МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт автоматики и информационных технологии

Кафедра «Электроники, телекоммуникации и космических технологии»

Бекмуратова Эльмира Маратовна

Исследование тенденций развития электронных компонентов систем безопасности

ДИПЛОМНАЯ РАБОТА

Образовательная программа 6B07104 – Electronic and Electrical Enhineering

Алматы 2023

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт автоматики и информационных технологии

Кафедра «Электроники, телекоммуникации и космических технологии

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой ЭТиКТ
_____ Таштай Е.Т.
«20» _____ 2023 г.

ДИПЛОМНАЯ РАБОТА

На тему: «Исследование тенденций развития электронных компонентов систем» по образовательной программе 6B07104 – Electronic and Electrical Engineering

Выполнил Бекмуратова Э.М.

Рецензент
Директор
«ARNAU» ЖШС

Баймухамед Т.С.
«01» 06 2023 г.

Научный руководитель

старший преподаватель каф.ЭТиКТ
КазНИТУ им.К.И.Сатпаева
Юсупова Г.М.
«16» 05 2023 г.

Алматы 2023

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт автоматики и информационных технологии

Кафедра «Электроники, телекоммуникации и космических технологии»

УТВЕРЖДАЮ
Заведующий кафедрой ЭТиКТ
_____ Таштай Е.Т.
«22» 01 2023 г.

ЗАДАНИЕ
на выполнение дипломной работы

Дипломнице Бекмуратовой Эльмире Маратовне
Тема: «Исследование тенденций развития электронных компонентов систем безопасности».
Утверждена приказом Ректора Университета № 408-П/Ө от «23» ноября 2022 года.
Срок сдачи законченной работы "30" апреля 2023 г.
Исходные данные к дипломной работе:
1. Функциональная беопасность электронных компонентов должны соответствовать требованиям международного стандарта ГОСТ Р МЭК 1508-2- 2007 [1].
2. В качестве исследование рассмотреть тенденции развития электронных компонентов систем контроля, управления и мониторинга систем беопасности [3,4,5,6 и 9].
3. Исследовать перспективные направления развития электронных компонентов на ближаийшие 10 лет [7,8 и 9]
4. Объектом защиты является испытательная лаборатория из двух комнат общей площадью 100 кв.м. [10]
Перечень вопросов подлежащих изучить и представить в дипломной работе:
а) Обзор электронных компонентов в мире, в том числе космической электроники.
б) Методы построения систем безопасности на базе электронных компонентов систем контроля, управления и мониторинга для технических систем
в)Тенденции развития электронных компонентов
д) Расчет стоимости на внедрение системы безопасности технической системы для объекта защиты
Перечень графического материала: изложить материалы диссертации в 25 -30 слайдах графического материала на PowerPointe.
Рекомендуемая основная литература:

1. ГОСТ Р МЭК – 2 – 2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью
2. Сканти навигатор в мире электронных компонентов, №2, 2020, 53 с.
3. Компоненты зарубежных электрических и электронных систем, Минск, БГАТУ, 2012, 64с

ГРАФИК

подготовки дипломной работы

Наименование разделов, перечень разрабатываемых вопросов	**Сроки представления научному руководителю**	**Примечание**
1. Обзор электронных компонентов в мире, в том числе космической электроники	1.09.2022-31.12.2022	Выполнено
2. Методы построения систем безопасности на базе электронных компонентов систем контроля, управления и мониторинга для технических систем	1.01.2023-30.01.2023	Выполнено
3.1 Тенденции развития электронных компонентов	1.02.2023-15.02.2023	Выполнено
3.2 Расчет стоимости на внедрение системы безопасности технической системы для объекта защиты	1.02.2023-15.03.2023	Выполнено
4. Написание дипломной работы	15.04.2023-30.04.2023	Выполнено

Подписи

консультантов и нормоконтролера на законченную магистерскую диссертацию с указанием относящихся к ним разделов диссертации

Наименование разделов	Консультанты Ф.И.О. (уч.степень, звание)	Дата подписания	Подпись
Нормоконтролер	м.т.н., ассистент Базарбай А.М	01.09.2023	

Научный руководитель Юсупова Г.М.

Задание принял к исполнению обучающийся Бекмуратова Э.М.

«1» 09 2022 г.

АННОТАЦИЯ

Работа посвящена вопросам, связанным с понятием тенденции развития электронных компонентов в системе безопасности.

Отличительной чертой работы заключается в исследовании перспективных направлении развития электронных компонентов на ближайшее десять лет, а именно компонентов системы безопасности, а также систем контроля, управления и мониторинга систем безопасности.

АННОТАЦИЯ

Жұмыс қауіпсіздік жүйесіндегі электрондық компоненттердің даму тенденциясы ұғымына қатысты мәселелерге арналған.

Жұмыстың айрықша ерекшелігі - алдағы он жылға арналған электрондық компоненттерді, қауіпсіздік жүйесінің компоненттерін, сондай-ақ қауіпсіздік жүйелерін бақылау және басқару жүйелерін дамытудың перспективалық бағыттарын зерттеу болып саналады.

ANNOTATION

The work is devoted to issues related to the concept of trends in the development of electronic components in the security system.

The distinctive feature of the work is the study of promising directions for the development of electronic components for the next ten years, namely, components of the security system, as well as access control and management system.

Issues in the selection of equipment for the introduction of technology have been resolved.

СОДЕРЖАНИЕ

Введение
1 Обзор электронных компонентов в мире, в том числе космической электроники 10
1.1 Датчики 10
1.2 Батареи и аккумуляторы 12
1.3 Компоненты электронных схем 13
1.4 Компоненты электрооборудования 15
2 Методы построения систем безопасности на базе электронных компонентов систем контроля, управления и мониторинга для технических систем 17
2.1 Выбор электронных компонентов для внедрения системы безопасности в помещение, а также для системы управления, контроля доступом и мониторинга 18
3 Исследовательская часть 30
3.1 Тенденции развития электронных компонентов 30
3.2. Расчет стоимости на внедрение системы безопасности технической системы для объекта защиты 42
Заключение 47
Список использованной литературы 48
Перечень терминов и сокращений 49

ВВЕДЕНИЕ

Современный мир нуждается о постоянной заботе безопасности, и главным способом обеспечения безопасности является использование систем безопасности на основе электронных компонентов. Также эти системы используются в различных отраслях промышленности, таких как медицина, авиация, промышленность, транспорт и многих других.

Целью данной работы является исследование тенденции развития электронных компонентов систем безопасности, а также возможности их использования для создания систем безопасности на базе электронных компонентов.

Задачами в данной дипломной работе являются:

- обзор электронных компонентов в мире, в том числе космической электроники;
- методы построения систем безопасности на базе электронных компонентов систем контроля, управления и мониторинга для технических систем;
- расчет стоимости на внедрение системы безопасности технической системы для объекта защиты.

Научной новизной в данной работе является исследование тенденции развития электронных компонентов за последние годы, для анализа их развития на ближайшие десять лет.

Актуальность работы составляет важность роли обеспечения безопасности людей в мире, так как обеспечения безопасности без электронных компонентов является невозможным, то их развития является очень важной задачи в данной работе.

Теоретической основой является электронные компоненты, нормативные и стандартные требования к электронным компонентам, принципы системы безопасности, а также основные требования к ним, и исследования технологических тенденций.

Методологической основой является исследования рынка, разрабатывающих электронные компоненты, анализ их требования и потребностей и анализ этих данных с помощью различных литератур в этой области.

В данной дипломной работе проводится исследование тенденции развития электронных компонентов систем безопасности, которые могут использоваться для создания систем безопасности на базе электронных компонентов для технических систем.

В первом разделе работы проводится обзор основных электронных компонентов и компонентов космической электроники систем безопасности.

Второй раздел посвящен методам построения систем безопасности на базе этих электронных компонентов для технических систем, а также выбору конкретных электронных приборов и некоторых космических компонентов.

Третий раздел работы посвящен тенденциям развития электронных компонентов, которые могут использоваться для систем безопасности, а также для улучшения систем безопасности в будущем. В заключительной части работы проводится расчет стоимости на внедрение системы безопасности технической

системы для защиты и охраны объекта на основе материалов, выбранных во втором разделе.

Исследование тенденции развития электронных компонентов в системе безопасности необходимо по нескольким причинам:

- повышение безопасности, что приводит к надежности и эффективности безопасности в реальной жизни;
- быстрое развитие технологий, что позволяет быть в курсе последних достижений и инноваций;
- улучшение функциональности и эффективности электронных компонентов с каждым годом;
- адаптация их к изменяющимся угрозам, что позволяет разрабатывать новые методы и технологии для обнаружения и предотвращения угроз в системе безопасности;
- конкурентное преимущество, что позволяет идентифицировать новые решения и инновации, которые могут помочь некоторым компаниям, разрабатывающие электронные компоненты в области безопасности из-за высокой конкуренции в сфере безопасности.

1 Обзор электронных компонентов в мире, в том числе космической электроники

Современные системы безопасности требуют использования современных электронных компонентов для обеспечения эффективной защиты от различных угроз. Электронные компоненты систем безопасности включают в себя различные устройства, такие как датчики, микроконтроллеры, передатчики, приемники, сенсоры и другие устройства, которые используются для обнаружения, обработки и передачи информации. Эти компоненты играют очень важную роль в обеспечении безопасности в различных сферах, таких как автомобильная промышленность, промышленность безопасности, медицинская и научная промышленности, автоматизации систем безопасности в любых объектах.

Также очень важным направлением развития электронных компонентов является космическая электроника. Космическая электроника имеет ряд уникальных особенностей, которые обуславливают ее высокую надежность в целом и особенно в системе безопасности, а также стабильность и долговечность. Это связано с очень важными особенностями, такие как эксплуатации компонентов в космическом пространстве, такими как воздействие космического излучения, экстремальные температуры, вакуум и еще другие факторы.

В данном обзоре рассмотрены основные электронные компоненты, включая компоненты космической электроники, которые могут быть использованы для систем безопасности и для обеспечения безопасности объектов, а также предоставлены крупнейшие компании мира, выпускающие данные электронные компоненты в обзоре.

1.1 Датчики

Датчики – это сенсоры, являющиеся первичными преобразователями, которые преобразовывают контролируемые величины, такие как давление, температура, расход, концентрация, частота, скорость, перемещение, напряжение, электрический ток и т.д. в сигналы, такие как электрические, оптические или пневматические.

По типу датчики бывают:

- датчики контроля уровня, содержащие поплавок с магнитом для воздействия на язычковый переключатель;
- датчики давления, осуществляющие переключение при достижения предварительного заданного давления;
- переключатели наклона, реагирующие на небольшие изменения угла наклона;
- емкостные датчики, выдающие сигнал, который изменяется в зависимости изменения емкости, если датчики находятся в веществах с различной ди-

электрической проницаемостью, они используются для контроля уровни жидкости;

- индуктивные датчики, состоящие из катушки, которая имеет свойство реагировать на изменения магнитного поля;

- оптические датчики, состоящие из источника модулированного излучения, фотоприемника, преобразователя, а также усилителя сигнала, где приемник может анализировать возможно поступивший световой поток и проверяет поступление светового потока от источника излучения, а также может передавать соответствующий сигнал на усилитель и в дальнейшем на исполнительное устройство [1].

PIR - инфракрасные датчики движения – это устройства, которые могут определять движения в окружающей среде при помощи инфракрасных лучей. Принципом действия инфракрасных PIR (passive infrared motion sensor) - датчиков движения является детектирование изменений в инфракрасном излучении, которое могут испускать все объекты с температурой выше абсолютного нуля.

Техническими характеристиками инфракрасных датчиков движения являются угол обзора, дальность действия, чувствительность, время задержки, режим работы и другие параметры. Недостатком является, что при использовании они могут иметь ложные срабатывания, но их можно предотвратить с помощью дополнительных датчиков, контролирующие чувствительность, а также необходимо соблюдать нужные требования к безопасности, например, правильную установку датчика, проверку работоспособности перед использованием и другие [1 с.49].

Космические инфракрасные датчики отличаются тем, что они имеют свойства выдерживать экстремальную температуру, воздействие радиации, и имеют высокие требования к техническим характеристикам датчика, такие как высокая точность измерений и высокая надежность работы в условиях космической эксплуатации, а также они имеют большую дальность обнаружения и большую чувствительность, чем обычные инфракрасные датчики, что позволяет им обнаруживать более слабые тепловые сигналы [2].

Один из хороших примеров космического инфракрасного датчика является датчик MODIS (Moderate Resolution Imaging Spectroradiometer), который используется на борту спутников NASA Terra и Aqua для мониторинга климата на Земле и окружающей среды. Он обнаруживает температурные изменения в пределах 0,5 градуса Цельсия и измерять температуру поверхности Земли с точностью до 1 градуса [3].

Ультразвуковые датчики - это сенсоры, которые используют ультразвук для измерения расстояния, скорости и других параметров. Они работают, основываясь на эффекте отражения звуковых волн от объектов в окружающей среде. В системе безопасности они могут использоваться для измерения расстояния до объекта, обнаружения наличия препятствий или измерения скорости движения определенного объекта.

Ультразвуковые датчики имеют намного больше преимуществ по сравнению с другими типами датчиков, например, высокая точность, широкий диапа-

зон рабочих температур и отсутствие воздействия электромагнитных полей. Однако они также имеют свои ограничения, такие как чувствительность к влажности и пыли в воздухе [4].

Сегодня многие компании занимаются производством ультразвуковых датчиков, включая Siemens, Honeywell, Pepperl&Fuchs, SICK и другие. Они используются в различных областях, начиная от автоматических дверей до медицинских устройств и систем контроля качества в промышленности [5].

Датчики газа – это сенсоры, которые используются для обнаружения наличия или уровня различных газов в воздухе.

Самыми распространенными типами датчиков газа являются электрохимические датчики. Они необходимы для обнаружения различных видов газов, таких как углекислый газ, оксид углерода, сероводород и другие. Такие датчики работают на основе изменения химической реакции между газом и электродом, что приводит к изменению электрического сигнала [4 с.54].

Датчик давления - это устройство, которое используется для измерения давления в газах или жидкостях. Датчик давления может измеряет давление относительно атмосферного давления (абсолютное давление) или относительно давления в другой среде (избыточное давление).

Примерами производителей датчиков давления являются Bosch, Honeywell, Sensata Technologies, Amphenol, TE Connectivity, Omron, STMicroelectronics и другие [4 с.37].

1.2 Батареи и аккумуляторы

Батареи – электронные компоненты, имеющие свойства преобразовывать химическую энергию в электрическую. Они разделяются на первичные батареи и вторичные батареи. Где они отличаются между собой тем, что первичные батареи нужны для однократного использования, так как химическая реакция, которая создает электрическую энергию является необратимой, в то время как вторичные батареи нужны для многократного использования, их можно заряжать и использовать заново, так как химическая реакция в таких батареях преобразовывается путем пропускания через них тока вместо нагружения. Вторичные батареи называются перезаряжаемыми, и используются для хранения энергии [1 с.227].

Солнечные батареи в космической электронике – устройства, которые используют энергию солнечного света для генерации электричества, которая используется для питания электронных устройств на космических аппаратах. Для использования в космической технике, солнечные батареи должны соответствовать определенным требованиям. Они должны быть легкими, прочными, стойкими к радиации и экстремальным температурам, а также обладать высокой эффективностью преобразования солнечной энергии в электрическую [3 с. 97].

Одной из компаний – лидеров в производстве солнечных батарей является китайская компания Jinko Solar, известная как крупнейшая в мире по производству солнечных батарей в данный. Годовая выручка компании составила 5,38 миллиарда долларов США в 2020 году при темпах роста 18 процентов [8].

Аккумуляторы – компоненты электроники, использующие для хранений электрической энергии в химической форме, которые могут освобождаться при необходимости в виде электрического тока, они могут использоваться для резервного источника питания в случае отключения солнечных батарей или других источников питания, которые необходимы для систем безопасности. Важнейшими характеристиками аккумуляторов являются емкость, напряжение и срок их службы. Емкость измеряется в ампер-часах, который определяет количество электрической энергии, хранящий в аккумуляторе.

Если взять космических аккумуляторов, то основными типами аккумуляторов, используемых в космической электронике являются:

- литий-йонные аккумуляторы, имеющие высокую плотность энергии и длительный срок службы, но недостатками материалов являются подверженность перегреву, который может привести к пожару;
- никель-кадмиевые аккумуляторы, имеющие более низкую плотность энергии и меньшую длительность службы, в отличии от литий-йонных аккумуляторов;
- серебряно-цинковые аккумуляторы, имеющие более высокую плотность энергии, в отличии от никель-кадмиевыех аккумуляторов, но также недостатком является более короткий срок службы [1 с.233].

В данный момент существуют немного крупных компаний в мире по производству обычных аккумуляторов, так же и космических. Например, Японская компания Panasonic, который производит различные типы аккумуляторов, включая литий-йоновые, никель-металл-гидридные и свинцово-кислотные. Южнокорейская компания LG Chem, который производит литий-йоновые аккумуляторы для различных приложений, такие как автомобили, стационарные системы хранения энергии и портативные устройства. А также американская компания Tesla, которая производит электрические автомобили и системы стационарного хранения энергий на основе литий-йонных аккумуляторов. Сейчас Tesla продолжает развивать свои аккумуляторные технологии, недавно представив новый батарейный блок, где батареи этого типа предполагаются использовать в космической отрасли [9].

1.3 Компоненты электронных схем

Резистор - это электронный компонент, ограничивающий ток в электрической цепи и создающий определенное сопротивление для электрического потока. Резисторы используются в различных электронных устройствах, например источники питания, сенсоры, фильтры, усилители, и другие [1 с. 112].

Космические резисторы - это резисторы, специально разработанные и протестированные для использования в космической технике. Космические резисторы, а также и другие космические электронные компоненты должны соответствовать строгим требованиям, связанным с эксплуатацией в условиях для космического пространства, особенно касающиеся высоких радиационных уровней, экстремальных температур и вибраций. Космические резисторы имеют более высокую надежность, эффективность и долговечность по сравнению с обычными резисторами. Они обычно используются в космических аппаратах, таких как спутники, ракеты и космические корабли [2 с. 501].

Конденсаторы – электронные компоненты для временного хранения электрической энергии. Также они используются в качестве дополнительного источника питания или для защиты технической системы от напряжения и скачков тока [1 с. 142].

Космические конденсаторы в отличии от обычных конденсаторов должны соответствовать строгим требованиям к надежности и устойчивости к радиации, для работы в космических условиях. Космические конденсаторы должны изготавливаться из материалов, таких как тантал, оксид ниобия и оксид алюминия, они проходят тщательную проверку перед эксплуатацией и отправкой на космические аппараты [2 с.256].

В данный момент существуют множество компании, производящих конденсаторы, некоторые из наиболее известных, которые производят как обычные, так и космические являются AVX Corporation, KEMET Corporation, Vishay Intertechnology, Panasonic Corporation [7].

В данный момент примерами производителей надежных космических резисторов являются Vishay, Ohmite, TT Electronics, KOA Speer Electronics, Bourns и другие. Некоторые производители обычных резисторов, такие как Panasonic, Murata и Yageo, также производят космические версии своих продуктов [9 с. 12].

Светодиод (LED) - это электронный компонент, преобразовывающий электрическую энергию в световую энергию. Он работает на основе электролюминесценции, явления, которые электроны в кристалле материала светодиода переходят на более низкий уровень энергии, из-за излучения фотоны света. Светодиоды имеют более преимуществ в отличии от других источников света, например, как галогенные лампы или люминесцентные лампы. У них более высокая эффективность, такие как преобразование большей части потребляемой энергии в свет, а не в тепло. Они также имеют качества более длительного срока службы, а также могут работать в более широком диапазоне температур [1 с. 159].

Самыми лидирующими странами по производству светодиодов в настоящий момент являются Япония, США, Китай, Корея, Германия. Например, из крупнейших производителей светодиодов и их компонентов в мире является японская компания Nichia, а в Корее компании Seoul Semiconductor, Samsung LED [11].

1.4 Компоненты электрооборудования

Реле – переключатели, которые необходимы для дистанционного управления электромеханическими устройствами, при помощи пропускания электрического тока через обмотку электромагнита. Главные различия между видами реле являются контактные функции и характеристики катушек [1 с.33].

Кабели – электрические или оптические проводники, состоящие вместе в общей оболочке, для передачи информации или связи различных компонентов между собой [1 с.76].

Микропроцессоры – центральный процессор компьютера или других электронных устройств, выполняющие арифметические арифметические, логические и управляющие операции над данными, а также инструкциями, хранящимися в памяти устройства. Есть две основные группы микропроцессоров, микропроцессоры, которые выполняют многосхемные решения, и микроконтроллеры, которые являются одночиповыми или одноблочными [1 с.246].

Космические микроконтроллеры от обычных отличаются радиационной стойкостью, стойкости широким температурным диапазонам, надежностью улучшенного качества, стойкостью к отказам, размером и массам меньше чем у обычного, более низким энергопотреблением, а также устойчивости к вибрациям, которые могут возникнуть во время работы космических аппаратов или старта [3 с. 289].

Трансиверы – электронные оборудования, комбинирующие функции передачи и приема сигналов в одном устройстве. Они могут использоваться в космической электронике в качестве связи между космическими аппаратами, а также в качестве связи между устройствами в радиосвязи. Основной функцией трансиверов является преобразования сигнала из одной функции в другую функцию, например, аналоговый в цифровой сигнал или наоборот, еще одной важной функцией является обеспечивать модуляцию и демодуляцию сигнала. Они широко применяются в сетях связи, например, как Wi-Fi, Bluetooth и мобильные сети. Также трансиверы используются в приборах, таких как радары, ультразвуковые датчики, системы контроля окружающей среды и в космической электронике [3 с.301].

Видеокамеры – это электронные устройства, которые нужны для использования записи видеоизображений на цифровые носители. Они широко применяются в системе безопасности для мониторинга. Основными структурными компонентами видеокамеры являются матрица (или CCD/CMOS-матрица), которая преобразовывает свет в электрический сигнал, объектив, собирающий свет и направляющий матрицу, процессор изображения, обрабатывающий сигналы, полученные от матрицы, и преобразовывающий их в видеоизображение, и носитель записи, которая записывает и сохраняет видеоизображение.

В данный момент из наиболее популярных производителей видеокамер для охраны объектов включают Hikvision, Dahua, Axis Communications, Bosch Security and Safety Systems, Hanwha Techwin, и Avigilon [5].

Крупнейшими компаниями в данный момент по производству обычных микроконтроллеров являются Microchip Technology Inc., имеющий широкий ассортимент продуктов, включая PIC, AVR, Texas Instrument, которая также производит разные спектры микроконтроллеров, включая серии MSP430 и Tiva. А по производству космических микроконтроллеров, лидирующими являются Gobham Gaislerm, Atmel и другие [9 с.5].

Выбор электронных компонентов для систем безопасности имеет очень важное значение для обеспечения их эффективной и надежной работы. Компоненты имеют необходимость соответствовать определенным требованиям, для обеспечения высокой точности и надежности в различных условиях. Кроме того, для космической электроники требуются еще более высокие требования, которые могут выдерживать экстремальные условия во время эксплуатации, например, такие условия как радиация, космическое излучение, экстремальные температуры и другие факторы, не встречающиеся на Земле.

Компоненты магнитной электроники являются магнитометры и градиентометры. Они предназначены для измерения магнитных полей в любых системах. В системах безопасности они могут использоваться для определения местонахождения металлических предметов, а также контроля за перемещением дверей и окон [6].

В настоящее время лидирующими компаниями по производству трансиверов являются Analog Devices, Broadcom, Qualcomm, Intel, Texas Instruments и др. Каждая из этих компаний могут предлагать свои собственные решения для различных областей применения трансиверов [8 с.19].

Компонентами систем связи являются такие как радио и спутниковые связи. Они могут использоваться для передачи данных между различными компонентами системы безопасности охраны объектов и для связи с центральной станцией мониторинга. Они также используются для вызова аварийных служб в случае возникновения проблем [8 с.14].

Беспроводные сети – они используются для передачи данных между различными электронными компонентами системы безопасности охраны объектов. Они используются для передачи сигналов от датчиков на центральную станцию мониторинга и для связи между различными компонентами системы безопасности [8 с.11].

Компонентами систем навигации являются такие устройства, как GPS-приемники и инерциальные навигационные системы. Они могут использоваться для определения местоположения объекта. В системах безопасности охраны объектов используются для мониторинга перемещения транспорта и ценных грузов [8 с.27].

В данный момент спутники системы GPS производятся компаниями Lockheed Martin, Boeing, а по производству устройств GPS приемников работают такие крупные компании, как Garmin, Tom Tom, Navman, Lowrance [10].

2 Методы построения систем безопасности на базе электронных компонентов систем контроля, управления и мониторинга для технических систем

Из-за того, что современные технические системы становятся все более сложными, их безопасность и надежность являются одним из ключевых факторов для обеспечения их эффективной работы. Для того, чтобы достичь высокий уровень безопасности в системах контроля, управления и мониторинга используются различные методы для надежной работы данных систем, которые основаны на электронных компонентах.

Построение систем безопасности на базе электронных компонентов систем контроля управления и мониторинга для технических систем включают в себя следующие главные методы:

1) использование датчиков, датчиков безопасности, где датчики могут использоваться для мониторинга параметров технических систем, таких как температура, давление, вибрация и т.д. Датчики безопасности устанавливаются для обнаружения опасных ситуаций, таких как проникновение в несанкционированные зоны или для обнаружения пожар;

2) использование контроллеров безопасности, где контроллеры безопасности могут использоваться для управления операциями технических систем, и действуют для предотвращения опасных ситуаций. Контроллеры безопасности обычно настраиваются для аварийного останова системы в случае опасности, но также и для управления скоростью и направлением движения системы;

3) использование системы видеонаблюдения, где системы видеонаблюдения используются для мониторинга технических систем и обнаружения опасных ситуаций. Видеокамеры должны быть установлены в критических зонах для наблюдения за работой технических систем и принятия мер по предотвращению аварий;

4) использование системы доступа, где системы доступа используются для управления доступом к критическим зонам технических систем. Системы доступа включают в себя ключевые карты, биометрические сканеры, которые должны использоваться для определения легальности доступа.

5) использование системы контроля доступа в сети, где системы контроля доступа в сети используются для защиты сети технических систем от несанкционированного доступа. Системы контроля доступа включают в себя пароли, шифрование, а также и другие меры безопасности для защиты сети от хакеров и злоумышленников;

6) использование системы резервирования, где системы резервирования используются для предотвращения аварийных ситуаций и увеличения надежности технических систем. Системы резервирования включают в себя резервные электронные компоненты и устройства, которые должны быть
включены в работу, если в случае основные компоненты будут работать некорректно, что позволяет уменьшить вероятность аварий и обеспечить бесперебойную работу технических систем;

7) использование системы мониторинга и управления, где системы мониторинга и управления используются для контроля параметров технических систем и быстрого реагирования на опасные ситуации. Эти системы включают в себя программное обеспечение для мониторинга параметров, определения аномалий и средства управления для быстрого реагирования на аварийные ситуации;

8) использование системы резервного питания, где системы резервного питания используются для обеспечения бесперебойной работы технических систем в случае отключения электроэнергии. Оно включает в себя установку аккумуляторов, генераторов или других источников энергии, которые могут быть использованы для питания системы при отключении электричества;

9) использование системы маркировки и идентификации, где системы маркировки и идентификации используются для обеспечения безопасной эксплуатации технических систем. Данный метод включает в себя маркировку компонентов, для того, чтобы они могли быть легко идентифицированы и заменены в случае необходимости;

10) использование системы резервного хранения данных, где системы резервного хранения данных используются для защиты данных технических систем от потери. Данный метод включает в себя установку резервных дисков или облачного хранилища, которые должны быть использованы для сохранения копий данных в случае их потери [12].

Эти десять методов могут использоваться в сочетании, для того, чтобы создать комплексную эффективную систему безопасности на базе электронных компонентов систем контроля управления и мониторинга для технических систем. Очень важно подобрать сочетание методов, чтобы данные методы могли наилучшим образом соответствовать требованиям конкретной технической системы и обеспечивать ее безопасную эксплуатацию.

2.1 Выбор электронных компонентов для внедрения системы безопасности в помещение, а также для системы управления, контроля доступом и мониторинга

Так как в качестве технической системы в данной работе является внедрение системы безопасности систем управления, контроля доступом и мониторинга в помещение, то можно исходя из вышеперечисленных методов выбрать необходимые электронные компоненты и компоненты космической электроники. В данной работе в качестве помещение дана двухкомнатная испытательная лаборатория размером сто квадратных метра, в которой находятся ценные электронные и космические приборы. Целью внедрения системы безопасности является охрана данного объекта, а также электронных приборов внутри помещения. Требованиями для данной технической системы являются установка камеры видеонаблюдения, датчиков движения, системы контроля доступа, тревожной сигнализации, резервное питание, а также контроль температуры и влажно-

сти и физическая безопасность [12]. На базе вышеперечисленных методов, электронные приборы и компоненты космической электроники были выбраны в соответствии стандартам ГОСТ Р МЭК 61508-2-2007.

2.1.1 Выбор программно-аппаратной платформы

Для начала, чтобы реализовать техническую структуры системы безопасности нужна программно-аппаратная платформа, согласно по стандарту соответствующим требованиям безопасности была выбрана плата Arduino 2560. Данная плата имеет третью уровень SIL (safety integrity level) функциональной безопасности, что означает, ее можно использовать в системах, требующих высокого уровня безопасности. На рисунке 2.1 показан вид платы Arduino 2560.

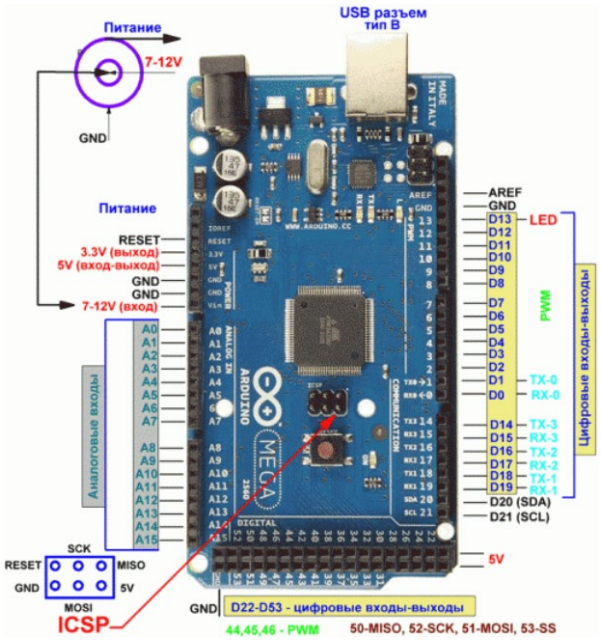

Рисунок 2.1 – Программно-аппаратная платформа Arduino Mega 2560

Плата Arduino 2560 оснащена микроконтроллером ATmega 2560 и предоставляет множество интерфейсов, таких как Ethernet, USB, RS232/485 и CAN. Это позволяет использовать ее для создания широкого спектра систем управления и мониторинга. Она также имеет функциональные возможности, необходимые для систем безопасности, такие как отслеживание ошибок, контроль доступа, мониторинг безопасности и регистрация событий, и имеет сертификацию от независимого органа. Важным аспектом, определяющим соответствие платы требованиям ГОСТ Р МЭК 61508-2-2007, является наличие сертификации. Данная плата имеет сертификацию от независимого органа TÜV Rheinland, который выполняет оценку соответствия уровню безопасности 3. Это подтверждает, что плата соответствует требованиям безопасности, установленным данным стандартом [13], [14].

2.1.2 Выбор дисплея

Далее для проекции вывода информации необходим дисплей. Так как с помощью дисплея можно получить информацию о фиксации аварийного события, режиме работы схемы и считывания незарегистрированной в памяти RFID карты и т.д. В качестве дисплея выбран дисплей LCD-1602, показан на рисунке 2.2.

Рисунок 2.2 – Дисплей LCD-1602

Данный дисплей имеет 4-битный или 8-битный режим работы, напряжение питания составляет 5В, имеет сертификацию FCC (Federal Communication Commission), условиями эксплуатации являются способность работать при температуре в диапазоне от минус двадцати, до семидесяти, имеет определенную степень защиты и вибрации, уровень стойкости к влажности является 80 процентов, и имеет стойкость к электромагнитным помехам, что соответствует необходимому стандарту для эксплуатации [14], [15].

2.1.3 Выбор датчика возгорания

В случае возникновения возгорания для построения системы безопасности нужен датчик огня. В соответствии со стандартом функциональной безопасности был выбран датчик KY-026 на рисунке 2.3. Этот датчик считывает открытый огонь с помощью реагирования на электромагнитных волнах в области инфракрасного излучения. Рабочее напряжение питания составляет 3,3-5 В, а ток потребления 10мА, максимальная дистанция на которую реагирует датчик составляет 4м. Данный датчик KY-026, реагирующий на пламя состоит из инфракрасного диода, двух компаратора-LM393, и потенциометра. Он реагирует на инфракрасное излучение длинами волн от 760 до 1100 нанометров. Имеет необходимую сертификацию удовлетворяющая требованиям системы безопасности, и имеет простое подключение к плате Arduino. Сам порог срабатывания

температуры датчика регулируется потенциометром. Недостатком является то, что датчик может случайно сработать на сильно яркий солнечный свет, в таком случае можно исправить с помощью регулировки чувствительности датчика [14], [16].

Рисунок 2.3 – Датчик пламени KY-026

2.1.4 Выбор датчика газа

В случае утечки газа, нужно выбрать соответствующий датчик реагирования. По стандарту, соответствующие требования функциональной безопасности был выбран модуль MQ-2 на рисунке 2.4, который состоит из полупроводникового газоанализатора, имеющую конструкцию из трубки из керамики, покрытая чувствительным материалом из диоксида олова. Внутри этой трубки есть специальный нагревательный материал, который реагирует на концентрацию молекулы газа, и с помощью аналогового сигнала датчик отслеживает ее на выходе напряжение, если выходное напряжение становится высоким, это означает большую концентрацию газа. Он имеет сертификацию соответствующий требованиям функциональной безопасности. При использовании датчика MQ-2 система безопасности может быстро обнаружить утечку и предупредить людей в помещении, а также вызвать аварийную службу. Другим применением датчика может быть его использование для обнаружения газов, которые могут возникнуть в результате пожара. Датчик может обнаруживать такие газы, как дым, угарный газ и другие опасные вещества, которые могут быть выделяться в результате горения. При обнаружении таких газов система безопасности может автоматически активировать систему пожарной сигнализации, вызвать службу пожаротушения и предупредить людей в помещении. Рабочее ее напряжение составляет 3-5 В, а ток потребления 160 мА. Недостатком этого датчика является ложные срабатывания из-за перегрева оборудования [14], [16 с.358].

Рисунок 2.4 – Датчик газа MQ-2

2.1.5 Выбор датчика, определяющий жидкости

В случае протечки воды был выбран датчик FC-37 на рисунке 2.5. Он измеряет влажность почвы в диапазоне от 0 до 100 процентов, имеет напряжение питания от 3,3 до 5 В, и имеет низкое энергопотребление. Конструкция датчика FC-37 состоит из двух электродов, которые размещены внутри пластмассового корпуса. Один из электродов находится на поверхности корпуса, а другой - внутри корпуса. Эти два электрода образуют конденсатор, который изменяет свою емкость в зависимости от влажности почвы. Контактная область датчика состоит из двух токопроводящих дорожек, которые не связаны друг с другом, в случае попадания воды одновременно на две дорожки, вода замыкает их, и датчик реагирует на это. Все функциональные параметры датчика удовлетворяют требованиям функциональной безопасности при эксплуатации данного датчика [14],[16 с.397].

Рисунок 2.5 – Датчик воды FC-37

2.1.6 Выбор магнитного датчика

В случае открытия входной двери и для ее фиксации выбран датчик KY-025, который показан на рисунке 2.6. Данный датчик содержит в своей конструкции геркон, электромеханический коммутационный компонент. Он работает с напряжением от 3,3 до 5 В, поддерживает подключение до 10 А нагрузки с помощью встроенного реле. Это электронное устройство, используемое в системах безопасности, которое может обнаруживать магнитные поля и помогает в преодолении рисков и проблем, связанных с их наличием. Одно из применений датчика KY-025 – это его использование в системе безопасности для обнаружения движения и распознавания приближения металлических предметов к защищаемой зоне. Этот датчик работает на основе принципа магнитоиндукции, который позволяет обнаруживать изменения магнитного поля вблизи датчика, вызванные движущимися металлическими предметами. Датчик KY-025 также может использоваться для обнаружения наличия и отсутствия магнитного поля. Например, он может использоваться для обнаружения открытия и закрытия дверей или окон в помещении. При открытии двери или окна изменяется магнитное поле, которое может быть обнаружено датчиком KY-025, что позволяет системе безопасности быстро реагировать на подобные изменения. Параметры данного датчика удовлетворяют требованиям безопасности.

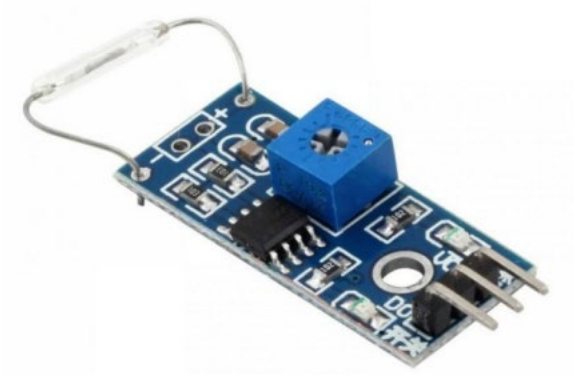

Рисунок 2.6 – Магнитный датчик KY-025

Конструкция датчика KY-025 состоит из двух частей: магнита и датчика Холла. Магнит представляет собой постоянный магнит, который создает постоянное магнитное поле вблизи датчика [14], [16 с.533].

2.1.7 Выбор инфракрасного датчика движения

Для контроля несанкционированного проникновение нужен датчик движения. И для этого был выбран PIR-датчика (инфракрасный датчик движения), а именно модуль HC-SR501 на рисунке 2.7, который легко соединяются с платформой Arduino. Он используется для обнаружения движения в заданном

диапазоне и является простым в использовании благодаря своей простой конструкции. Внешний вид датчика движения HC-SR501 включает в себя плату с микросхемами и устройствами, а также модуль инфракрасных датчиков. Эти датчики используются для обнаружения теплового излучения от живых существ или других источников тепла, что позволяет датчику определить наличие движения. Все функциональные параметра датчика удовлетворяют стандарту функциональной безопасности.

Рисунок 2.7 – Инфракрасный датчик движения HC-SR501

Данный инфракрасный датчик имеет угол обзор 120 градусов, напряжение питания от 4,5 до 20 В, обнаруживает движение в радиусе 7 метров, время задержки и чувствительность настраивается. Он удовлетворяет стандартам функциональной безопасности [14], [16 с.458].

2.1.8 Расширение

Чтобы подключить все собранные компоненты и датчики и для сборки микроконтроллера, стоит выбрать самое удобное подключение, для этого нужен плата расширения, в данном случае выбран расширитель Sensor shield. Он действительно позволяет подключить модулей, датчиков и других элементов электроники без пайки к контроллеру [13 с.195]. Расширитель показан на рисунке 2.8.

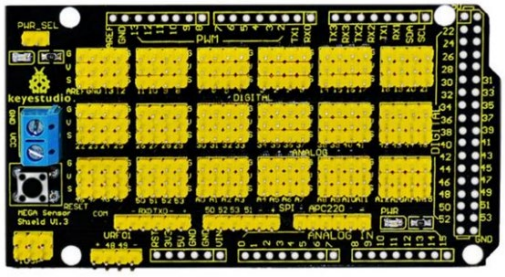

Рисунок 2.8 – Расширитель Sensor Shield Arduino

2.1.9 Выбор видеокамеры

Для отслеживания действии на объекте нужны компоненты, которые могут записывать видео и фотографии, для этого используют видеокамеру. В соответствии с необходимым стандартом удовлетворяющие требования функциональной безопасности электронных систем был выбран модуль Wyze Cam v3 на рисунке 2.9. Данная камера имеет разрешение видео до 1080p Full HD, угол обзора 130 градусов, инфракрасную подсветку для ночной съемки до 7,5 метров, карту памяти до 32 ГБ, рабочую температуру от минус 20 до 50 градусов по Цельсию, а также имеет поддержку с соединением Wi-Fi [13 с.201], [14].

Рисунок 2.9 – Камера Wyze Cam v3

2.1.10 Выбор компонента для контроля доступом

Для контроля доступом выбран модуль RC522 на рисунке 2.10, который состоит в своей конструкции RFID считывающее устройство, RFID-метки и RFID-карты для считывания и записывания данных. Модуль RC522 работает на частоте 13,56 МГц, имеет дальность считывания карты до 3 см, скорость передачи данных до 10 Мбит/с, работает от напряжения 3,3 В. Все его параметры удовлетворяют по необходимому данному стандарту требованиям функциональной безопасности систем.

Он состоит из антенны, усилителя, декодера, контроллера и других компонентов, которые обеспечивают надежную и быструю работу устройства. Один из главных преимуществ, его способность обрабатывать большое количество информации и быстро определять идентификаторы карт. Это позволяет использовать его в системах безопасности, которые требуют быстрого и точного распознавания пользователей. Кроме того, модуль RC522 может быть легко интегрирован в различные системы безопасности, такие как системы контроля доступа к помещениям, автоматические ворота и двери, системы учета рабочего времени и т.д. [13, с.398], [14].

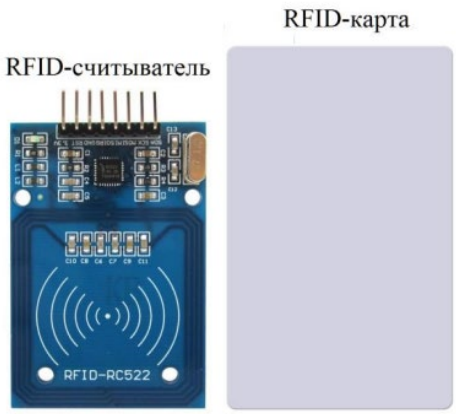

Рисунок 2.10 – Модуль контроля доступа RFID – система

2.1.11 Выбор компонента для исполнительного механизма

Для управления различными исполнительными механизмами и их подключения к Arduino нужны коммутирующие компоненты. В данном случае выбрана модуль четырехканального реле на рисунке 2.11. Оно имеет 4 независимых канала управления, рабочее напряжение от 5 В, максимальный ток коммутации до 10 А, коммутационную мощность до 2500 Вт, и имеет механическую жизнь до 10000000 циклов коммутации. Оно может быть использовано для управления четырьмя электрическими цепями, например, для управления четырьмя лампами или для управления двигателями. Оно подключается к плате Arduino через GPIO-пины, которые используются для управления реле [13 с.101].

Рисунок 2.11 – Четырех канальное реле

2.1.12 Выбор компонента для управления доступом в сети

Для дистанционного управления системой в случае срабатывания датчиков был выбран модуль Bluetooth HC-05 на рисунке 2.12. Он имеет дальность передачи до 10 метров, рабочую частоту 2,4 ГГц, максимальную скорость передачи данных до 2,1 Мбит/с и рабочее напряжение 3,3 В. Недостатком является малое расстояние обеспечения безопасности, Bluetooth в отличие от Интернет или GSM-связи не может передавать данные на большие расстояния. Но выбор пал именно на эту модуль из-за эффективную защищенность передаваемых данных, при этом ограниченность радиус действия работает также и в пользу, а также низкое потребление питания. Данный Bluetooth HC-05 осуществляет обмен данных с платой Arduino с помощью двух вывод TX, RX по универсальному асинхронному приемопередатчику интерфейса UART [14], [16 с.113].

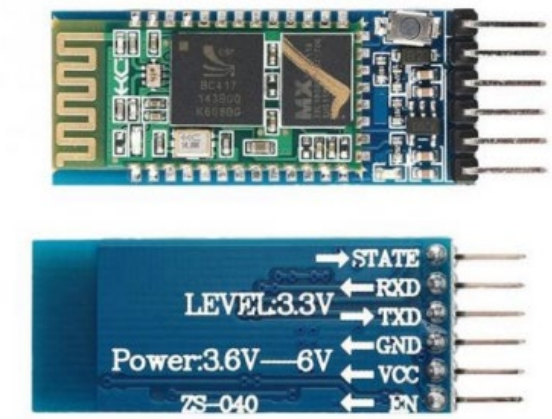

Рисунок 2.12 – Модуль Bluetooth HC-05

2.1.13 Выбор космических датчиков

Из космических приборов будут выбраны такие датчики, как датчики радиации, они должны обнаружить утечки радиоактивных веществ в лаборатории, которые могут быть опасными для людей и окружающей среды. Также некоторые космические датчики, которые могут помочь отслеживать условия хранения ценных электронных приборов и химических веществ в лаборатории, что может предотвратить их повреждение и порчу, они также соответствуютт со стандартом требующие фунциональную безопасность электронных систем.

Датичк Geiger-Muller.

Для измерения потока заряженных частиц нужен датчик Geiger-Muller, в данном случае выбран модуль SEN-10724 от компании Sparkfun. Данный модуль имеет диапазон измерения от 0 до 1 мСв/ч, частоту обновления 5 Гц, питание 5 В. Данный датчик обладает высокой чувствительностью к гамме и рентгеновским излучателям, а также заряженным частицам. На риснуке 2.13 показана конструкция датчика Geiger-Muller.

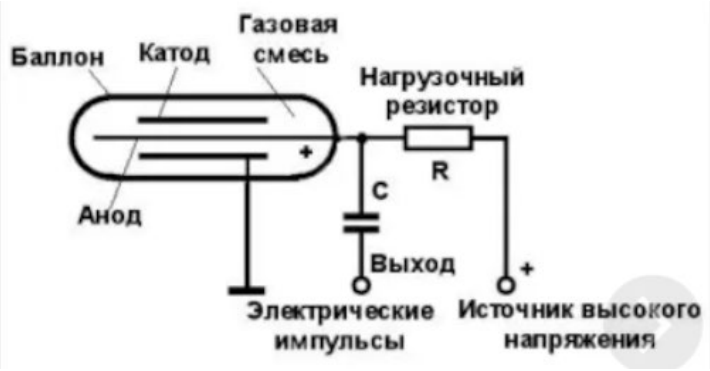

Рисунок 2.13 - Конструкция счетчика Гейгера-Мюллера

Датчик Гейгер-Мюллер так же широко применяется для измерения радиоактивности, контроля уровня радиации и обнаружения радиоактивных материалов в различных областях включая научные исследования, медицину, промышленность и ядерную энергетику. Они обычно используются для обнаружения гамма-излучения.

Датчик контроля радиации.

В качестве компонента для контроля радиации и солнечной активности в помещении можно выбрать датчик солнечной радиации. По необходимому стандарту был выбран модуль GY-302 на рисунке 2.14, который предназначен для измерения интенсивности солнечного излучения в спектральном диапазоне от 300 до 1100 нм. Имеет диапазон измерения от 300 до 1100 нм, чувствительность от 4 до 5 В/люкс, напряжение питания 3,3-5 В, и аналоговый интерфейс.

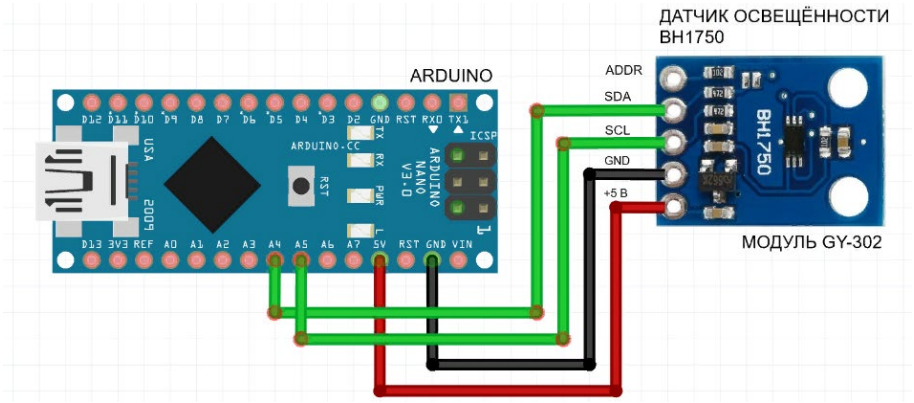

Рисунок 2.14 - Модуль GY-302 подключенный к плате Arduino

Датчик для мониторинга температуры и влажности.

Для использования мониторинга условий в лаборатории нужен датчик температуры и влажности. В данном случае был выбран модуль DHT22 на рисунке 2.15. Данный датчик может измерять температуру от минус 40 до 80 градусов Цельсия и относительную влажность в диапазоне от 0 до 100 процентов, также он использует протокол однопроводной передачи данных, что позволяет подключить несколько датчиков к одному контроллеру. Данные выдаются в

формате цифровых сигналов, что делает датчик более устойчивым к помехам и шумам.

Рисунок 2.15 – Датчик температуры и влажности - модуль DHT22

В данном разделе были перечислены только основные необходимые компоненты для проекции систем безопасности объекта. В качестве дополнительных исполняющих механизмов для проекции эффективной системы безопасности нужны устройства, такие как USB кабели, блок питания, резисторы, конденсаторы, светодиоды и т.п. А также в случае утечки газа вентилятор, который необходим для отсеивания в помещении различных видов газа [14], [17].

Таким образом все перечисленные космические электронные датчики необходимы для обеспечения безопасности объекта. Например, датчики радиации, такие как Geiger-Muller, могут предупредить о возможных утечках радиоактивных материалов, а датчики солнечной радиации помогут контролировать уровень излучения и обеспечить защиту электронных приборов от сильных солнечных вспышек. В целом комбинация космических и обычных электронных компонентов позволяет создать более надежную систему безопасности, способную обнаруживать и предотвращать различные угрозы. Так же эти датчики были выбраны на основе методов построения систем безопасности на базе электронных компонентов.

Самой крупной компанией в Казахстане работающей по внедрению системы безопасности для объекта защиты, а также интеграций беспроводной системы является Litehouse kz, которая работает уже на протяжении шести лет, так же все электронные оборудования, которые они предоставляют для интеграции являются сертифицированными в соответствии со стандартами Республики Казахстан.

3 Исследовательская часть

3.1 Тенденции развития электронных компонентов

После выбора необходимых компонентов для внедрения системы безопасности в помещение, можно рассмотреть тенденции их развития, а также эти тенденции могут применяться для электронных компонентов в целом. В данном разделе будут рассмотрены тенденции развития электронных компонентов системы безопасности, исследования тенденции в развитии, а также необходимые анализы в области одних из тенденций. Основные тенденции развития электронных компонентов показаны на рисунке 3.1.

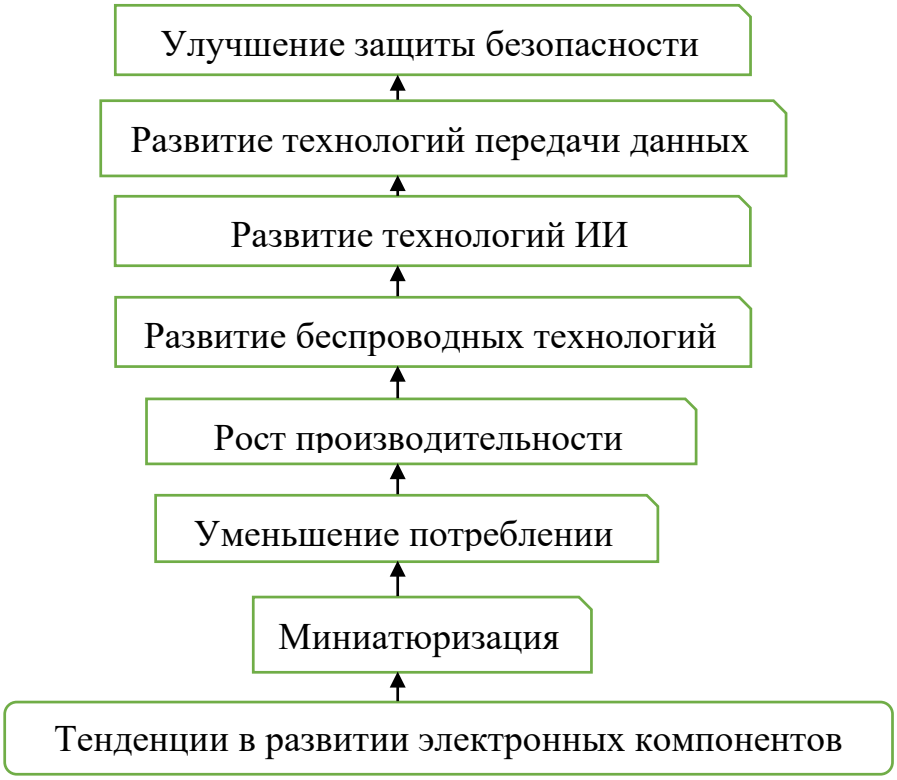

Рисунок 3.1 – Основные тенденции в развитии электронных компонентов

3.1.1 Миниатюризация и уменьшение потребления энергии

Миниатюризация компонентов в электронике приводит к значительному уменьшению размера и веса устройств, а также к повышению эффективности энергии работы электронных компонентов, именно поэтому она является очень важной тенденцией в развитие электронных компонентов в данный момент. Одним из примеров занимающиеся подобными исследованиями является компания Intel, эта компания в 2020 году рассматривала тренды продолжительности уменьшении размеров электронных компонентов, особенно в области микропроцессора и микроконтроллера. Например, сейчас современные микро-

контроллеры имеют размеры всего несколько миллиметров и потребляют несколько микроватт энергии во время работы в режиме ожидания. Примерами уже добившихся успехов в этой области являются микропроцессоры Intel Atom и ARM Cortex-A7, имеющие размеры всего 14 и 12 мм соответственно. Если говорить о конкретных примерах дальнейших исследований и разработок компонентов электроники, которые нацелены на дальнейшую миниатюризацию и уменьшение потребления энергии, то сейчас такие компании, как IBM, Google, Intel, Microsoft ведут исследования в разработке квантовых компьютеров, которые имеют более высокую плотность информации и работают над потреблением меньше энергии, чем классические биты. Но на данный момент квантовые компьютеры находятся в стадии разработки [9].

И так следующими примерами данной тенденции являются:

- квантовые точки - нано-частицы, которые используются в качестве полупроводников, они имеют потенциал для создания более эффективных, надежных и компактных компонентов, например, для структуры солнечных батарей и светодиод;

- интернет вещей – IoT (Internet of Things) - сеть объектов, которые обмениваются данными между собой и электронными устройствами автоматически, без участия человека. Устройства IoT интернет вещей имеют требования низкого энергопотребления и маленького размера, именно поэтому многие компании работают над разработкой новых компонентов в этой области и технологий для создания более компактных и с более эффективными энергиями устройств [16].

Опираясь из последних данных отчетам исследований компании Intel, можно подчеркнуть частое упоминание тенденции развития уменьшений размеров транзисторов и миниатюризации электроники в целом. Например, в отчете о состоянии технологий производящих данной компании 2019 года, Intel отмечает, что они достигли производства транзисторов размером 10 нм и собираются планировать перехождение к 7-нм технологии, а согласно отчета 2020 года компания продолжает работу по миниатюризации своих чипов и дальнейшим планированием является начать выпускать продукцию на 7-нм и т.д. По данным отчета 2019 года о состоянии технологий, производящие данной компании является также переход от 14-нм технологии к 10-нм технологии, что привел к увеличению плотности транзисторов на чипе на 2,7 раза и снижению энергопотребления на 30 процентов при одинаковой производительности. Переход от 10-нм технологии к 7-нм технологии должен был привести к дополнительному увеличению плотности транзисторов и снижению энергопотребления на 25-30 процентов по сравнению с 10-нм компонентами [18]. Исходя из этого можно сделать анализ уменьшение транзистора и его энергопотребления с каждым годом. Данный анализ показан на рисунке 3.2.

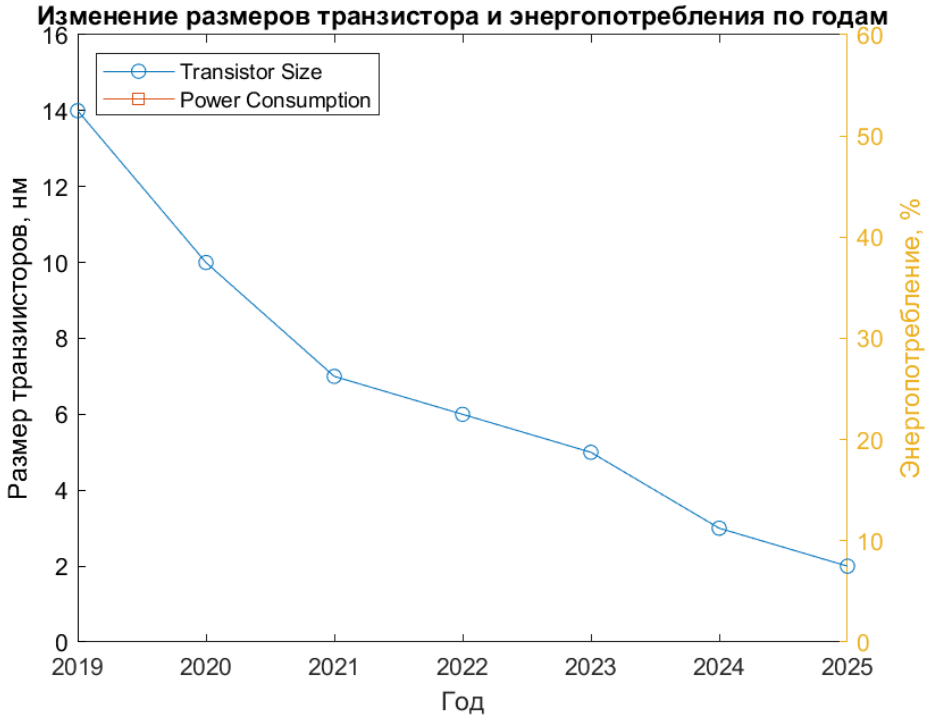

Рисунок 3.2 – График изменения размеров транзистора и энергопотребления начиная с 2019 года

3.1.1.2 Анализ сравнения ПК с квантовыми компьютерами в соответствии с миниатюризацией и уменьшении потребления энергии

Здесь необходимо дать приблизительную оценку и расчет энергопотребления микроконтроллера и квантового компьютера при выполнении работы с одним и тем же объемом данных.

Для персонального компьютера были взяты параметры из модели Alienware Aurora R10, которая является одним из мощнейших компьютеров в настоящее время:

- максимальная мощность блока питания P – 1000 Вт;
- напряжение питания процессора V – 1,35 В;
- тактовая частота процессора – 4,9 ГГц;
- время выполнения задачи t – 0,001 (сортировка массива из 1000 элементов).

Параметры квантового компьютера:

- напряжение питания квантового компьютера V - 10 В;
- сила тока, потребляемая квантовым компьютером I - 5 А;
- время выполнения задачи t - 0,01 с (сортировка массива из 1000 элементов) [19].

Для расчета энергопотребления использовалась следующие формулы:

$$E = P \times t, \tag{3.1}$$

$$E = V \times I \times t, \quad (3.2)$$

где E – потребленная энергия, Дж;
P – мощность потребления, Вт;
I – сила тока, А;
t – время работы, с.
Расчет энергопотребления персонального компьютера (3.1):

$$E = P \times t = 1000\text{Вт} \times 0{,}001\text{с} = 1\ \text{Дж}$$

Расчет энергопотребления квантового компьютера (3.2):

$$E = V \times I \times t = 10\text{В} \times 5\text{А} \times 0{,}01\text{с} = 0{,}5\text{Дж}$$

Исходя из расчёта, можно сделать вывод, что самый мощный персональный компьютер потребляет в два раза больше энергии, чем квантовый компьютер при выполнении задачи сортировки одинакового массива. Притом, что квантовый компьютер использует более сложные алгоритмы. А также размер квантового компьютера на порядок меньше. Следовательно, можно сделать вывод, что квантовые компьютеры полностью удовлетворяют тенденцию миниатюризации и уменьшение потребления энергии.

3.1.2 Рост производительности

Рост производительности электронных компонентов, и наличие способности улучшение качеств и жизненного цикла некоторых из них, например, микропроцессоров и микроконтроллеров высокой вычислительной мощности и их способности обрабатывать большие объемы данных позволяет создавать более сложные, функциональные и надежные системы управления, контроля и мониторинга. В настоящее время существует множество примеров тенденции роста производительности электронных компонентов. Некоторые из наиболее ярких примеров включают в себя графические процессоры (GPU), обладающие более чем в 10 раз большей производительностью, в отличии от тех, что были доступны 10 лет назад, SSD-накопители - Solid State Drive (SSD), которые сейчас имеют до 16 терабайт памяти, что в несколько раз больше, чем было возможно несколько лет назад, мобильные процессоры, которые используются в смартфонах и планшетах, оперативная память (RAM), являющийся ключевым компонентом для работы современных компьютеров и устройств, квантовые компьютеры, которые обладают способностью обрабатывать огромные объемы данных и решать сложные задачи в несколько раз быстрее современных компьютеров [20].

На рисунке 3.3 показан рост производительности качества SSD накопителей с течением времени.

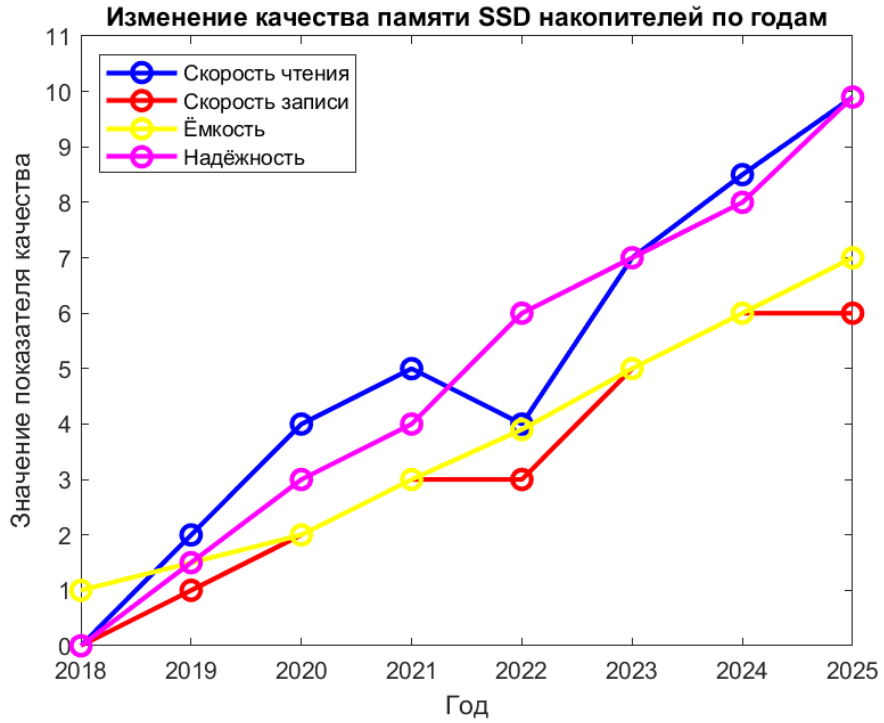

Рисунок 3.3 – График роста производительности на примере улучшения качества SSD накопителей с течением времени

3.1.3 Развитие беспроводных технологий

Из-за того, что беспроводные модули и сенсоры позволяют создавать более гибкие и масштабируемые системы управления, контроля и мониторинга, развитие тенденции беспроводных технологий является еще одним важным направлением в системе безопасности. С помощью беспроводных технологий и систем можно создавать датчики, которые могут передавать данные на расстояние нескольких километров без необходимости проводной связи.

Настоящими примерами, являются:

- Wi-Fi 6, который может обеспечивать высокую скорость передачи данных и лучшую производительность в загруженных сетях, а также данная связь использует технологию MIMO (Multiple-Input Multiple-Output), позволяющая передавать данные одновременно на нескольких частотах и уменьшающая пересечение сигналов между устройствами;

- 5G, являющийся новым стандартом мобильной связи, который предоставляет более высокую скорость передачи данных и лучшую производительность в загруженных сетях, и данная связь обеспечивает меньшую задержку и большую емкость сети, что позволяет более эффективно использовать мобильные устройства;

- Bluetooth 5, обеспечивающий более дальнюю дальность действия и более высокую скорость передачи данных, также Bluetooth 5 имеет меньшее потребление энергии, в отличии от других беспроводных связь, что позволяет батареям устройств работать дольше;

- NFC, в основном использующийся для считывания информации с устройств и обмена данными между устройствами, одним из преимуществ является, что NFC используется для бесконтактной оплаты и доступа в здания;

- Интернет вещей (IoT), позволяющий устройствам обмениваться данными между собой через Интернет.

Каждая из данных связи имеют свои преимущества и характеристики, и для выбора при использовании в системе безопасности стоит рассмотреть требования к данным связям, чтобы понять какая из них будет наиболее эффективной.

3.1.3.1 Расчет уровня эффективности беспроводных технологий

Для расчета уровня эффективности беспроводных технологий, необходимо определить параметры и метрики для использования оценки каждой из данных технологии. Этими параметрами являются максимальная скорость передачи данных в Мбит/с, пропускная способность в Мбит/с, задержка в мс, дальность передачи в метрах. Значения всех этих параметров данных технологий предоставлены в таблице 3.1.

Таблица 3.1 – Значение и данные параметров беспроводных технологий

Технология	Максимальная скорость передачи данных (Мбит/с)	Пропускная способность (Мбит/с)	Задержка (мс)	Дальность передачи (м)
Wi-fi 6	9.6 Гбит/с	3.5 Гбит/с	2.3	38
5G	20 Гбит/с	10 Гбит/с	1	1000
Bluetooth 5	2 Мбит/с	1 Мбит/с	10	10
NFC	0.424 Мбит/с	0.106 Мбит/с	1	0.1

Далее, для оценки уровня эффективности каждой из данных технологии, необходимо создать векторы со значениями параметров и определить метрики для каждой технологии. В качестве метрики будет использоваться гармоническое среднее от значений параметров, которое будет показателем эффективности технологий. Расчет сделан в программе Matlab, и предоставлен ниже на рисунке 3.4

```
Command Window
>> % Создаем векторы с параметрами каждой технологии
>> wifi_params = [9600 3500 2.3 38];
>> nr_params = [20000 10000 1 1000];
>> bt_params = [2 1 10 10];
>> nfc_params = [0.424 0.106 1 0.1];
>> % Создаем матрицу с параметрами каждой технологии
>> params = [wifi_params; nr_params; bt_params; nfc_params];
>> % Вычисляем гармоническое среднее для каждой технологии
>> harmonic_mean = harmmean(params, 2);
>> % Создаем вектор с именами технологий
>> names = {'Wi-Fi 6', '5G', 'Bluetooth 5', 'NFC'};
>> % Выводим результаты
>> disp(table(names', harmonic_mean, 'VariableNames', {'Technology', 'Efficiency'}));
    Technology       Efficiency
    _____________    __________

    {'Wi-Fi 6'    }      8.6676
    {'5G'         }      3.9954
    {'Bluetooth 5'}      2.3529
    {'NFC'        }      0.1755
```

Рисунок 3.4 – Расчет уровня эффективности беспроводных технологий

Из таблицы, которую нам вывела программа Matlab видно, что наиболее эффективной технологией является wi-fi 6 с наивысшим уровнем эффективности 8.6676. Технология 5G также показала хорошие результаты с уровнем эффективности 3.9954. Bluetooth и NFC имеют более низкие уровни эффективонсти соотвественно.

Далее можно подсчитать сколько процентов эффективности занимают каждая данная технология. Эти данные показаны на рисунке 3.5.

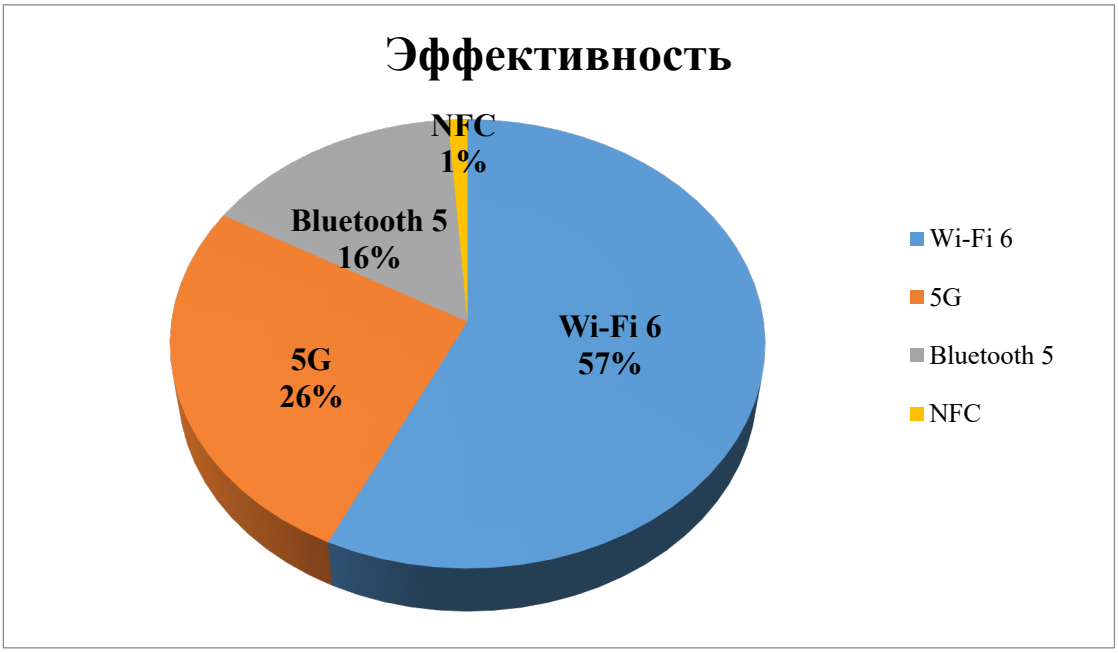

Рисунок 3.5 – Процент эффективности беспроводных технологий.

3.1.4 Развитие технологий искусственного интеллекта

Данная тенденция является основой в будущем для построения новых и эффективнейших систем безопасности. С развитием электронных компонентов технологий искусственного интеллекта начинают свое активное использование в создании новых и надежных систем управления, контроля и мониторинга, которые умеют обучаться и адаптироваться к изменяющимся условиям. Например, системы искусственного зрения могут иметь использование для мониторинга и анализа видеопотока с камер безопасности, а системы машинного обучения для анализа данных с датчиков, а также определения нештатных ситуаций.

Самые основные тенденции развития искусственного интеллекта показана на рисунке 3.6

Глубокое обучение | Машинное обучение | Роботехника | Генеративные модели

Рисунок 3.6 – Тенденции развития ИИ

В настоящее время существуют множество тенденций в развитии искусственного интеллекта, над которыми работают ответственные в развития ИИ компании и работники, и эти тенденций будут производиться в ближайшем будущем. Некоторые из наиболее ярких примеров включают в себя:

- глубокое обучение, технология, которая использует нейронные сети для анализа больших объемов данных и автоматического извлечения полезных признаков из этих данных. Данная тенденция ИИ уже используется в различных областях, такие как компьютерное зрение, обработку естественного языка и рекомендательные системы;

- машинное обучение, область искусственного интеллекта, занимающийся разработкой алгоритмов, позволяющих компьютерам обучаться на основе данных и делать предсказания на новых данных. Машинное обучение уже используется в различных областях, такие как анализ данных, распознавание образов и рекомендательные системы;

- робототехника, область, которая занимается разработкой роботов, выполняющие различные задачи, так как роботы могут использоваться в различных областях, такие как производство, медицину и автономную навигацию, и в системах безопасности;

- генеративные модели, технология, использующий искусственный интеллект для генерации новых данных, таких как изображения, музыка и текст.

Генеративные модели уже используются в различных областях, например, в графических дизайнах, музыке и играх, а также они могут быть полезными и для систем безопасности.

3.1.5 Улучшение защиты и безопасности

Так как современные системы управления, контроля и мониторинга должны обеспечивать высокий уровень защиты и безопасности. В связи с этим, разработчики электронных компонентов в данный момент уделяют все большее внимание вопросам безопасности и созданию компонентов, способные предотвратить несанкционированный доступ и утечку данных. Основные тенденции в развитии электронных компонентов СБ показана на рисунке 3.7.

Рисунок 3.7 – Тенденции развития электронных компонентов СБ

В настоящее время существуют несколько тенденций в развитии электронных компонентов для систем безопасности, особенно в предотвращении несанкционированного доступа. Основными тенденциями в данной области являются:

- биометрическая аутентификация, технология, которая использует физические или поведенческие характеристики человека, например, отпечатки пальцев, лица, радужной оболочки глаза и голоса, для идентификации и аутентификации пользователей. Биометрическая аутентификация показана на рисунке 3.8, она используется в различных системах безопасности, такие как замки, устройства для контроля доступа и мобильные устройства;

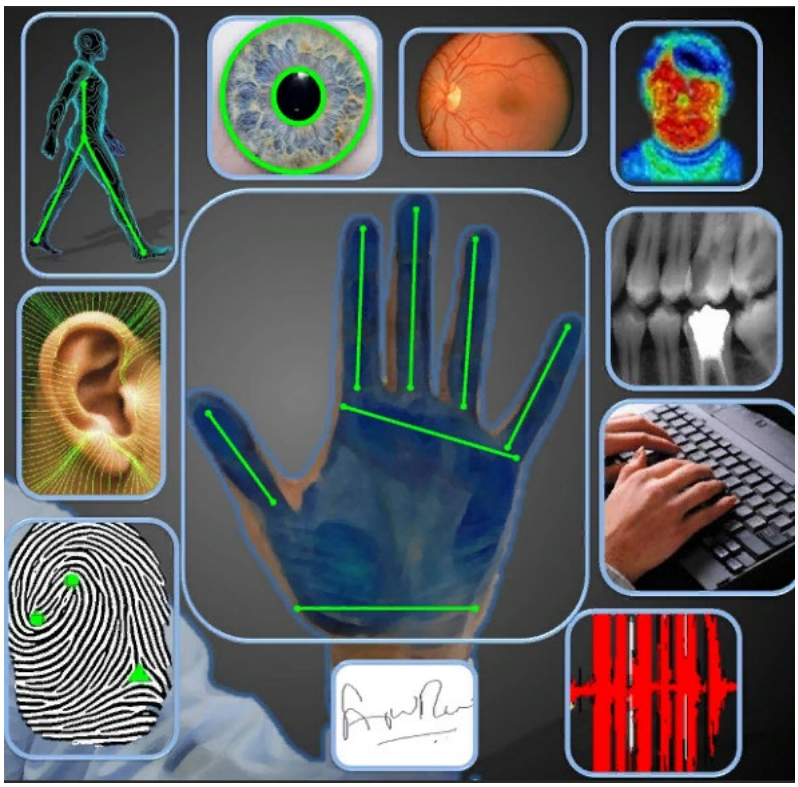

Рисунок 3.8 – Биометрическая аутентификация

- криптографические ключи, технология, которая использует криптографические ключи для шифрования и защиты данных. Криптографические ключи будут полезными для пользования в различных системах безопасности, включая системы контроля доступа и системы защиты данных.

Ярким примером криптографического ключа является AES-256 (Advanced Encryption Standard). Данный ключ используется только одним участником, который имеет доступ к ключу. Он состоит из 256 битов (32 байтов), генерируется с помощью криптографических алгоритмов; Алгоритм шифрование AES показана на рисунке 3.9.

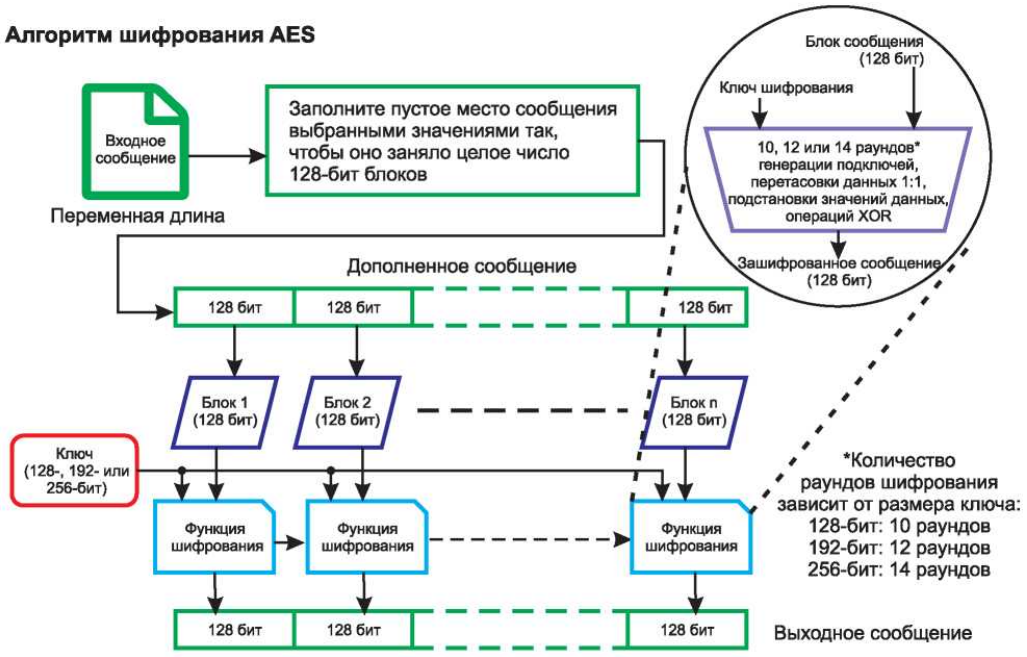

Рисунок 3.9 – Алгоритм шифрование AES

- системы контроля доступа, технология, которая используется для контроля доступа к зданиям, помещениям или компьютерным системам. Системы контроля доступа включают в себя биометрические устройства, RFID-метки, электронные замки и системы распознавания лиц;

- сетевые устройства безопасности, устройства, которые используются для защиты сетевых ресурсов и предотвращения несанкционированного доступа к ним. Сетевые устройства безопасности включают в себя брандмауэры, виртуальные частные сети (VPN) и устройства контроля доступа.

3.1.6 Развитие технологий передачи данных

При проектировании системы безопасности, важно отметить, что современные системы управления, контроля и мониторинга генерируют большие объемы данных, которые необходимы для передачи и анализа в режиме реального времени. Поэтому, в настоящее время разработчики электронных компонентов уделяют все большее внимание развитию технологий передачи данных. Например, современные чипы Bluetooth и Wi-Fi обеспечивают высокую скорость передачи данных, а также широкий диапазон действия.

Исходя из данной тенденции можно сделать анализ, что в будущем технологии передачи данных будут продолжать развиваться, и некоторые из возможных направлений являются:

- более высокие скорости передачи данных. Так как по мере увеличения объемов данных, передаваемых через сети, потребуется увеличивать скорость передачи данных, для обеспечения эффективности и удобства использования.

- более широкий доступ к сетям. Так как в будущем сети связи будут более доступными для людей по всему миру, это позволит им общаться и получать доступ к информации.

- более надежные и безопасные сети. Из-за того, что технологии будут развиваться, они должны обеспечить безопасность передачи данных и защитить их от кибератак и других угроз.

Исходя из вышеперечисленных факторов, можно сказать, что самыми важными для проекции системы безопасности являются тенденция улучшения защиты безопасности, так как именно новые и улучшенные системы безопасности строятся на этих четырех базах, как биометрическая аутентификация, криптографический ключ, система контроля доступа и развитие технологий передачи данных. Но проекция такой системы безопасности стоит очень дорого, в отличие от классической проекции системы безопасности охраны объекта, которая приведена в пример во второй части дипломной работы [18], [20].

Таким образом все эти тенденций являются самыми перспективными направлениями в развитии электронных компонентов в настоящий момент и для ближайшего будущего, так как они открывают новые возможности для создания более интеллектуальных и связанных между собой устройств и систем, а также продвигают направления новых технологий или постоянных улучшении уже имеющихся технологий. В настоящее время над исследованием тенденции электронных компонентов, а также их развитием работают многие компании, такие как Intel, Samsung, Qualcomm, NVIDIA, Apple и другие.

В ходе исследования в данном разделе были рассмотрены основные тенденции развития электронных компонентов, были проанализированы общие преимущества, эффективность, и недостатки каждой тенденции и технологии, а также возможности их применение в системах безопасности.

3.2 Расчет стоимости на внедрение системы безопасности технической системы для объекта защиты

В качестве примера дана двухкомнатная испытательная лаборатория на рисунке 3.10, в которой хранятся ценные электронные и космические приборы, для которой были выбраны необходимые электронные компоненты, в том числе и космические для проектирования системы безопасности (в подразделе 2.1). А ниже представлена таблица 3.2, где расписаны выбранные компоненты с расчетом стоимости. Необходимые количества компонентов для внедрения системы безопасности в двухкомнатной испытательной лаборатории были оценены настоящими инженерами, разрабатываемые проектирование систем безопасности для охраны объектов.

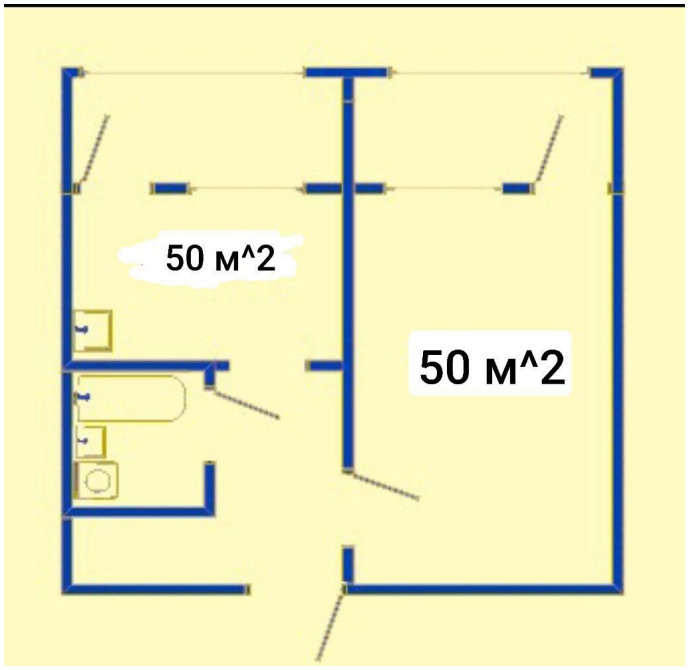

Рисунок 3.10 – Двухкомнатная испытательная лаборатория, имеющая общий размер сто квадратных метра

Расчет стоимости на внедрение системы безопасности технической системы для двухкомнатной лаборатории:

Таблица 3.2 – Исходные материалы и расчет стоимости

Наименование статьи расходов			**Размер затрат (тг)**
Материальные расходы			
Вид материальных расходов	Цена	Количество	
Расходные материалы			

Продолжение таблицы 3.2

Программно-аппаратные продукты:			
Arduino Mega 2560	29990	1	29990
Компоненты проектируемой системы			
USB-кабель	465	1	465
Блок питания	4500	1	4500
Блок бесперебойного питания	23000	1	23000
Breadboard	590	1	590
Резистор	500	5	2500
Конденсатор	100	4	400
Светодиод	300	6	1800
LCD-дисплей	600	1	1200
KY-026 датчик огня	275	1	275
MQ-2 датчик газа	1012	1	1012
FC-37 датчик протечки воды	500	1	500
KY-025	200	3	600
Четырехканальное реле	250	1	250
Bluetooth HC-05	3000	1	3000
RFID RC-522	1010	1	1010
Sensor shield	1175	1	1175
HC-SR501	630	1	630
Wyze Cam v3	25000	3	75000
Вентилятор	2100	1	2100
Электромагнитный клапан	3500	1	3500
Электромагнитная дверная задвижка	500	3	1500
Световое сигнальное устройство	6500	1	6500
Звуковая сигнализация	1500	1	1500
Датчик SEN-10724		1	24000
модуль GY-302		1	13000

Продолжение таблицы 3.2

модуль DHT22		1	29000
Итого	228997		

Из представленных данных следует, что для установки системы охранной безопасности в 2-х комнатной лаборатории необходимо установить определенные количество датчиков и других электронных компонентов для проекции системы, которые удовлетворяют требования хорошего качества охранной безопасности данного помещения. Общая стоимость компонентов может различаться в зависимости от рынка и места покупки, но приблизительно она будет составлять 228997 тенге.

Исходя из представленной информации, можно провести расчет энергопотребления системы охранной безопасности для двух комнат. Для этого нужно знать мощность каждого компонента и время работы этих компонентов. Даны: Arduino Mega 2560 – 5 Вт, USB - кабель - 2 Вт, блок питания 20 Вт, блок бесперебойного питания – 50 Вт, breadboard - 1 Вт, светодиоды – 0.1 Вт (на каждый), конденсатор – 0.1 Вт (на каждый), дисплей – 2 Вт, KY-026 датчик огня - 0.5 Вт, MQ-2 датчик газа – 0.5 Вт, FC-37 датчик протечки воды – 0.5 Вт, KY-025 датчик – 0.5 Вт, четырех канальное реле – 2 Вт, Bluetooth HC-05 – 0.2 Вт, RFID RC-522 – 0.5 Вт, Wyze Cam V3 – 5 Вт, вентилятор – 10 Вт, электромагнитный клапан – 2 Вт, световое сигнальное устройство – 2 Вт, звуковая сигнализация – 2 Вт, датчик SEN-10724 – 0.5 Вт, GY-302 – 0.5 Вт, DHT22 – 0.5 Вт.

Расчет средней мощности:

$$\text{средняя мощность} = \frac{(\text{сумма кол-во мощности всех компонентов})}{(\text{количество компонентов})} \quad (3.3)$$

Таким образом общая мощность составляет 6.1 Вт, а время работы в день 24 часа.

Расчет энергопотребления в час:

$$6.1\text{Вт} \times 24\text{часа} = 146.4\ \text{Втч} \quad (3.4)$$

Расчет энергопотребления в месяц (30 дней):

$$146.4\text{Втч} \times 30\text{дней} = 4392\ \text{Втч} \quad (3.5)$$

Расчет энергопотребления в год (365 дней):

$$46.4\text{Втс} \times 365\text{дней} = 53376\text{Втч} \quad (3.6)$$

Для обеспечения питания данной системы необходимо выбрать источник питания, который обеспечит потребляемую мощность. Один из вариантов – использование аккумулятора солнечной батареи, который обеспечивает постоянное питание. Для этого необходимо рассчитать емкость аккумулятора, исходя из потребляемой мощности, и определить стоимость его покупки и обслуживания. в данном случае выбрана модель Sunstone Power SP12-100, которая имеет емкость 100Ач и напряжение 12 В. Ее стоимость на местном рынке в Алматы составляет примерно 45 000 тенге.

Расчет стоимости электроэнергии за месяц.

Для расчета стоимости электроэнергии за месяц с использованием аккумулятора солнечной батареи нужно учитывать, что он заряжается от солнечной энергии в течение дня и выдает свою энергию в ночное время, когда нет солнечного света.

Рассчитаем потребление энергии в месяц.

Потребление энергии в месяц = 4392 Втч.

Так как используется аккумулятор солнечной батареи ёмкостью 100 Ач, то его емкость в Втч составляет:

$$\text{Емкость аккумулятора} = 100\text{Ач} \times 12\text{В} = 1200\text{Втч} \qquad (3.7)$$

Это значит, что аккумулятор может выдавать 1200 Втч энергии в течение одного заряда.

Чтобы рассчитать количество зарядок, которые необходимы в месяц, чтобы удовлетворить потребление энергии, нужно разделить потребление на емкость аккумулятора:

$$\text{Кол} - \text{во зарядок в месяц} = \frac{\text{Потребление}}{\text{Емкость аккумулятора}} = \frac{4392\text{Втч}}{1200\text{Втч}} = 3.66. \qquad (3.8)$$

Так как аккумулятор может работать на солнце около 5 часов, то каждый день он может зарядиться примерно на 600 Втч (1200 Втч / 2). Это значит, что для обеспечения потребления энергии в месяц нужно производить около 6 зарядок аккумулятора.

Теперь рассчитаем стоимость электроэнергии в месяц, по данным информационного портала «ЭнергоТариф» на май 2023 года стоимость электроэнергии для населения в Алматы составляет 24,54 тенге за кВт·ч [21]

Тогда:

$$\text{Стоимость электроэнергии в месяц} = \frac{(\frac{25\text{тенге}}{\text{кВтч}} \times 4392)}{1000} = 109.8 \text{ тенге}. \qquad (3.9)$$

Таким образом, исходя из этих данных выше, если источник питания проектируемой системы будет заряжаться на аккумуляторе солнечных батарей, то можно значительно сэкономить и уменьшить стоимость электроэнергии.

Стоимость на внедрение системы безопасности данной технической системы для объекта защиты составляет 228997 тенге, тогда вместе с солнечным аккумулятором будет составлять 273997 тенге. В данном расчете не учитывается стоимость обслуживания на внедрение системы безопасности, а учитываются только стоимости электронных компонентов для интеграции системы безопасности для объекта защиты, а также электроэнергии.

ЗАКЛЮЧЕНИЕ

Исходя из обзора электронных компонентов и компонентов космической электроники систем безопасности, а также методов построения систем безопасности на базе электронных компонентов для технических систем, можно сделать вывод, что значимость электронных компонентов в области безопасности является очень важным и стоящим данного исследования.

В данной работе были рассмотрены конкретные электронные приборы и некоторые из космических приборов, которые могут использоваться для системы безопасности, также были выявлены тенденции развития электронных компонентов, применяемые для систем безопасности в будущем.

Кроме того, в данный работе был проведен расчет стоимости электронных компонентов, проектируемой технической системы, для примерной ориентации вклада бюджета электронных и космическо-электронных оборудований для проекции подобных технических систем.

Таким образом, исследование тенденции развития электронных компонентов системы безопасности позволило получить ценные знания об улучшений качеств электронных компонентов и их применение в области безопасности, а также возможность сделать вывод об их использования в будущем.

Это исследование имеет большое значение также для различных отраслей промышленности, где безопасность является первостепенной задачей. Результаты этого исследования могут быть использованы для разработки новых систем безопасности на базе электронных компонентов и повышения качества существующих систем. В целом, данное исследование тенденции развития электронных компонентов систем безопасности доказало, о важности занимаемой роли электронных компонентов в обеспечении безопасности объектов в будущем.

На основе проведенного исследования можно дать следующие рекомендации:

- при выборе электронных компонентов для систем безопасности необходимо учитывать, требования к параметрам электронных компонентов, особенности объекта защиты и требования к системе безопасности;
- следует тщательно исследовать новейшие разработки и инновации в области электронных компонентов, для использования их в создании более эффективных и надежных систем безопасности;
- необходимо уделять нужное внимание обучению и подготовке специалистов, работающих с электронными компонентами в системах безопасности;
- регулярно проводить тестирование и проверку систем электронных компонентов, чтобы убедиться в их работоспособности и эффективности в условиях реальной эксплуатации.

Все вышеперечисленные меры помогут создать более эффективные и надежные системы безопасности на основе электронных компонентов.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Компоненты зарубежных электрических и электронных систем: пособие / И. Н. Шило [и др.]. – Минск : БГАТУ, 2012, с. 39-43
2. Белоусова А.И., Солодуха В.А., Шведов С.В. Космическая электроника книга 1, 2015, с. 161-162
3. Белоусова А.И. Космическая электроника, книга 2, Изд. Техносфера, Москва, 2015, с. 108
4. Современные датчики и измерительные системы/ А.А. Гурьев, А.В. Никонов - НТЛ 2021, стр. 24
5. http://SecurityInformed.com
6. Свистова Т.В. , Функциональная электроника, Воронеж , 2014, с. 56
7. IEE Transaction on Plasma Science ISSN 0093-3813
8. Электронные компоненты и системы., ISSN 1817-2369, №4, 2019, стр. 31
9. Сканти навигатор в мире электронных компонентов, №2, 2020, с. 17.
10. IEE Transaction on Plasma Science ISSN 0093-3813, 2018
11. LED Professional Review ISSN 2018-890X, с 35
12. В.А. Рыжова Проектирование и исследование комплексных систем безопасности – Санкт-Петербург, 2013, с. 42
13. Tarakan V. Trends in Nanoscale Mechanics - Kluwer Academic Publishers, 2012, с.190
14. ГОСТ Р МЭК 61508 – 2 -2007 Функциональная безопасность систем электрических, электронных, программи руемых электронных, связанных с без опасностью, Санкт-Петербург, 2013, с 42
15. Stiven Halil Electronic Components – Elsevier, 2018, с. 115
16. Шарыпов А.Г., Шарыпова А.В. Учебное пособие Датчики и сенсоры – Моксва: Техносфера, 2012, с. 570
17. Н. Н. Боголюбов Измерительные приборы для космических исследований, Москва, 2012, с 109
18. Левашев С. Future Trends in Microelectronics: Up the Nano Creek, 2017, с. 96
19. https://community.st.com/s/
20. Шелеванова Г.Н., Актуальные проблемы современной электроники и наноэлектроники, - Красноярск : ИПК СФУ, 2009, с 58
21. https://esalmaty.kz/ru/home-tariffs

Перечень терминов и сокращений

PIR – Passive Infrared – пассивный инфракрасный датчик.

GPS – Global Positioning System – глобальная система позиционирования.

ГОСТ Р МЭК – Государственный стандарт Российской Федерации Международной электротехнической комиссии.

SIL - safety integrity level – метрика, используемая в области функциональной безопасности, которая оценивает уровень интегрированной безопасности системы.

TÜV Rheinland – независимая организация, специализирующаяся на предоставлении услуг по сертификации, инспекции, тестированию и консультированию в области качества, безопасности и устойчивого развития, основанная в Германии в 1872 году, и являющейся на протяжении 150 лет одним из ведущих провайдеров сертификационных услуг.

LCD – Liquid Crystal Display – жидкокристаллический дисплей.

IoT – Internet of Things – Интернет вещей – сеть передачи данных, связывающий физические устройства с интернетом.

ПК – персональный компьютер.

СБ – система безопасности.

GPU – Graphics Processing Unit – Графический процессор.

LCD – Liquid Crystal Display – жидкокристаллический дисплей.

SSD – Solid State Drive – твердотельный накопитель, который является типом хранения данных.

Wi-Fi – Wireless Fidelity – беспроводная точность, являющаяся технологией беспроводной связи.

5G – 5^{th} Generation, что в переводе означает «пятого поколения», являющийся технологией последнего этапа стандарта беспроводной связи.

NFC – Near Field Communication, переводится как «ближнепольная связь», и является технологией беспроводной связи.

ИИ – Искусственный Интеллект.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
НАО Казахский национальный исследовательский технический университет им.К.И.Сатпаева

РЕЦЕНЗИЯ

на дипломную работу

Бекмуратова Эльмира Маратовна

6B07104 «Electronic and Electrical Engineering»

Тема Исследование тенденций развития электронных компонентов систем безопасности

Структура дипломной работы включает в себя: введение, три основных раздела, заключение, список использованной литературы.

В первом разделе определена актуальность исследования, описывается обзор электронных компонентов и космической электроники.

Во втором разделе рассмотрены методы построения систем безопасности на базе этих электронных компонентов для технических систем, а также выбор конкретных электронных приборов и некоторые космические компоненты.

В третьем разделе была проведена исследовательская работа и был сделан расчет стоимости на внедрение системы безопасности технической системы.

В заключении даны основные выводы по проделанной работе.

Общие требования к составлению, изложению, оформлению и содержанию текстовых и графических материалов работы выполнены в соответствии с ГОСТ

Дипломная работа выполнена на оценку 90/A-/«отлично», а дипломант, Бекмуратова Эльмира Маратовна степени бакалавра специальности 6B07104 - Electronic and Electrical Engineering.

Рецензент:
Директор
«ARNAU ENEGERY» ЖШС
Баймухамед Т.С.

«01» 06 2023 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

ОТЗЫВ
НАУЧНОГО РУКОВОДИТЕЛЯ

на дипломную работу
(наименование вида работы)
Бекмуратова Эльмира Маратовна
(Ф.И.О. обучающегося)
6B07104 – Electronic and Electrical Engineering
(шифр и наименование специальности)

Тема: «Исследование тенденций развития электронных компонентов систем безопасности»

В настоящей дипломной работе представлены 3 основных раздела, текст которой изложен на 42 страницах, на которых имеется 25 рисунков. При написании работы использовалось 21 источников.

Исследования тенденций электронных компонентов систем безопасности является актуальной в современном мире, так как позволяет выявить новые технологии, компоненты и решения, используемые для создания более эффективных систем защиты.

Первая глава посвящена обзору электронных компонентов. Вторая глава посвящена методам построения систем безопасности на базе этих электронных компонентов для технических систем. В третьей главе проведен исследование тенденций электронных компонентов, а также расчет стоимости на внедрение системы безопасности технической системы для объекта защиты.

Работа написана логически, последовательно, чётко и ясно. Выполненная работа в полной мере отвечает поставленной цели и является законченным исследованием. Обоснованность и убедительность фактов свидетельствуют о полноте исследований, представленных в научной работе. Оформление работы отвечает принятым стандартам.

Таким образом, дипломная работа ***Бекмуратовой Эльмиры Маратовны*** актуальна, отличается значимой практической ценностью, выполнена по всем требованиям ГАК на должном научном уровне. Автор заслуживает оценки «отлично».

Научный руководитель
Старший преподаватель, Phd
(должность, ученая степень, звание)
Юсупова Г.М.
(подпись)
«16» мая 2023г.

Университеттің жүйе администраторы мен Академиялық мәселелер департаменті директорының ұқсастық есебіне талдау хаттамасы

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Бекмуратова Эльмира Маратовна

Тақырыбы: Исследование тенденций развития электронных компонентов систем безопасности

Жетекшісі: Ерлан Таштай

1-ұқсастық коэффициенті (30): 2.6

2-ұқсастық коэффициенті (5): 0

Дәйексөз (35): 0.3

Әріптерді ауыстыру: 0

Аралықтар: 0

Шағын кеңістіктер: 3

Ақ белгілер: 0

Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :

☒ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

1.06.2023
Күні

Кафедра меңгерушісі

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Бекмуратова Эльмира Маратовна

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Исследование тенденций развития электронных компонентов систем безопасности

Научный руководитель: Ерлан Таштай

Коэффициент Подобия 1: 2.6

Коэффициент Подобия 2: 0

Микропробелы: 3

Знаки из здругих алфавитов: 0

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

1.06.2023
Дата

Заведующий кафедрой

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Бекмуратова Эльмира Маратовна

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Исследование тенденций развития электронных компонентов систем безопасности

Научный руководитель: Ерлан Таштай

Коэффициент Подобия 1: 2.6

Коэффициент Подобия 2: 0

Микропробелы: 3

Знаки из здругих алфавитов: 0

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

1.01.2025
Дата

Мурлеуа С
проверяющий эксперт