

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение высшего
образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет информационных
технологий и электроники

Специальность 10.05.03 –

Специализация -

Кафедра
«Информационная безопасность
систем и технологий»

Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

Модель автоматизированного рабочего места для обработки конфиденциальной
информации на основе отечественных комплектующих и программного
обеспечения

Студент

Водянов Владислав Олегович

Руководитель

Яшин Е.В.

Нормоконтролёр

Иванов А.П.

Рецензент инженер 1 категории АО "НПП "Рубин"

Евстигнеев С.А.

Работа допущена к защите (протокол заседания кафедры от 16.06.23 № 10)

Заведующий кафедрой

С.Л. Зефилов

Работа защищена с отметкой
от 28.06.23 № 13

хорошо

(протокол заседания ГЭК

Секретарь ГЭК

А.П. Иванов

Пенза 2023

*Подпись руководителя практики
Специалист 1 категории*



*Пробирка прошена
9.06.23*

Оглавление

Введение	4
1 Нормативно-правовая база в области конфиденциальной информации	6
2 Разработка схемы автоматизированного рабочего места для обработки конфиденциальной информации	10
3 Определение технических каналов утечки информации для автоматизированного рабочего места обрабатывающего конфиденциальную информацию.	11
4 Классификация автоматизированного рабочего места по требованиям защиты информации.....	17
5 Определение актуальных угроз безопасности информации, обрабатываемой на автоматизированном рабочем месте	20
6.1 Принципы разработки модели угроз.....	22
6.2 Описание АРМ.....	22
6.3 Определение пользователей АРМ	23
7 Определение требования к системе защиты информации, обрабатываемой автоматизированным рабочим местом	36
8 Сравнительный анализ и выбор комплектующих автоматизированного рабочего места, обрабатывающего конфиденциальную информацию.....	40
9 Сравнительный анализ и выбор программного обеспечения автоматизированного рабочего места, обрабатывающего конфиденциальную информацию	47

10 Сравнительный анализ и выбор программно-аппаратных средств защиты для автоматизированного рабочего места, обрабатывающего конфиденциальную информацию	51
11 Модель автоматизированного рабочего места для обработки конфиденциальной информации	61
12 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	63
Заключение	67
Список использованных источников	68

Введение

Современное информационное общество требует надежной защиты конфиденциальной информации, которая является ключевым активом многих организаций. С учетом развития информационных технологий и растущих угроз безопасности, разработка модели автоматизированного рабочего места, обеспечивающего безопасную обработку конфиденциальной информации, является актуальной задачей.

Целью данного дипломного проекта является разработка модели автоматизированного рабочего места для обработки конфиденциальной информации на основе отечественных комплектующих и программного обеспечения. Это позволит организациям иметь надежную и безопасную систему для работы с чувствительными данными, минимизируя риски утечки или неразрешенного доступа.

В ходе работы над проектом будут анализированы требования безопасности и уровня конфиденциальности информации, которая будет обрабатываться на данном рабочем месте. Также будет выполнена оценка отечественных комплектующих и программного обеспечения с точки зрения их соответствия требованиям безопасности.

Важным аспектом проекта является учет использования отечественных комплектующих и программного обеспечения. Это позволяет не только обеспечить безопасность информации, но и поддерживать отечественную технологическую базу и развитие отечественных производителей.

Предполагается, что разработанная модель автоматизированного рабочего места будет включать в себя такие аспекты, как защита от неразрешенного доступа, шифрование данных, системы контроля доступа, антивирусную защиту, мониторинг и аудит безопасности. Будут рассмотрены возможности применения современных технологий, таких как использование средств идентификации и аутентификации.

Результатом данного дипломного проекта будет разработанная модель автоматизированного рабочего места, которая удовлетворяет требованиям безопасности и способствует эффективной и безопасной обработке конфиденциальной информации.

Разработка такой модели имеет значимость как для организаций, работающих с конфиденциальными данными, так и для национального информационного пространства в целом, поскольку обеспечение безопасности и защиты отечественных данных становится все более важным аспектом в современном мире.

1 Нормативно-правовая база в области конфиденциальной информации

Нормативно-правовая база в области конфиденциальной информации является базой для обеспечения безопасности информации на организациях. В Российской Федерации главными из основных законодательных актов, регулирующих вопросы защиты конфиденциальной информации, являются:

1. Федеральный закон "О государственной тайне" от 21 июля 1993 года № 5485-1 (с последующими изменениями и дополнениями);
2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года № 149-ФЗ (с последующими изменениями и дополнениями);
3. Федеральный закон "О персональных данных" от 27 июля 2006 года № 152-ФЗ (с последующими изменениями и дополнениями);
4. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 года № 51-ФЗ (с последующими изменениями и дополнениями);
5. Постановление Правительства РФ (Российской Федерации) от 01.11.2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
6. Федеральный закон "Об информации, ее защите и доступе к ней" от 27 июля 2006 года № 149-ФЗ (с последующими изменениями и дополнениями).
7. Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 года № 335 "Об утверждении Правил экспортного контроля криптографических средств защиты информации";
8. Федеральный закон "О государственной тайне" определяет порядок обращения с государственной тайной, включая правила ее классификации, рассекречивания и хранения.

Закон устанавливает требования к порядку определения государственной тайны, ее хранения, использования и распространения. Также он определяет круг

лиц, которые имеют право на доступ к государственной тайне, а также требования к их проверке и обучению.

Кроме того, закон "О государственной тайне" устанавливает ответственность за нарушение порядка создания, использования и защиты государственной тайны. Нарушение порядка хранения и использования государственной тайны может привести к административной, гражданской или уголовной ответственности в зависимости от характера нарушения.

9. Федеральный закон "Об информации, информационных технологиях и о защите информации" определяет правовые основы организации и функционирования системы защиты информации, в том числе правила использования информационных технологий и услуг в целях обеспечения безопасности информации.

Закон определяет три уровня конфиденциальности информации: общего, ограниченного и секретного. При этом для каждого уровня устанавливаются соответствующие требования к защите информации.

Закон также определяет основные понятия и термины, связанные с защитой информации, такие как "криптографические средства защиты информации", "лицензия на разработку и производство криптографических средств защиты информации" и др.

10. Федеральный закон "О персональных данных" от 27 июля 2006 года № 152-ФЗ (с последующими изменениями и дополнениями).

Закон устанавливает правила анализа персональных данных, которые включают в себя любую информацию, относящуюся к определенному или определяемому физическому лицу. Данный закон определяет порядок сбора, использования, хранения, обработки и передачи персональных данных, а также права субъектов персональных данных.

Основной целью закона является обеспечение права на конфиденциальность и защиту персональных данных граждан Российской Федерации. Закон также определяет требования к обеспечению безопасности персональных дан-

ных, в том числе к использованию технических и организационных мер защиты информации.

11. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 года № 51-ФЗ (с последующими изменениями и дополнениями).

Гражданский кодекс устанавливает правовые основы гражданского оборота и определяет порядок защиты прав и интересов граждан и организаций в сфере обработки и защиты информации. В частности, Гражданский кодекс содержит нормы, определяющие правила использования информации и защиты информационных прав.

Согласно статье 152.1 Гражданского кодекса, владелец информации имеет право на ее защиту от незаконного использования, а также на возмещение убытков, причиненных в результате нарушения прав на информацию.

Кроме того, Гражданский кодекс устанавливает правила ответственности за нарушение прав на информацию, включая права на конфиденциальность и тайну переписки.

12. Постановление Правительства РФ от 01.11.2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Постановление устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных. В нем определяются правила обеспечения безопасности персональных данных

13. Федеральный закон "Об информации, ее защите и доступе к ней" от 27 июля 2006 года № 149-ФЗ (с последующими изменениями и дополнениями).

Закон устанавливает правила доступа к информации, а также порядок ее защиты. Он определяет правила обработки информации, включая ее сбор, хранение и распространение.

Закон также определяет права и обязанности субъектов информационных отношений, а также правила обращения с конфиденциальной информацией.

14. Приказ Федеральной службы по техническому и экспортному кон-

тролю от 14 марта 2014 года № 335 "Об утверждении Правил экспортного контроля криптографических средств защиты информации".

Приказ устанавливает правила экспортного контроля криптографических средств защиты, которые используются для защиты информации в электронном виде.

Правила экспортного контроля криптографических средств защиты информации устанавливают требования к процедуре экспорта криптографических средств защиты информации, включая процедуру получения разрешительной документации на экспорт.

Эти правила также содержат перечень криптографических средств защиты информации, экспорт которых запрещен в соответствии с законодательством РФ.

Нормативно-правовая база в области конфиденциальной информации включает законы, постановления Правительства РФ и другие правовые акты, которые регулируют обработку, хранение и защиту информации в России.

Эта база является необходимой для обеспечения безопасности информации и защиты прав на ее использование. Специалисты по информационной безопасности должны иметь хорошее знание этих нормативно-правовых актов, чтобы грамотно выполнять свои задачи и защищать конфиденциальную информацию от неразрешенного доступа и использования.

2 Разработка схемы автоматизированного рабочего места для обработки конфиденциальной информации

Перед разработкой модели автоматизированного рабочего места, нужно создать схему разрабатываемого в последующем автоматизированного рабочего места.

В нашем автоматизированном рабочем месте будет использоваться не только системный блок, но также устройства ввода и вывода, такие как: клавиатура, устройство ввода типа «мышь», принтер, монитор, ИБП.

На рисунке 2.1 показана схема автоматизированного рабочего места, которое будет спроектировано.

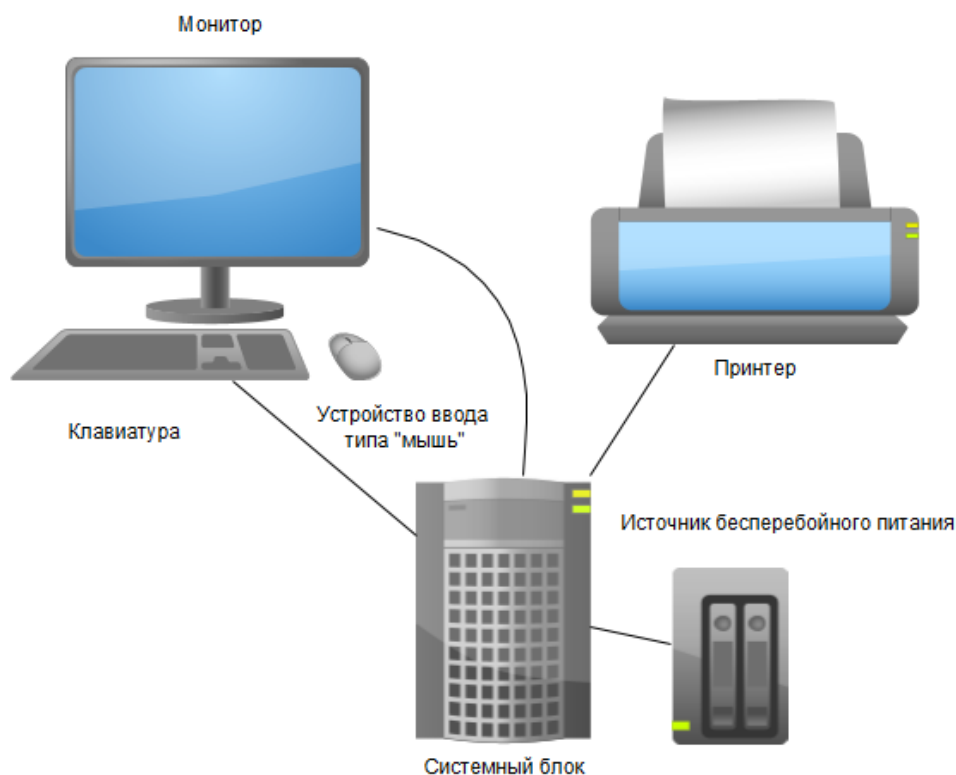


Рисунок 2.1 – Схема автоматизированного рабочего места

3 Определение технических каналов утечки информации для автоматизированного рабочего места обрабатывающего конфиденциальную информацию.

Нарушение конфиденциальности информации на съёмных носителях может привести к её неправомерной передаче лицами, не имеющим на это права. Это явление называется утечкой информации. Утечка информации схожа с потоком жидкости или газа, но имеет свои особенности. Она описывает процесс незаконного перемещения информации от источника к злоумышленникам.

- утечка информации происходит только при передаче её лицами, не имеющим авторизованного доступа к ней;

- утечка информации включает в себя распространение информации без изменения её характеристик, что приводит к снижению её стоимости в результате повсеместного распространения.

- обнаружение факта утечки информации обычно происходит с опозданием, часто после того, как стали очевидны её последствия. В таких случаях принимаемые меры по обеспечению безопасности могут оказаться неэффективными;

При передаче информации через технический канал, если это канал утечки или функциональный канал, требуется наличие нескольких базовых компонентов: источника сигнала, среды распространения и приемника. Общая структура канала передачи информации приведена на рисунке 3.1.



Рисунок 3.1 - Структура канала передачи информации.

Информация поступает на вход канала в виде первичного сигнала. Этот сигнал является источником информации, содержащей данные от источника или с предыдущего канала. Источником сигнала может быть:

- предмет, который показывает акустические и электромагнитные колебания;
- предметом является объект, который испускает собственные электромагнитные волны;
- устройство, ответственное за передачу информации по функциональному каналу связи;
- закладное устройство;
- источник сигнала, представляющего опасность;
- источник звуковых волн, на которых носится информация;

На данной иллюстрации представлены стрелки, которые обозначают направление потока информации. Эти пути связаны с первичными сигналами, содержащими информацию, которую источник информации передает на своем собственном языке в форме знаков, символов, сигналов или звуков. Передатчик выполняет задачу преобразования этой формы информации в такую, которая может записаться на другой источник информации и соответствующей среде. Помимо этого, передатчик выполняет следующие функции:

- генерирует электрический ток или поля, которые переносят информацию;
- управляет процессом записи информации на носитель;

- усиливает мощность сигнала;

- определяет передачу сигнала в среду распространения в определенном пространственном секторе.

Различные термины и типы источников конфиденциальной информации. Источники, которые являются хранилищами важной и ограниченной информации, представляют собой совокупность источников этой информации. Основными категориями конфиденциальной информации являются люди, сотрудники, связанные с организацией, документы, материалы, связанные с разработками компании, рекламные и выставочные материалы, а также физические поля, волны и излучения.

Существуют следующие виды конфиденциальной информации:

- служебная, научно-техническая и технологическая информация организации, включая публикации, такие как книги, статьи и доклады, созданные сотрудниками организации;
- информация о делах организации
- правовая, учредительная, организационная и распорядительная документация;
- записи о работе, служебные дневники и личные планы сотрудников, а также коммерческая и научная переписка;
- архивы личного сотрудников.

К научно-технической и технологической информации можно отнести данные о моделях устройств, схемах машин, устройствах и компонентах, используемых средствах, их внутренней структуре, методах и способах создания, актуальных устройствах, изменениях в реальных машинах и аппаратуре, а также актуальных методах и путях из изменения. Также в эту категорию входят пакеты прикладных программ для ЭВМ.

Данные, являющиеся основой для реализации прибыльной продукции орга-

низации, могут быть неоднократно украдены врагами данной компании. Организация этой документации осложняется из-за её разбросанности по рабочим местам, отделам и зданиям, где готовится и хранится информация, используемая для создания продукции. Уровень риска утечки данных зависит от стоимости организации и контроля за обращением КТ (конфиденциальной информации), которая достигает рабочих мест в соответствии с установленным порядком внутри компании.

Описание информации о разработке актуальных устройств и изменениях существующих, отчеты о проводимых научно-исследовательских и опытно-конструкторских работах требуют постоянной защиты на всех этапах разработки, начиная с концепции и заканчивая созданием прототипа.

Важным источником информации могут быть деловые данные организации, включая информацию о финансовой деятельности, денежных отчетах, кредитах, платежеспособности, стратегических и тактических планах развития, разработке новых продуктов с использованием передовых технологий, анализе конкурентов и элементах, производительности, импорте и экспорте, способах продвижения продукции, маркетинговых методах, информации о высоких ценовых позициях и наличии на рынке.

К другим важным источникам информации относятся базы данных клиентов, посредников, конкурентов, содержащие данные о взаимоотношениях с ними и общих операциях

- кассету с записью текста документа, аудиозапись, записи заседаний;
- передачу или раскрытие содержания документа, ознакомление с которым осуществлялось авторизовано или конфиденциально;
- устное изложение текста документа по телефону, громкой связи, специальной радиосвязи;
- аналог документа, отправленного по факсу или электронной почте;
- визуальную или устную запись текста, выполненную с помощью раз-

ведывательной техники. Получение важных документов может быть случайным или продолжительным процессом, протекающим в течение длительного времени.

Информация, содержащаяся на каждом носителе, передается во внешнюю среду. Каналы передачи информации различаются по активности и включают в себя: управленческие, научные, деловые, коммерческие, регулируемые и коммуникационные связи, естественные технические каналы и информационные сети.

Канал передачи информации представляет собой путь перемещения важных сведений от одного носителя к другому в официальном режиме или в соответствии с объективными закономерностями.

Потеря ограниченного доступа к информационным ресурсам может произойти в следующих случаях

- при заинтересованности противника, компаний, лиц или фирм в определенной информации;
- при возникновении риска угрозы, созданной противником или случайно возникших обстоятельствах;
- при наличии условий, позволяющих противнику совершить необходимые действия и получить информацию.

Эти предпосылки могут включать:

- недостаток систематического контроля и аналитической работы по обнаружению и анализу угроз, каналов и степени риска нарушений безопасности информационных ресурсов;
- несовременную систему защиты информации или отсутствие данной системы;
- неудачно разработанную технологию обработки и хранения конфиденциальных документов;
- неправильный подбор сотрудников и перестановки кадров, неблагоприятные психологические условия в коллективе;

- отсутствие системы обучения персонала правилам защиты информации ограниченного доступа;
- непрофессиональный контроль со стороны руководства компании за выполнением персоналом условий нормативных документов по работе с информационными ресурсами ограниченного доступа;
- отсутствие режима пропуска в помещение фирмы.

Для данного автоматизированного рабочего места были выявлены технические каналы утечки информации, которые представлены в таблице 3.1.

Таблица 3.1 – Технические каналы утечки информации

№	Возможный канал утечки информации	Источник информации	Путь утечки информации
Первый	Оптический	Монитор	Открытые двери, окна, дефекты стен
Второй	Радиоэлектронный	Автоматизированное рабочее место(АРМ)	Окна, стены, пол, двери, оптоволоконные кабели, сети электропитания
Третий	Материально-вещественный	АРМ	Хищение носителей информации, порча оборудования.

4 Классификация автоматизированного рабочего места по требованиям защиты информации

Для данного автоматизированного рабочего места был определен класс обеспечения безопасности информации.

Каждый уровень характеризуется конкретным минимальным набором требований по безопасности.

Уровни разделены на три типа, которые отличаются в обработке информации в автоматизированной системе(АС).

В каждой категории соблюдается иерархия требований по безопасности, зависящая от значимости информации, и, соответственно, иерархия уровней безопасности АС.

Третья категория классифицирует АС, где функционирует один пользователь, имеющий доступ ко всей информации АС, хранящейся на носителях одного уровня конфиденциальности. В этой категории содержатся два уровня – 3А и 3Б.

Вторая категория классифицирует АС, где пользователи обладают одинаковыми правами доступа к информации АС, обрабатываемой и хранящейся на носителях разных уровней конфиденциальности.

Эта категория включает два уровня – 2А и 2Б.

Первая категория определяет АС, где сразу обрабатывается информация разных уровней конфиденциальности, и не все пользователи имеют доступ ко всей информации. В данной категории всего пять уровней – 1А, 1Б, 1В, 1Г, 1Д.

Требования по обеспечению безопасности автоматизированного рабочего места представлены в таблице 4.1.

В соответствии с этими требованиями был выбран уровень обеспечения безопасности 1Г.

Таблица 4.1 - Требования к защищенности АРМ

Подсистемы и требования	Классы								
	ЗБ	ЗА	2Б	2А	1Д	1Г	1В	1Б	1А
1.Подсистема управления доступом									
1.1 Идентификация, проверка подлинности и контроль доступа субъектов: в систему	+	+	+	+	+	+	+	+	+
К терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	+	-	+	+	+	+
К программам	-	-	-	+	-	+	+	+	+
К томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
1.2 Управление потоками информации	-	-	-	+	-	-	+	+	+
2.Подсистема регистрации и учета									
2.1 Регистрация и учет: входа/выхода субъектов доступа	+	+	+	+	+	+	+	+	+
Выдачи печатных выходных документов	-	+	-	+	-	+	+	+	+
Запуска/завершения программ и процессов	-	-	-	+	-	+	+	+	+
Доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи	-	-	-	+	-	+	+	+	+
Изменения полномочий субъектов доступа	-	-	-	-	-	+	+	+	+
Создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
2.2 Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3 Очистка освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+
2.4 Сигнализация попыток нарушения защиты	-	-	-	-	-	-	+	+	+
3.Криптографическая подсистема									
3.1 Шифрование конфиденциальной информации.	-	-	-	+	-	-	-	+	+
3.2 Шифрование информации, принадлежащей различным субъектам доступа на разных ключах	-	-	-	-	-	-	-	-	+
3.3 Использование аттестованных криптографических средств	-	-	-	+	-	-	-	+	+

Продолжение таблицы 4.1

Подсистемы и требования	Классы								
	ЗБ	3А	2Б	2А	1Д	1Г	1В	1Б	1А
4.Подсистема обеспечения целостности									
4.1 Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2 Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3 Наличие администратора информации в АС	-	-	-	+	-	-	+	+	+
4.4 Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5 Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6 Использование сертифицированных средств защиты	-	+	-	+	-	-	+	+	+

5 Определение актуальных угроз безопасности информации, обрабатываемой на автоматизированном рабочем месте

При работе с секретной информацией на автоматизированном рабочем месте, не имеющем доступа к сетям, можно применить определить следующие угрозы безопасности:

- потенциальные опасности раскрытия информации через технические каналы;
- угрозы нарушения нераспространения конфиденциальной информации, которая обрабатывается на АРМ;
- возможные риски утечки информации через технические каналы включают:
 - возможные опасности разглашения акустической информации;
 - возможные риски утечки видовой информации;
 - возможные угрозы передачи информации через канал ПЭМИН.

Возникновение опасности выдачи акустической информации, содержащейся прямо в произносимой речи пользователя ИСК конфиденциальной информации, возможно при наличии функций голосового ввода конфиденциальной информации или функций воспроизведения конфиденциальной информации акустическими средствами информационной системы конфиденциальной информации.

Реализация опасности утечки видовой информации возможна путем просмотра информации с использованием средств с дисплеем и других средств отображения ВТ, информационных ВТ, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав информационной системы КИ.

Опасности утечки информации по каналу ПЭМИН возможны из-за наличия излучений, дисплея и системного блока. Главным источником является угроза утечки из-за электромагнитных излучений дисплея.

Риски нарушения нераспространения конфиденциальной информации в автономном АРМ связаны с действиями врагов, имеющих доступ к информационной системе конфиденциальной информации, включая персонал ИС КИ, осуществляющих опасности непосредственно в ИС КИ. Кроме того, источниками рисков нарушения нераспространения информации в автоматизированном рабочем месте могут быть аппаратные подслушивающие разработки и съемные носители вирусного ПО.

В информационной системе конфиденциальной информации на основе автономного автоматизированного рабочего места могут быть все типы уязвимостей информационной системы конфиденциальной информации, кроме уязвимостей, связанных с выполнением сетевых протоколов и каналов ПД. В таких информационных системах КИ могут возникать:

- угрозы внедрения вирусных программ;
- угрозы, реализуемые после запуска операционной системы и направленные на несанкционированный доступ с использованием базовых операций к операционной системе или любой программе, с использованием программ для осуществления НСД
- угрозы осуществляемые в процессе запуска операционной системы , которые перехватывают идентификаторы и пароли.

6 Модель угроз для автоматизированного рабочего места.

Работы по разработке модели угроз безопасности КИ, при их анализе в автоматизированном рабочем месте с применением средств автоматизированного рабочего места.

6.1 Принципы разработки модели угроз

Разработка модели угроз должна базироваться на следующих принципах:

- безопасность конфиденциальной информации при их обработке в автоматизированном рабочем месте обеспечивается с помощью СЗИ;
- при формировании модели угроз необходимо учитывать, как угрозы, осуществление которых нарушает безопасность конфиденциальной информации так и угрозы, создающие условия для появления прямых угроз или косвенных угроз.

6.2 Описание АРМ

Описание АРМ производится на основании информации приведенной ниже. Данные по АРМ берутся из следующих документов:

- технический паспорт на АРМ;
- описание технологического процесса обработки информации в АРМ.

Основные характеристики АРМ представлены в таблице 6.1

Таблица 6.1 – Основные характеристики АРМ

Заданные характеристики безопасности персональных данных	Типовая информационная система / специальная информационная система
Структура информационной системы	Локальная информационная система
Подключение информационной системы к сетям общего пользования и / или сетям международного информационного обмена	Не имеется
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	Система с разграничением доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации

6.3 Определение пользователей АРМ

Необходимо составить матрицу доступа. Матрица доступа в табличной форме отражает права всех групп пользователей АРМ на действия с коммерческой тайной. Действия (операции) с коммерческой тайной, включают сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение конфиденциальной информации).

Составляется на основе перечня лиц, допущенных к работе на автоматизированном рабочем месте для обработки КИ (конфиденциальной информации).

Есть три основные группы пользователей:

- администраторы;
- разработчики;
- операторы.

Матрица доступа для АРМ представлена в таблице 6.2.

Таблица 6.2 - Матрица доступа

Типовая роль	Уровень доступа к конфиденциальной информации	Разрешенные действия
Администратор	<p>Обладает полной информацией о системном и прикладном программном обеспечении.</p> <p>Обладает полной информацией о технических средствах и конфигурации.</p> <p>Имеет доступ ко всем техническим средствам обработки информации и данным.</p> <p>Обладает правами конфигурирования и административной настройки технических средств.</p> <p>Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов.</p>	<p>Сбор</p> <p>Систематизация</p> <p>Накопление</p> <p>Хранение</p> <p>Уточнение</p> <p>Использование</p> <p>Распространение</p> <p>Обезличивание</p> <p>Блокирование</p> <p>Уничтожение</p>

Актуальной считается угроза, которая может быть реализована в АРМ и представляет опасность для конфиденциальной информации.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности АРМ и частота (вероятность) реализации рассматриваемой угрозы.

Продолжение таблицы 6.2

Типовая роль	Уровень доступа к конфиденциальной информации	Разрешенные действия
Разработчик	<p>Обладает информацией об алгоритмах и программах обработки информации на.</p> <p>Обладает правами внесения изменений в программное обеспечение на стадии ее разработки, внедрения и сопровождения.</p> <p>Располагает всей информацией о топологии и технических средствах обработки и защиты конфиденциальной информации, обрабатываемая в</p>	<p>систематизация</p> <p>накопление</p> <p>хранение</p> <p>уточнение</p> <p>обезличивание</p> <p>блокирование</p> <p>уничтожение</p>
Оператор	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к конфиденциальной информации.	<p>сбор</p> <p>систематизация</p> <p>накопление</p> <p>уточнение</p> <p>использование</p>

Под уровнем исходной защищенности АРМ понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик АРМ, приведенных в таблице 6.3.

Таблица 6.3 - Показатели исходной защищенности АРМ

Технические и эксплуатационные характеристики АРМ	Уровень защищенности		
	Высокий	Средний	Низкий
<p>1. По территориальному размещению:</p> <p>- локальное АРМ, развернутая в пределах одного здания.</p>	-	+	-

Продолжение таблицы 6.3

Технические и эксплуатационные характеристики АРМ	Уровень защищенности		
	Высокий	Средний	Низкий
<p>2. По наличию соединения с сетями общего пользования:</p> <p>- АРМ, имеющая многоточечный выход в сеть общего пользования;</p>	+	-	-
<p>3. По встроенным (легальным) операциям с записями баз персональных данных:</p> <p>- чтение, поиск;</p> <p>- запись, удаление, сортировка;</p> <p>- модификация, передача.</p>	- + +	+ - -	- - -
<p>4. По разграничению доступа к персональным:</p> <p>- АРМ, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем АРМ</p>	-	+	-
<p>5. По наличию соединений с другими базами:</p> <p>- АРМ, в которой используется одна база для конфиденциальной информации, принадлежащая организации - владельцу.</p>	+	-	-
<p>6. По уровню обобщения (обезличивания):</p> <p>- АРМ, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;</p>	-	+	-

Продолжение таблицы 6.3

Технические и эксплуатационные характеристики АРМ	Уровень защищенности		
	Высокий	Средний	Низкий
<p>7. По объему конфиденциальной информации, которая предоставляется сторонним пользователям АРМ без предварительной обработки:</p> <p>- АРМ, не предоставляющие никакой информации.</p>	+	-	-

АРМ имеет высокую степень исходной защищенности.

При составлении перечня актуальных угроз безопасности конфиденциальной информации каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1 , а именно:

- 0 для высокой степени исходной защищенности;
- 5 для средней степени исходной защищенности;
- 10 для низкой степени исходной защищенности.

Для нашей АРМ этот коэффициент (Y_1) равен 0

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показателя, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности конфиденциальной информации для данной АРМ в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

– низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

– средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности конфиденциальной информации недостаточны;

– высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности конфиденциальной информации не приняты.

При составлении перечня актуальных угроз безопасности конфиденциальной информации каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2 , а именно:

- 0 для маловероятной угрозы;
- 2 для низкой вероятности угрозы;
- 5 для средней вероятности угрозы;
- 10 для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением

$$Y = (Y_1 + Y_2) / 20 .$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если $0 \leq Y \leq 0,3$, то возможность реализации угрозы признается низкой;

если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признается средней;

если $0,6 < Y \leq 0,8$, то возможность реализации угрозы признается высокой;

если $Y > 0,8$, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой АРМ. Этот показатель имеет три значения:

- незначительные негативные последствия (показатель опасности – низкий) – последствия для субъекта мало ощутимы (незначительный финансовый или моральный ущерб, при этом репутация субъекта, его материальное благополучие, жизнь и здоровье не затронуты);
- негативные последствия (показатель опасности – средний) – последствия приводят к ощутимым по объему или значению финансовым и (или) моральным и (или) репутационным потерям. Основные интересы и права личности, закрепленные Конституцией РФ, не затронуты;
- значительные негативные последствия (показатель опасности – высокий) – последствия приводят к критическим финансовым, моральным, репутационным потерям для субъекта, вплоть до потери средств к существованию, здоровья, жизни.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной АРМ, в соответствии с правилами, показанными в таблице 6.4.

Таблица 6.4 - Правила отнесения угрозы безопасности конфиденциальной информации к актуальной

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

После оценки актуальности угроз в таблице 6.5 представлена частная модель угроз.

Таблица 6.5 - Модель угроз безопасности конфиденциальной информации

Описание угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Последствия
1. Угрозы утечки информации по техническим каналам	Маловероятная	Низкая	Низкая	Неактуальная	К, Д
2. Угрозы НСД к конфиденциальной информации, обрабатываемым на автоматизированном рабочем месте	Средняя	Средняя	Средняя	Актуальная	К
3. Угрозы утечки акустической (речевой) информации	Маловероятная	Низкая	Низкая	Неактуальная	К
Описание угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Последствия
4. Угрозы утечки видовой информации	Средняя	Средняя	Средняя	Актуальная	К, Д, Ц
5. Угрозы утечки информации по каналу ПЭМИН	Маловероятная	Низкая	Низкая	Неактуальная	К, Ц
Описание угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Последствия
8. Угрозы внедрения ложного объекта как в АРМ	Высокая	Средняя	Высокая	Актуальная	К, Д, Ц

Продолжение таблицы 6.5

Описание угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Последствия
9. Угрозы подмены доверенного объекта	Высокая	Средняя	Высокая	Актуальная	К, Д, Ц
11. Угрозы выявления паролей	Средняя	Средняя	Высокая	Актуальная	К, Ц
12. Угрозы типа «Отказ в обслуживании»	Высокая	Средняя	Высокая	Актуальная	К, Д, Ц
13. Угрозы внедрения локальных вредоносных программ	Высокая	Высокая	Высокая	Актуальная	К, Д, Ц

Таким образом, актуальными угрозами безопасности конфиденциальной информации в распределенной ИС II типа, являются:

- угрозы НСД к конфиденциальной информации, обрабатываемым на автоматизированном рабочем месте;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем;
- угрозы утечки видовой информации;
- угрозы внедрения ложного объекта как в АРМ;
- угрозы подмены доверенного объекта;
- угрозы выявления паролей;
- угрозы типа «Отказ в обслуживании»;
- угрозы внедрения локальных вредоносных программ.

После выполнения всех шагов была сформирована частная модель угроз. Результатами работ по разработке частной модели угроз безопасности конфиденциальной информации является частная модель угроз безопасности АРМ.

Класс защищенности АРМ относится к 1Г.

Требования к классу защищенности 1Г:

Подсистема управления доступом:

- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
 - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
 - результат попытки входа: успешная или неуспешная - несанкционированная;
 - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
 - код или пароль, предъявленный при неуспешной попытке;
 - должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются:
 - дата и время выдачи (обращения к подсистеме вывода);

- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;
- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов.

В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный - несанкционированный);
- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)];
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды.

При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
- должно проводиться периодическое тестирование функций СЗИ НСД

при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

7 Определение требования к системе защиты информации, обрабатываемой автоматизированным рабочим местом

Подсистема управления доступом:

- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
 - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
 - результат попытки входа: успешная или неуспешная - несанкционированная;
 - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
 - код или пароль, предъявленный при неуспешной попытке;

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

- идентификатор субъекта доступа, запросившего документ;
- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов.

В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);

- результат запуска (успешный, неуспешный - несанкционированный);
- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)];
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды.

При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного

проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;
- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

8 Сравнительный анализ и выбор комплектующих автоматизированного рабочего места, обрабатывающего конфиденциальную информацию

При выборе комплектующих рассматривались такие пункты как: микропроцессор, оперативная память, видеоподсистема, дисковая подсистема, порты ввода/вывода, форм фактор, звук, корпус, материнская плата, принтер, клавиатура и мышь, монитор.

Выбирая микропроцессор, были изучены модели процессоров от производителей Baikal и Эльбрус. От производителя Baikal, были изучены такие модели как:

- Baikal-T1 – двухъядерный процессор на архитектуре MIPS. Создан для всевозможных встраиваемых систем, таких как роутеры, банкоматы, станки и так далее. Выпускался на фабрике TSMC по техпроцессу 28 нм.
- Baikal-M1 – процессор для офисных ПК и неттопов на архитектуре ARM. Под этот процессор было разработано больше 10 материнских плат и больше 50 различных устройств. Выпускался на фабрике TSMC по техпроцессу 28 нм.
- Baikal-S – модель для серверов и систем хранения данных. 48 ARM ядер – выпуск все на той же TSMC по техпроцессу 16 нм.

От производителя Эльбрус были изучены следующие модели:

- микропроцессор Эльбрус-4С (1891ВМ8Я) – многоядерный универсальный высокопроизводительный микропроцессор, построенный в соответствии с улучшенной архитектурой «Эльбрус». Каждое ядро процессора декодирует и отправляет на исполнение до 23 операций за такт.
- «Эльбрус-2С3» (К1891ВМ068) — высокоинтегрированный процессор общего назначения архитектуры Эльбрус со встроенными ускорителями 2D/3D-графики и кодирования-декодирования видео. Микропроцессор является «системой на кристалле» — содержит встроенный контроллер периферийных интерфейсов. Компактность и малое энергопотребление позволяют применять данную мик-

росхему во встраиваемых системах, решениях для АСУ ТП, миниатюрных персональных компьютерах, носимых терминалах, планшетах, тонких клиентах.

- микропроцессор Эльбрус-8С (1891ВМ028) — высокопроизводительный процессор общего назначения с улучшенной архитектурой Эльбрус.
- микросхема центрального процессора 1891ВМ018 — вычислитель серверного класса. Содержит 8 ядер архитектуры «SPARC» 9-й версии с тактовой частотой до 2000 МГц. Позволяет строить многопроцессорные серверы и рабочие станции, а также бортовые вычислители, требовательные к скорости обработки и передачи информации.

В ходе анализа и выбора определенного процессора, были рассмотрены такие факторы как, совместимость с отечественным программным обеспечением и отечественными комплектующими, которые будут выбраны в дальнейшем, стоимость, форм-фактор и производительность процессора. Выбор пал на микропроцессор Эльбрус-4С (1891ВМ8Я), это самый оптимальный выбор для офисного использования. Этот процессор был множество раз протестирован с различным программным обеспечением и даже имея частоту в 800МГц показывал отличные результаты. Выбранный микропроцессор представлен на рисунке 8.1.



Рисунок 8.1 - Выбранный процессор для автоматизированного рабочего места

На основе выбора микропроцессора Эльбрус-4С, была выбрана интегрированная видеокарта на основе СБИС Silicon Motion SM718. Так как у этих комплектующих проводились тесты производительности, на которых были показаны неплохие результаты.

Далее производился анализ и выбор жёсткого диска отечественного производства. В ходе анализа была выявлена только две компании, которые производят жёсткие диски в России, в городе Гусев это компания GS Nanotech, а вторая компания это ТМИ – Телеком и Микроэлектроник Индастриз. Были рассмотрены такие модели как:

- ТМИ SSD 512Гб в форм-факторе 2.5"
- ТМИ SSD 512Гб в форм-факторе M.2 2280
- GS SSD 512-16 российский SSD (512 Гб) твердотельный накопитель с SATA-интерфейсом в форм-факторе 2.5"
- GS SSD 512-16 российский SSD (512 Гб) твердотельный накопитель с SATA-интерфейсом в форм-факторе M.2 2280

Так как все накопители имели одинаковую скорость записи и чтения, среди них был выбран SSD накопитель от компании GS Nanotech, так как он единственный обладал двумя факторами, нужным объёмом памяти и занесён в реестр мин-промторг России. Выбранный жёсткий диск представлен на рисунке 8.2



Рисунок 8.2 - Выбранный жёсткий диск для автоматизированного рабочего места

Далее проводился анализ и выбор звукового оборудования для автоматизированного рабочего места. Была выбрана отечественная разработка интегрированная звуковая карта AC-97 (стерео). Выбранная аудиосистема для АРМ представлена на рисунке 8.3

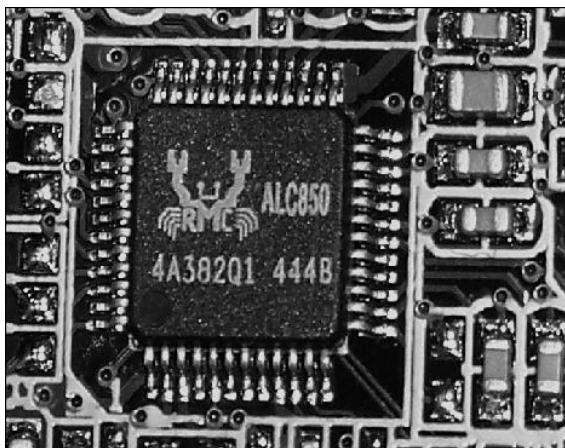


Рисунок 8.3 - Выбранная аудиосистема для автоматизированного рабочего места

Далее проводился анализ выбора кулера для автоматизированного рабочего места. Из-за отсутствия компаний, разрабатывающих данную продукцию был выбран кулер компании Деерскул, модель TF120S. Он представлен на следующем рисунке 8.4.



Рисунок 8.4 - Выбранный кулер TF120S для автоматизированного рабочего места

После выбора был произведен анализ и выбор блока питания для автоматизированного рабочего места. Был выбран блок питания Sven 500W [PU-500AN], так как его номинала хватает для данного АРМ. Он представлен на рисунке 8.5.



Рисунок 8.5 - Блок питания, выбранный для АРМ.

Далее был проведен анализ устройств ввода, таких как клавиатура, и устройство ввода типа «мышь».

При выборе клавиатуры, были проанализированы защищенные клавиатуры. Была выбрана переносная защищённая промышленная клавиатура ТКВ-500 «Сигнал», которая является отечественной разработкой. Выбранная клавиатура представлена на рисунке 8.6



Рисунок 8.6 - Выбранная клавиатура ТКВ-500 «Сигнал» для автоматизированного рабочего места.

К плюсам данной клавиатуры можно отнести:

1. защита от кражи данных через ПЭМИН;
2. пониженный уровень радиопомех, генерируемых изделием.

Далее производился анализ и выбор устройства вывода для нашего автоматизированного рабочего места. При выборе монитора рассматривались 2 отечественные компании, это V-MAX и RDW. При соотношении их продукции по

принципу цена-качество, был выбран монитор V-Max российский монитор 27", разрешение 1920x1080, TFT на основе технологии IPS.

Далее при анализе устройств ввода типа «мышь», была выбрана модель TCM-2277 (ЗМКС-2277.130), которая так же является отечественной разработкой. Выбранное устройство ввода типа «мышь» представлена на рисунке 8.7.



Рисунок 8.7 - Выбранное устройство ввода TCM-2277 для автоматизированного рабочего места.

Далее был произведен анализ принтеров отечественного производства, таких компаний как: Катюша, ОАО «ЛЕНПОЛИГРАФМАШ» и Pantum.

Наиболее подходящими были принтеры ОАО «ЛЕНПОЛИГРАФМАШ», среди которых был выбран матричный принтер УДМ серия 1, который представлен на рисунке 8.8



Рисунок 8.8 - Выбранный матричный принтер УДМ серия 1 для автоматизированного рабочего места

Далее проводился выбор отечественного источника бесперебойного питания, среди всех отечественных было выбрано устройство ATS 1000, которое представлено на рисунке 8.9.



Рисунок 8.9 - Источник бесперебойного питания ATS 1000

9 Сравнительный анализ и выбор программного обеспечения автоматизированного рабочего места, обрабатывающего конфиденциальную информацию

При выборе операционной системы, анализировались различные версии Linux и операционная система QP разработанная компанией Криптософт. Мы не рассматриваем версии операционных систем Windows, так как они не являются отечественной разработкой.

Компания Криптософт, назвала свою операционную систему QP «Импорт-замещением на основе отечественной операционной системы».

Главными плюсами данной ОС (операционной системы), являются:

1. Все исходные коды разрабатываются в России;
2. Для каждого компонента программного обеспечения имеются компетенции, позволяющие модифицировать исходный код;
3. НТП «Криптософт» самостоятельно разрабатывает код создаваемых информационных систем.

Данная операционная система сертифицирована ФСБ России и может применяться для построения защищённых информационных систем до уровня «совершенно секретно».

В состав данной ОС уже входит пакет офисных программ, таких как:

1. Редактор текстовых документов - Глагол;

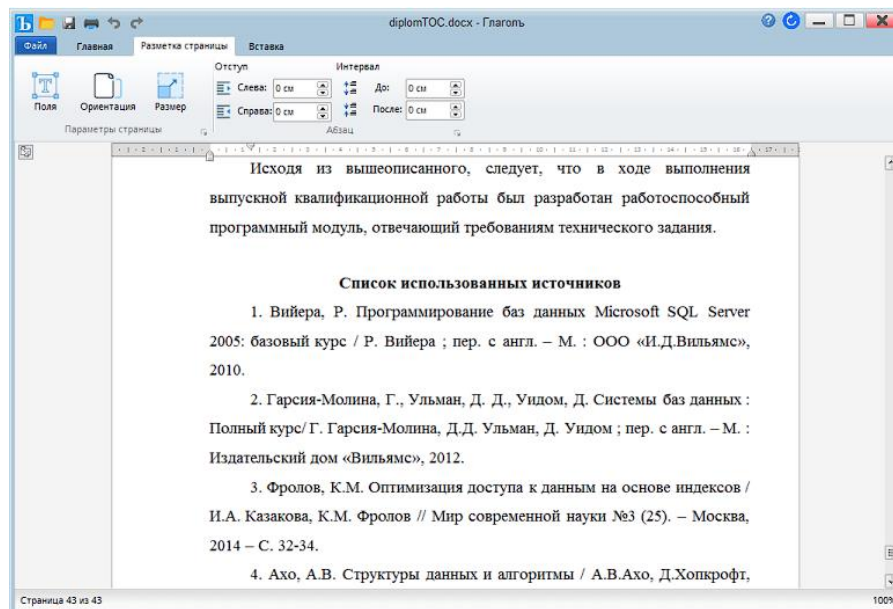


Рисунок 9.1 - Скриншот из программы Глагол.

2. Редактор таблиц - Таблица;

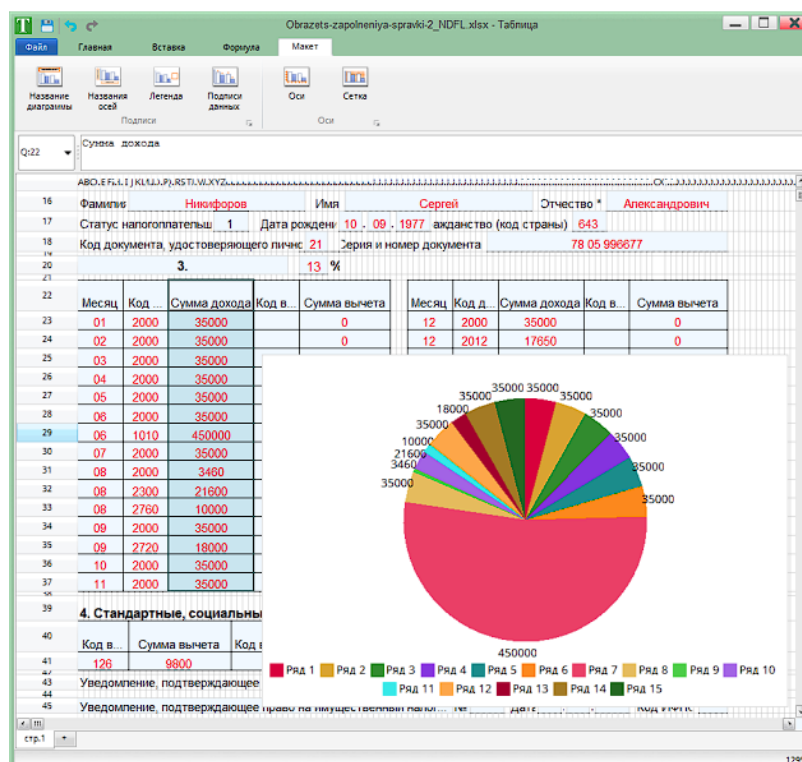


Рисунок 9.2 - Скриншот из программы Таблица.

3. Менеджер презентаций - Презентация.

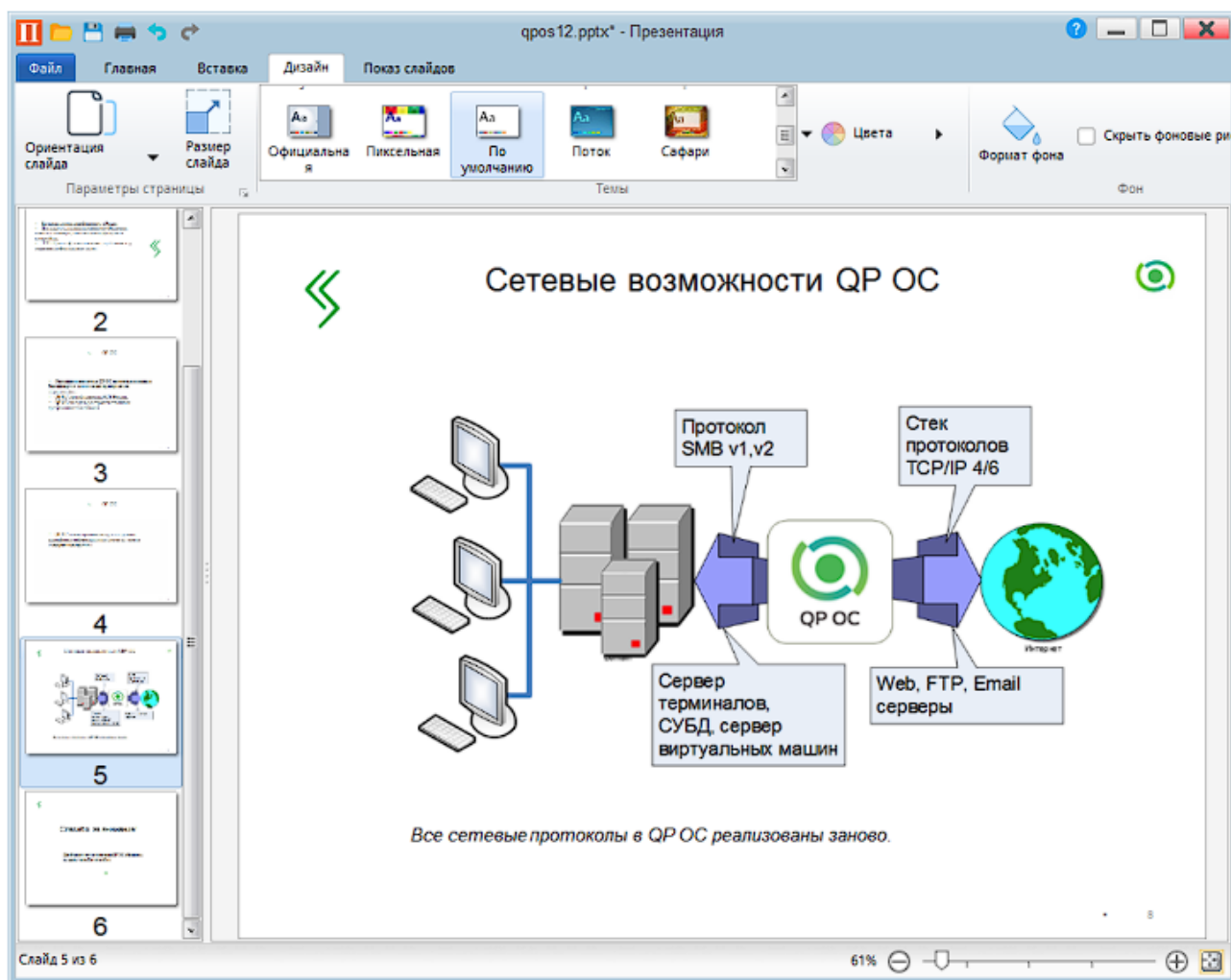


Рисунок 9.3 - Скриншот из программы Презентация.

Но не смотря на такое огромное количество плюсов, данная разработка всё ещё находится в тестовом режиме, и не может быть использована на нашем АРМ.

Поэтому мы останавливаемся на выборе операционной системы полностью отечественного производства на базе Astra Linux.

Далее мы проводим анализ и выбор отечественного офисного пакета программ. Из таких пакетов были выделены: Мой Офис, Р7-Офис и Офис 365.

Было проведено сравнение функционала данных пакетов, и максимальным количеством функций обладал пакет программ «Мой офис», который и был выбран для нашего АРМ и который совместим с выбранной нами операционной системой.

Среди антивирусных программ безоговорочным лидером считается разработка компании «Лаборатория Касперского». Данное ПО так же совместимо с нашей операционной системой, поэтому выбор пал на неё.

10 Сравнительный анализ и выбор программно-аппаратных средств защиты для автоматизированного рабочего места, обрабатывающего конфиденциальную информацию

Для анализа средств защиты информации (СЗИ) от несанкционированного доступа (НСД) были выбраны такие продукты как, Страж NT, Secret Net, Полный комплект СЗИ в операционной системе (ОС) Astra Linux Special Edition в режиме функционирования «Базовый», «Усиленный», «Максимальный».

СЗИ будет выбрано согласно параметрам, выбранным в техническом задании (ТЗ) на выпускную квалификационную работу (ВКР):

1. многокомпонентная проверка подлинности перед загрузкой операционной системы (включая виртуальную среду) с использованием аппаратных маркеров, таких как Ibutton или USB-маркеров
2. фиксация событий безопасности, включая активности администратора;
3. создание изолированной программной среды пользователя, позволяющей запускать только разрешенные приложения;
4. пометка печатаемых документов независимо от используемого приложения для печати;
5. принцип дискреционного управления доступом к ресурсам системы.

Рассмотрим характеристики Стража NT:

Двухфакторная аутентификация до загрузки операционной системы (в том числе и для виртуальной среды) с использованием аппаратных идентификаторов:

- USB-идентификаторов типа Guardant ID, Рутокен, eToken, JaCarta, ESMART Token;
- смарт-карт Рутокен, eToken, JaCarta, ESMART;
- iButton;
- дискета 3,5”;

Дискреционный принцип контроля доступа к ресурсам системы;

Мандатный принцип контроля доступа к ресурсам системы, в том числе:

- возможность одновременной работы с документами разных уровней конфиденциальности в одном сеансе (без смены сеанса пользователя);

- контроль именованных каналов;

Создание замкнутой программной среды пользователя, позволяющей ему запуск только разрешенных приложений;

Регистрация событий безопасности, в том числе и действий администратора;

Маркировка выдаваемых на печать документов независимо от печатающего их приложения;

- гарантированная очистка:

- освобождаемой оперативной памяти;

- содержимого защищаемых файлов при их удалении;

- файла(ов) подкачки при завершении работы системы;

- контроль целостности защищаемых ресурсов системы и компонентов системы защиты информации;

- управление пользователями;

- управление носителями информации;

- управление устройствами;

- преобразование информации на отчуждаемых носителях;

- тестирование системы защиты информации.

Данное СЗИ полностью подходит нам исходя из параметров, но есть пункты совместимости, согласно которым данное ПО не работает с операционной системой на базе Astra Linux. А также его можно использовать только в автоматизированных системах до класса защищенности А2. Наш же класс защищенности В2, согласно этим данным, мы не можем выбрать Страж NT для нашего АРМ.

Далее будем рассматривать СЗИ от НСД Secret Net:

1. Политики безопасности

Secret Net позволяет настроить гибкую систему управления с помощью группировки рабочих станций и серверов, и назначения политик безопасности для каждого отдельного подразделения или группы, согласно принятой в компании иерархии.

Групповые политики – стандартные механизмы управления политиками аналогичные Active Directory. Имеют низкий приоритет и распределяются согласно выстроенной иерархии в организации.

Политики сервера безопасности – политики на сервера безопасности имеют высокий приоритет. Большой приоритет у политик, назначенных на сервера, стоящие выше в иерархии.

Политики организационных подразделений – расширение стандартных механизмов, возможность назначения в доменах безопасности без глобальных административных прав, заменяют групповые политики. Большой приоритет у политик, назначенных на подразделения, стоящие ниже в иерархии. (аналогично Active Directory).

В версии Secret Net 7.3 добавлена возможность назначения политик на сервера безопасности. При этом наследование политик между серверами обратное, т.е. чем ниже уровень сервера безопасности, тем ниже приоритет его политик. Это значит, что на верхнем сервере можно настроить политики, которые нельзя изменить с подчиненных серверов безопасности.

2. Защита входа в систему.

Secret Net обеспечивает усиленную защиту входа в систему. Помимо собственных механизмов парольной аутентификации Secret Net позволяет использовать режимы идентификации и аутентификации пользователей с использованием аппаратных идентификаторов, таких как:

- eToken
- Рутокен
- Jakarta

– Ibutton

Идентификаторы присваиваются к каждому пользователю в панели управления паролями безопасности. После этого пользователь может авторизоваться по паролю или просто подключить идентификатор к рабочей станции.

3. Разграничение доступа.

В Secret Net реализовано дискреционное и полномочное управление доступом.

Дискреционный принцип доступа подразумевает задание каждому пользователю «своих» папок

Механизм полномочного разграничения доступа обеспечивает контроль подключения и использования устройств с назначенными категориями конфиденциальности, контроль сетевых интерфейсов и печати конфиденциальных документов. Всего Secret Net позволяет задать до 16 уровней конфиденциальности с именами, соответствующими стандартам Вашей организации. Обеспечение строгого соответствия принципам полномочного доступа осуществляется включением контроля потоков конфиденциальной информации в системе. При входе в систему пользователь может самостоятельно выбрать категорию конфиденциальной информации, с которой он будет работать. Кроме того, при установке соответствующих прав доступа пользователь может сам задавать уровень конфиденциальности файлов и папок.

4. Контроль устройств.

Secret Net позволяет ограничить доступ практически к любым устройствам, как централизованно, так и локально. Настройка осуществляется для отдельных устройств, классов или групп. Это означает, что можно задать политику для всех сетевых плат, всех флешек, а также устройств по их серийному номеру или модели.

В соответствии с политиками безопасности, подключение может разрешаться или запрещаться, варианты контроля могут варьироваться. Например, компьютер при подключении может блокироваться или отключаться. Политики работы с

устройствами складываются. На устройства в Secret Net можно добавить возможность запрета или разрешения устройства в зависимости от уровня конфиденциальности пользователя. Новое устройство в системе включается в соответствующую ему группу, класс или модель. Доступ к нему устанавливается автоматически, в соответствии с верхними правилами.

Принтеры в Secret Net контролируются по аналогии с другими устройствами. Для них также можно настроить дискреционные и мандатные разрешения. Для расследования инцидентов можно включить теневое копирование распечатанных документов. В Secret Net поддерживается маркировка выводимых на печать документов в соответствии с требованиями законодательства для работы с государственной тайной.

5. Контроль целостности и замкнутая программная среда.

В Secret Net реализован механизм контроля целостности, который позволяет поставить на контроль изменения ресурсов компьютера, файлов, директорий, элементов реестра windows. Для элементов Secret Net и Windows в модуле контроль программ и данных есть шаблоны, которые включаются по умолчанию. При этом администратор может создавать свои задания и шаблоны реакции на изменения, менять методы контроля.

Контроль целостности может осуществляться как по содержимому файлов, так и по атрибутам, правам доступа, дате и времени последнего изменения. При обнаружении несоответствия можно игнорировать инцидент, блокировать компьютер или автоматически восстанавливать измененные файлы.

Контроль целостности может производиться по расписанию:

- в указанные даты
- при загрузке
- при авторизации
- при завершении работы пользователя

Замкнутая программная среда позволяет ограничить список запускаемых пользователем приложений. При запуске приложений может автоматически про-

веряться его целостность. Благодаря этому механизму пользователь не сможет подменить приложения простым переименованием программ.

6. Оперативное управление

Программа оперативного управления позволяет одновременно видеть все компьютеры и пользователей системы, а также их статусы и события НСД. Оперативное управление в Secret Net предусматривает отправку оперативных команд на все компьютеры и сервера, стоящие ниже по иерархии. Это могут быть команды оперативного управления, такие как блокировка, перезагрузка, включение/выключение компьютера, обновление политик, управление механизмами защиты, утверждение изменений аппаратной конфигурации. Доступна также отправка команд к компьютерам, подключенным к подчиненным серверам, с передачей команды по иерархии серверов.

7. Работа с журналами и отчетами.

Secret Net записывает все события безопасности на локальную рабочую станцию. Централизованно доступен сбор журналов. В программе управления настраиваются журналы и периодичность сбора, определяется какие журналы нужно собирать и что делать при заполнении.

События НСД это критичные события безопасности – помимо журналов они попадают в отдельную вкладку, и собираются не по расписанию, а моментально приходят как сигнал тревоги офицерам безопасности, отслеживаются и фильтруются на всех вышестоящих серверах безопасности в реальном времени. Работать с событиями НСД могут сразу несколько администраторов системы Secret Net. Для информирования об обработке события реализован механизм квитирования НСД - Можно отмечать их как рассмотренные или требующие дополнительного разбирательства, добавлять комментарии и т.д.

Наряду с критичными событиями, в Secret Net ведется журналирование всех событий и действий пользователей. Кроме того, в Secret Net реализован механизм отчетов. Отчет можно создать по ресурсам автоматизированного рабочего места, электронным идентификаторам или построить связанные отчеты с ПАК «Со-

боль». Отчет может быть персонализирован с помощью добавления информации об организации. Это позволяет администраторам максимально быстро создать отчет для руководства.

Данное СЗИ так же подходит нам по параметрам, выбранным в ТЗ, но оно не работает с операционной системой на базе Linux. Исходя из этого, мы не можем выбрать СЗИ от НСД Secret Net для нашего АРМ.

Далее мы рассмотрим полный комплект СЗИ в ОС Astra Linux Special Edition в режиме функционирования «Базовый», «Усиленный», «Максимальный».

Уже начиная с режима функционирования СЗИ «Базовый» в ОС Astra Linux Special Edition доступны такие функции безопасности, как изоляция процессов, защита памяти, регистрация событий безопасности и др. Однако в части используемого механизма управления доступом этот режим функционирования СЗИ мало чем отличается от того, что можно увидеть в большинстве ОС семейства Linux, в том числе отечественных. Как говорят, это режим, в котором работает только дискреционное управление доступом. Т.е. когда администраторы или даже обычные пользователи сами, без каких-то общих правил, решают кому и к каким файлам или каталогам предоставить права доступа на чтение, запись или выполнение. Это очень просто для реализации и использования, но лишает возможности определить корректность установки этих прав. При этом сложность архитектуры ОС, неочевидные зависимости её компонент друг от друга, или просто ошибки при администрировании ОС могут привести к тому, что к некоторым важным для её безопасности файлам или каталогам будут установлены неверные права доступа. Причем это не будет явно сказываться на функционировании ОС и, как следствие, не будет оперативно выявлено. Кроме того, ОС только с дискреционным управлением доступом, как правило, уязвима для типовых атак, которые разрабатывают хакеры по всему миру, так как нет того, что могло бы ее дополнительно защитить.

Поэтому часто в ОС семейства Linux используют дополнительные механизмы, позволяющие задавать сложные политики управления доступом, учитывающие особенности функционирования компонент ОС, их взаимодействия между

собой. Примерами таких механизмов являются AppArmor и Security Enhanced Linux (SELinux). Первый из них расширяет дискреционное управление за счет возможности задания политик, ограничивающих доступ к компонентам ОС. Второй механизм помимо этого включает элементы типизированного, ролевого и мандатного управления доступом.

Казалось бы, всё уже есть, и не надо делать ничего своего. Так в чем проблема? А она, как обычно, кроется в фундаменте этих технологий и упирается в математику. Во-первых, несмотря на существующие исходные тексты программного кода AppArmor и SELinux, ввиду его значительного объема и сложности, это не оказывает значительного влияния на возможность проверки эффективности данных механизмов, их доработки, сопровождения, т. е. обеспечения доверия к ним. Во-вторых, собственно доверие к механизмам управления доступом, как правило, основывается на наличии для них формальной (выраженной на математическом языке) модели управления доступом. Без такой модели невозможна верификация как самих AppArmor и SELinux, так и всей системы защиты ОС.

Дело в том, что с одной стороны, формальная модель задает четкие правила игры для ОС, а именно: как назначать права доступа процессам к файлам и каталогам, как их помечать метками конфиденциальности или целостности, управлять доступом на основе этих меток в самых разных ситуациях, например, создания нового файла, учетной записи пользователя или запуска процесса. С другой стороны, модель позволяет на своем уровне абстракции сформулировать условия безопасности ОС и математически доказать, что при их выполнении защиту ОС невозможно взломать.

Однако о существовании развитой модели управления доступом для AppArmor или SELinux авторам настоящей статьи ничего неизвестно. Разработанные в 70-е годы прошлого столетия модели Белла-ЛаПадулы или Биба, иногда упоминаемые в этом контексте, не заслуживают серьезного обсуждения как безнадежно устаревшие. В результате, использовать SELinux или AppArmor для управления доступом в ОС – это сродни созданию отечественного самолета с ино-

странными двигателями без тщательного тестирования, возможности технической поддержки и развития: летать будет, но долго ли или высоко ли – большой вопрос.

В связи с этим даже в «Базовом» режиме разработчики ГК «Астра» отказались от использования заимствованных механизмов защиты SELinux и AppArmor, чтобы в последующих режимах заместить их собственными СЗИ.

Следующий режим функционирования СЗИ в ОС Astra Linux Special Edition – это «Усиленный». Он самый интересный, т. к. с него начинают действовать СЗИ собственной разработки, входящие в подсистему безопасности PARSEC. В первую очередь это противостоящие угрозе целостности информации механизмы мандатного контроля целостности (МКЦ) и замкнутой программной среды (ЗПС). Самое главное, что делают эти СЗИ — существенно повышают защищенность ОС от взлома, заражения вирусами, внедрения закладок, захвата повышенных привилегий и т. д. Ведь для любой защищенной системы важно, чтобы ее механизмы защиты работали корректно. А если система взломана, нарушена целостность ее программной среды или ее контролирует нарушитель, то не имеет смысла говорить о каких-то еще защитных функциях такой системы, например, позволяющих предотвратить утечку конфиденциальных данных. При этом по сравнению с SELinux или AppArmor подсистема безопасности PARSEC разработана на основе адаптированной для ОС семейства Linux современной верифицированной формальной модели безопасности управления доступом и информационными потоками (МРОСЛ ДП-модели), значительную часть описания которой и необходимую для этого теорию можно увидеть в учебном пособии.

Таким образом, режим «Усиленный» либо непосредственно, либо как входящий в режим «Максимальный», желателен для применения большинством пользователей ОС Astra Linux Special Edition. Именно он позволяет значительно усилить защиту от многих типовых атак.

Полный комплект СЗИ в ОС Astra Linux Special Edition доступен в режиме функционирования «Максимальный». В первую очередь здесь идет речь о воз-

возможности использования мандатного управления доступом (МРД) для защиты от угрозы конфиденциальности информации. Самое главное в МРД то, что оно необходимо гораздо в более широком спектре случаев, чем может показаться на первый взгляд. Не только в случаях, когда речь идет о защите государственной тайны.

Исходя из этой информации можно сделать вывод, что для нашего АРМ подойдет полный комплект СЗИ в ОС Astra Linux Special Edition в режиме функционирования «Максимальный».

11 Модель автоматизированного рабочего места для обработки конфиденциальной информации

Подводя итоги можно увидеть модель автоматизированного рабочего места на рисунке 11.1.



Рисунок 11.1 - Модель автоматизированного рабочего места

Так же все выбранные комплектующие и ПО (программное обеспечение), представлены далее.

Выбранные комплектующие, представлены далее:

- микропроцессор Эльбрус-4С (1891ВМ8Я);

- GS SSD 512-16 российский SSD (512 Гб) твердотельный накопитель с SATA-интерфейсом в форм-факторе 2.5”;
- интегрированная звуковая карта AC-97 (стерео);
- кулер компании Deercool, модель TF120S;
- клавиатура ТКВ-500 «Сигнал»;
- устройство ввода TCM-2277;
- блок питания SVEN 500W [PU-500AN]
- источник бесперебойного питания ATS 1000;
- матричный принтер УДМ серия 1.
- V-Max российский монитор 27'

Ниже представлен список выбранного программного обеспечения:

- операционная система Astra Linux;
- антивирус компании «Лаборатория Касперского»;
- пакет программ «Мой офис»;
- полный комплект СЗИ в ОС Astra Linux Special Edition в режиме функционирования «Максимальный».

12 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Специалисту по защите информации по роду своей деятельности приходится, как никому другому, выполнять свои должностные обязанности долгое время в сидячем положении, работая за компьютером. В связи с этим, такой малоподвижный образ жизни негативно влияет на здоровье и жизнедеятельность человека. Могут возникать и развиваться заболевания кистей рук и локтевых суставов, позвоночника, нервной системы, кожи, органов дыхания и пищеварения, прямой кишки, заболевания, связанные с нарушением зрения. Но одними из самых опасных и распространенных являются заболевания сердечно-сосудистой системы.

К вредным психофизиологическим факторам, влияющим на сердечно-сосудистую систему специалиста по защите информации, относят:

малоподвижный образ жизни. Это вызывает проблемы с кровообращением, которые могут привести к повышенному тромбообразованию. Эритроциты сворачиваются, тем самым нарушая насыщение тканей кислородом, в том числе сердечной мышцы. Постепенно замедляется обмен веществ и растет лишний вес, что вынуждает сердечную мышцу работать более усиленно;

постоянное нахождение в сидячем положении. Это приводит к застою крови в нижних конечностях и повышенному растяжению клапанов вен. Из-за чего стенки сосудов растягиваются и становятся менее эластичными, что вызывает развитие варикозной болезни;

электромагнитное излучение. Постоянное воздействие электромагнитного излучения негативно влияет на форменные элементы крови, клетки. Они имеют электрические потенциалы, положительные и отрицательные заряды. Воздействие излучения происходит на тонком уровне,

поэтому развитие заболевания невозможно предугадать и обнаружить. Также излучение может влиять на селезенку, спинной мозг, ухудшать процесс кроветворения. Постепенно угнетается гормональная система, которая вырабатывает большое количество адреналина в ответ на длительное воздействие излучения. Это негативно влияет на артериальное давление и затрудняет работу сердечной мышцы. В редких случаях излучение является причиной аритмий и может негативно сказываться на проводимости миокарда;

нагрузка на кисти рук. Также в процессе деятельности человек, работающий за компьютером, совершает однообразные движения кистями рук, что усиливает приток крови к работающим частям тела. Это может вызвать защемление нервов и негативно сказаться на кровообращении человека.

Чтобы снизить негативное воздействие психофизиологических факторов на здоровье специалиста по защите информации необходимо, в первую очередь, соблюдать профилактические меры. К ним относятся:

ограничение непрерывной работы за компьютером. По санитарным нормам человеку допускается работать за компьютером не более 6 часов;

уход за зрением. Необходимо выполнять регулярную разминку глаз, при необходимости принимать витамины и минералы для зрения и использовать капли от сухости глаз;

периодические перерывы во время работы для соблюдения режима питания;

выбор качественного жидкокристаллического монитора. Монитор не должен обладать эффектом мерцания. Также при необходимости можно использовать специальный защитный экран;

правильное положение тела за рабочим местом. На рисунке * показано правильное положение тела за рабочим местом. Монитор должен находиться от глаз на расстоянии вытянутой руки желательно под прямым углом. Необходимо держать спину ровно, плечи расправить. Руки

рекомендуется держать в согнутом положении под углом 90 градусов. Не следует опираться локтями на стол. Сидя на стуле ноги у человека должны быть в согнутом положении под углом чуть больше 90 градусов, ступни должны находиться на полу или на подставке;

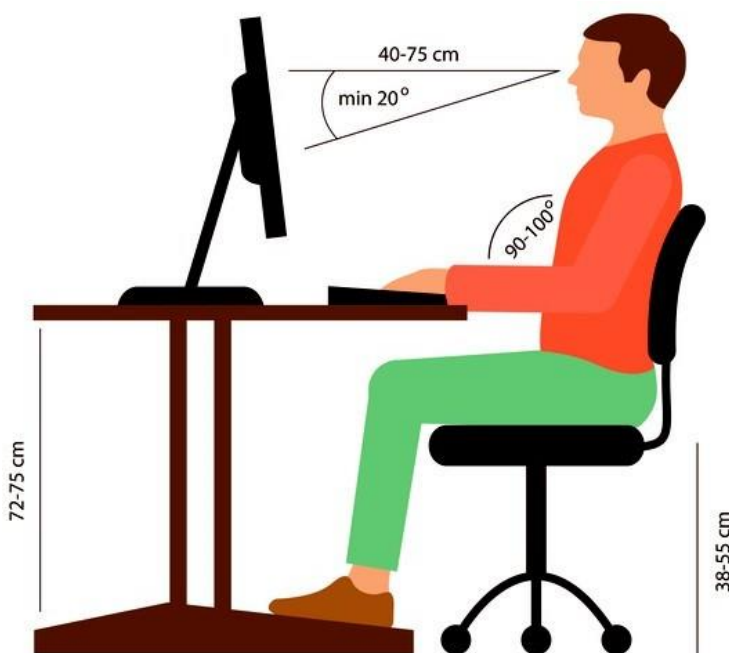


Рисунок 12.1 — Правильное положение тела за рабочим местом

- использование комфортной и подходящей по анатомическим признакам мебели;
- регулярная уборка рабочего места и помещения от пыли с помощью антибактериальных средств. Также следует периодически проветривать помещение;
- регулярное препровождение личного времени на свежем воздухе.

Помимо вышеперечисленного регулярно необходимо уделять время физической культуре, а именно выполнять упражнения, которые снижают негативное воздействие психофизиологических факторов на сердечно-сосудистую систему специалиста по защите информации. К таким

упражнениям относятся:

— упражнение 1. Сидя за стулом, необходимо завести руки за спинку стула, ноги перекрестить и поднять от пола в горизонтальное положение. Также можно передвигать ноги поочередно то влево, то вправо, при этом напрягая мышцы ног;

— упражнение 2. Необходимо взять лист бумаги, положить его на пальцы обеих рук, поднять его вверх и удерживаться в таком положении несколько секунд;

— упражнение 3. Необходимо встать возле рабочего места, ноги расположить на ширине плеч и, держась руками о стул или стол, выполнить несколько приседаний;

— упражнение 4. Необходимо встать прямо и сцепить руки в замок за спиной. После этого нужно приподняться на носки, при этом расцепив руки и вытянув их вверх. Также можно при подъеме выполнять повороты рук поочередно влево и вправо, одновременно выполняя повороты головой. Данное упражнение уменьшает напряжение в мышцах ног, спины и шеи;

— упражнение 5. Необходимо встать ровно и расслабиться. Затем поочередно выполнять глубокий вдох, задержку дыхания и выдох.

Физическая зарядка за рабочим местом очень полезна. Она уменьшает риск заболеваний, связанных с сердечно-сосудистой системой, повышает продуктивность и работоспособность.

Заключение

В данном дипломном проекте был проведен анализ и выбор комплектующих и программного обеспечения для создания модели автоматизированного рабочего места на основе отечественных комплектующих и программного обеспечения. Основной целью проекта было обеспечение безопасности и защищенности автоматизированного рабочего места, а также определение соответствующего класса защищенности.

В ходе проекта была выполнена оценка угроз для АРМ, что позволило определить потенциальные угрозы. На основе этой модели угроз были приняты меры по обеспечению безопасности, включая выбор комплектующих и программного обеспечения, соответствующих требованиям защищенности.

Был проведен анализ доступных отечественных комплектующих и ПО, с учетом их функциональности и безопасности. На основе этого анализа были выбраны комплектующие, способствующие обеспечению высокого уровня безопасности и соответствующие поставленным требованиям.

В результате работы была разработана модель АРМ, учитывающая не только функциональность, но и аспекты безопасности. Эта модель представляет собой интегрированную систему, обеспечивающую защиту от угроз и несанкционированного доступа.

В целом, дипломный проект успешно решает задачи по созданию модели АРМ на основе отечественных комплектующих и программного обеспечения, удовлетворяющей требованиям безопасности и защищенности.

Этот проект имеет практическую значимость и может быть использован в различных сферах, где безопасность ИС является приоритетом.

Таким образом, все пункты технического задания на ВКР выполнены в полном объеме.

Список использованных источников

1. Садыков Р.М. Основы защиты информации: учебник. - М.: КНО-РУС, 2019. - 448 с.
2. Пучков А.М. Защита информации: Учебное пособие. - М.: Юрайт, 2017. - 352 с.
3. Безопасность и защита информации: Учебник для вузов / Под ред. Л.С. Голубева. - М.: Юрайт, 2018. - 352 с.
4. ГОСТ Р 51504-2013 "Системы обработки информации. Архитектура защиты информации. Общие требования".
5. ГОСТ Р ИСО/МЭК 27001-2015 "Информационные технологии. Методы обеспечения информационной безопасности. Системы менеджмента информационной безопасности".
6. Антонов Ю.В. Компьютерная безопасность: Учебник. - М.: КНО-РУС, 2020. - 368 с.
7. Руководство пользователя программного обеспечения "КриптоПРО CSP" версии 4.0.
8. Федеральный закон "О государственной тайне" от 21 июля 1993 года № 5485-1.
9. Международный стандарт ISO/IEC 27001:2013 "Информационная технология. Техника безопасности. Системы управления информационной безопасностью. Требования".
10. Серия ГОСТ Р ИСО/МЭК 27000 "Информационная технология. Техника безопасности. Серия стандартов по системам управления информационной безопасностью".
11. Болдин А.И. Информационная безопасность. Понятие, принципы, методы. – М.: Издательство ЭКО-ТРЕНДЗ, 2018. – 288 с.
12. Капустин А.В. Анализ требований к средствам защиты информации // Молодежный научный вестник. – 2019. – № 24. – С. 49-52