МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет приборостроения, информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»
Специальность 10.05.03 –	Информационная безопасность автоматизированных систем
Специализация -	Защищенные автоматизированные системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

АППАРАТНОЕ ОБЕСПЕЧЕНИЕ УСТРОЙСТВА ВВОДА КЛЮЧЕВОЙ ИНФОРМАЦИИ ДЛЯ АППАРАТУРЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Студент _____ Кобзева Евгения Сергеевна

Руководитель _____ Морозов А.А.

Нормоконтролёр _____ Иванов А.П.

Рецензент начальник НИО АО «ПНИЭИ» _____ Оборин Р.А.

Работа допущена к защите (протокол заседания кафедры от 21.06.19 № 16)

Заведующий кафедрой _____ С.Л. Зефиров

Работа защищена с отметкой отлично (протокол заседания ГЭК от 25.06.19 № 20)

Секретарь ГЭК _____ А.П. Иванов

Проверка ВКР Юбалов
С.Л. Зефиров

Пенза 2019

Оглавление

Введение....4
1 Анализ существующих носителей информации....6
2 Обзор существующих устройств считывания информации с бумажного носителя....15
3 Анализ требований к устройству ввода ключевой информации....24
3.1 Общие сведения....24
3.2 Конструктивные требования....24
3.3 Схемотехнические требования....26
3.4 Специальные требования....27
3.5 Требования к электронной компонентной базе....28
3.6 Требования по стойкости к внешним воздействующим факторам....29
4 Анализ технических каналов утечки ключевой информации при ее обработке устройством ввода ключевой информации и передаче блоку преобразования данных....30
5 Выбор мер защиты информации, обрабатываемой устройством ввода ключевой информации....36
5.1 Меры защиты ключевой информации от утечки по каналу побочных электромагнитных излучений и наводок....36
5.2 Меры защиты от утечки ключевой информации по питающим и сигнальным цепям....39
5.3 Меры защиты ключевой информации от утечки по визуально-оптическому каналу....40
5.4 Меры защиты ключевой информации от несанкционированного доступа....42
5.5 Инженерно-криптографические требования....43
6 Разработка структурной схемы устройства ввода ключевой информации....46
7 Выбор электронной компонентной базы....49

7.1 Сравнительный анализ и рекомендации по выбору электронной компонентной базы.....49
7.2 Проблема внедрения вредоносных элементов в аппаратное обеспечение устройств.....61
8 Разработка функциональной схемы устройства ввода ключевой информации.....65
9 Описание функционирования устройства ввода ключевой информации.....72
10 Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....75
Заключение.....81
Список использованных источников.....83

Введение

Проблеме безопасности информации, обеспечению ее конфиденциальности уделялось существенное внимание на протяжении всего времени. Существуют различные способы защиты информации, например, охрана носителей защищаемой информации физическими лицами, стеганография, предполагающая сокрытие самого факта наличия информации ограниченного доступа, и шифрование (криптографическое преобразование), которое является наиболее надежным и широко применяется в настоящее время.

Шифрование заключается в криптографическом преобразовании данных с использованием ключа — изменяемого параметра в виде последовательности символов, определяющего криптографическое преобразование. В симметричных криптосистемах для зашифрования и расшифрования применяется один и тот же секретный ключ. Его утрата приводит к практической невозможности расшифровать информацию, а раскрытие ключа третьими лицами — к нарушению конфиденциальности защищаемой информации. Этим объясняются важность ключевой информации и необходимость обеспечения ее защищенности.

Для ввода ключа в аппаратуру криптографической защиты требуется разработка специализированного устройства ввода ключевой информации (УВК), которое должно соответствовать ряду требований по защите информации. Именно поэтому выбранная тема выпускной квалификационной работы является актуальной.

Целью выпускной квалификационной работы является разработка аппаратного обеспечения устройства ввода ключевой информации для аппаратуры криптографической защиты таким образом, чтобы оно обладало теми конструктивными, схемотехническими, специальными, инженерно-криптографическими и другими свойствами, которые необходимы для

обеспечения безопасности ключевой информации, которыми не обладают существующие устройства ввода, что свидетельствует о новизне выпускной квалификационной работы.

Задачами, поставленными на дипломное проектирование, являются:

- выбор наиболее предпочтительного носителя ключевой информации;
- обзор существующих устройств считывания информации с бумажного носителя;
- анализ требований к УВК;
- анализ актуальных технических каналов утечки ключевой информации при ее обработке УВК и передаче внешнему устройству;
- выбор мер защиты ключевой информации;
- разработка структурной схемы УВК;
- выбор электронной компонентной базы;
- разработка функциональной схемы УВК;
- описание функционирования УВК.

1 Анализ существующих носителей информации

Для определения наиболее предпочтительного типа носителя ключевой информации были рассмотрены следующие:

- дискета;
- компакт-диск;
- электронный ключ;
- российская интеллектуальная карта (РИК);
- бумага;
- кассетное запоминающее устройство:
  - К-128;
  - К-4 (К-213);
- запоминающие устройства на основе флеш-памяти;
- жесткий диск (HDD);
- съемное энергонезависимое запоминающее устройство СЭНЗУ-2М-(01).

Кассетные запоминающие устройства (КЗУ) представляют собой устройства для хранения информации специального назначения. КЗУ могут быть выполнены на основе оперативного запоминающего устройства (ОЗУ) или флеш-памяти.

КЗУ «К-128» разработано на базе микросхем энергонезависимой («FLASH») памяти Am29FOIO производства фирмы «Advanced Micro Devices» и предназначено для использования в качестве съемного носителя информации. Данное КЗУ обеспечивает хранение массива информации объемом 128 Кбайт. Его масса составляет 75 плюс/минус 7,5 г. Период сохранения данных:

- не менее 10 лет при температуре 150 °С;
- не менее 20 лет при температуре 125 °С [1].

КЗУ «К-4» («К-213») - статическое ОЗУ емкостью 4 Кбайт, потребляемое энергию от батарейки.

Флеш-память — разновидность полупроводниковой технологии электрически перепрограммируемой памяти. Благодаря компактности, дешевизне, механической прочности, большому объёму, скорости работы и низкому энергопотреблению, флеш-память широко используется в цифровых портативных устройствах и носителях информации. Запоминающие устройства на основе флеш-памяти представлены в виде USB-флеш-накопителей и карт памяти [2].

USB-флеш-накопитель — запоминающее устройство, использующее в качестве носителя флеш-память и подключаемое к компьютеру или иному считывающему устройству по интерфейсу USB, иногда microUSB. Обычный размер — от 3 до 5 см, вес — меньше 60 г. Они меньше, быстрее, имеют гораздо большую ёмкость и более прочны и надежны, по сравнению с компакт-дисками и дискетами, потому что у них нет движущихся частей. Кроме того, они невосприимчивы к магнитным полям и не подвергаются воздействию поверхностных царапин [3].

Карта памяти — компактное электронное запоминающее устройство, используемое для хранения цифровой информации. Форматы карты памяти:

- SD емкости от 128 Мб до 2 Гб;
- SDHC (SD High Capacity Высокая Емкость) емкости от 4 Гб до 32 Гб;
- SDXC (SD Extended Capacity Расширенная Емкость) емкости от 64 Гб до 2 Тб [4];
- SDUC (SD Ultra Capacity) емкости до 128 Тб [4].

Для миниатюрных приборов разработаны miniSD размером 20×21,5×1,4 мм и самая маленькая из всех карт — MicroSD размером 11×15×1 мм [5].

Накопитель на жёстких магнитных дисках, жёсткий диск, винчестер (HDD) — запоминающее устройство (устройство хранения информации)

произвольного доступа, основанное на принципе магнитной записи. Данный носитель предназначен для длительного хранения записанной на него информации. Основой HDD являются жесткие (алюминиевые) диски со специальным покрытием, на которое при помощи специальных головок записывается информация. Самые распространенные размеры жесткого диска — 2,5 и 3,5 дюйма. Показатель максимально возможного количества данных, которые можно будет вместить на диске (объем жесткого диска) может достигать 10 Тб [6].

Съемные энергонезависимые запоминающие устройства (СЭНЗУ), например СЭНЗУ-2М, могут поставляться в металлическом или в пластмассовом корпусе, их габаритные чертежи приведены на рисунке 1.

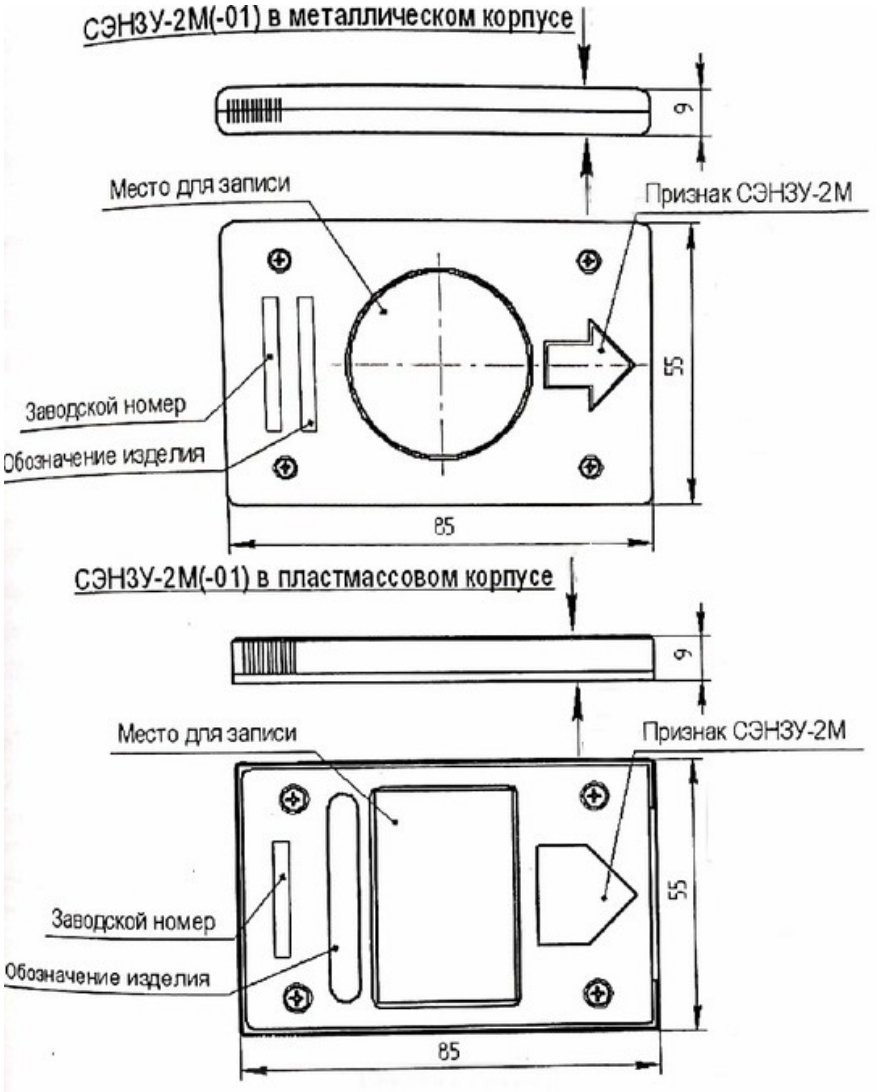


Рисунок 1 - Габаритный чертеж СЭНЗУ-2М-(01)

Энергонезависимая память позволяет хранить данные при отсутствии электрического питания. СЭНЗУ-2М имеет 2 Мбайт полной емкости и обеспечивает хранение информации в течение 30000 часов. Данное устройство рекомендуется использовать в качестве носителя информации, предназначенной для передачи по каналам связи [7].

Однако хранение именно ключевой информации на КЗУ, флеш-накопителях, жестких дисках и СЭНЗУ не допускается экспертной организацией, в отличие от других видов носителей, приведенных в списке выше.

Дискета — сменный носитель информации, используемый для многократной записи и хранения данных. Представляет собой помещённый в защитный пластиковый корпус диск, покрытый ферромагнитным слоем.

Габариты существующих дискет варьируются от 2 до 8 дюймов с различной плотностью записи данных (одинарной, двойной, четверной, высокой и расширенной). Информационная емкость дискет составляет от 80 до 1440 Кбайт. Срок хранения информации — не более 5 лет.

Компакт-диск (CD) — переносной оптический диск для хранения информации в цифровом виде.

Стандартные CD имеют диаметр 120 мм, могут вместить около 700 Мбайт данных. Срок хранения информации — не более 5 лет. Mini CD имеют разные диаметры в интервале от 60 до 80 мм.

CD изготавливаются из 1,2 мм поликарбонатного пластика и весит 15-20 г. Тонкий слой алюминия наносится на поверхность, что делает ее отражающей для световых лучей. Металл защищен пленкой лака. CD подвержены повреждениям при использовании и от воздействия окружающей среды.

Устройство электронное «К1634ДК6» имеет информационную емкость 512 Кбайт. Время хранения информации при любых режимах непрерывного обращения к устройству составляет 5 лет. Масса устройства не превышает 7,5 г. Габаритный чертеж электронного ключа представлен на рисунке 2.

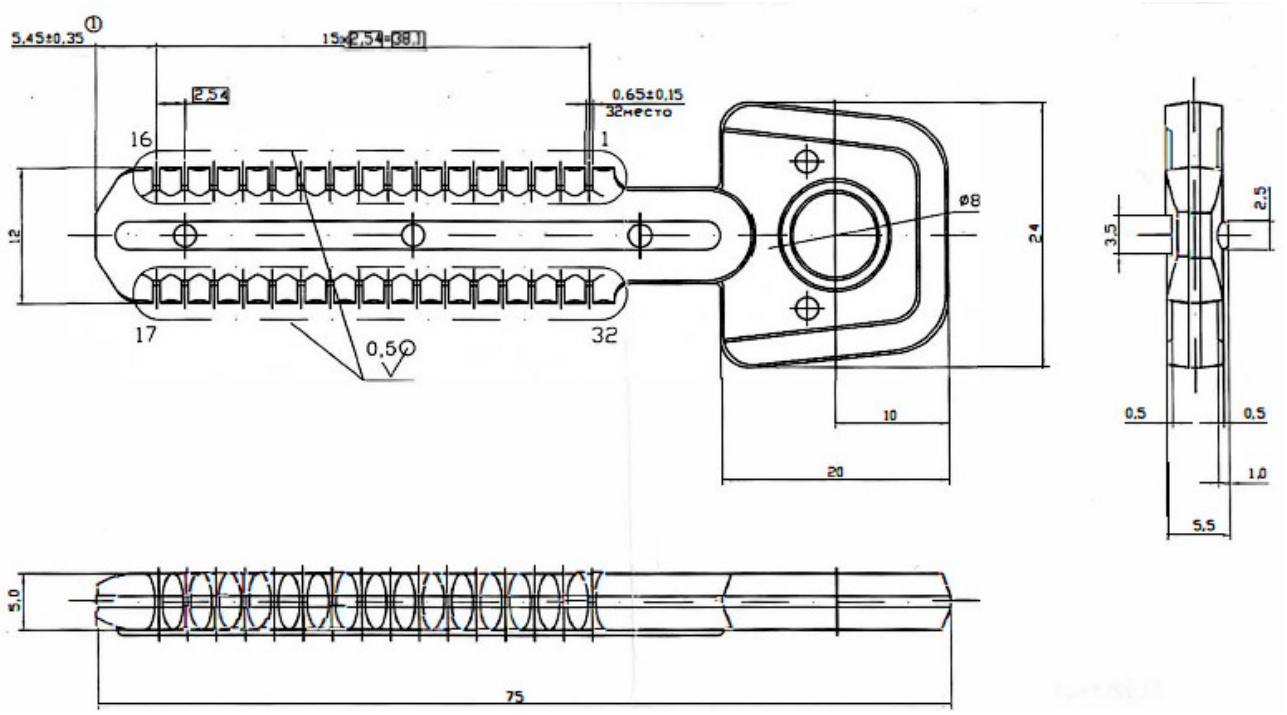


Рисунок 2 - Габаритный чертеж устройства «К1634ДК6» [8]

На рисунке 2 также приведена нумерация выводов электронного ключа (против часовой стрелки). Назначение выводов устройства приведено в таблице 1.

Таблица 1 - Назначение выводов

Номер вывода	Назначение вывода
1-12, 22, 25-30	Вход разряда адреса
13-15, 17-20, 24	Вход/выход разряда данных
16	Общий вывод
21	Вход сигнала разрешения выдачи данных
23	Сигнал разрешения обращения к устройству
31	Вывод разрешения записи
32	Вывод питания

Российская интеллектуальная карта (РИК) — микропроцессорная карта, которая выполнена на основе отечественного микроконтроллера КБ5004ВЕ1 с операционной системой ОС UniCos. Структура карты и операционная система

обеспечивают возможность реализации широкого спектра различных приложений на базе РИК.

Список приложений, использующих РИК, а также тех, в которых ее применение является перспективным, широк и включает в себя следующие области:

- электронные удостоверения различного рода;
- носитель ключевой информации для систем защищенного электронного документооборота и других приложений;
- защита компьютера от несанкционированного доступа.

Основные технические характеристики РИК:

- 8-разрядный микроконтроллер с RISC-архитектурой;
- 256 байт оперативной памяти (ОЗУ);
- электрически стираемое перепрограммируемое постоянное запоминающее устройство (ЭСППЗУ) емкостью 2 Кбайт;
- не менее 10 лет хранения записанной информации;
- не менее 100000 циклов стирания/записи;
- технология изготовления микросхемы — комплементарная структура металл-оксид-полупроводник (КМОП).

Внешний вид РИК приведен на рисунке 3.

Рисунок 3 - Российская интеллектуальная карта [9]

Бумажные носители информации обладают следующими достоинствами:

- длительный срок хранения информации (до 12 лет);
- простота экстренного уничтожения;
- низкая стоимость;
- легкость транспортировки;
- простота изготовления.

Ключевая информация на бумажном носителе может храниться в нескольких вариантах:

- ключевая информация нанесена на перфоленту;
- ключевая информация хранится на бумажном носителе в открытом виде для непосредственного ввода ее в аппаратуру с помощью устройства ввода;
- ключевая информация закодирована и представлена на бумажном носителе в виде штрих-кода.

Перфолента — носитель информации в виде бумажной ленты с отверстиями, неудобен в использовании. Емкость информации, нанесенной на перфоленту, составляет от единиц байт до нескольких килобайт, при этом увеличивается длина самой перфоленты.

Хранение ключевой информации в открытом виде и ее непосредственный ввод порождает угрозы утечки ключевой информации по оптическому каналу.

Наиболее безопасным является хранение ключевой информации на бумажном носителе в виде штрих-кода, что обеспечивает конфиденциальность ключевой информации. Ее ввод осуществляется с помощью специальных устройств считывания (сканеров) с последующим декодированием штрихового кода.

Существуют различные виды штриховых кодов, примеры некоторых из них приведены на рисунках 4 и 5.

Рисунок 4 - Примеры штриховых кодов (часть 1)

Рисунок 5 - Примеры штриховых кодов (часть 2)

На сегодняшний день сертифицирован и стандартизирован штриховой код PDF417 [10], а также перспективным является использование символик QR Code и Data Matrix.

Емкость закодированной информации, нанесенной на бумажный носитель в виде штрих-кода, зависит от геометрических размеров его области, версии символа штрих-кода, уровня коррекции ошибок, ширины модуля, числа строк и столбцов в матрице символа и других параметров. В настоящее время экспертной организацией сертифицированы носители со штриховым кодом PDF417, содержащим 64 и 108 байт полезной информации. Изменяя параметры штрих-кода, но сохраняя при этом его геометрические размеры, теоретически можно достичь до 800 байт полезной информации.

Символ штрих-кода Data Matrix может иметь, к примеру, 576 байт полезной информации при геометрических размерах его области 20×20 мм.

Информационная емкость символа QR Code может составлять:

- 718 байт при низком уровне коррекции ошибок;
- 560 байт при среднем уровне коррекции ошибок;
- 394 байт при повышенном уровне коррекции ошибок;
- 310 байт при высоком уровне коррекции ошибок.

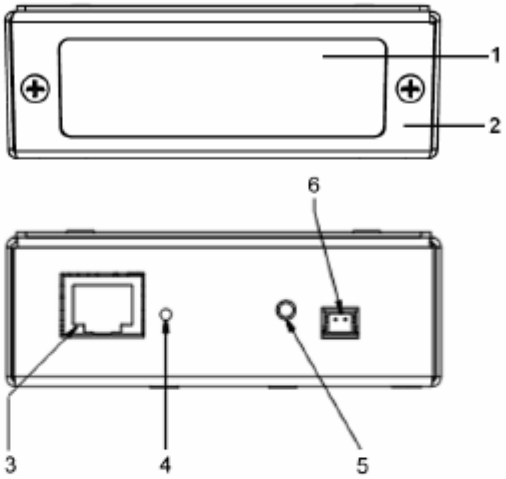
Таким образом, в результате анализа существующих носителей информации был сделан вывод о том, что наиболее подходящим для хранения ключевой информации является бумажный носитель с нанесенным штриховым кодом.

2 Обзор существующих устройств считывания информации с бумажного носителя

На основании полученного вывода о том, что наиболее предпочтительным является представление ключевой информации в виде штрих-кода на бумажном носителе, был выполнен обзор существующих устройств считывания (сканеров) информации с бумажных носителей.

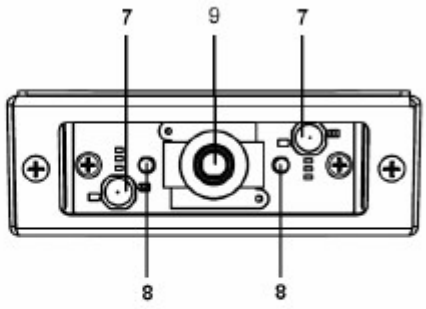
Встраиваемый сканер «IronScan» фирмы «VMC» предназначен для чтения линейных (EAN-13, Code 39, Code 128 и т. п.), гибридных (PDF417 и т. п.) и двухмерных (Aztec, Data Matrix, QR Code и т. п.) штриховых символик с любой поверхности в стационарном режиме работы. Чтение штрих-кода происходит в стационарном режиме при проявлении штрих-кода в зоне видимости сканера.

Внешний вид сканера и считывающая область представлена на рисунках 6 и 7 соответственно.



1. Считывающая область.
2. Корпус.
3. Интерфейсный разъём.
4. Кнопка настройки.
5. Индикатор считывания ШК
6. Разъем для подключения внешней кнопки управления считыванием

Рисунок 6 - Внешний вид сканера «IronScan»



7. Прицельные светодиоды.
8. Светодиоды подсветки.
9. Объектив.

Рисунок 7 - Считывающая область сканера «IronScan»

Технические характеристики сканера «IronScan»:

– габаритные размеры сканера: 80×88×31 мм;

– масса: 300 г;

– размер зоны сканирования зависит от расстояния до сканера (расстояние: ширина×высота):

а) 50 мм: 31×22 мм;

б) 100 мм: 62×45 мм;

в) 150 мм: 94×67 мм;

г) 200 мм: 125×89 мм;

д) 250 мм: 156×111 мм;

– угол обзора:

а) по ширине — 32º;

б) по высоте — 24º;

– поддерживаемые интерфейсы: RS232, USB;

– считываемые символики штрихового кода: EAN-13, EAN-8, UPC-A, UPC-E, Code 39, Code 128, Interleaved 2 of 5, PDF417, Aztec, DataMatrix, QR Code, Micro QR Code, Pharma Code (список поддерживаемых символик пополняется);

– температура эксплуатации: от минус 5 до плюс 40 °С [11].

Ручной сканер штриховых кодов «BurstScan» фирмы «VMC» предназначен для чтения линейных (EAN-13, Code 39, Code 128 и т. п.), гибридных (PDF417 и т. п.) и двухмерных (Aztec, Data Matrix, QR Code и т. п.) штриховых символик с любой поверхности. Он может быть использован в следующих режимах работы:

– в ручном режиме считывание штрих-кода инициируется нажатием на курок;

– в стационарном режиме активация алгоритмов чтения штрих-кода происходит при детекции движения в поле зрения сканера; до момента детектирования движения сканер находится в режиме малого энергопотребления;

– в конвейерном режиме алгоритмы считывания штрих-кода работают постоянно, осуществляя попытки распознавания штрих-кода в поле зрения сканера; режим характеризуется максимальной скоростью распознавания, но при этом повышенным энергопотреблением.

Внешний вид и считывающее окно сканера «BurstScan» приведены на рисунках 8 и 9 соответственно.

1. Считывающее окно;
2. Курок;
3. Индикатор считывания ШК;
4. Корпус;
5. Разъём;
6. Кабель;

Рисунок 8 - Внешний вид сканера «BurstScan»

7. Объектив;
8. Прицельные светодиоды;
9. Светодиоды подсветки.

Рисунок 9 - Считывающее окно сканера «BurstScan»

Технические характеристики сканера «BurstScan»:

- габаритные размеры сканера: 149×145×72 мм;
- масса: 180 г;
- минимальная ширина элемента штрих-кода: 0,12 мм;
- угол обзора:

а) по ширине — 32º;

б) по высоте — 24º;

- поддерживаемые интерфейсы: RS232, USB;
- считываемые символики штрихового кода: EAN-13, EAN-8, UPC-A, UPC-E, Code 39, Code 93, Code 128, 2 of 5 interleaved, PDF417, MicroPDF417, Aztec Code, Aztec Runes, DataMatrix, QR Code, Micro QR Code, Pharma Code;
- рабочая температура: от минус 5 до плюс 50 °С;
- рабочая влажность (без конденсата): от 10 до 90 % [12].

Модели MS9520 и MS9540 одноплоскостных ручных лазерных сканеров «Voyager» американской компании «Metrologic» предназначены для считывания всех стандартных штрих-кодов. Способны работать как в ручном, так и в стационарном режимах. Внешний вид сканера представлен на рисунке 10.

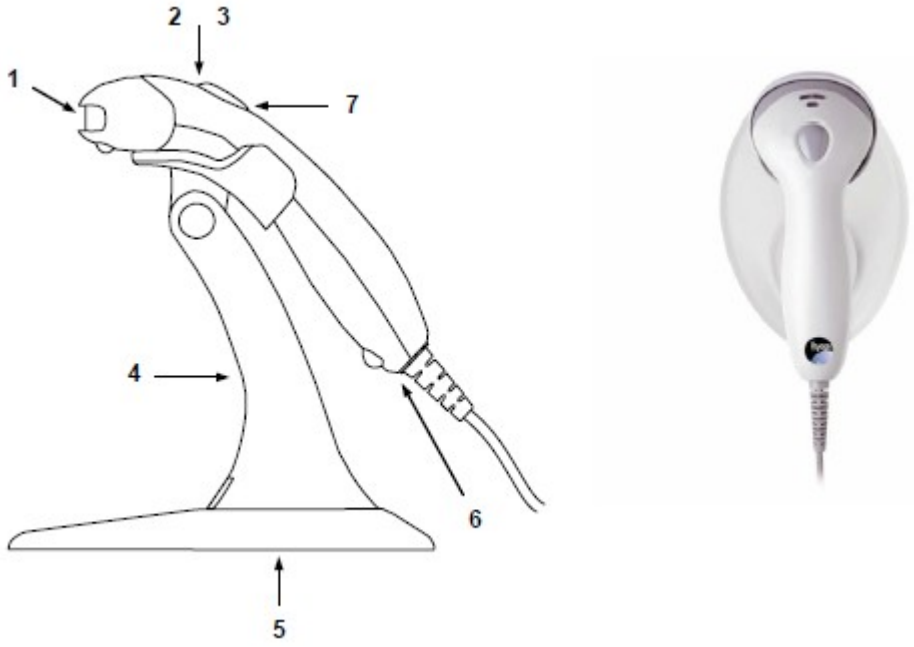


Рисунок 10 - Внешний вид сканера Metrologic MS9520 (MS9540) Voyager

На рисунке 9 приведены следующие обозначения:

- 1: окно сканирования;
- 2: красный и зеленый светодиоды;
- 3: желтый светодиод (активен при использовании сканера в стационарном режиме, только для модели сканера MS9540);
- 4: подставка:
- 5: платформа:
- 6: гнездо для подключения 10-контактного разъема;
- 7: кнопка (для передачи считанного штрихового кода, только для модели сканера MS9540).

Технические характеристики:

- габаритные размеры: 40×198×78 мм;
- масса: 149 г;
- минимальная ширина штриха: 0,132 мм;
- читаемые штриховые коды: автоматическое распознавание всех стандартных штриховых кодов;

- вращение, угол, наклон: 42º, 68º, 52º;
- температура эксплуатации: от 0 до плюс 40 ℃;
- влажность: от 5 до 95 % при отсутствии конденсата;
- уровень освещенности: до 4842 люкс;
- температура хранения: от минус 40 до плюс 60 ℃;
- вентиляция не требуется [13].

Цифровой планшетный сканер HP Scanjet 3770 предназначен для получения изображений и документов в цифровом виде. Внешний вид сканера HP Scanjet 3770 со встроенным адаптером прозрачных материалов представлен на рисунке 11.

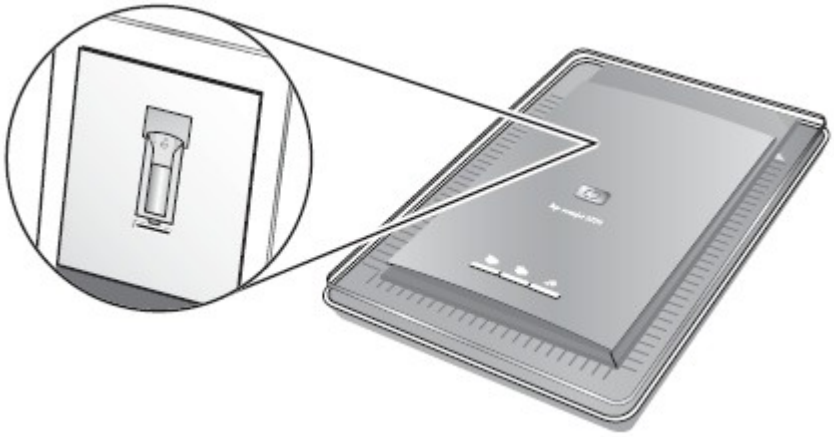


Рисунок 11 - Внешний вид сканера «HP Scanjet 3770»

Технические характеристики:

- масса: 2,008 кг;
- габаритные размеры (с крышкой): 286,85×435,51×65,46 мм;
- выбираемое разрешение: от 12 точек на дюйм (dpi) до 999999 точек на дюйм (dpi) при масштабировании 100 %;
- температура эксплуатации: от плюс 10 до плюс 35 ℃;
- температура хранения: от минус 40 до плюс 70 ℃;
- относительная влажность: от 15 до 80 % без конденсации [14].

Сканер штрих-кодов «ICS-7199» фирмы «Proton» - сканер, в основе оптической системы которого используется фотоматрица, позволяющая считывать как линейные, так и двухмерные коды. В дополнение обладает способностью сканирования OCR-символов, номеров с банкнот и изображений. Внешний вид сканера «ICS-7199» приведен на рисунке 12.

Рисунок 12 - Внешний вид сканера «ICS-7199»

Технические характеристики:

- масса: 146 г;
- длина: 165 мм;
- ширина ручки: 32 мм;
- ширина «головы»: 72,8 мм;
- высота ручки: 54,7 мм;
- высота «головы»: 82,5 мм;
- поддерживаемые интерфейсы: RS232, USB HID, USB-COM;

– читаемые штриховые коды: UPC-A, UPC-Eo, EAN-13, EAN-8, Code-39, Interleaved 2 of 5, Industrial 2 of 5, Codabar, Code-128, Code-93, GS1 DataBar, PosiCode A&B, Code 49, PDF417, MicroPDF417;

– расстояние считывания: для линейных кодов 37-175 мм, для двухмерных кодов 62-137 мм;

– температура эксплуатации: от 0 до плюс 50 ℃;

– температура хранения: от минус 20 до плюс 60 ℃;

– допустимая влажность: до 95 % без конденсата;

– ударопрочность: выдерживает многократные падения с высоты 1,8 м на бетонную поверхность [15].

Результаты обзора существующих устройств считывания информации с бумажного носителя были сведены в таблицу 2.

Таблица 2 - Результаты обзора существующих сканирующих устройств

Наименование	Назначение	Страна-производитель	Основные считываемые штрих-коды	Конструкция	Температура окружающей среды при эксплуатации, ℃
VMC IronScan	Сканер штрих-кодов	Россия	PDF417, QR Code, Data Matrix	Встраиваемый сканер	от минус 5 до плюс 40
VMC BurstScan	Сканер штрих-кодов	Россия	PDF417, QR Code, Data Matrix	Ручной сканер	от минус 5 до плюс 50
Metrologic MS9520 (MS9540) Voyager	Сканер штрих-кодов	США	PDF417, QR Code, Data Matrix	Ручной сканер	от 0 до плюс 40
HP Scanjet 3770	Сканер изображений и документов	США	-	Планшетный сканер	от плюс 10 до плюс 35
Proton ICS-7199	Сканер штрих-кодов	Россия	PDF417	Ручной сканер	от 0 до плюс 50

По итогам обзора существующих устройств считывания ключевой информации с бумажного носителя был сделан вывод о недопустимости их применения в аппаратуре криптографической защиты информации и необходимости разработки нового устройства.

Совместно с возможностью считывания информации с бумажного носителя необходима поддержка ввода ключевой информации большего объема с электронного ключа «К1634ДК6». Существующие устройства такой особенностью не обладают.

Актуальность выбранной темы выпускной квалификационной работы объясняется также необходимостью применения в составе устройства только отечественных комплектующих изделий и только доверенного программного обеспечения (ПО) собственной разработки. Большинство существующих устройств считывания информации являются изделиями импортного производства, что влечет за собой отсутствие полного комплекта документации на данные изделия (перечень элементов, описания на электрорадиоизделия, схемы электрические и др.), применение недоверенной электронной компонентной базы и ПО. Указанные факторы приводят к возникновению угрозы внедрения аппаратных и программных закладок и утечки ключевой информации, обрабатываемой в процессе эксплуатации устройства.

Разработка нового устройства ввода ключевой информации с применением только отечественной электронной компонентной базы и доверенного ПО обеспечивает независимость от импорта в случае прекращения производства необходимых изделий за рубежом, либо прекращения поставок на российский рынок, что актуально на сегодняшний день в условиях применения санкций.

3 Анализ требований к устройству ввода ключевой информации

3.1 Общие сведения

Устройство ввода ключевой информации для аппаратуры криптографической защиты должно соответствовать ряду требований, которые были разделены на следующие группы:

- конструктивные;
- схемотехнические;
- специальные;
- требования к электронной компонентной базе (ЭКБ);
- требования по стойкости к внешним воздействующим факторам.

3.2 Конструктивные требования

УВК является устройством в составе аппаратуры криптографической защиты информации, поэтому оно должно быть выполнено в виде отдельного законченного блока. Аппаратура должна размещаться на объекте эксплуатации в стойке 19".

Узел установки бумажного носителя и узел установки ДК6 должны быть выведены на лицевую панель УВК.

Узел установки бумажного носителя ключевой информации должен иметь подвижную крышку, которая должна обеспечивать прижатие носителя к защитному стеклу для удобной ручной фиксированной установки бумажного носителя. Крышка в закрытом положении должна иметь приспособление для опечатывания. Работа с открытой крышкой должна блокироваться.

Узел установки ДК6 должен представлять собой устройство контактное, закрываемое крышкой с приспособлением для опечатывания. Работа с открытой крышкой узла установки ДК6 должна блокироваться.

В УВК должна быть предусмотрена выдача сообщений о неисправностях, и выходе из строя составных частей устройства с помощью внешнего индикатора, осветителя и по внешнему интерфейсу. Индикатор должен быть расположен на лицевой панели устройства, чтобы обеспечивалось удобное наблюдение из рабочего положения оператора.

Масса УВК не должна превышать 3 кг. Габаритные размеры устройства должны соответствовать следующим параметрам:

- длина — не более 350 мм;
- ширина — не более 300 мм;
- высота — не более 120 мм.

УВК должно обеспечивать механическое и электрическое сопряжение с блоком преобразования данных (БПД) для гарантированной и надежной передачи считанной с бумажного носителя или ДК6 и декодированной ключевой информации.

К УВК предъявляются требования к покрытиям, наносящимся на поверхность устройства, и маркировке. Согласно ГОСТ РВ 20.39.309-98 [16], при выборе металлических, неметаллических, неорганических и лакокрасочных покрытий предпочтение должно быть отдано покрытиям, удаление пыли и грязи с которых производится без затруднений. Покрытия должны обеспечивать необходимую коррозионную стойкость и декоративный вид УВК при эксплуатации, при хранении с соблюдением требований по консервации, а также при хранении изделия при производстве и эксплуатации.

Лицевая панель УВК во избежание возникновения бликов должна иметь матовое или полуматовое покрытие. Цвет лицевой панели должен отличаться от цвета внешних управляющих элементов (ВУЭ) и формообразующих поверхностей устройства. Цветовой контраст между лицевой панелью и ВУЭ должен быть сильнее, чем между лицевой панелью и формообразующими поверхностями УВК. Цвет ВУЭ должен соответствовать общему цветовому

оформлению устройства. Для цветового кодирования отдельных ВУЭ (аварийных, требуемых для немедленного использования и т.п.) допускается пользоваться яркими хроматическими цветами.

Маркировку следует наносить на несъемных частях УВК, доступных для обзора. Маркировка должна быть устойчивой в течение всего срока службы устройства, механически прочной и не должна стираться или смазываться жидкостями, используемыми при эксплуатации, или должна легко восстанавливаться в процессе эксплуатации. Маркировка не должна раскрывать назначение устройства, его характеристики и параметры.

На УВК должно быть нанесено обозначение электрического соединителя, позволяющее определить сопрягаемые части. Индикаторы, внешние крышки узлов установки носителей ключевой информации должны быть промаркированы. На поверхности УВК должны быть нанесены наименование устройства и заводской номер.

На концы проводов, междуплатных кабелей и жгутов в устройстве должны быть нанесены цветные, буквенные, цифровые или буквенно-цифровые обозначения. Общее число различных по цвету надписей или символов на одном приборе не должно превышать пяти.

3.3 Схемотехнические требования

УВК должно соответствовать следующим схемотехническим требованиям:

- УВК должно быть разбито на отдельные функциональные части (платы, ячейки, узлы и т. п.);
- связи между функциональными частями УВК должны быть выполнены гибкими кабелями;
- внешний соединитель должен позволять осуществлять сопряжение с БПД методом «врубания»;

– сильно нагревающиеся и потребляющие элементы (силовые транзисторы, модули питания и т. п.) должны размещаться на корпусе УВК;

– для экономии и снижения потребления энергоемкие узлы УВК в статическом режиме должны переходить в режим пониженного потребления (режим «сна»);

– на печатных платах должны быть заложены контрольные точки, тестовые и технологические соединители, обеспечивающие контроль печатных плат при изготовлении и проверке;

– с целью исключения повышенных токов утечки, образования коротких замыканий между выводами электрорадиоизделий, загрязнения, попадания влаги необходимо проводить дополнительную защиту печатных плат (герметизацию). В качестве дополнительной защиты необходимо использовать защитные покрытия из органических материалов.

3.4 Специальные требования

Для выполнения требований по электромагнитной совместимости и помехозащищенности в УВК должны быть предусмотрены следующие меры:

– непрерывное экранирование внутреннего пространства от радиоизлучений;

– непрерывное экранирование внутреннего пространства от светового излучения;

– непрерывное экранирование источника демаскирующих излучений;

– фильтрация питающих и сигнальных внешних цепей;

– использование низковольтных сигналов на внешних стыках;

– контроль сигналов датчиков несанкционированного доступа к внутренним узлам;

– контроль сигналов датчиков положения внешних крышек узлов установки носителей;

– минимальное количество съемных крышек;

– опечатывание внешних крышек;

– контроль напряжений питания;

– дублирование критических цепей;

– выполнение начального, динамического и периодического контроля;

– отсутствие повторов при передаче ключевой информации;

– невозможность изменения штатного ПО через внешний интерфейс.

3.5 Требования к электронной компонентной базе

В составе УВК должна применяться перспективная ЭКБ, соответствующая современному уровню развития электрорадиоизделий (ЭРИ).

ЭКБ должна соответствовать следующим требованиям:

– в составе УВК должна применяться только ЭКБ отечественного производства;

– в составе УВК должны быть применены элементы, которые приведены в перечнях электрорадиоизделий, разрешенных для применения при разработке, модернизации, производстве и эксплуатации вооружения, военной и специальной техники;

– должна применяться ЭКБ категории качества «ОС», «ОСМ», а при их отсутствии - «ВП»;

– в разрабатываемом УВК, в первую очередь, должны применяться комплектующие элементы, предназначенные для автоматизированного монтажа;

– разработчиком ЭКБ должен быть выпущен полный комплект документации;

– ЭКБ должна соответствовать требованиям по стойкости к внешним воздействующим факторам;

– применять элементы, не удовлетворяющие требованиям, предъявляемым к аппаратуре по стойкости к внешним воздействующим факторам, допускается при обеспечении конструктивных мер индивидуальной или общей защиты (амортизация, термостатирование, экранирование, герметизация и т.п.), обеспечивающих условия работы этих элементов.

3.6 Требования по стойкости к внешним воздействующим факторам

УВК должно быть стойким к воздействию механических и климатических факторов:

– рабочая температура среды — от минус 40 до плюс 50 °С;

– температура среды при хранении (предельная температура) — от минус 60 до плюс 70 °С;

– относительная влажность при температуре 25 °С — 80 %;

– не допускается наличие резонанса элементов конструкции УВК в диапазоне до 25 Гц.

4 Анализ технических каналов утечки ключевой информации при ее обработке устройством ввода ключевой информации и передаче блоку преобразования данных

При обработке УВК и передаче БПД ключевой информации существует риск ее утечки по следующим каналам:

- по каналу побочных электромагнитных излучений и наводок (далее — ПЭМИН);
- по питающим и сигнальным цепям;
- по визуально-оптическому каналу.

Одним из основных каналов утечки ключевой информации при ее обработке УВК и передаче БПД является электромагнитный канал, порождаемый побочными электромагнитными излучениями его составляющих элементов. Побочные электромагнитные излучения (ПЭМИ) — это паразитные электромагнитные излучения радиодиапазона, создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными [17].

Существуют три вида паразитных связей:

- емкостная;
- индуктивная;
- гальваническая.

Емкостная паразитная связь обусловлена воздействием электрического поля, индуктивная — воздействием магнитного поля, гальваническая паразитная связь образуется через общее активное сопротивление.

С целью раскрытия защищаемой ключевой информации возможен перехват побочных электромагнитных излучений элементов УВК, как технического средства приема, обработки и хранения информации (ТСПИ). В УВК, в частности и в линиях связи, входящих в его состав, носителем

информации является электрический ток, характеристики которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по проводникам вокруг них в окружающем пространстве возникает электрическое и магнитное поля. По этой причине элементы УВК можно рассматривать как излучатели электромагнитного поля, составляющие которого модулированы по закону изменения информационного сигнала.

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования [17].

ПЭМИ являются причиной возникновения наводки опасных сигналов в посторонних токоведущих линиях и конструкциях. Наводки электромагнитных излучений возникают при излучении элементами и соединительными линиями, входящими в состав УВК, информационных сигналов, при наличии гальванической связи соединительных линий УВК и посторонних проводников либо линий вспомогательных технических средств и систем (ВТСС).

Цепь ВТСС, посторонние проводники, способные принимать побочные электромагнитные излучения, называются случайной антенной.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенная случайная антенна представляет собой компактное техническое средство, например, телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д. К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации [18].

Уровень наводимых сигналов в большей степени зависит от мощности излучаемых сигналов, расстояния до проводников и линий ВТСС, а также совместного пробега линий ТСПИ и посторонних проводников либо линий ВТСС.

Схема канала утечки ключевой информации, обусловленного побочными электромагнитными излучениями и наводками, представлена на рисунке 13.

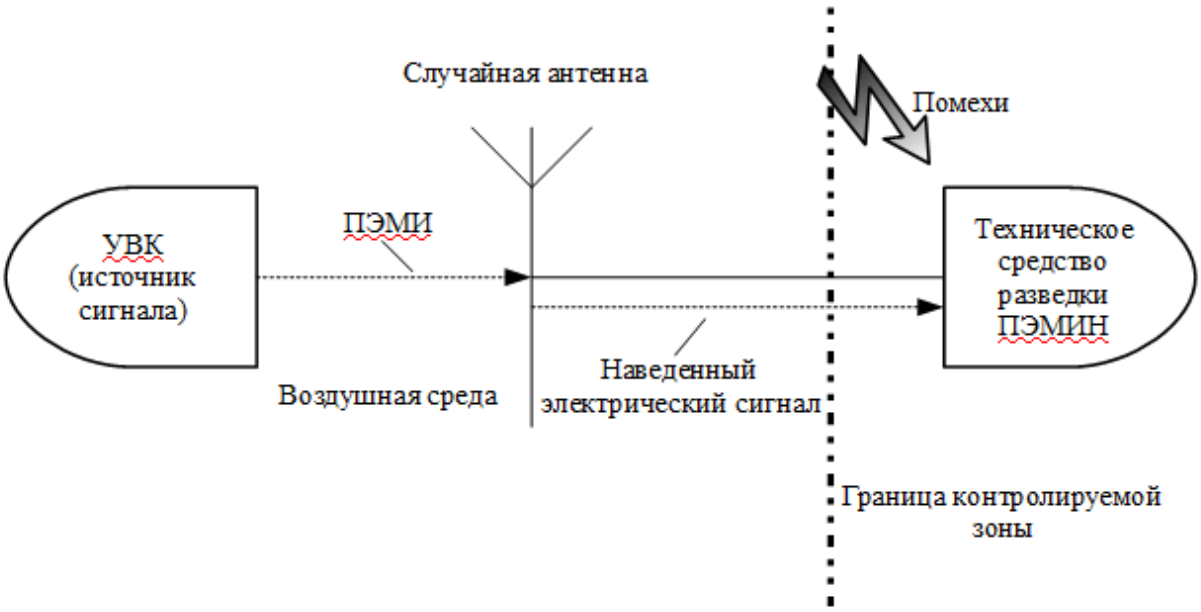


Рисунок 13 - Схема канала утечки информации посредством ПЭМИН

Визуально-оптический канал утечки информации реализуется при непосредственном восприятием глазом человека объектов окружающей обстановки путем наблюдения с использованием специальных технических средств, позволяющих расширить возможности по сбору информации в условиях плохой видимости: недостаточной освещенности, при удаленности объектов наблюдения, недостаточности углового разрешения. Перехват ключевой информации по рассматриваемому каналу ведется путем наблюдения за объектами и местностью с помощью различных увеличительных оптических или усиливающих яркость изображения приборов видимого и инфракрасного (ИК) диапазона (биноклей, стереотруб, перископов, приборов ночного видения, тепловизоров и т.п.).

В оптическом диапазоне (совокупности видимого и инфракрасного света) добывание защищаемой ключевой информации возможно следующими способами:

– визуальным и визуально-оптическим наблюдением;

– фото и видеосъемкой;

– наблюдением с применением приборов ночного видения и тепловизоров.

Тепловизор – измерительный прибор, который позволяет видеть тепловое (инфракрасное) излучение окружающих объектов в любое время суток, измерять температуру в любой точке на поверхности с точностью 0,1 °С и выше.

Схема визуально-оптического канала утечки ключевой информации представлена на рисунке 14.

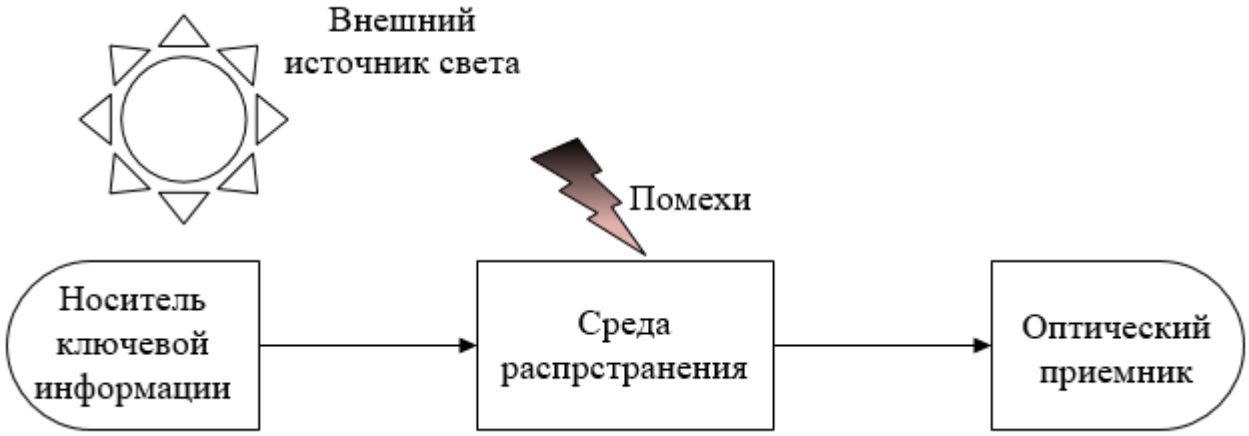


Рисунок 14 - Схема визуально-оптического канала утечки информации

Канал утечки по питающим и сигнальным цепям обусловлен возникающими в них наводками. Наводка - ток и напряжение в токопроводящих элементах, вызванный электромагнитным излучением, емкостными и индуктивными связями [19]. Различают симметричные и асимметричные наводки.

Асимметричные наводки имеют место быть, когда провода сети питания источника и приемника наводки прокладываются вместе и имеют одинаковые емкости относительно источника и приемника наводки. В них наводятся одинаковые по величине и по фазе относительно земли и корпусов приборов напряжения. В этом случае оба провода сети питания передают сигнал наводки в одном направлении. Обратным проводом является земля.

Симметричное распространение наводки имеет место быть, когда на проводах сети индуцируются различные напряжения относительно земли. Между проводами образуется высокочастотная разность потенциалов, и по проводам сети проходят токи наводки в разных направлениях. В приемнике наводки индуцируются равные по величине и обратные по знаку напряжения, которые не могут проникнуть в высокочастотную часть приемника и не являются опасными.

Опасный сигнал может проникнуть в цепи электропитания в результате того, что среднее значение потребляемого тока в большей или меньшей степени зависит от амплитуды информационного сигнала, что приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Одними из основных устройств, без которых невозможна работа любого технического средства, являются вторичные источники питания. Эти источники предназначены для преобразования подводимой к ним энергии от сети переменного тока или постоянного тока (например, напряжением 27 В) в энергию постоянного или переменного тока с напряжением, необходимым для питания аппаратуры технических средств. При определенных условиях вторичные источники питания совместно с подводящими питающими линиями могут создавать условия для утечки информации, циркулирующей в техническом средстве. Несмотря на большое разнообразие конкретных технических решений схем построения таких источников питания, все они содержат в своем составе трансформаторы, выпрямители, сглаживающие фильтры, стабилизаторы и обладают конечным внутренним сопротивлением. При наличии в составе технических средств усилительных каскадов токи усиливаемых в них сигналов замыкаются через вторичный источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, изменяющееся в соответствии с законом изменения усиливаемого (опасного) сигнала.

В процессе обработки ключевой информации процессор, входящий в состав узла вычислителя, потребляет разный ток в зависимости от режима работы (считывание из памяти, декодирование, обнаружение и исправление ошибок, передача информации и т. д.). Данный фактор является демаскирующим и позволяет злоумышленнику отследить динамику потребления тока вычислителем, проанализировать, как процесс потребления меняется во времени, определить и отследить режимы работы УВК.

Перехват информационных сигналов возможен путем непосредственного подключения к цепям электропитания. Для этих целей используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Для перехвата информации по цепям электропитания злоумышленник может применять специальные закладные устройства, встраиваемые в приборы, питающиеся от сети.

Передающее устройство состоит из микрофона, усилителя и передатчика несущей низкой частоты. Оно легко камуфлируется под различного рода электроприборы, не требуют дополнительного питания от батарей и трудно обнаруживаются при использовании поисковой аппаратуры, широко применяемой в настоящее время.

5 Выбор мер защиты информации, обрабатываемой устройством ввода ключевой информации

5.1 Меры защиты ключевой информации от утечки по каналу побочных электромагнитных излучений и наводок

Основным способом защиты ключевой информации от утечки за счет ПЭМИН, который необходимо применить, является экранирование.

Экранирование направлено на уменьшение паразитных связей и преграждение распространения побочной электромагнитной энергии за пределы контролируемой зоны.

Так как введение экранов часто требует значительного изменения конструкции, компоновки, а иногда и габаритов изделия, рекомендуется уже на начальном этапе конструирования применять все возможные меры для уменьшения паразитных связей.

Для экранирования внутреннего пространства корпус УВК необходимо выполнить из таких материалов, как: медь, алюминий, свинец, сталь. Тогда сам корпус устройства будет выполнять роль защитного экрана. Исходя из требований к массе устройства, предпочтение отдается алюминиевому корпусу.

Увеличение толщины стенок экрана приводит к повышению эффективности экранирования, однако увеличивает массу и габариты устройства.

Для предотвращения распространения ПЭМИ съемная крышка корпуса УВК и крышки узлов установки носителей по всему периметру должны быть оборудованы выступами типа «лабиринт» со специальным уплотнителем из токопроводящего материала. Данный способ защиты также применяется к внешнему разъему, предназначенному для сопряжения с БПД.

Экранированию подлежит не только блок УВК целиком, но и отдельные его элементы, в том числе и соединительные линии.

Наилучшую защиту как от электрического, так и от магнитного полей обеспечивают информационные линии связи типа экранированного бифиляра, трифиляра (трех скрученных вместе проводов из которых один используется в качестве электрического экрана), триаксиального кабеля (изолированного коаксиального кабеля, помещенного в электрический экран), экранированного плоского кабеля (плоского многопроводного кабеля, покрытого с одной или обеих сторон медной фольгой). Высокая эффективность экранирования обеспечивается при использовании витой пары, защищенной экранирующей оболочкой.

Для эффективной защиты передаваемой по линиям связи информации и уменьшения уровня ПЭМИ, необходимо тщательно выполнить соединение экрана с корпусом УВК. Такое соединение нужно осуществить путем непосредственного контакта (пайки или сварки) с корпусом.

Экранированию подлежат, в первую очередь, линии связи, по которым передаются аналоговые сигналы, так как они более подвержены воздействиям наводок, по сравнению с цифровыми сигналами.

Для обеспечения защищенности ключевой информации должны быть экранированы печатные платы. Для этого несколько слоев печатной платы (как правило, два внешних слоя) заливаются сплошным слоем металла и заземляются на корпус устройства.

Необходимо обеспечить экранирование индикатора устройства для предотвращения распространения ПЭМИ. Для этого с внутренней стороны корпуса УВК на индикатор устанавливается экранирующая сетка, например, из меди.

Экранирующий эффект повышается с увеличением магнитной проницаемости и проводимости экрана, поэтому экранирующий эффект поглощения у магнитных экранов существенно больше, чем у немагнитных экранов. Так экранирующий эффект поглощения стали приблизительно в четыре раза выше, чем экранирующий эффект поглощения меди.

Наибольшей величиной экранного затухания поглощения для немагнитных экранов обладает медь, затем идёт алюминий и свинец. Величина экранного затухания поглощения для свинца в 100 раз меньше, чем для меди. Это объясняется плохой проводимостью свинца. В частотном диапазоне примерно до 1 МГц наибольшим эффектом обладают медные и алюминиевые экраны, а в более высоком спектре частот преимущество остаётся за стальными экранами.

Количественно эффективность электромагнитного экранирования (Э) можно определить отношением напряженностей поля в защищаемой области пространства при отсутствии экрана E_0 (H_0) и при его наличии E (H). Расчет эффективности экранирования осуществляется по формулам (1) и (2) для электрического и магнитного поля соответственно.

$$Э = E_0 / E \qquad (1)$$

$$Э = H_0 / H \qquad (2)$$

Для защиты от распространения ПЭМИН, а также для экранирования внутреннего пространства от радиоизлучений и светового излучения узлы установки бумажного и электронного носителей ключевой информации оборудованы внешними подвижными крышками с приспособлениями для опечатывания. На узлах установки бумажного носителя и ДК6 установлены датчики положения внешних крышек, с помощью которых обеспечивается контроль положения внешних крышек, и работа УВК с открытыми крышками, таким образом, становится невозможна.

Для защиты ключевой информации от ее утечки за счет ПЭМИН целесообразно использование низковольтных сигналов на внешних стыках. Чем выше уровень передаваемого информационного сигнала, тем больше величина порождаемого излучения. Вследствие высокого уровня передаваемого сигнала

перехват излучения и распознавание информационного сигнала злоумышленником с применением технических средств разведки (ТСР) значительно упрощается. Чтобы избежать подобного случая и обеспечить низкий уровень напряжения сигналов на внешних стыках, сигнал с высоким уровнем напряжения предварительно поступает на микросхему (буфер), на выходе которой приобретает допустимый уровень напряжения. Использование дифференциального сигнала (LVDS) позволяет добиться помехозащищенности и низкого уровня опасного сигнала.

С целью снижения риска перехвата защищаемой ключевой информации при ее обработке и передаче между отдельными узлами УВК необходимо добиться отсутствия повторов при передаче ключевой информации. С этой целью после обработки ключевая информация не накапливается в памяти вычислителя, а передается в узел интерфейса для последующей передачи БПД.

5.2 Меры защиты от утечки ключевой информации по питающим и сигнальным цепям

Для защиты от утечки ключевой информации по питающим и сигнальным цепям за счет ПЭМИН необходимо обеспечить экранирование внутреннего пространства УВК, а также фильтрацию внешних сигнальных и питающих цепей.

LC-фильтр предназначен для подавления высокочастотных помех и для сглаживания пульсаций напряжения. При подаче сигнала определённой частоты на вход фильтра напряжение на выходе фильтра определяется отношением реактивных сопротивлений катушки индуктивности и конденсатора. Применение фильтров нижних частот (ФНЧ) обеспечивает предотвращение распространения высокочастотного сигнала, наведенного с узла вычислителя.

Для снижения уровня помех может применяться оптоэлектронная развязка — передача сигнала между электрическими цепями без электрического

контакта между ними. Оптоэлектронное развязывающее устройство называется оптопарой или оптроном, состоит из светоизлучающего элемента (светодиода) и приемника (фототранзистора). Принцип действия основан на излучении света каким-либо управляемым электрическим сигналом светоизлучателем, передаче оптического сигнала в гальванически изолированную часть и обратное преобразование излучения в электрический сигнал. К достоинствам данного метода относятся:

- возможность осуществлять в широком диапазоне напряжений;
- возможность передавать сигналы на высокой частоте;
- малые габариты.

С целью обеспечения защищенности ключевой информации от утечки по цепям электропитания возможно применение разделительных трансформаторов. Разделительный трансформатор — это трансформатор, первичная обмотка которого изолирована от вторичных обмоток при помощи защитного электрического разделения цепей с помощью двойной или усиленной изоляции, т.е. между обмотками имеется заземленный металлический защитный экран. Разделительные трансформаторы предназначены для повышения безопасности электросетей, а также могут обеспечивать гальваническую развязку электрических цепей.

5.3 Меры защиты ключевой информации от утечки по визуально-оптическому каналу

Для защиты ключевой информации, обрабатываемой УВК, от утечки по оптическому каналу необходимо применение технических и организационных мер.

К техническим мерам относятся:

– оборудование узла установки бумажного носителя внешней подвижной крышкой, которая обеспечивает прижатие бумажного носителя к защитному стеклу, делая ключевую информацию недоступной для наблюдения;

– установка аппаратуры криптографической защиты информации, в состав которой входит УВК, в непрозрачную стойку;

– контроль сигналов датчиков положения внешних крышек, что обеспечивает невозможность работы УВК с открытыми крышками;

– установка на оконных проемах объекта эксплуатации штор из плотной ткани, либо вертикальных и горизонтальных жалюзи;

– установка двойных дверей с тамбуром, либо одной двери и шторы из плотной ткани при входе на объект эксплуатации.

Организационные защитные меры включают в себя:

– размещение аппаратуры криптографической защиты, в составе которой находится УВК, на объектах эксплуатации в контролируемой зоне таким образом, чтобы обеспечивалась невозможность ознакомления третьих лиц с защищаемой информацией путем наблюдения через дверные и оконные проемы с использованием оптических приборов, приборов ночного видения и тепловизоров;

– хранение носителей ключевой информации в нерабочее время в специальных опечатываемых хранилищах (сейфах);

– определение круга лиц, имеющих право доступа на объект эксплуатации;

– определение круга лиц, имеющих право на участие в работах с применением аппаратуры криптографической защиты в целом и, в частности, УВК;

– определение круга лиц, имеющих право доступа к носителям ключевой информации.

5.4 Меры защиты ключевой информации от несанкционированного доступа

Для защиты ключевой информации, обрабатываемой УВК, от НСД необходимо применение технических и организационных мер.

К техническим мерам относятся:

- оборудование узла установки ДК6 и узла установки бумажного носителя подвижными крышками с приспособлениями для опечатывания;
- контроль сигналов датчиков положения внешней крышки, что обеспечивает невозможность работы УВК с открытой крышкой;
- контроль сигналов датчиков НСД к внутренним узлам;
- оборудование входной двери объекта эксплуатации кодовым замком, звонком и приспособлением для опечатывания;
- оборудование помещения эксплуатации датчиками движения, а окон и входной двери датчиками вскрытия с выводом сигналов на пульт охраны.

Организационные защитные меры включают в себя:

- определение круга лиц, имеющих право доступа на объект эксплуатации;
- определение круга лиц, имеющих право на участие в работах с применением аппаратуры криптографической защиты в целом и, в частности, УВК;
- определение круга лиц, имеющих право доступа к носителям ключевой информации;
- хранение носителей ключевой информации в нерабочее время в специальных опечатываемых хранилищах (сейфах);
- ведение журналов учета работы с аппаратурой, журналов учета ввода ключевой информации, журналов учета вскрытия помещения и др.;

– контроль отсутствия бумажного и электронного носителей ключевой информации в соответствующих узлах установки УВК по завершении работы аппаратуры криптографической защиты.

5.5 Инженерно-криптографические требования

Для обеспечения защищенности ключевой информации при ее обработке УВК и передаче БПД необходимо принятие следующих инженерно-криптографических решений:

– контроль напряжений питания;

– дублирование критических цепей;

– выполнение начального, динамического и периодического контроля;

– опечатывание внешних крышек.

Контроль напряжений питания необходим по следующим причинам. В случае, если подается напряжение питания, значение которого выше допустимого, отдельные узлы либо элементы, входящие в состав УВК, будут неправильно функционировать или полностью выйдут из строя.

При неправильном функционировании процессы обработки ключевой информации (считывание, декодирование, обнаружение и исправление ошибок) будут нарушены, что приведет к искажению защищаемой информации, то есть нарушению ее целостности.

При понижении напряжения питания ниже допустимого уровня корректная работа ЭРИ не гарантируется, возможны сбои и отказы. Полное или частичное прекращение функционирования узлов или элементов УВК приведет к нарушению доступности ключевой информации и, как следствие, невозможности дальнейшей работы с аппаратурой криптографической защиты информации.

Дублирование критических цепей необходимо для обеспечения непрерывного функционирования УВК при выходе из строя какого-либо элемента или соединительных линий. В первую очередь, дублированию подлежат цепи, предназначенные для обнаружения НСД к внутренним узлам УВК. В данном случае дублируются датчики НСД, соединительные линии, по которым передаются сигналы датчиков НСД, микросхемы на печатной плате, отвечающие за обработку сигналов датчиков НСД. Дублируются цепи, предназначенные для обработки сигналов датчиков положения внешних крышек узлов носителей ключевой информации.

В работе УВК предусмотрены следующие виды контроля:

- начальный (пусковой);
- динамический;
- периодический.

Начальный контроль производится при включении. Осуществляется проверка состояния всех узлов УВК, внутренней и внешней памяти, напряжений питания, системы контроля напряжений, положения внешних крышек узла установки бумажного носителя и узла установки ДК6, калибровка оптической системы (выполняется без носителя по белому фону крышки). Результат контроля выводится на единичный индикатор и сигнал во внешний интерфейс.

Динамический контроль осуществляется в процессе работы УВК автоматически. При этом отслеживаются значения питающих напряжений и их выход за допустимые пределы и положение крышек носителей ключевой информации и попытки НСД.

Периодический контроль проводится автоматически в процессе работы УВК через определенные промежутки времени. Данный вид контроля повторяет начальный контроль.

УВК должно иметь только одну съемную крышку. Крышка должна иметь приспособления для опечатывания на заводе-изготовителе. Печати позволяют гарантировать отсутствие НСД к внутреннему пространству при транспортировании и эксплуатации. Когда УВК не используется крышки узлов установки носителей тоже опечатываются, номера печатей записываются в журнал.

6 Разработка структурной схемы устройства ввода ключевой информации

В состав УВК входят следующие структурные элементы:

- узел вычислителя;
- узел интерфейса;
- оптический узел;
- узел установки ДК6;
- узел индикации;
- узел электропитания и контроля.

Узел вычислителя выполняет функции управления процессом ввода ключевой информации, обработки (декодирования, обнаружения и исправления ошибок), передачи ключевой информации БПД, а также контроля состояния всех узлов УВК. Узел вычислителя включает в себя следующие основные элементы:

- процессор;
- память;
- аналого-цифровой преобразователь (АЦП).

Процессор обеспечивает процедуры распознавания, декодирования, обнаружения и исправления ошибок, возникших в процессе считывания информации с бумажного носителя, контроля и управление всеми остальными узлами и системами блока.

Память обеспечивает хранение промежуточных данных, считанного и декодированного изображения, исполняемого кода программ, а также длительное хранение исполняемого ПО процессора.

АЦП выполняет преобразование аналогового электрического сигнала, поступившего с фотоприемника, в цифровой сигнал.

Узел интерфейса предназначен для сопряжения с БПД и передачи ему декодированной ключевой информации после обнаружения и исправления ошибок .

Оптический узел предназначен для удобной ручной установки бумажного носителя ключевой информации для последующего экспонирования, считывания и преобразования изображения носителя ключевой информации в электрический сигнал. Оптический узел включает в себя:

- узел установки бумажного носителя;
- осветитель;
- объектив;
- фотоприемник.

Узел установки ДК6 представляет собой устройство контактное, закрываемое внешней подвижной крышкой с приспособлением для опечатывания.

Осветитель обеспечивает равномерное освещение бумажного носителя при экспонировании.

Объектив предназначен для проецирования изображения освещённого носителя информации на фоточувствительное поле фотоприемника.

Фотоприемник предназначен для преобразования изображения бумажного носителя ключевой информации (свет) в электрический аналоговый сигнал.

Узел индикации отвечает за вывод сигнала об ошибке в случае обнаружения неисправности устройства и блокирования при получении соответствующего сигнала от процессора.

Узел электропитания и контроля обеспечивает преобразование входного напряжения электропитания постоянного тока 27 В плюс/минус 10 % в ряд фиксированных напряжений электропитания для всех узлов УВК. Также узел осуществляет контроль питающих напряжений за выход за допустимые пределы.

Была разработана структурная схема УВК, результаты приведены на рисунке 15.

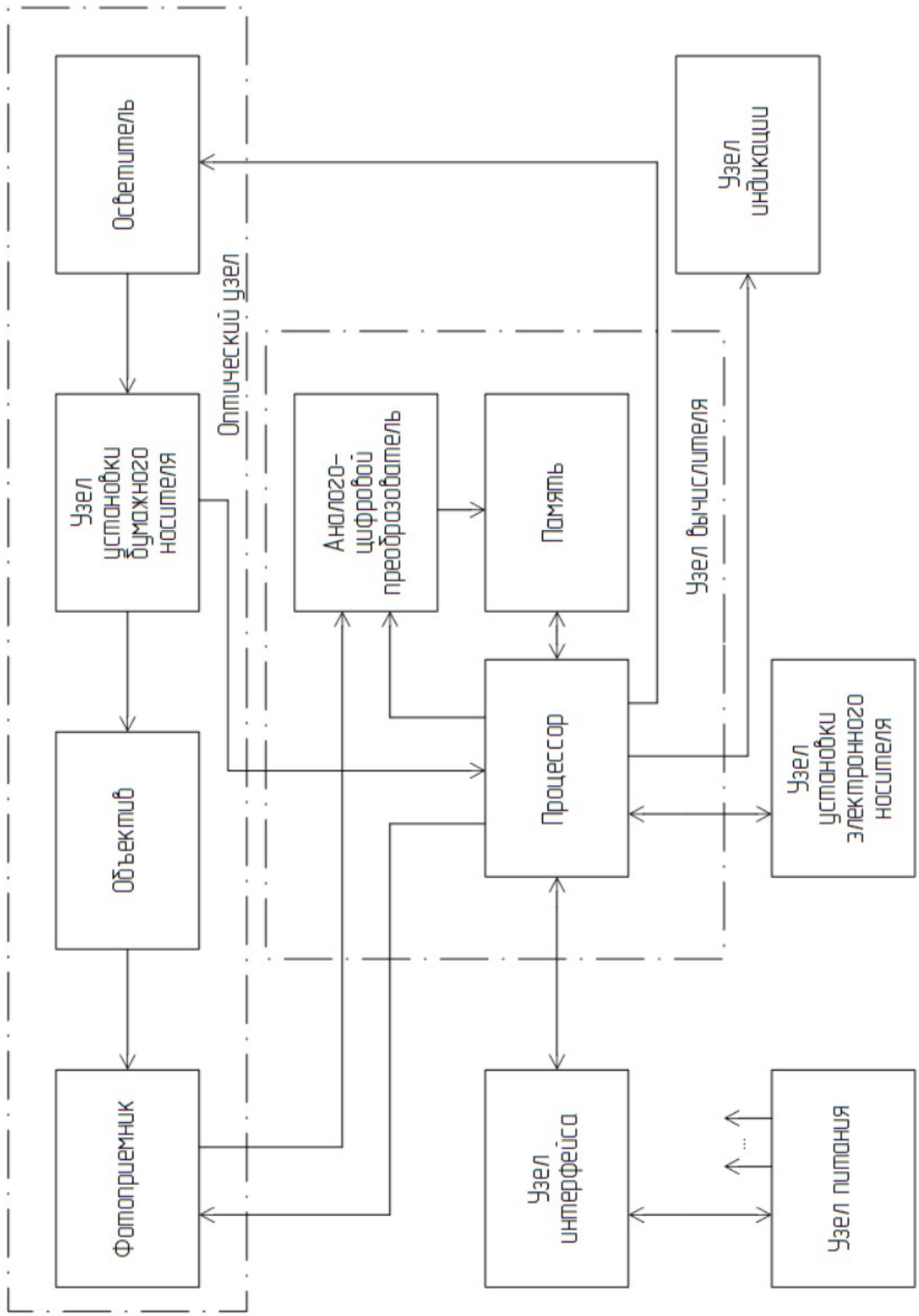


Рисунок 15 - Структурная схема УВК

7 Выбор электронной компонентной базы

7.1 Сравнительный анализ и рекомендации по выбору электронной компонентной базы

Как указано в подразделе 1.5, в составе УВК должна применяться только отечественная ЭКБ категории качества «ОС», «ОСМ», а при их отсутствии — категории качества «ВП».

Категория качества «ОС» (особая серия) — изделия, в отношении которых устанавливаемый в конструкторской, технологической документации, технических условиях и других стандартах уровень требований к надежности, другим эксплуатационным свойствам, а также к обеспечению и контролю качества обуславливает пригодность их применения в аппаратуре, отказ которой ведет к катастрофическим последствиям (а ремонт и замена которой труднодоступны или невозможны).

Категория качества «ОСМ» — изделия категории качества «ОС», поставляемые малыми партиями и имеющие особенности в обеспечении и контроле их качества, указываемые в технологической документации, стандартах и технических условиях на них.

Категория качества «ВП» — приемка военным представительством (ВП) или Представителем Заказчика (ПЗ – представительство Генерального заказчика) изделий, в отношении которых устанавливаемый в конструкторской, технологической документации, технических условиях и других стандартах уровень требований к надежности и другим эксплуатационным свойствам, а также к обеспечению и контролю качества обусловливает пригодность их применения в наземной, морской и авиационной аппаратуре, отказ которой ведет к существенным последствиям (ремонт и замена ведется на уровне ячеек и блоков).

Применяемые в составе УВК изделия должны входить в Перечень электронной компонентной базы, разрешенной для применения при разработке,

модернизации, производстве и эксплуатации вооружения, военной и специальной техники.

Сравнительные характеристики микропроцессоров приведены в таблице 3.

Таблица 3 - Сравнительные характеристики микропроцессоров

Характеристика	Микропроцессоры (микроконтроллеры)				
	1892ВМ10Я	1986ВЕ91Т	1901ВЦ1Т	1921ВК035	1921ВК024
Размер корпуса	21 мм × 21 мм	28 мм × 28 мм	28 мм × 28 мм	6 мм × 6 мм	29 мм × 29 мм
Диапазон рабочих температур	от минус 60 до плюс 85 °С	от минус 60 до плюс 125 °С	от минус 60 до плюс 85 °С	от минус 60 до плюс 85 °С	от минус 60 до плюс 85 °С
Напряжение питания	1,2 В/3,3 В (плюс/минус 5 %)	от 2,2 до 3,6 В	от 2,2 до 3,6 В	1,8 В/3,3 В (плюс/минус 5 %)	1,8 В/3,3 В (плюс/минус 5 %)
Тактовая частота микропроцессора	250 МГц	80 МГц	80 МГц	100 МГц	200 МГц
Количество ядер	3	1	2	1	1
Производительность	250 млн. операций/с.	125 млн. операций/с.	125 млн. операций/с.	125 млн. операций/с.	250 млн. операций/с.
Встроенная память	CPU: 128 Кбайт, DSP: 320 Кбайт	32 Кбайт ОЗУ, 128 Кбайт ПЗУ	CPU: 32 Кбайт, DSP: память данных - 128 Кбайт, память программ - 128 Кбайт	8 Кбайт ОЗУ, 16 Кбайт ПЗУ	256 Кбайт ОЗУ, 1 Мбайт ПЗУ

Для применения в составе узла вычислителя УВК был выбран процессор 1892ВМ10Я [20], обладающий наибольшими значениями тактовой частоты, количества ядер, а также приемлемыми габаритами, хорошей производительностью и подходящим потреблением.

Сравнительные характеристики статических оперативных запоминающих устройств (СОЗУ) приведен в таблице 4.

Таблица 4 - Сравнительные характеристики СОЗУ

Характеристика	СОЗУ				
	1645РУ6У1	1645РУ4АУ	1663РУ1Т	1663РУ4Т	1657РУ1У
Размер корпуса	13,95 мм × 13,95 мм	18,3 мм × 18,3 мм	22 мм × 22 мм	22 мм × 22 мм	16,5 мм × 16,5 мм
Емкость	16 Мбит	16 Мбит	16 Мбит	32 Мбит	4 Мбит
Организация памяти	1 М × 16 бит	1 М ×16 бит	512 К × 32 бит	2048 К × 16 бит	512 К × 8 бит
Время выборки данных по адресу	не более 10 нс	не более 30 нс	не более 10 нс	не более 10 нс	не более 25 нс
Динамический ток потребления	200 мА	150 мА	200 мА	220 мА	200 мА
Ток потребления в режиме хранения	30 мА	15 мА	30 мА	60 мА	30 мА
Диапазон рабочих температур	от минус 60 до плюс 100 °С	от минус 60 до плюс 125 °С	от минус 60 до плюс 125 °С	от минус 60 до плюс 125 °С	от минус 60 до плюс 125 °С
Напряжение питания	от 3,0 до 3,6 В	от 3,0 до 3,6 В, 1,8 В	от 2,25 до 2,75 В	2,5 В	2,5 В и 3,3 В

Для хранения промежуточных данных, исполняемого кода программ, считанного и декодированного изображения в качестве СОЗУ была выбрана микросхема 1645РУ6У1 [21], обладающая достаточной емкость, малым временем выборки данных по адресу, приемлемым потреблением, напряжением питания как у выбранного процессора и наименьшими из рассматриваемых габаритами корпуса.

Сравнительные характеристики постоянного запоминающего устройства (ПЗУ) приведены в таблице 5.

Таблица 5 - Сравнительные характеристики ПЗУ

Характеристика	ПЗУ				
	1661РР2У	1661РЕ2У	1636РР4У	1638РРхх	1665РЕ2У
Тип	ЭСППЗУ	Масочное ПЗУ	ЭСППЗУ	ЭСППЗУ	Масочное ПЗУ
Размер корпуса	19,6 мм × 19,6 мм	19,6 мм × 19,6 мм	15,5 мм × 15,5 мм	13,3 мм × 13,3 мм	18,3 мм × 18,3 мм
Емкость	8 Мбит	16 Мбит	16 Мбит	1 Мбит	16 Мбит
Организация памяти	1 М × 8 бит	1 М × 16 бит	2 М × 8 бит	128 К × 8 бит	512 К × 32 бит
Время выборки данных по адресу	не более 70 нс	не более 65 нс	не более 65 нс	не более 60 нс	не более 60 нс
Динамический ток потребления	не более 70 мА	не более 35 мА	не более 50 мА	не более 40 мА	не более 50 мА
Диапазон рабочих температур	от минус 60 до плюс 85 °С	от минус 60 до плюс 85 °С	от минус 60 до плюс 125 °С	от минус 60 до плюс 125 °С	от минус 60 до плюс 125 °С
Напряжение питания	от 2,7 до 6 В	3,3 В	от 3,0 до 3,6 В	от 4,5 до 5,5 В	3,8 В

Для долговременного хранения ПО процессора в качестве ПЗУ было выбрано ЭСППЗУ 1636РР4У [22], обладающая большой емкостью, небольшим временем выборки данных, подходящими габаритами корпуса и величиной необходимого напряжения питания.

Сравнительные характеристики АЦП приведены в таблице 6.

Таблица 6 - Сравнительные характеристики АЦП

Характеристика	АЦП				
	5101НВ015	5108ПВ3У	1299ПВ1У	1887ВЕ4У	1887ВЕ7Т
Размер корпуса	11,3 мм × 11,3 мм	10,68 мм × 10,68 мм	12,7 мм × 12,7 мм	16,2 мм × 16,2 мм	15,8 мм × 15,8 мм
Частота выборки (преобразования)	от 15 до 125 МГц	40 МГц	50 МГц	16 МГц	8 МГц

Продолжение таблицы 6

Характеристика	АЦП				
	5101НВ015	5108ПВЗУ	1299ПВ1У	1887ВЕ4У	1887ВЕ7Т
Количество разрядов	14	8	10	10	10
Динамический ток потребления	не более 70 мА	не более 140 мА	не более 450 мА	не более 30 мА	не более 50 мА
Диапазон рабочих температур	от минус 60 до плюс 85 °С	от минус 45 до плюс 85 °С	от минус 60 до плюс 85 °С	от минус 60 до плюс 85 °С	от минус 60 до плюс 85 °С
Напряжение питания	от 1,71 до 1,89 В	от 4,75 до 5,25 В	3,3 В	3,3 В и 5,0 В	5,0 В

В качестве АЦП в составе узла вычислителя была выбрана микросхема 5101НВ015 [23], обладающая приемлемым напряжением питания, размером корпуса и частотой преобразования.

Для сопряжения интерфейсных шин, имеющих разные уровни питающих напряжений была выбрана микросхема 5572ИН1АУ1 [24], представляющая собой шестнадцатиразрядный формирователь выходных уровней. Основные технические характеристики:

- напряжение питания портов — от 1,65 до 5,5 В;
- рабочий диапазон температур — от минус 60 до плюс 125 °С.

Буферы 5514БЦ1У1-9А5 [25] по устройству и принципу действия представляют собой триггер Шмитта. При распространении цифрового сигнала по сигнальным цепям и прохождения через ФНЧ, он будет искажен, вследствие чего фронты сигнала будут завалены. Триггер Шмитта обладает верхним и нижним пороговыми значениями напряжений сигнала, при достижении которых происходит переключение с низкого уровня на высокий и наоборот. Данное свойство триггера Шмитта называется гистерезисом. Разница между верхним и нижним пороговыми значениями определяет ширину области гистерезиса. Чем она уже, тем выше чувствительность триггера. Таким образом,

буфер 5514БЦ1У1-9А5 предназначен для восстановления цифрового сигнала прямоугольной формы.

Для обеспечения помехозащищенности и низкого уровня опасного сигнала на внешних стыках была выбрана микросхема 5559ИН19У [26], содержащая две пары LVDS передатчиков и приемников. Буферы на LVDS входах имеют схему помехозащищающего смещения, которая устанавливает на выходах приемника высокий логический сигна.

Для формирования питающих напряжений различных узлов УВК были выбраны следующие микросхемы:

- МДМ15 [27];
- 1310ПН1У [28];
- 1156ЕУ1 [29];
- 1303ЕН1.8П [30].

Характеристики представленных микросхем и узлы УВК, которые от них питаются, представлены в таблице 7.

Таблица 7 - Характеристики преобразователей напряжений

Микросхема	Характеристики			
	Входное напряжение, В	Выходное напряжение, В	Выходной ток, А	Узлы УВК
МДМ15	27	3,3	4,5	Периферия процессора, СОЗУ, ЭСППЗУ, осветитель, регистры, буферы
		плюс 15/ минус 15	0,5/0,5	Усилители сигналов управления ФПЗС и аналогового сигнала
1310ПН1У	3,3	1,2	1,5	Ядро процессора
1156ЕУ1	3,3	5	0,1	Узел установки ДК6
1303ЕН1.8П	3,3	1,8	5	АЦП, буферы

Для системы контроля питания были выбраны микросхемы серии 1230ДН1У [31]. Данные микросхемы представляют собой универсальные детекторы напряжений, предназначенные использования в устройствах, требующих контроля напряжения. Применяются в качестве средств защиты от неправильного функционирования микропроцессорной системы при включениях/выключениях питания, а также в результате случайных перебоев подачи питания. Детектор напряжения 1230ДН1У обладает следующими особенностями:

- контроль превышения, понижения и выхода напряжения за определенные границы;
- контроль положительного и отрицательного напряжений;
- низкое энергопотребление.

В качестве регистров были выбраны микросхемы интегральные 5574ИР2У ГПКФ.431233.002-01 ТО [32]. Микросхемы предназначены для применения в вычислительной технике с высоким быстродействием и низким энергопотреблением. Могут использоваться в электронных устройствах и системах с двойным 3,3 В/5,0 В напряжением внешнего сигнала для передачи данных по шине. Предназначены для функционирования при повышенной нагрузке.

Микросхемы интегральные 5574ИР2У состоят из двух аналогичных независимых восьмиразрядных регистров с импульсным управлением и тремя состояниями на выходе, с напряжением питания (3,3 плюс/минус 0,3) В, буферизированными управляющими входами (тактовый вход и вход разрешения выхода данных). Предоставляют возможность хранения данных в регистрах каждого разряда. Запись данных в регистр происходит по переднему фронту изменения тактового сигнала (при переключении тактового сигнала CLK из состояния низкого уровня в состояние высокого уровня).

Микросхемы имеют блоки удержания состояния входа, которые сохраняют последнее состояние при отключении внешних сигналов на входах микросхем. Все входы микросхем могут управляться сигналами как 3,3 В, так и 5 В, что позволяет использовать микросхемы как преобразователь в системах со смешанным напряжением питания.

В качестве источника тактовой частоты в составе узла вычислителя был выбран генератор ГК109-С АФТП.433520.008 ТУ [33]. Основные технические характеристики:

- диапазон частот — от 1 до 125 МГц;
- интервал рабочих температур — от минус 60 до плюс 85 °С;
- форма выходного сигнала — импульсная, прямоугольная;
- длительность фронта нарастания и спада импульса на нагрузке — не более 5 нс;
- напряжение питания — 5 В плюс/минус 10 % или 3,3 В плюс/минус 10 %.

Для фотоприемника была выбрана микросхема ФПЗС45М ЯЛАР.433832.005 ТУ [34]. ФПЗС — фоточувствительный прибор с зарядовой связью, предназначен для устройства считывания информации. Изделие выполнено на основе кристалла матричного фоточувствительного прибора с зарядовой связью, установленного в герметичный корпус.

ФПЗС45М представляет собой односекционный матричный приемник изображения, содержащий фоточувствительную зону (далее — фотозона) форматом 900 (Г) × 320 (В) фоточувствительных элементов (ячеек) размером 20×20 мкм, буферное устройство и трехфазный регистр считывания с выходным устройством. Буферное устройство расположено между фотозоной и выходным регистром. Оно обеспечивает хранение и передачу в него из фотозоны заряда во время работы выходного регистра.

Для оптического узла был выбран объектив НБПИ.202361.007 ТУ [35], который предназначен для использования в специализированной фотокамере. Основные параметры и характеристики:

- максимальный размер изображения — (50×50) плюс/минус 0,05 мм;
- коэффициент рассеяния — не более 0,05;
- падение освещенности — не более 30 %;
- масса — не более 0,2 кг.

Объектив сохраняет свои параметры при воздействии следующих факторов:

- пониженной температуры окружающей среды до минус 50 °С;
- повышенной температуры окружающей среды до 60 °С;
- атмосферного давления в диапазоне от 65 кПа (450 мм рт. ст.) до 112 кПа (780 мм рт. ст.).

Для управления фотоприемником по усилению сигналов были выбраны микросхемы 1432УД1АР1 [36] широкополосного операционного усилителя с токовой обратной связью, предназначенные для использования в качестве драйверов АЦП, кабелей и больших емкостей, а также в качестве видеоусилителей, широкополосных высокочастотных усилителей. Основные технические характеристики:

- максимальное выходное напряжение — не менее 10 В;
- ток потребления — не более 20 мА;
- максимальная скорость нарастания выходного напряжения — не менее 800 В/мкс.

Для формирования осветителя и узла индикации были выбраны индикаторы полупроводниковые единичные типа ИПД132 [37] со специальным покрытием в пластмассовом оптически прозрачном корпусе. Индикаторы

данного типа предназначены для отображения сигнальной информации в аппаратуре специального назначения. Основные технические характеристики:

- постоянное прямое напряжение — не более 2,4 В;
- сила света — не менее 200 мкд;
- доминирующая длина волны излучения — от 620 до 630 нм.

Для узла установки электронного носителя было выбрано устройство контактное УК-ДК4-32 РИВУ.469115.407ТУ [38], предназначенное для соединения контактов устройства электронного К1634ДК6 АДБК.431210.730ТУ с электрическими цепями аппаратуры. Устройство обеспечивает:

- прохождение тока для всех контактов — от 50 мкА до 100 мА;
- максимальное допустимое напряжение между контактами и между контактами и корпусом — 30 В;
- сопротивление каждого сигнального контакта — не более 80 мОм, а двух контактов управления питанием — не более 200 мОм;
- количество подключений — не менее 20 тысяч.

Устройство УК-ДК4-32 сохраняет свои параметры при эксплуатации в условиях:

- температуры окружающей среды от минус 50 до плюс 70 °С при эксплуатации в составе аппаратуры без устройств электронных;
- температуры окружающей среды от минус 45 до плюс 70 °С при эксплуатации с вставленным устройством электронным К1634ДК6;
- относительной влажности окружающей среды не более 98 % при температуре не выше плюс 25 °С;
- пониженного атмосферного давления до 53 кПа.

Для использования в качестве датчиков НСД к внутренним узлам УВК, датчиков положения внешних крышек узлов носителей ключевой информации был выбран микропереключатель ПМ21В АГ0.360.013 ТУ [39],

предназначенный для работы в электрических цепях постоянного и переменного тока. Основные технические характеристики:

- масса — не более 0,7 г;
- минимальное расстояние от корпуса микропереключателя до места пайки — не менее 0,5 мм;
- время срабатывания подвижных контактов микропереключателей — не более 0,01 с.

Фильтры Б26 АЖЯР.431145.005 ТУ [40] и Б24 АЖЯР.431145.003 ТУ [41] предназначены для подавления высокочастотных помех в диапазоне частот от 700 кГц до 10 ГГц в цепях постоянного и переменного токов и в импульсных режимах. Основные технические характеристики фильтров приведены в таблице 8.

Таблица 8 - Технические характеристики фильтров Б26 и Б24

Характеристика	Б26					Б24				
Номинальное напряжение, В	32; 50; 100; 250					100				
Номинальная емкость	0,015...22 мкФ					3300...10000 пФ				
Интервал рабочих температур	от минус 60 до плюс 85 °С					от минус 60 до плюс 85 °С				
Срок сохраняемости, лет	25					25				
Номинальная емкость	Вносимое затухание, дБ, не менее на частоте, МГц									
	1	10	100	300	1000	1	10	100	300	1000
3300 пФ	3	12	30	35	40	0,05	25	45	60	60
0,01 мкФ	4	21	37	45	55	0,1	40	60	60	60
6,8 мкФ	52	65	70	70	75	-	-	-	-	-

Для фильтрации сигнальных цепей был выбран фильтр Б24, который пропускает низкочастотные гармоники сигнала (до 1 МГц), практически не внося затухания, что является достаточным для передачи полезной информации с минимальными искажениями.

Для питающих цепей был выбран фильтр Б26. Он обеспечивает большее затухание передаваемого опасного сигнала как на высоких, так и на низких частотах. Таким образом обеспечивается отсутствие в питающих цепях наводок опасного сигнала.

Для узла интерфейса был выбран соединитель ГРПМШ-2. Они предназначены для работы в электрических цепях постоянного, переменного и импульсного токов. Вилки и розетки имеют однотипные и совмещенные направляющие элементы — ловители. Основные технические характеристики:

- максимальное рабочее напряжение — 250 В;
- рабочий ток на каждый контакт соединителя при его равномерной нагрузке — 3 А;
- интервал рабочих температур — от минус 60 до плюс 85 ℃;
- повышенная влажность воздуха при температуре 35 ℃ — 98 %.

По результатам сравнительного анализа ЭКБ был составлен перечень выбранной ЭКБ, который приведен в таблице 9.

Таблица 9 - Перечень выбранной ЭКБ

№ п/п	Назначение	Наименование
1	Процессор	1892ВМ10Я
2	СОЗУ	1645РУ6У1
3	ПЗУ	1636РР4У
4	АЦП	5101НВ015
5	Буфер с преобразованием уровня напряжения	5572ИН1АУ
6	Буфер с триггером Шмитта	5514БЦ1У1-9А5
7	Буфер-преобразователь TTL ↔ LVDS	5559ИН19У
8	Преобразователь напряжения (27 В → 3,3 В; 27 В→ ±15 В)	МДМ15

Продолжение таблицы 9

№ п/п	Назначение	Наименование
9	Преобразователь напряжения (3,3 В → 1,2 В)	1310ПН1У
10	Преобразователь напряжения (3,3 В → 1,8 В)	1303ЕН1.8П
11	Преобразователь напряжения (3,3 В → 5 В)	1156ЕУ1
12	Система контроля питания	1230ДН1У
13	Регистр	5574ИР2У
14	Генератор тактовой частоты	ГК109-С
15	Фотоприемник	ФПЗС45М
16	Усилитель	1432УД1АР1
17	Объектив	НБПИ.202361.007 ТУ
18	Индикатор	ИПД132
19	Узел установки ДК6	УК-ДК4-32
20	Датчик НСД (микропереключатель)	ПМ21В
21	Фильтр сигнальных цепей	Б24
22	Фильтр цепей электропитания	Б26
23	Соединитель	ГРПМШ-2

7.2 Проблема внедрения вредоносных элементов в аппаратное обеспечение устройств

В настоящее время широко распространена проблема внедрения иностранными разработчиками вредоносных элементов, в частности программных и аппаратных троянов, которые во всем мире стали серьезной проблемой для безопасности информационных систем.

Аппаратный троян — это вредоносная модификация микросхемы, результатом работы которой может быть как полное выведение из строя самой микросхемы и/или электронной системы, которая спроектирована с использованием «зараженной» микросхемы, так и нарушение нормального режима функционирования, обеспечение НСД к информации, изменение, блокирование доступа или полное уничтожение информации [42].

Вредоносные элементы могут быть внедрены в аппаратное обеспечение различными методами. Например, разработчик-злоумышленник может внедрить в конструкцию базовой микросхемы специальную неуказанную в документации функцию, добавив всего лишь несколько строк к исходному оригинальному коду аппаратного описания. Кроме того, злоумышленники могут модифицировать инструмент синтеза таким образом, чтобы синтезируемое аппаратное описание изменялось определенным образом. Еще один метод является ресурсоемким и дорогостоящим, но его тоже нельзя исключать: производитель микросхемы может воспроизвести конструкцию таким образом, чтобы она включала в себя определенную «теневую» схемотехнику на физическом уровне [43].

Методы выявления аппаратных троянов должны соответствовать эволюции самих вредоносных элементов. Но существует ряд свойств, которые являются общими для всех поколений троянов. Например, для выполнения своих задач аппаратные трояны должны проходить функциональные испытания, оставаясь незамеченными. Они включают в себя два основных механизма: триггер и полезную нагрузку.

Триггер активирует заряд при определенных условиях: при наступлении определенного события, после заданного интервала времени, при определенном состоянии окружающей среды. Наиболее важным требованием к условию срабатывания триггера является требование его невыявления (несрабатывания) в ходе функциональных тестов, которые представляют собой важнейшие элементы процесса производства микросхем. Иначе триггер может запустить

срабатывание трояна в ходе финишных производственных испытаний, благодаря чему его станет легко обнаружить.

Механизм полезной нагрузки выполняет фактическую целевую функцию трояна, которая может заключаться, например, в полном отключении аппаратной системы, перехвате чувствительных данных (криптографического ключа), дистанционном управлении аппаратной системы (что соответствует созданию обходного пути в работе аппаратного обеспечения) [43].

Злоумышленники могут размещать в микроконтроллерах аппаратные трояны, действующие без необходимости использования прямого внешнего управления по радиоканалу. Эти аппаратные трояны относятся к классу так называемых часовых бомб. В простейшем случае схема трояна состоит из небольшого количества элементов, образующих счетчик, простейший автомат конечных состояний, компаратор данных и ряд дополнительных проводников и транзисторов, обеспечивающих электрическое подключение трояна к жизненно важным блокам атакуемой микросхемы [42].

В нужный злоумышленнику момент времени (через месяц, неделю или даже несколько лет) аппаратный троян активизируется, реализуя свою основную функцию (выключение, разрушение микросхемы, отправка на обработку некорректных данных, стирание или искажение содержимого запоминающего устройства).

Визуально обнаружить вредоносный фрагмент среди сотен тысяч транзисторов практически невозможно. В пассивном состоянии закладка не затрагивает функций кристалла и поэтому крайне трудно выявляется.

В случае внедрения аппаратного трояна в центральный процессор электронной системы вносятся две модификации, которые реализуют механизм, обеспечивающий злоумышленнику свободный доступ в защищенные области памяти, и специальный теневой режим, позволяющий незаметно для оператора системы выполнить вредоносную скрытую встроенную программу.

В настоящее время существуют различные методы выявления и нейтрализации аппаратных троянов, например:

- с помощью анализа спектров электромагнитных излучений;
- метод минимизации пусковой схемы, который основан на снижении общей энергетической активности исследуемой микросхемы и обеспечения на этом фоне возможности измерения активности трояна при его наличии;
- методы характеризации логических элементов;
- использование специальных шинных архитектур, защищенных от троянов и др.

Реализация методов выявления аппаратных троянов является трудоемкой, требует временных и материальных затрат. Эффективность и гарантия того, что трояны будут обнаружены и нейтрализованы, не доказаны. Таким образом, для избежания внедрения вредоносных элементов в используемые электрорадиоизделия необходимо применять в составе разрабатываемой аппаратуры ЭКБ только отечественного производства.

8 Разработка функциональной схемы устройства ввода ключевой информации

Была разработана функциональная схема УВК, представленная на рисунке 16.

Осветитель, входящий в состав оптического узла, предназначен для освещения бумажного носителя при экспонировании. Осветитель реализован на индикаторах единичных ИПД132 (светодиодах), сгруппированных в две линейки. Каждая линейка состоит из восьми индикаторов, смонтированных на печатной плате. Платы расположены вдоль длинных сторон носителя.

Узел установки бумажного носителя предназначен для удобной ручной установки бумажного носителя информации для последующего считывания. Узел установки носителя имеет подвижную крышку, которая обеспечивает прижатие носителя к защитному стеклу, а также экранирование внутреннего пространства от проникновения светового и радиоизлучений как во внутрь, так и наружу. Узел установки носителя снабжен датчиком положения, предназначенным для оповещения вычислителя о состоянии крышки.

Объектив НБПИ.202361.007 ТУ предназначен для проецирования изображения освещённого носителя информации на фоточувствительное поле фотоприемника.

В качестве фотоприемника применяется фоточувствительный прибор с зарядовой связью ФПЗС45М. Он представляет собой односекционный матричный приемник изображения, содержащий фоточувствительную зону, буферное устройство и трехфазный регистр считывания с выходным устройством. ФПЗС45М предназначен для преобразования поступающего изображения бумажного носителя (света) в электрический сигнал.

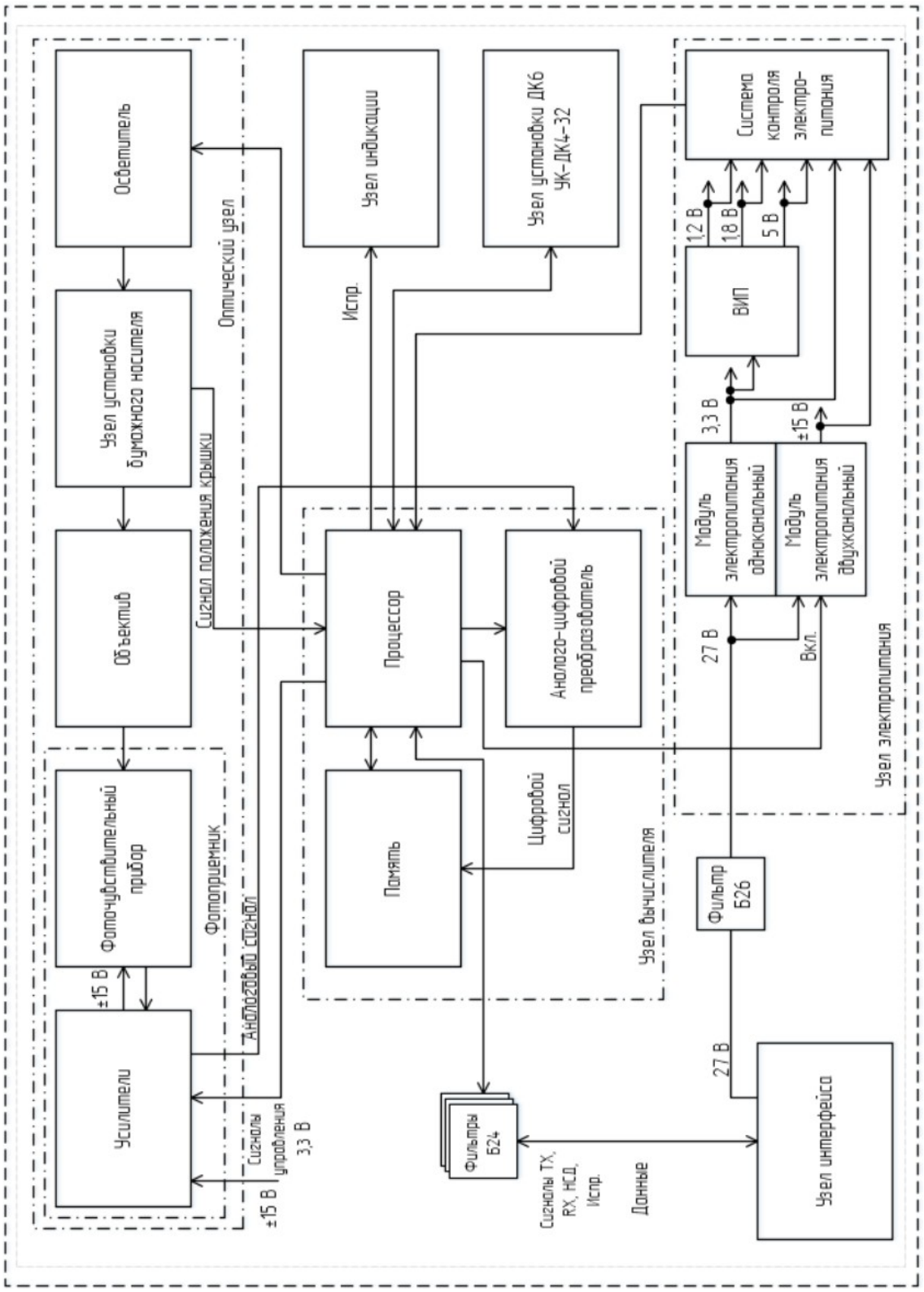


Рисунок 16 - Функциональная схема УВК

Усилитель 1432УД1АР1 предназначен для усиления поступающего с ФПЗС45М аналогового сигнала по току. Усилители также отвечают за преобразование управляющих сигналов (сигналы 3,3 В), поступающих с процессора на ФПЗС45М.

Для узла индикации применяется индикатор ИПД132. После проведения начального контроля, если все узлы УВК исправны и крышки узлов установки бумажного и электронного носителей находятся в закрытом положении, индикатор светится зеленым цветом.

Узел установки электронного носителя ДК6 представляет собой устройство контактное, выведенное на лицевую панель устройства и закрываемое крышкой. Крышка снабжена датчиком положения, в закрытом положении имеет приспособление для опечатывания.

На функциональной схеме УВК показано расположение фильтров нижних частот Б24 в сигнальных цепях и фильтра Б26 в цепях электропитания. Через узел интерфейса в БПД с процессора передаются сигнал «Испр.», сигнал ТХ (отправление данных). Из БПД на процессор УВК поступают сигналы НСД, сигнал RX (прием данных).

Отдельно была разработана функциональная схема узла вычислителя, представленная на рисунке 17.

Усиленный аналоговый сигнал с фотоприемника поступает на АЦП 5101НВ015. Одновременно на АЦП с процессора 1892ВМ10Я поступают сигналы управления и тактирования через буфер 5572ИН1АУ (Буфер 1) для преобразования уровня сигнала с процессора на АЦП (3,3 В → 1,8 В). Для преобразования уровня напряжения 1,8 В в 3,3 В так же применяется микросхема 5572ИН1АУ (Буфер 2). Для согласования задержки преобразования АЦП применяются 2 микросхемы 5574ИР2У, состоящие из двух восьмиразрядных регистров. При прохождении сигнала данных через АЦП и буфер, происходит его смещение относительно тактового сигнала, поступающего с процессора.

Для восстановления цифрового сигнала прямоугольной формы используется микросхема 5514БЦ1У1-9А5 (Буфер с триггером Шмитта).

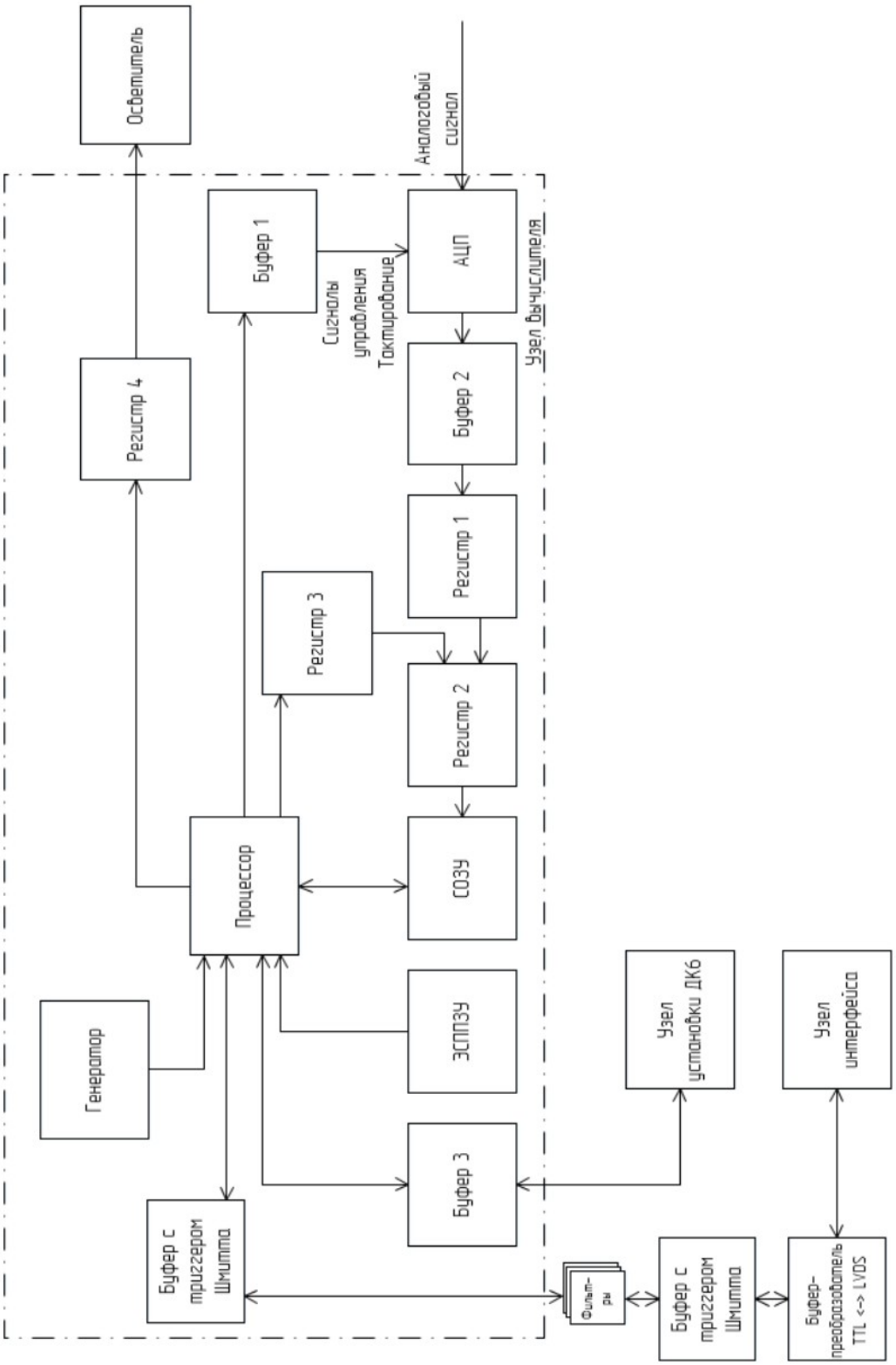


Рисунок 17 - Функциональная схема узла вычислителя

Первая пара регистров (Регистр 1) предназначена для выравнивания фазы цифрового сигнала данных и синхросигнала. Затем данные поступают на вторую микросхему 5574ИР2У (Регистр 2). Запись данных в регистры второй микросхемы 5574ИР2У осуществляется при подаче тактового сигнала с процессора на входы регистров. При этом тактовый сигнал проходит через еще одну пару регистров (Регистр 3) для согласования задержки преобразования АЦП. По окончании записи данных в Регистр 2 с процессора поступает сигнал на его входы разрешения выхода данных.

ЭСППЗУ 1636РР4У отвечает за долговременное хранение ПО процессора.

СОЗУ 1645РУ6У1 предназначено для хранения исполняемого кода программ, считанного и декодированного изображения, а также промежуточных данных.

При считывания ключевой информации с электронного носителя ДК6 для согласования уровней напряжения (5 В → 3,3 В) сигнал с ДК6 проходит через буфер 5572ИН1АУ1 (Буфер 3).

Генератор ГК109-С является источником опорной тактовой частоты, которая преобразуется процессором 1892ВМ10Я максимум до 250 МГц.

Для управления осветителем используется регистр 5574ИР2У (Регистр 4). С процессора подается сигнал на входы разрешения выхода данных регистров микросхемы 5574ИР2У, тактовый сигнал. Одновременно на входы данных регистров микросхемы 5574ИР2У подаются 16 бит (для 16 светодиодов узла осветителя) младших разрядов шины данных процессора.

Узел электропитания включает в себя:

- модуль электропитания одноканальный (3,3 В);
- модуль электропитания двухканальный (плюс/минус 15 В);
- вторичные источники питания (далее — ВИП; 1,2 В; 1,8 В; 5 В).

Была разработана схема электропитания УВК, результаты приведены на рисунке 18.

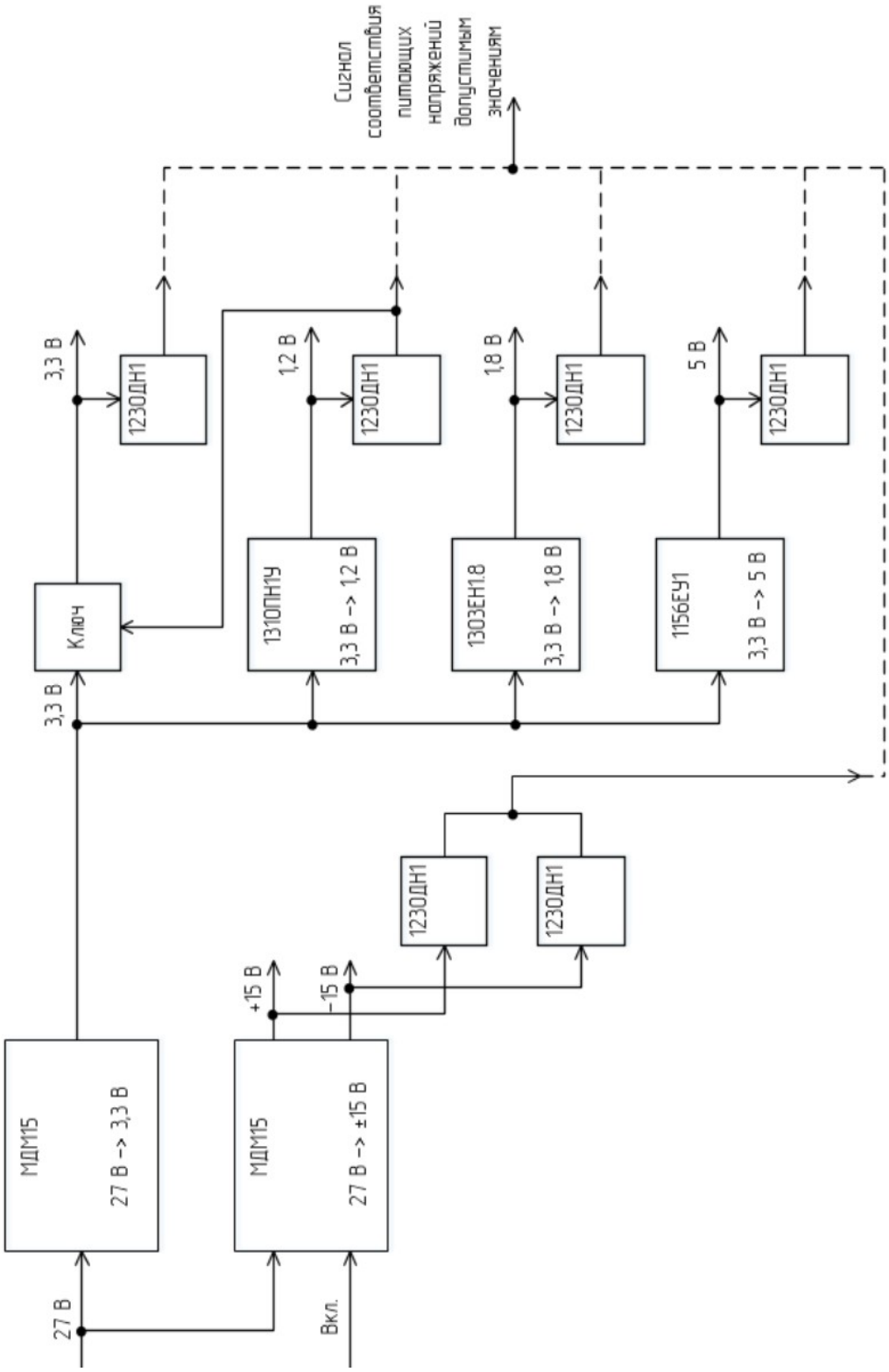


Рисунок 18 - Схема электропитания УВК

Электропитание УВК осуществляется от постоянного напряжения плюс 27 В. С помощью микросхем типа МДМ15 выполняется:

- преобразование входного напряжения плюс 27 В в плюс 3,3 В для питания цифровых узлов устройства;
- преобразование входного напряжения плюс 27 В в плюс/минус 15 В для питания усилителей сигналов управления фотоприемником, поступающих от процессора, и аналогового сигнала.

С помощью микросхемы 1310ПН1У осуществляется преобразование напряжения 3,3 В в 1,2 В для питания ядра процессора. Когда на ядро процессора поступило напряжение 1,2 В, с выхода микросхемы 1230ДН1У системы контроля питания поступает сигнал на ключ, ключ открывается, после чего напряжение питания 3,3 В подается на периферию процессора и соответствующие цифровые узлы УВК.

Микросхема 1303ЕН1.8П выполняет преобразование напряжения 3,3 В в 1,8 В для питания АЦП.

С помощью микросхемы 1156ЕУ1 осуществляется преобразование питающего напряжения 3,3 В в 5 В для питания узла установки ДК6.

Контроль питающих напряжений и их выход за допустимые пределы осуществляется с использованием микросхем 1230ДН1У, образующих систему контроля питания. После формирования питающих напряжений, в случае их соответствия допустимым значениям, на процессор подается соответствующий сигнал.

9 Описание функционирования устройства ввода ключевой информации

Перед началом работы оператором осуществляется проверка целостности оттисков печатей крышек узлов носителей ключевой информации.

Оператор с пульта управления БПД выбирает режим ввода ключевой информации (с бумажного носителя или с электронного устройства ДК6).

БПД подает команду на подачу электропитания плюс 27 В через узел интерфейса. Включается одноканальный модуль электропитания 3,3 В. Включается ВИП 1,2 В. После установления напряжения 1,2 В для питания ядра процессора подается напряжение 3,3 В для питания периферии процессора, СОЗУ, ЭСППЗУ, включаются ВИП 1,8 В и 5 В.

Процессор стартует из ЭСППЗУ, где хранится ПО процессора.

Осуществляется начальное самотестирование (пусковой контроль). Оно включает в себя:

- проверку ЭСППЗУ;
- проверку внутренней памяти процессора и СОЗУ;
- проверку системы контроля напряжений питания;
- проверку всех питающих напряжений;
- включение/выключение и контроль двухканального модуля плюс/минус 15 В;
- проверку закрытия крышек узла установки бумажного носителя и узла установки ДК6;
- проверку отсутствия признаков НСД;
- калибровку оптической системы;
- проверку АЦП.

После завершения начального самотестирования в случае исправности устройства и закрытого положения крышек узлов носителей ключевой

информации в БПД передается соответствующий сигнал, индикатор светится зеленым цветом.

При выборе режима ввода ключевой информации с ДК6 оператор открывает крышку, устанавливает ДК6 в узел установки электронного носителя, поворачивает по часовой стрелке до упора, закрывает крышку узла установки и с пульта управления БПД подает команду в УВК на начало ввода ключевой информации.

Процессор проверяет наличие электронного носителя и закрытое положение крышки. Далее выполняет побайтное считывание ключевой информации и ее передачу БПД через узел интерфейса.

По завершении считывания ключевой информации с ДК6 на индикатор пульта управления выводится соответствующее сообщение. Оператор открывает крышку, извлекает электронный носитель, закрывает крышку, производит опечатывание крышки узла установки ДК6, делает запись в журнале учета о вводе ключевой информации с указанием даты, времени, фамилии, номера печати, проставляет подпись. Отключается питание УВК.

В случае выбора режима ввода ключевой информации с бумажного носителя оператор открывает крышку, устанавливает бумажный носитель, закрывает крышку узла установки и с пульта управления БПД подает команду в УВК на начало ввода ключевой информации.

Процессор проверяет закрытое положение крышки узла установки. Процессор подает сигнал на включение модуля электропитания плюс/минус 15 В и проверяет уровни напряжения, подает сигнал на осветитель оптического узла и управляющие сигналы на фотоприемник и АЦП.

С помощью осветителя производится экспонирование, далее считанное изображение (свет) через объектив поступает на матрицу ФПЗС, преобразующую свет в аналоговый сигнал.

Через усилитель аналоговый сигнал поступает на АЦП, где выполняется его преобразование в цифровой сигнал. Полученные данные записываются в СОЗУ.

Так как считывание изображения штрихового кода с бумажного носителя осуществляется построчно, оцифровка аналогового сигнала и запись данных в СОЗУ выполняются несколько раз.

Обработка полученного изображения штрихового кода осуществляется в несколько этапов. Производится многократное считывание из СОЗУ во внутреннюю память процессора. Процессор выполняет обработку данных, включающую распознавание, декодирование, обнаружение и исправление ошибок. Полученные данные записываются в ОЗУ. На последнем этапе обработки изображения декодированные данные остаются во внутренней памяти процессора. Полученная ключевая информация из внутренней памяти процессора передается в БПД.

После того, как вся ключевая информация была передана БПД, осуществляется многократное стирание всех полученных ранее данных.

По завершении считывания ключевой информации с бумажного носителя на индикатор пульта управления БПД выводится соответствующее сообщение. Оператор открывает крышку, извлекает бумажный носитель ключевой информации, закрывает крышку, производит опечатывание крышки узла установки носителя, делает запись в журнале учета о вводе ключевой информации с указанием даты, времени, фамилии, номера печати, проставляет подпись. Отключается питание УВК.

В случае если во время ввода ключевой информации были открыты крышки или выявлены попытки НСД к внутреннему пространству УВК, отклонения, неисправности узлов, работа УВК блокируется и осуществляется стирание всех ранее полученных данных.

10 Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

К вредным производственным факторам, обладающим свойствами психофизиологического воздействия на нервную систему специалиста по защите информации, относятся нервно-психические перегрузки, связанные с напряженностью трудового процесса.

Согласно ГОСТ 12.003-2015 [44], нервно-психические перегрузки подразделяют на:

- умственное перенапряжение, в том числе вызванное информационной нагрузкой;
- перенапряжение анализаторов, в том числе вызванное информационной нагрузкой;
- монотонность труда, вызывающая монотонию;
- эмоциональные перегрузки.

Основная деятельность специалистов по защите информации связана с умственным напряжением, эмоционально-умственным напряжением, творческим и умственным трудом.

Умственная деятельность — это деятельность, прежде всего, центральной нервной системы, ее высшего отдела — коры человеческого мозга.

При умственной работе, как и при физической, изменяются обменные процессы, происходит сужение сосудов конечностей и расширение сосудов внутренних органов, пульс изменяется незначительно, потребление кислорода мозгом увеличивается в 15-20 раз при умственной работе, по сравнению с физической.

Кроме того, в случаях, когда умственная работа сопровождается нервно-эмоциональным напряжением, то возможны значительные изменения кровяного давления, пульса, повышение уровня сахара в крови [45].

Самым естественным и простым вариантом устранения умственного переутомления является сон. Во время сна упорядочивается и фильтруется информация, полученная в процессе дневной умственной деятельности. Кроме того, клетки головного мозга очищаются от нейротоксинов. Способность к концентрации внимания и запоминанию большого объема информации тоже зависят от качества и продолжительности сна. Считается, что нормальная продолжительность сна составляет около 8 часов в сутки, но, если сотрудник страдает от умственной усталости, ему понадобится увеличить его продолжительность до 10÷12 часов. Для лечения и профилактики умственного перенапряжения применяются также медитация, экотерапия (созерцание красот природы или природных явлений), «информационное голодание» или «разгрузочные дни» для ума [46].

Центральная нервная система получает информацию от внешнего мира, внешней среды с помощью чувствительных аппаратов, воспринимающих сигналы, то есть анализаторами.

Основная характеристика анализаторов – высокая чувствительность, хотя не каждый раздражитель, действующий на анализатор, вызывает ощущение. Чтобы ощущение проявилось, необходима определенная интенсивность раздражителя. Воздействие, превышающее предел интенсивности, вызывает боль и нарушение деятельности анализаторов.

В центральную нервную систему в процессе труда поступает большой объем информации. Мозг ее перерабатывает и сортирует по степени важности. Самыми важными являются сигналы, имеющие значение для жизнедеятельности всего организма; затем воспринимаются сигналы, имеющие значение для отдельных систем и органов.

Задача правильного проектирования технологического процесса – не допустить перенапряжения анализаторов, которое может привести к стрессам [47].

Одним из заболеваний нервной системы, связанных с перенапряжением анализаторов, является координаторный невроз. Это своеобразное профессиональное заболевание наблюдаеся у операторов ПЭВМ, офисных работников, телеграфистов, музыкантов и др. Заболевание характеризуется нарушением функции двигательного анализатора по обеспечению координации строго дифференцированных движений рук. В результате повторяющихся движений в быстром темпе возникают условия для перенапряжения специфической функции руки, лежащей в основе профессиональной деятельности.

Монотонность – это психическое состояние человека, вызванное однообразием восприятия или действий. Общими признаками для всех видов монотонии являются перегрузка информацией при выполнении работы или, наоборот, ее недостаток, что накладывает на состояние человека определенный отпечаток: работник теряет интерес к выполняемой работе и у него возникает состояние, которое называется производственной скукой. Монотонная работа ухудшает экономические показатели, повышается травматизм, аварийность, растет текучесть кадров.

Основные меры по уменьшению влияния монотонности на человека:

- проектирование технического процесса, каждой трудовой операции, необходимых производству, так, чтобы сделать каждую операцию содержательной, вызывающей интерес у исполнителей;
- осуществлять перевод рабочих с одной на другую производственные операции в течение смены или рабочей недели;
- применять оптимальные режимы труда и отдыха в течение рабочего дня. При монотонной работе целесообразны частые, но короткие перерывы – от 2 до 5 минут через час или полчаса работы;

– не допускать принудительный темп работы: быстрый или медленный;

– необходимо соблюдать эстетичность производства, можно осуществлять музыкальное оформление производственного процесса.

Эмоциональные перегрузки характеризуются таким состоянием сотрудника, как утомление. Под утомлением принято понимать функциональное состояние, которое возникает на временной основе под воздействием определенных факторов и причин, формирующихся при продолжительной и интенсивной работе и приводящих к существенному снижению ее результативности. Основными проявлениями утомления можно назвать общее снижение выносливости и силы, ухудшение координации движений, существенное увеличение временных затрат на выполнение обычной работы и т. п.

Регулярное исполнение работы в условиях недостаточного восстановления, нерационально организованный труд и нервно-психическое напряжение на практике непременно ведут к переутомлению, вследствие чего возникает перенапряжение нервной системы, обострение различных заболеваний. Базисом всех указанных выше отклонений является нарушение возбудительно-тормозных нервных процессов.

Важно понимать, что переутомление чрезмерно опасно для человека, оно появляется в результате продолжительного отсутствия полноценного отдыха, когда в рамках определенного периода времени не происходит восстановления организма. Переутомление накладывает отпечаток как на физическое, так и на эмоциональное состояние человека, что приводит к значительному снижению эффективности его деятельности [48].

Таким образом, основными последствиями эмоциональных перегрузок являются расстройство сна, повышенная возбудимость, рассеянность.

Ликвидация утомления возможна только при повышении общего и специального уровня тренированности организма, рационализации физической,

интеллектуальной и эмоциональной активности. Профилактикой умственной усталости служит активизация таких сторон психической и физической активности, которые не связаны непосредственно с теми, которые привели к формированию данного состояния организма. Поэтому необходимы активный отдых, переключения с одной работы на другую, применение средств восстановления. Оптимальное и разумное сочетание и чередование физических нагрузок и отдыха позволяет не только формировать и сохранять, но и развивать способность организма к наиболее эффективному и менее затратному процессу восстановления.

Для восстановления организма на практике часто применяются такие средства, как массаж, рациональное питание, витамины и т. д. Помимо этого, очень важно уделять повышенное внимание особенностям организации занятий физическими нагрузками [49].

Ритмопластические упражнения применяются, в том числе, в неврологической практике, выполняются в музыкальном сопровождении с заданными ритмом и тональностью, в зависимости от функционального состояния организма, типа высшей нервной деятельности, возраста и толерантности к нагрузке.

Спортивно-прикладные упражнения (это ходьба, бег, лазанье и ползание, плавание и многое другое) повышают тонус центральной нервной системы. Наиболее широко в практике лечебной физической культуры используется ходьба — упражнение, восстанавливающее опороспособность, улучшающее подвижность суставов и укрепляющее мышцы средних конечностей, стимулирующее вегетативные функции, восстанавливающее адаптацию к нагрузкам различной интенсивности. Ходьба может выполняться с разгрузкой и в обычном режиме, может применяться как специальное упражнение или в форме прогулок.

Для достижения оптимального эффекта от занятий физическими упражнениями необходимо учитывать следующие факторы:

– индивидуальные особенности занимающихся (возраст, пол, состояние здоровья, физическое развитие, уровень физической подготовленности);

– особенности физических упражнений (сложность, новизна, специализированность, техническая характеристика);

– внешние условия: режим труда, конкретные условия двигательной деятельности (метеорологические условия, качество оборудования и инвентаря, гигиена мест занятий) [50].

Стоит отметить, что повторные нагрузки могут принести максимальный эффект исключительно на стадии повышенной работоспособности, а слишком длительные периоды отдыха значительно снижают результативность тренировок.

Таким образом, можно сформулировать основные правила борьбы с перегрузками:

– рационально организовать режим дня со сменой деятельности и активным отдыхом;

– уменьшить количество нагрузок на организм, необходимо объективно оценивать собственные силы и рационально их направлять;

– грамотно распоряжаться потоком информации;

– рационализировать питание;

– увеличить число пеших прогулок. Если 3÷5 раз в неделю совершать пешие прогулки по 20÷30 минут не позднее чем за 2 часа до сна, что уже через 1÷2 недели восстанавливается нарушенный сон и увеличивается работоспособность;

– больше времени проводить на солнце. Солнечные лучи существенно увеличивают выработку в организме серотонина, который положительно воздействует на организм человека в целом;

– полноценно отдыхать. Сон должен быть не менее 7÷8 часов в день [51].

Заключение

В начале дипломного проектирования, целью которого являлась разработка аппаратного обеспечения устройства ввода ключевой информации для аппаратуры криптографической защиты, был проведен анализ возможных носителей информации, по итогам которого в качестве наиболее подходящего для хранения ключевой информации был выбран бумажный носитель.

Далее был произведен обзор существующих устройств считывания (сканеров) информации с бумажного носителя. По результатам обзора был сделан вывод о недопустимости их применения в аппаратуре криптографической защиты информации и необходимости разработки нового устройства.

На следующем этапе дипломного проектирования был проведен анализ требований к УВК. Были рассмотрены конструктивные, схемотехнические, специальные, инженерно-криптографические требования, а также требования к ЭКБ и требования по стойкости к внешним воздействующим факторам.

Далее был выполнен анализ технических каналов утечки ключевой информации при ее обработке УВК и передаче блоку преобразования данных. Были рассмотрены такие актуальные каналы утечки информации, как канал ПЭМИН, питающие и сигнальные цепи и визуально-оптический канал.

На следующем этапе дипломного проектирования были рассмотрены защитные меры от утечки ключевой информации по каналам, указанным выше. Также были рекомендованы меры защиты ключевой информации от НСД и выполнение инженерно-криптографических требований. Для обеспечения комплексной защиты ключевой информации были рассмотрены и рекомендованы к применению как технические, так и организационные защитные меры.

Затем была разработана структурная схема УВК. В ходе ее разработки были выделены основные структурные элементы (узлы) УВК и указано их предназначение.

На следующем этапе был произведен выбор электронной компонентной базы. Выбранная ЭКБ приведена в перечнях электрорадиоизделий, разрешенных для применения при разработке, модернизации, производстве и эксплуатации вооружения, военной и специальной техники. На данном этапе была также рассмотрена проблема внедрения вредоносных элементов в аппаратное обеспечение устройств как обоснование необходимости применения ЭКБ только отечественного производства.

Далее была разработана функциональная схема УВК, более подробно отражающая устройство и связи между элементами УВК. Отдельно были составлены функциональные схемы узла вычислителя и узла электропитания.

На завершающем этапе дипломного проектирования было составлено описание функционирования УВК, включающее в себя последовательность действий при старте работы устройства, а также при считывании ключевой информации с электронного устройства ДК6 и бумажного носителя.

Таким образом, задание на дипломное проектирование было выполнено в полном объеме.

Список использованных источников

1 Блок К-128. Технические условия. ВАЯП3.065.002 ТУ. Введены в действие с 4.04.1997. - 43 с.

2 Флеш-память. - [Электронный ресурс]. - URL: https://ru.wikipedia.org/wiki/Флеш-память. - Режим доступа: свободный. - (Дата обращения: 23.02.2019).

3 USB-флеш-накопитель. - [Электронный ресурс]. - URL: https://ru.wikipedia.org/wiki/USB-флеш-накопитель. - Режим доступа: свободный. - (Дата обращения: 23.02.2019).

4 SD/SDHC/SDXC Спецификации и совместимость. - [Электронный ресурс]. - URL: https://kb-ru.sandisk.com/app/answers/detail/a_id/9977/~/sd%2Fsdhc%2Fsdxc-спецификации-и-совместимость. - Режим доступа: свободный. - (Дата обращения: 24.02.2019).

5 Карта памяти. - [Электронный ресурс]. - URL: https://ru.wikipedia.org/wiki/Карта_памяти. - Режим доступа: свободный. - (Дата обращения: 24.02.2019).

6 Что такое жесткий диск компьютера? - [Электронный ресурс]. - URL: https://geekkies.in.ua/pc/chto-takoe-zhestkij-disk-kompjutera.html. - Режим доступа: свободный. - (Дата обращения: 24.02.2019).

7 Устройство запоминающее СЭНЗУ-2М. Технические условия. ДЦ3.069.003 ТУ. - 2013 г. - 71 с.

8 Устройство электронное К1634ДК6. Технические условия. АДБК.431210.730 ТУ. Введены в действие с 1.03.2000. - 74 с.

9 Обзор РИК — Российской интеллектуальной карты. - [Электронный ресурс]. - URL: https://www.smarttelemax.ru/publications/rik.html. - Режим доступа: свободный. - (Дата обращения: 26.02.2019).

10 ГОСТ Р 51294.9-2002. Автоматическая идентификация. Кодирование штриховое. Спецификации символики PDF417 (ПДФ417). Принят

и введен в действие Постановлением Госстандарта России от 26 августа 2002 г. №314-ст. - Москва, М.: Издательство стандартов, 2002. - 94 с.

11 Встраиваемый сканер IronScan. Инструкция по эксплуатации. - Москва, 2012. - 18 с.

12 Ручной сканер штриховых кодов BurstScan. Инструкция по эксплуатации. - Москва, 2013. - 21 с.

13 Сканер штрих-кода Metrologic MS9520 MS9540 Voyager. Руководство по настройке и эксплуатации. - Москва, 2013. - 32 с.

14 Цифровой планшетный сканер HP Scanjet 3770. Руководство пользователя. - 32 с.

15 Сканер штрих-кода Proton ICS-7199. Исчерпывающее руководство. - 98 с.

16 ГОСТ РВ 20.39.309-98. Комплексная система общих технических требований. Аппаратура, приборы и оборудование военного назначения. Конструктивно-технические требования. Принят и введен в действие Постановлением Госстандарта России от 26 мая 1998 г. № 232. - М.: Издательство стандартов. - Москва, 1998 г.

17 Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

18 Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: учеб. пособие. – М.: Гостехкомиссия РФ, 1998. – 320 с.

19 ГОСТ Р 56115-2014. Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Утвержден и введен в действие Приказом Федерального агентства по техническому

регулированию и метрологии от 18 сентября 2014 г. N 1123-ст. - М.: Стандартинформ, 2015.

20 Микросхема интегральная 1892ВМ10Я. Руководство пользователя РАЯЖ.431282.012Д17. АО НПЦ «Элвис», 2018 г. - 402 с.

21 Микросхема статического оперативного запоминающего устройства (СОЗУ) емкостью 16М (1М х 16 бит) 1645РУ6У, К1645РУ6У, К1645РУ6УК, 1645РУ6У1, К1645РУ6У1, К1645РУ6У1К, 1645РУ6Н4, К1645РУ6Н4. Спецификация ТСКЯ.431223.011СП. Версия 2.2.0 от 20.06.2017- АО «ПКК Миландр», 2017 г. - 30 с.

22 ПЗУ с электрическим перепрограммированием Flash-типа, 1636РР4У, К1636РР4У, К1636РР4УК, 1636РР4Н4, К1636РР4Н4. Спецификация ТСКЯ.431214.005СП. Версия 1.1.0 от 22.09.2015. - АО «ПКК Миландр», 2015 г. - 54 с.

23 Микросхема быстродействующего малопотребляющего 12/14-разрядного АЦП конвейерного типа 5101НВ015, К5101НВ015, К5101НВ015К, К5101НВ01Н4. Спецификация ТСКЯ.431324.004СП. Версия 2.3.0 от 08.02.2018. - АО «ПКК Миландр», 2018 г. - 52 с.

24 Комплект микросхем 8-разрядных шинных формирователей выходных уровней 5572ИН2АУ, К5572ИН2АУ, К5572ИН2АУК, 5572ИН2БУ, К5572ИН2БУ, К5572ИН2БУК, К5572ИН2АН4, К5572ИН2БН4. Спецификация ТСКЯ.431323.014-01СП. Версия 2.5.0 от 25.02.2016. - АО «ПКК Миландр», 2016 г. - 22 с.

25 Микросхемы 5514БЦ1Т2-9А5. Технические условия АЕЯР.431260.179 ТУ. Карта заказа ЩИЗ.414.534-9А5 Д. - АО «Ангстрем», 2003 г. - 7 с.

26 Микросхема двухканального LVDS приемопередатчика 5559ИН19У, К5559ИН19У, К5559ИН19Н4. Спецификация ТСКЯ.431323.005СП. Версия 2.2.0 от 11.07.2012. - АО «ПКК Миландр», 2012 г. - 19 с.

27 Модули питания серии МДМ. Общие технические условия БКЮС.430609.001 ТУ. - АО «АЛЕКСАНДЕР ЭЛЕКТРИК источники электропитания», 2006 г. - 92 с.

28 Микросхема понижающего преобразователя напряжения 1310ПН1У, К1310ПН1У, К1310ПН1Н4. Спецификация ТСКЯ.431329.001СП. Версия 2.11.0 от 31.03.2017. - АО «ПКК Миландр», 2017 г. - 17 с.

29 Микросхемы интегральные 1156ЕУ1. Технические условия АЕЯР.431 420.007-01 ТУ. АО «Группа Кремний Эл», 2015 г. - 65 с.

30 Микросхемы интегральные 1303ЕН1.5П, 1303ЕН1.8П, 1303ЕН2.5П, 1303ЕН3.3П, 1303ЕН5П. Технические условия АЕЯР.431420.638 ТУ. - АО «НПП «ЭлТом», 2017 г. - 76 с.

31 Микросхемы интегральные 1230ДН1У, 1230ДН1Т. Технические условия АЕЯР.431340.771 ТУ. АО «Группа компаний «Кремний Эл», 2017 г. - 80 с.

32 Микросхемы интегральные 5574ИР2У. Техническое описание ГПКФ.431233.002-01 ТО. - АО «КТЦ «Электроника». -11 с.

33 Генераторы кварцевые однократно программированные ГК109-С. Технические условия АФТП.433520.008 ТУ. ПАО «ЛИТ-ФОНОН», 2009 г. - 64 с.

34 Микросхема ФПЗС45М. Технические условия: ЯЛАР 433832.005 ТУ. ЗАО «НПП «Элар», 2015 г. - 59 с.

35 Объектив. Технические условия: НБПИ.202361. 007 ТУ. ОАО «ТКС-Оптика», 2009 г. - 19 с.

36 Микросхемы интегральные 1432УД1АР, 1432УД1БР, 1432УД7АР, 1432УД7БР. Технические условия исполнения АЕЯР.431100.280-01 ТУ. АО «НПП «Пульсар», 2003 г. - 94 с.

37 Индикаторы полупроводниковые единичные типа ИПД 132. Технические условия АЕЯР.432220.320 ТУ. ОАО «Протон», г. Орёл, 2006 г. - 83 с.

38 Устройства контактные УК-ДК4-32. Технические условия: РИВУ.469115.407 ТУ, 2002 г. - 56 с.

39 Микропереключатели типа ПМ21В. Технические условия: АГ0.360.013 ТУ. АО «НПП «Кузбассрадио», 2015 г. - 27 с.

40 Керамические помехоподавляющие фильтры Б26. Технические условия: АЖЯР.431145.005 ТУ. АО «НИИ «Гириконд». - 11 с.

41 Керамические помехоподавляющие фильтры Б24, Б24-1. Технические условия: АЖЯР.431145.003 ТУ. АО «НИИ «Гириконд». - 9 с.

42 Белоус А.И., Солодуха В.А., Шведов С.В. Программные и аппаратные трояны — способы внедрения и методы противодействия. Первая техническая энциклопедия. Под общей редакцией Белоуса А.И. В 2-х книгах. Книга 1. - Москва: Техносфера, 2018. - 688 с.

43 Белоус А.И., Солодуха В.А., Шведов С.В. Программные и аппаратные трояны — способы внедрения и методы противодействия. Первая техническая энциклопедия. Под общей редакцией Белоуса А.И. В 2-х книгах. Книга 2. - Москва: Техносфера, 2018. - 630 с.

44 ГОСТ 12.0.003-2015. Система стандартов безопасности труда (ССБТ). Опасные и вредные производственные факторы. Классификация. - Приказом Федерального агентства по техническому регулированию и метрологии от 9 июня 2016 г. N 602-ст введен в действие в качестве национального стандарта Российской Федерации с 1 марта 2017 г. - Взамен ГОСТ 12.0.003-74. - М.: Стандартинформ, 2016.

45 Перегрузки эмоциональные и умственные. - [Электронный ресурс]. - URL: https://studfiles.net/preview/5638826/page:11/. - Режим доступа: свободный. - (Дата обращения: 22.05.2019).

46 Умственное переутомление. - [Электронный ресурс]. - URL: http://nataliaprahova.ru/soveti-psihologa/umstvennoe-pereutomlenie/. - Режим доступа: свободный. - (Дата обращения: 22.05.2019).

47 Перенапряжение анализаторов. - [Электронный ресурс]. - URL: https://studfiles.net/preview/5638826/page:12/. - Режим доступа: свободный. - (Дата обращения: 22.05.2019).

48 Физические перегрузки и функциональное перенапряжение организма работников. - [Электронный ресурс]. - URL: http://www.kiout.ru/info/publish/27857 - Режим доступа: свободный. - (Дата обращения: 23.05.2019).

49 Шохин В.Е. Физические и эмоциональные перегрузки в процессе освоения программ профессиональной подготовки. Вестник краснодарского университета МВД России, 2017, № 1 (35), 183-185.

50 Лечебная физическая культура [Текст] : учеб.пособие / Виталий Александрович Епифанов. - М. : ГЭОТАР-МЕД, 2002. - 560 с.

51 Шохин В.Е. Физические и эмоциональные перегрузки в процессе освоения программ профессиональной подготовки. Вестник краснодарского университета МВД России, 2017, № 1 (35), 185-186.