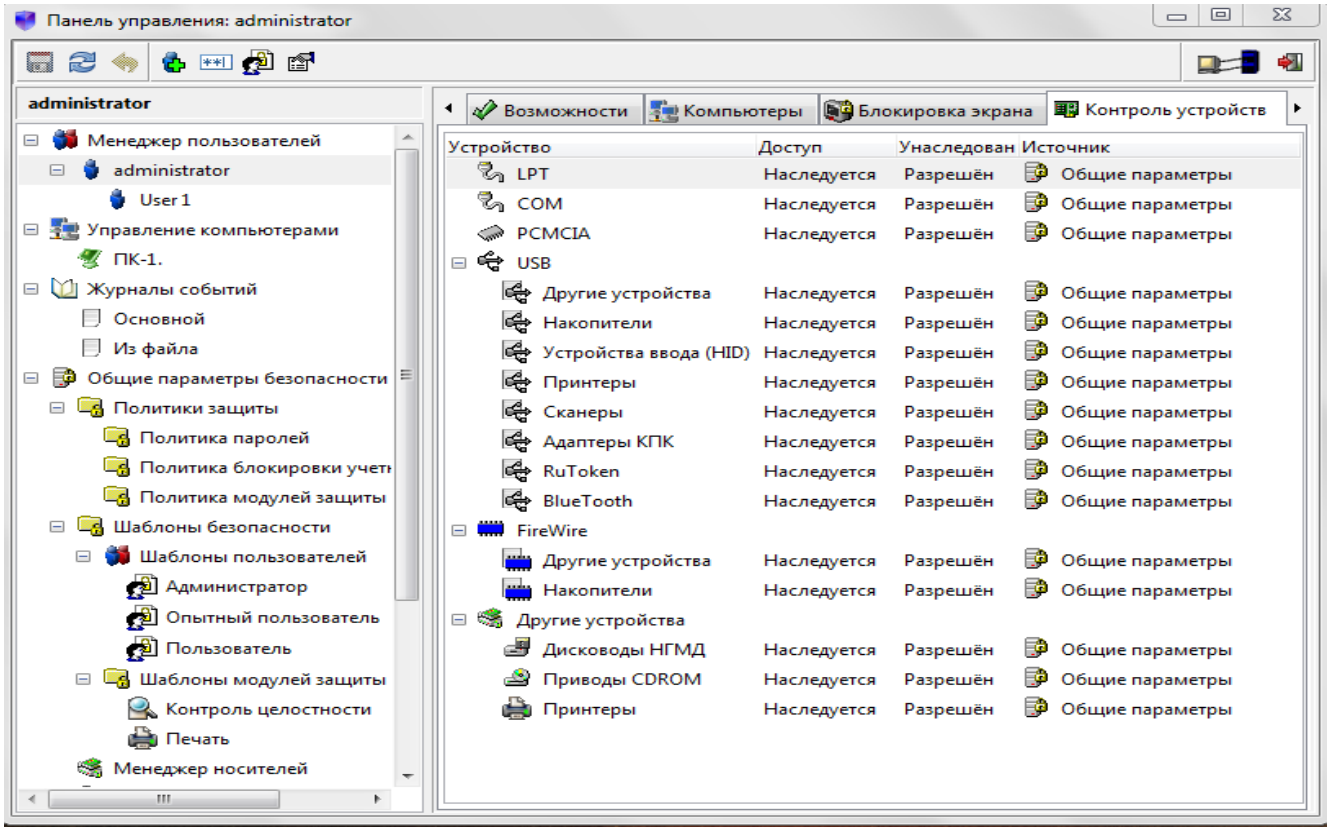

Рисунок И 1 – Доступ к устройствам для администратора

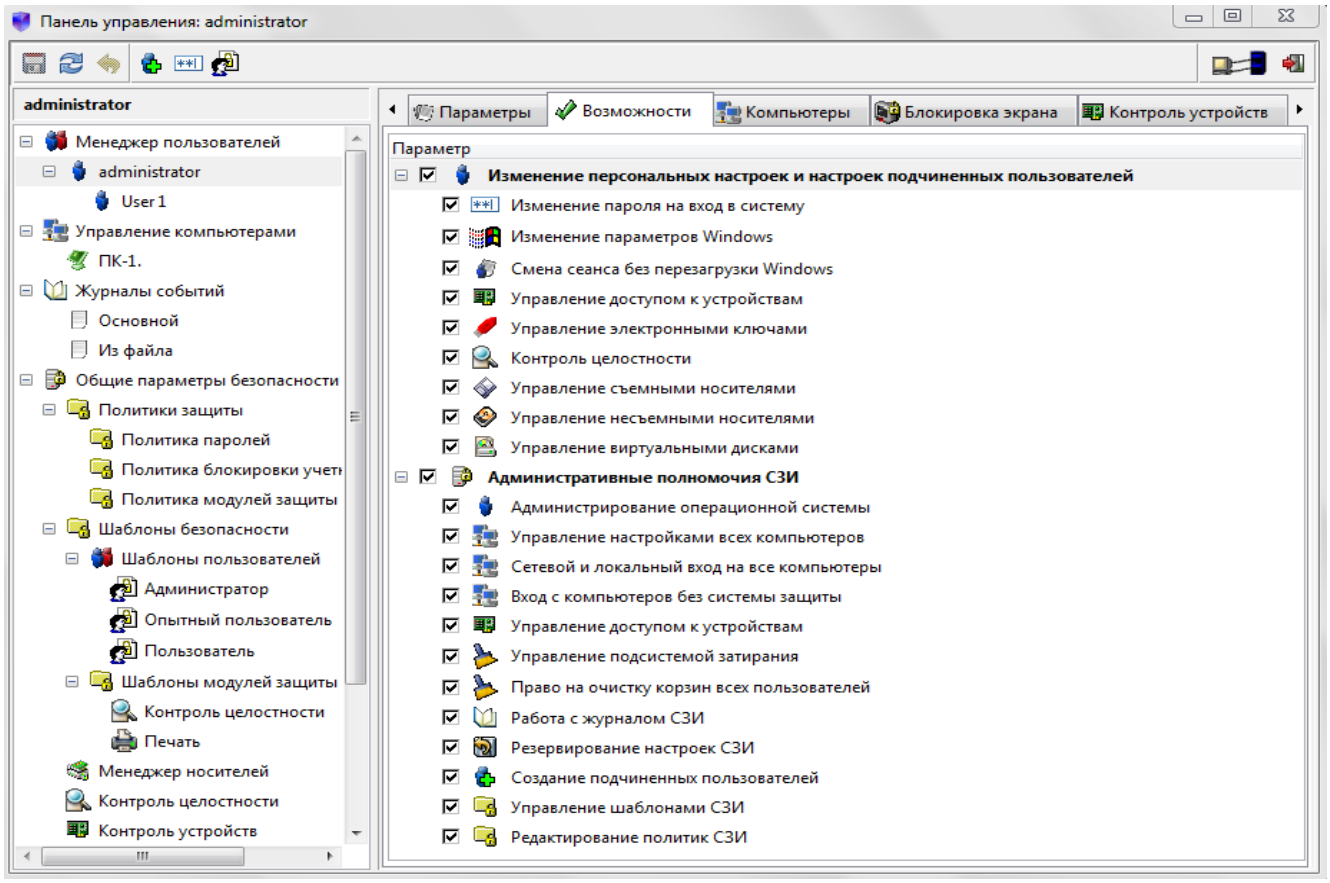

Рисунок И 2 – Параметры администратора

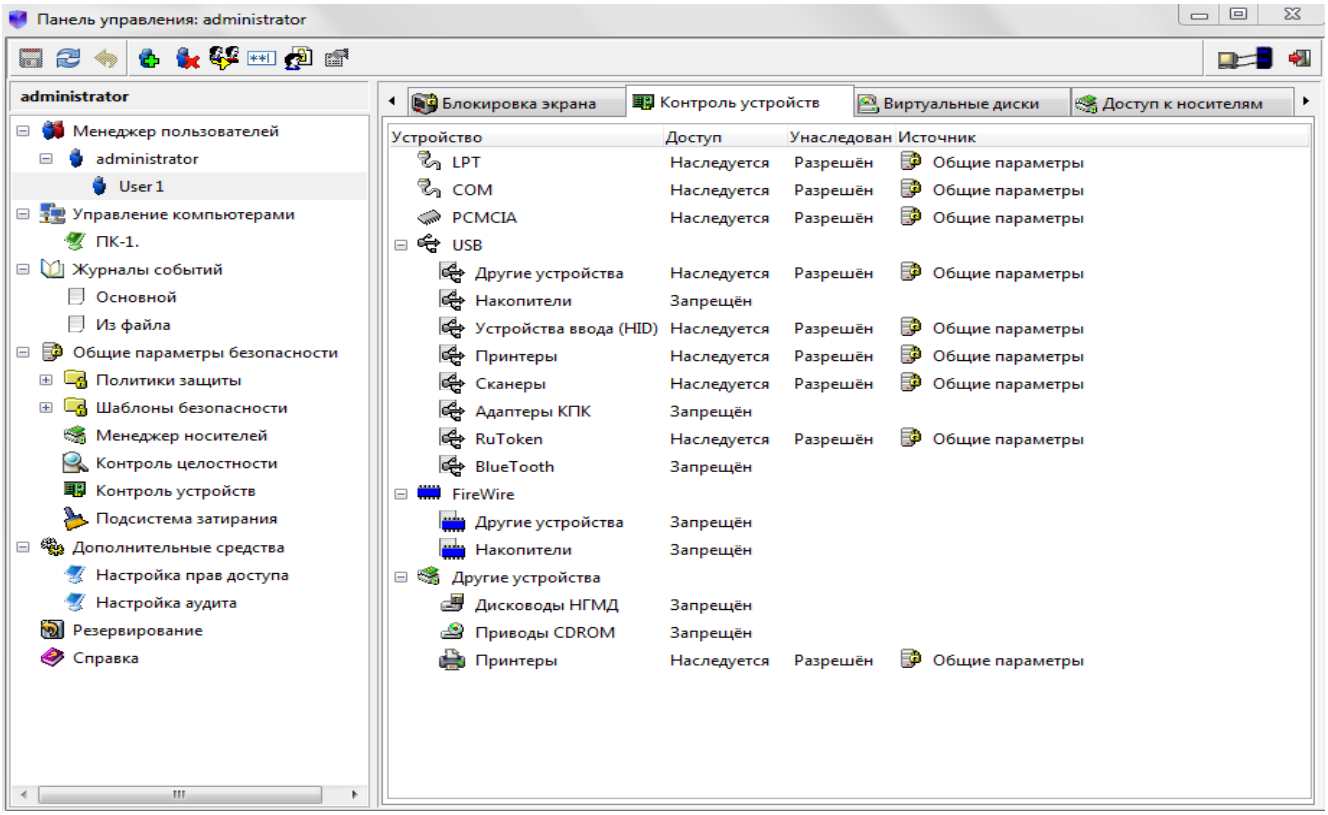

Рисунок И 3 – Доступ к устройствам для пользователя

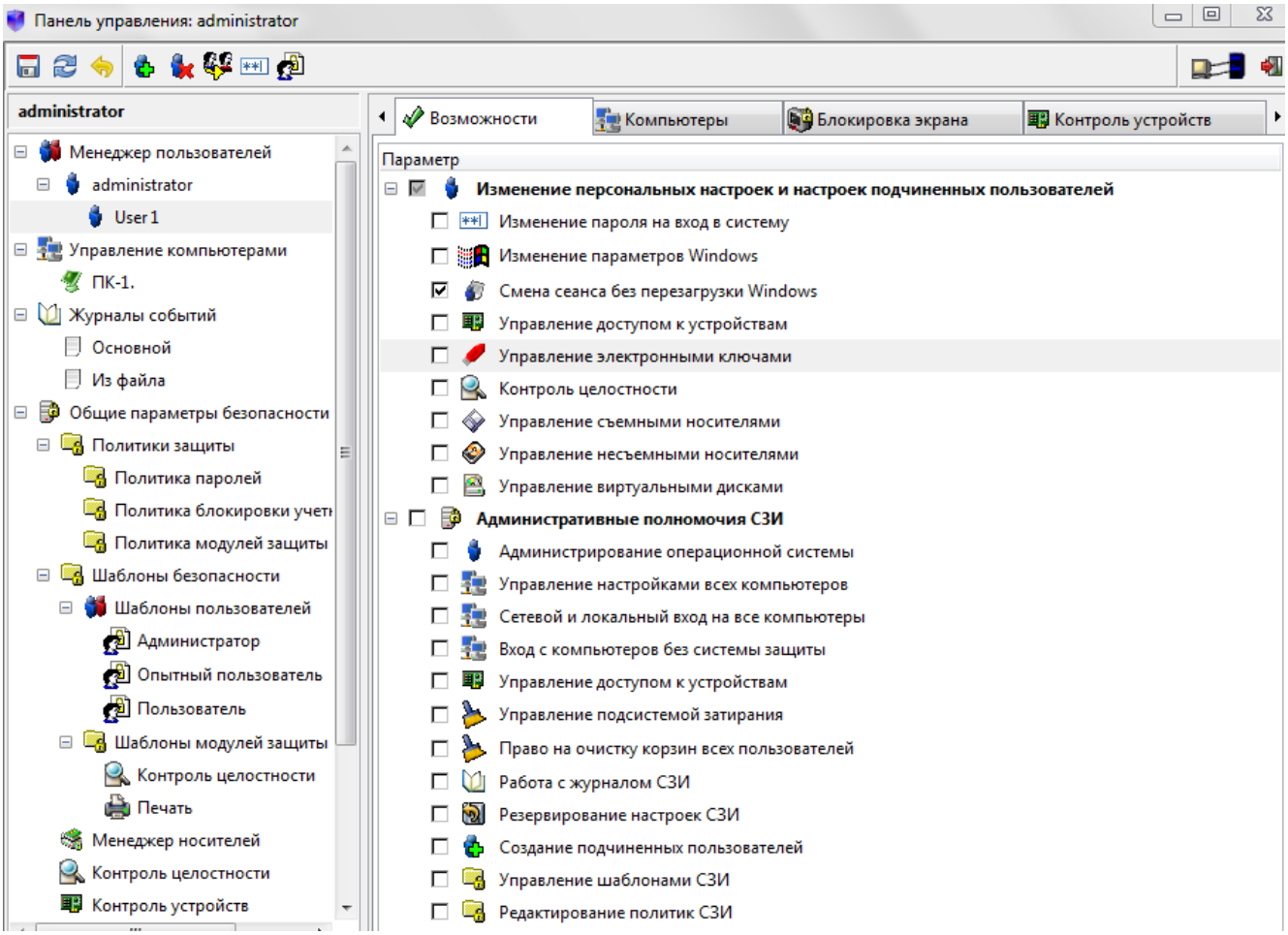

Рисунок И 4 – Параметры пользователя

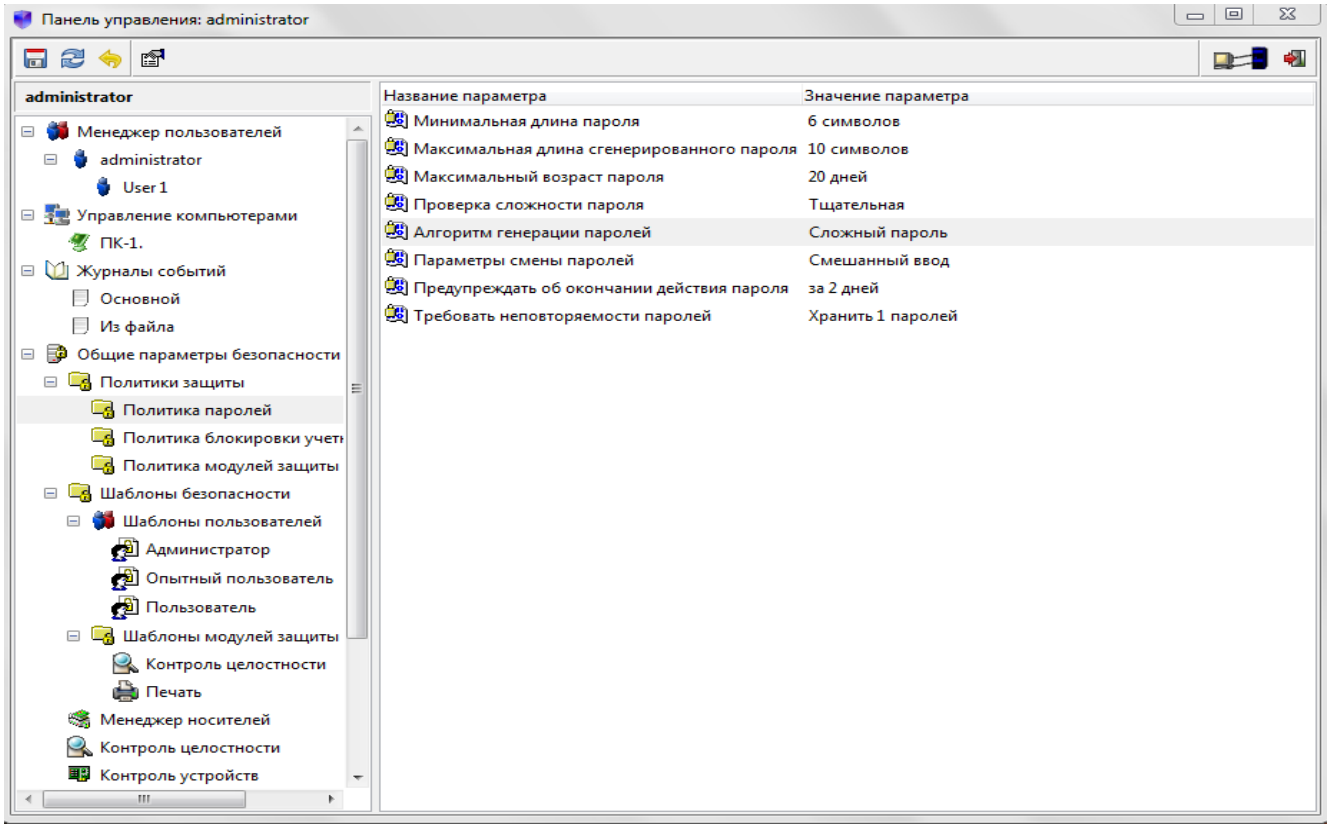

Рисунок И 5 – Политика паролей

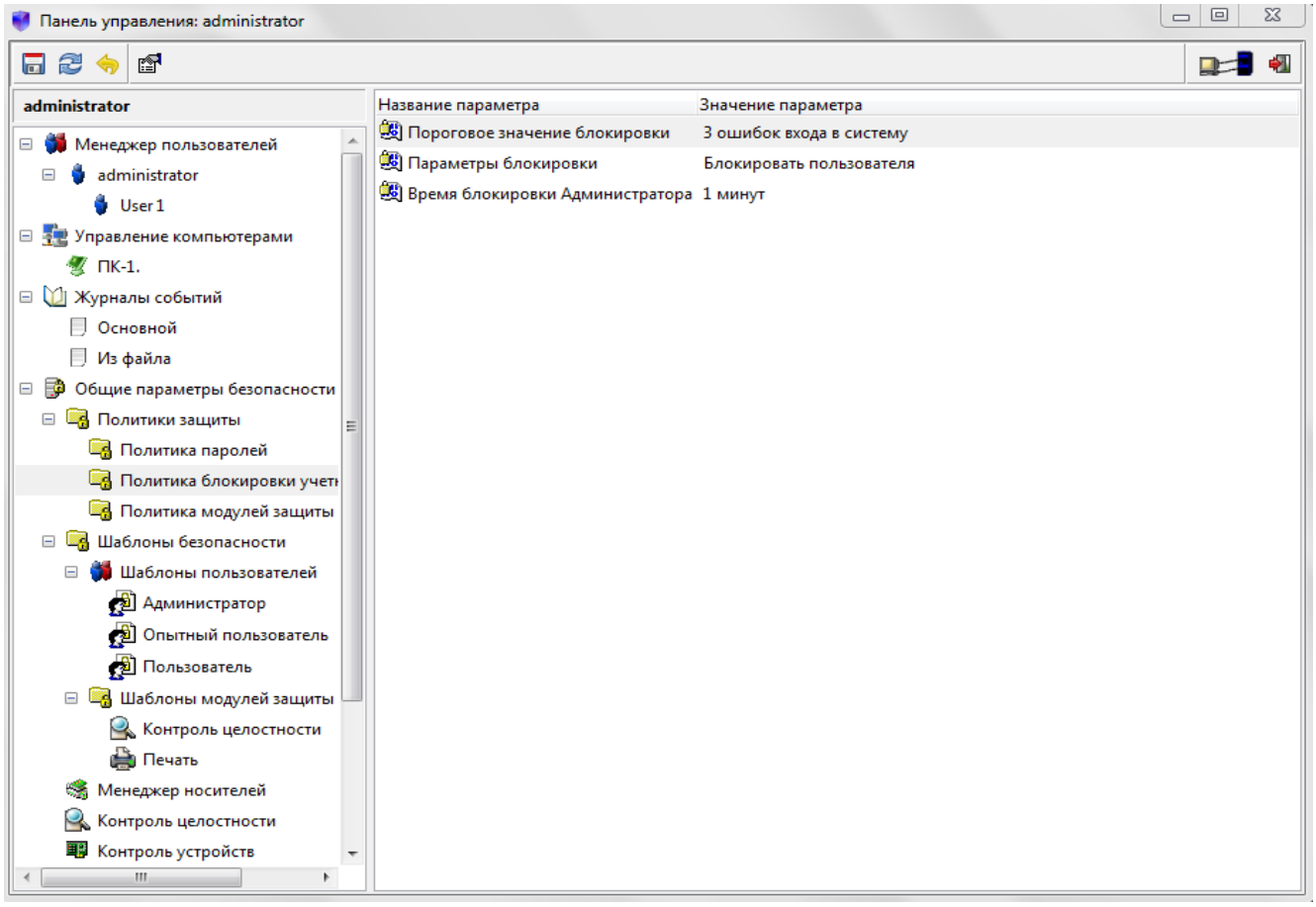

Рисунок И 6 – Политика блокировки учетной записи

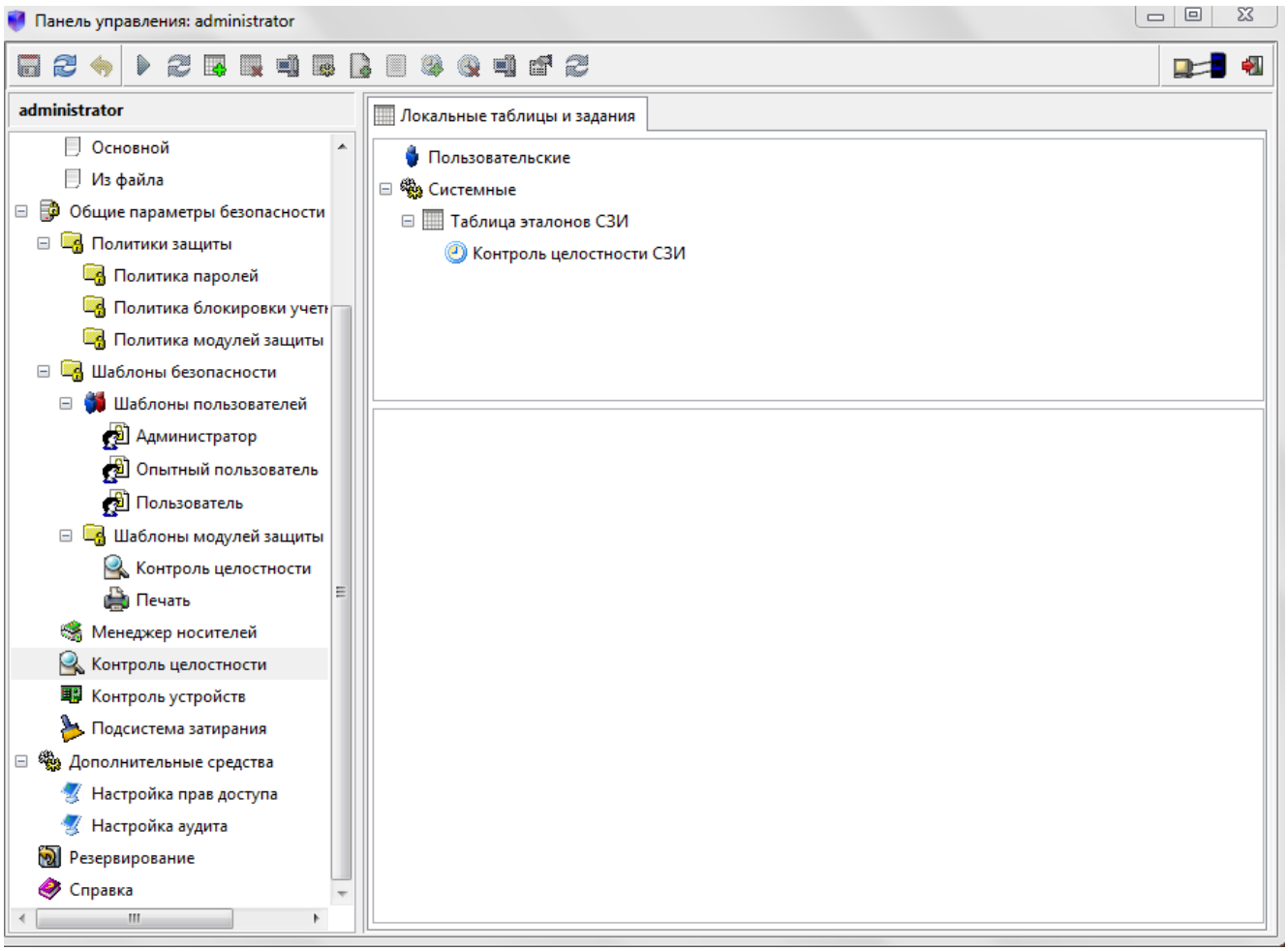

Рисунок И 7 – Контроль целостности