Тема 6. Организация службы защиты информации (СЗИ)

1. Организационное проектирование СлЗИ

2. Определение организационной структуры СлЗИ

3. Определение численного состава СлЗИ

4. Организация информационного обеспечения СлЗИ

5. Определение взаимодействия службы с другими структурными подразделениями предприятия

6. Экономическая обоснованность организационного проектирования службы

7. Структура СлЗИ. Руководитель службы защиты информации. Сотрудники службы защиты информации. Должностные инструкции

Основной задачей службы информационной безопасности является определение направления развития и поддержки усилий организации, направленных на защиту информации от несанкционированного ознакомления, изменения, разрушения или отказа в доступе. Это достигается путем внедрения соответствующих правил, инструкций и указаний

6.1. Организационное проектирование СлЗИ

Организационное проектирование — это комплекс работ по созданию службы, формированию структуры и системы управления, обеспечению ее деятельности всем необходимым.

Целью организационного проектирования является обеспечение высокого уровня организованности деятельности службы.

Этапы организационного проектирования СлЗИ:

- анализ рисков и структуризация проблем;
- определение организационной структуры службы;
- определение необходимого персонала и его подбор
- организация информационного обеспечения службы;
- определение взаимодействия службы с другими структурными подразделениями фирмы;
- экономическая обоснованность проектируемой службы.

Анализ рисков и структуризация проблем

Этапы анализа рисков на предприятии:

1 этап - определяются сведения, представляющие для предприятия какую-либо ценность, которые предстоит защищать

2 этап – построение схем каналов доступа, утечки или воздействия на информационные ресурсы

3 этап - анализ способов защиты всех возможных точек атак, соответствующих целям защиты

4 этап - определение вероятности реализации угроз по каждой из возможных точек атак

5 этап - оценка ущерба предприятию в случае реализации каждой из атак

Методики оценки угроз и уязвимостей

Для оценки угроз и уязвимостей используются различные методы, в основе которых лежат:

- экспертные оценки;
- статистические данные;
- учет факторов, влияющих на уровни угроз и уязвимостей.

Методика 1 – накопление статистических данных о реально случившихся происшествиях, анализ и классификация их причин, выявление факторов, от которых они зависят. На основе этой информации можно оценить угрозы и уязвимости в других информационных системах.

Методика 2 – учет различных факторов, влияющих на уровни угроз и уязвимостей.

Измерение рисков

Оценка рисков по двум факторам

Фактор 1 - вероятность происшествия
Фактор 2 - тяжесть возможных последствий.

$$U = Рпр. * V$$

где:
U – риск,
Рпр. – вероятность что событие произойдет, %;
V – стоимость потери.

Переменные выражения являются качественными величинами, поэтому рассмотрим вариант использования качественных величин

Ситуация / действие		Negligible	Minor	Moderate	Serious	Critical
		Воздействием можно пренебречь	Незначительное происшествие	Происшествие с умеренными результатами	Происшествие с серьезными последствиями	Происшествие приводит к критическим последствиям
A	Событие практически никогда не происходит	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
B	Событие случается редко	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
C	Вероятность события около 0.5	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
D	Скорее всего, событие произойдет	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
E	Событие почти обязательно произойдет	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

Оценка рисков по трем факторам

Фактор 1 - угроза,
Фактор 2 - уязвимость,
Фактор 3 - цена потери

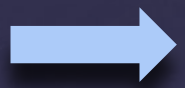
Угроза — **совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.**

Уязвимость — **слабость в системе защиты, которая делает возможным реализацию угрозы.**

$$Рпр. = Руг. * Руязв.$$

где:
Рпр. – вероятность что событие произойдет, %;
Руг. – вероятность угрозы, %;
Руязв.- вероятность уязвимости, %.

Рпр. = Руг. * Руязв.



U = Рпр. * V

U = Руг. * Руязв. * V

Где:
Рпр – вероятность что событие произойдет, %;
Ру – вероятность угрозы, %;
Руязв- вероятность уязвимости, %.

Выбор допустимого уровня риска

- Первый подход - базовый уровень безопасности
- Второй подход - повышенный уровень безопасности

Определение каналов утечки

- предмет защиты (охраняемая информация)
- источник информации (носители информации, ПЭМИН и т. п.)
- место «циркуляции» информации (сл. Кабинеты, переговорные и т.п.)

Возможные каналы утечки информации

Построение модели нарушителя

По глобальному признаку модели нарушителя ранжируются на:

- внешних (категория А)
- внутренних (категория В)

По технической оснащенности и используемым методам и средствам нарушители подразделяются на:

- применяющих пассивные средства (средства перехвата без модификации компонентов системы);
- использующих только штатные средства и недостатки системы защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств);
- применяющих методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

Оценка тяжести ущерба

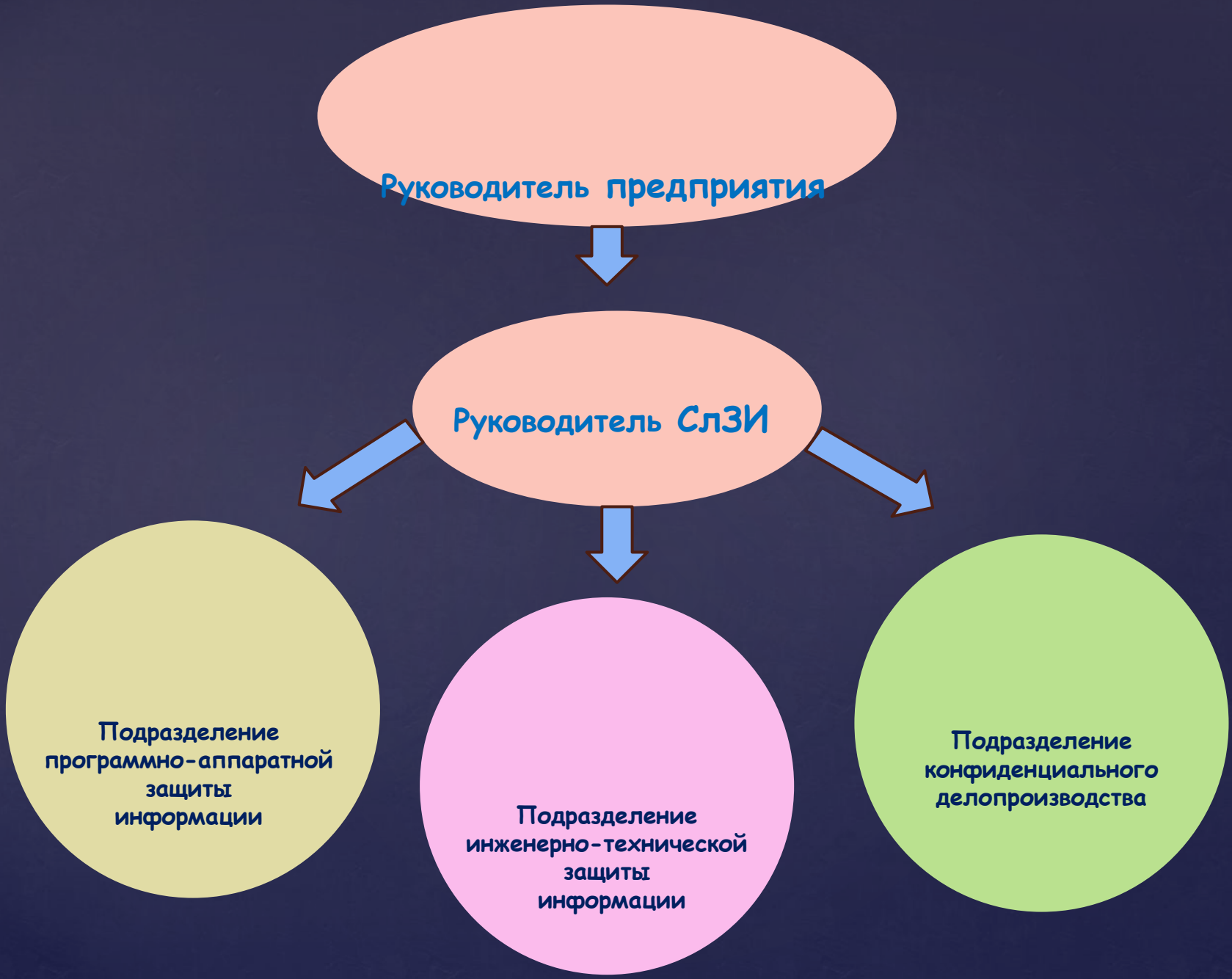
При оценке тяжести ущерба необходимо учитывать:

- непосредственные расходы на замену оборудования, анализ и исследование причин и величины ущерба, восстановление информации и функций АС по ее обработке;
- косвенные потери, связанные со снижением банковского доверия, потерей клиентуры, подрывом репутации, ослаблением позиций на рынке.

6.2. Определение организационной структуры СлЗИ

СлЗИ представляет собой штатное или нештатное подразделение, создаваемой для организации квалифицированной разработки системы ЗИ и обеспечении ее функционирования.

СлЗИ является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю фирмы.


Руководитель предприятия
Руководитель СлЗИ
Подразделение программно-аппаратной защиты информации
Подразделение инженерно-технической защиты информации
Подразделение конфиденциального делопроизводства

Задачи службы защиты информации

- обеспечение безопасности деятельности предприятия и защиты информации и сведений, являющихся коммерческой тайной;
- организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;
- организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;
- предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;
- выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;
- обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством, как на национальном, так и на международном уровне;
- обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;
- обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
- оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

Служба защиты информации отвечает:

- за разработку и издание правил (инструкций и указаний) по обеспечению безопасности, соответствующих общим правилам работы организации и требованиям к обработке информации;
- внедрение программы обеспечения безопасности, включая классификацию степени секретности информации (если таковая имеется) и оценку деятельности;
- разработку и обеспечение выполнения программы обучения и ознакомления с основами информационной безопасности в масштабах организации;
- разработку и сопровождение перечня минимальных требований к процедурам контроля за доступом ко всем компьютерным системам, независимо от их размера;
- отбор, внедрение, проверку и эксплуатацию соответствующих методик планирования восстановления работы для всех подразделений организации, принимающих участие в автоматизированной обработке самой важной информации;
- разработку и внедрение процедур пересмотра правил обеспечения информационной безопасности, а также рабочих программ, предназначенных для поддержки правил, инструкций, стандартов и указаний организации;
- участие в описании, конструировании, создании и приобретении систем в целях соблюдения правил безопасности при автоматизации производственных процессов;
- изучение, оценку, выбор и внедрение аппаратных и программных средств, функций и методик обеспечения информационной безопасности, применимых для компьютерных систем организации.

Функции службы защиты информации

- формирование требований к СЗИ в процессе создания автоматизированной системы;
- участие в проектировании системы защиты, ее испытаниях и приемки в эксплуатацию;
- планирование и организация, обеспечение функционирования системы ЗИ в процессе функционирования АС;
- распределение между пользователями необходимых реквизитов защиты (порядок доступа к системе, в помещение);
- наблюдение за функционированием СЗИ и ее элементов;
- организация проверок надежности функционирования системы защиты (соответствие параметров установленным требованиям, выяснение, сама служба делает или плановые проверки: нарушения, защита от атак, нанимается фирма для атак);
- обучение пользователей и персонала АС правилам безопасной обработки информации;
- контроль за соблюдением пользователями и персоналом АС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
- принятие мер при попытках НСД к информации и нарушение правил функционирования систем защиты.

Основные организационные вопросы принятой политики безопасности

- должностные обязанности групп пользователей;
- правила доступа (разграничения доступа) к информации;
- мероприятия по обеспечению контроля и функционирования системы защиты информации;
- меры реагирования на нарушение режима безопасности;
- планирование и организация восстановительных работ.

Права и обязанности службы по вопросам защиты информации на объекте

- численность службы должна быть достаточной для выполнения всех перечисленных выше функций;
- служба должна подчиняться тому лицу, которое в данном учреждении несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;
- штатный состав службы не должен иметь других обязанностей, связанных с функционированием АС;
- сотрудники службы должны иметь право доступа во все помещения, где установлена аппаратура АС и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;
- руководителю службы должно быть предоставлено право запрещать включение в число действующих новые элементы АС, если они не отвечают требованиям защиты информации;
- службе информационной безопасности должны быть обеспечены все условия, необходимые для выполнения своих функций.

Виды мероприятий выполняемых персоналом СлЗИ

- разовые – однократно проводимые и повторяемые только при полном пересмотре принятых решений;
- мероприятия, проводимые при осуществлении или возникновении изменений в самой СЗИ или в АС или внешней среде (мероприятия по необходимости);
- периодически проводимые мероприятия;
- постоянно проводимые мероприятия.

К разовым мероприятиям относятся:

- общесистемные мероприятия по созданию научно-технических и методологических основ защиты АС;
- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и др. объектов автоматизированной системы;
- мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка, сертификация технических и программных средств, документирования осуществляемых работ);
- проведение спецпроверок всех применяемых в АС средств, вычислительной техники и проведение мероприятия по защите информации от утечки по каналам побочных излучений и наводок (фильтры, зашумление);
- разработка и утверждение функциональных обязанностей должностных лиц;
- оформление юридических документов (договора, приказы, распоряжения) по вопросам регламентации отношений с пользователями/клиентами, работающими в автоматизированной системе, а также между участниками информационного обмена о правилах разрешение споров, связанных с применением ЭЦП;
- определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к системе (ее ресурсам);
- мероприятия по созданию системы защиты и созданию инфраструктуры;
- мероприятия по разработке правил управления доступом к ресурсам системы (каналы НСД, методы);
- организация надежного пропускного режима;
- определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации;
- определение порядка проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ на рабочих местах защищенной системы;
- создание отделов СлЗИ, которые осуществляют внедрение, контроль, эксплуатацию системы защиты;
- определение перечня необходимых, регулярно проводимых превентивных мер и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса АС в критических ситуациях, возникающих как следствие НСД, сбоев и отказов СВТ, ошибок в программах и персонала, стихийных бедствий.

К периодически проводимым мероприятиям относятся:

- определение реквизитов разграничения доступа (паролей, ключей шифрования);
- анализ системных журналов, принятие мер по обнаруженным нарушениям правил работы;
- мероприятия по пересмотру правил разграничения доступа пользователей к информации в организации;
- периодические с привлечением сторонних специалистов осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты, на основе полученной в результате такого анализа информации принимать необходимые меры по совершению системы защиты;
- мероприятия по пересмотру состава и построения СлЗИ.

Мероприятия, проводимые по необходимости:

- мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;
- мероприятия, осуществляемые при ремонте и модификации оборудования и программного обеспечения (строго санкционированные действия, документирование, контроль требований);
- мероприятия по подбору и расстановке кадров (проверка, ознакомление с инструкцией, правилами, последствиями нарушения требований).

Постоянно проводимые мероприятия:

- по обеспечению достаточного уровня защиты всех компонентов (пожар, охрана помещения, доступ, сохранность техники, носителей);
- по непрерывной поддержке функционирования и управления, используемыми программными средствами;
- явный и скрытый контроль за работой персонала системы;
- контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования АС.

Постоянно силами СлЗИ осуществляется анализ состояния и оценка эффективности мер и применяемых средств защиты.

6.3. Определение численного состава СлЗИ

Цель методики определения численного состава СлЗИ заключается в определении нормы времени на работы, выполняемые подразделениями СлЗИ, которые предназначены для нормирования и определения трудоемкости работ, выполняемых сотрудниками этих подразделений при организации защиты информации.

Нормы времени рекомендуются для определения необходимой численности сотрудников подразделений, разработки и корректировки их организационно-штатных структур.

Для достижения поставленной цели в методике решаются следующие задачи:

- Подготовка к проектированию нормативов и сбор исходных данных

- Анализ состояния нормирования труда, производство расчетов норм времени на работы, выполняемые СлЗИ.

При разработке методики были использованы следующие нормативные и методические материалы:

- Постановление Государственного комитета СССР по труду и социальным вопросам и президиума ВЦСПС от 19 июня 1986 г. № 226/П-6 "Об утверждении положения об организации нормирования труда в народном хозяйстве". М.: Экономика, 1987.
- Межотраслевые методические рекомендации по разработке нормативных материалов для нормирования труда в непроизводственных отраслях народного хозяйства. М: Экономика, НИИ труда Государственного комитета СССР по труду и социальным вопросам, 1988.
- Положение о порядке разработки нормативных материалов для нормирования труда. М.:, Государственный комитет Совета Министров СССР по вопросам труда и заработной платы и президиум ВЦСПС, 1968.
- Нормирование труда служащих. Методические указания. Издание второе исправленное. М.: НИИ труда Государственного комитета Совета Министров СССР по труду и социальным вопросам, 1976.
- Методические рекомендации по анализу качества норм. М.: НИИ труда Государственного комитета совета министров СССР по вопросам труда и заработной платы, 1969.
- Пашуто В.П. Организация и нормирование труда на предприятии: Учеб. пособие. – Мн.: Новое знание, 2001.
- Нормы времени на работы по документационному обеспечению управленческих структур федеральных органов исполнительной власти, утвержденные постановлением Министерства труда и социального развития Российской Федерации от 26 марта 2002 г. № 23.
- Межотраслевые типовые нормы времени на работы по сервисному обслуживанию персональных электронно-вычислительных машин и организационной техники и сопровождению программных средств, утвержденные постановлением Министерства труда и социального развития Российской Федерации от 23 июля 1998 г. № 28.
- Постановление Правительства РФ от 11 ноября 2002 г. N 804 "О Правилах разработки и утверждения типовых норм труда".

Расчет нормативной части

Нормирование труда — это вид деятельности по управлению производством, направленный на установление необходимых затрат и результатов труда, а также необходимых соотношений между численностью работников различных групп и количеством единиц оборудования.

Норма численности работников - это численность работников, необходимую для выполнения определенного объема работы.

Норма времени — это необходимые затраты времени одного работника или бригады (звена) на выполнение единицы работы (продукции). Она измеряется в человеко-минутах (человеко-часах).

Нормативная трудоемкость – это затраты рабочего времени на единицу продукции, установленные по действующим нормам времени, нормам обслуживания, штатным расписанием и т. п.

Предприятие составляет свои нормы времени исходя из методов определения и расчёта норм времени, а именно методами:

1. экспертных оценок,
2. моментных наблюдений,
3. хронометражных измерений.

Произведём расчёт численности работников, осуществляющих ежемесячное обслуживание средств вычислительной и оргтехники учитывая что на предприятии имеется 10 комплектов средств вычислительной и оргтехники:

Исходные данные для расчёта численности работников, осуществляющих ежемесячное обслуживание средств вычислительной и оргтехники учитывая что на предприятии имеется 10 комплектов средств вычислительной и оргтехники (пример):

№ норм	Наименование работы	Единица измерения	Норм. врем./ ед. ч.	Год-й объем	Норм-ая труд-ть, ч
1	Полное тестирование всех устройств ПЭВМ с выдачей протокола, в том числе и ЛВС	1 ПЭВМ	1,70	120	204
2	Поставка обновленных антивирусных программ и полная проверка дисковой памяти на наличие вирусов	1 ПЭВМ	0,48	120	57,6
3	Очистка от пыли внутренних объемов ПЭВМ с разборкой	1 ПЭВМ	0,37	120	44,4
4	Очистка от пыли и грязи видеомониторов и LSD панелей	1 монитор	0,35	120	42
5	Очистка от использованного тонера элементов печати лазерных принтеров, заправка тонера	1 принтер	0,34	120	40,8
6	Очистка от пыли и промывка считывающего элемента в сканерах и смазка механических частей	1 сканер	0,28	120	33,6
7	Очистка от использованного тонера элементов печати ксероксов, заправка тонера	1 копир	0,31	120	27,2
8	Очистка от пыли и промывка считывающего элемента в ксероксах и смазка механических частей	1 копир	0,20	12	24
9	Очистка узлов и промывка печатающей головки аппарата для факсимильной связи	1 аппарат	0,15	120	18
10	Очистка и промывка оптических узлов и их юстировка, удаление пыли из внутренних объемов проекторов	1 проектор	0,40	120	48
Трудоемкость, итого					521,6

Суммарная годовая трудоемкость работ по осуществлению ежемесячного обслуживания средств вычислительной и оргтехники составит:

$$T_{\Sigma} = T_{норм} * K_{попр}$$

$$T_{\Sigma} = 1{,}15 \times 521{,}6 = 599{,}84 \text{ ч.}$$

Полезный фонд рабочего времени $Ф_п$ одного сотрудника расчитывается по формуле и будет составлять:

$$Ф_п = Ф_о * K_{отп} * K_п$$

$$Ф_п = 2000 \times 0{,}9 \times 0{,}9 = 1620 \text{ ч.}$$

где:

- $Ф_о$ – общий фонд рабочего времени одного сотрудника за год, определяемый как рабочее время в рабочие дни года (в среднем равен 2000 час.)
- $K_{отп}$ – поправочный коэффициент, учитывающий отпуска сотрудников, составляет 0,9.
- $K_п$ - поправочный коэффициент, (болезнь, командировки, работа в комиссиях, повышение квалификации и иные отвлечения от выполнения работ), составляет 0,9.

Необходимая численность сотрудников ($N_{сотр.}$) будет составлять:

$$N_{сотр.} = T_{\Sigma} / Ф_{п}$$

$$N_{сотр.} = 599,84 / 1620 = 0,37 \text{ чел.}$$

Таким образом, для осуществления ежемесячного обслуживания 10 комплектов средств вычислительной и оргтехники по выполняемым функциям указанным в табл. вполне достаточно одного работника на 0,4 ставки