**Тип работы:** Дипломная работа

**Предмет:** Информационные системы и процессы

Введение 3
1. Анализ предметной области 5
1.1. Анализ необходимости использования системы видеонаблюдения 5
1.2 Общая характеристика ТЦ Бастион 12
1.3. Общая характеристика объектов физической защиты. Определение требований к проекту системы видеонаблюдения 13
2. Разработка проекта внедрения системы видеонаблюдения 15
2.1. Выбор аппаратных решений 15
2.2 Выбор программных систем управления видеонаблюдением 17
2.3 Интеграция СКУД и системы видеонаблюдения 22
Заключение 26
Список использованных источников 27

Введение

Проблематика обеспечения физической защиты на объектах обусловлена необходимостью сохранности материальных ценностей и информационных активов. Одним из компонентов систем физической защиты являются системы видеонаблюдения, функционал которых включает ведение архивов видеоизображений, проведение съемки на охраняемых объектах компаний. Просмотр изображений с видеокамер обеспечивает возможности расследования инцидентов, мониторинга активности сотрудников и состояния охраны объектов.
Компонентами систем видеонаблюдения являются: видеокамеры, установленные на охраняемых объектах, кабельная система, программное обеспечение (посредством которого проводится настройка системы видеонаблюдения, работа с видеоархивом) и видеорегистраторы.
Цель выпускной квалификационной работы – создание проекта внедрения системы видеонаблюдения.
Задачи исследования:
- анализ нормативной базы по обеспечению физической защиты объектов;
- исследование специфики защищаемых объектов в современных условиях;
- анализ требований к обеспечению физической защиты объектов предприятия с использованием видеонаблюдения;
- анализ основных компонент физической защиты на предприятии;
- анализ архитектуры и функционала программного обеспечения, используемого для автоматизации системы видеонаблюдения;
- анализ недостатков существующей системы видеонаблюдения;
- разработка проекта модернизации системы видеонаблюдения.
Объект исследования - системы физической защиты
Предмет исследования – система видеонаблюдения ООО «ТЦ Бастион».
1. Анализ предметной области
1.1. Анализ необходимости использования системы видеонаблюдения

В рамках данной работы проведено проектирование системы видеонаблюдения для коммерческой организации. Системы видеонаблюдения являются компонентой физической защиты и используются в целях мониторинга состояния объектов в режиме реального времени.
Инженерно-технические и программные системы для управления доступом на объекты является одной из важнейших составляющих комплекса мер по обеспечению информационной безопасности, включают в себя комплекс нормативно-правовых документов, организационных и технических мер, направленных на выполнение требований разграничения доступа на объекты.
Системы видеонаблюдения используются для автоматизации работы службы охраны, а также

сотрудниками структурных подразделения компании в целях мониторинга состояния объектов.
Системы видеонаблюдения могут также являться компонентами систем контроля и управления доступом (СКУД), которые представляют собой комплекс аппаратных и программных технических средств безопасности, основным предназначением которых является разграничение и регистрация доступа объектов на заданную территорию через «точки прохода»[1].
Основными сферами применения СКУД являются [14]:
 контроль доступа работников на объекты предприятий;
 контроль доступа в помещения с ограниченным доступом.
Использование систем видеонаблюдения должно регламентироваться внутренними нормативными документами, принятыми на предприятии. Так, данные регламенты могут быть приняты в документах следующих типов [12]:
 Устав предприятия;
 Положение о пропускном режиме;
 Порядок оформления доступа на территорию ограниченного доступа;
 Правила внутреннего распорядка.
Локальные нормативные документы должны определять:
- порядок использования СКУД;
- полномочия сотрудников – операторов СКУД (поста охраны);
- порядок использования информации, полученной с использованием СКУД;
- регламент оборота идентификаторов сотрудников.
Ознакомление сотрудников с локальными нормативными актами производится под роспись при приеме на работу.
Главная задача систем физической защиты и систем видеонаблюдения – управление доступом на объекты ограниченного доступа предполагает принятие ряда следующих технологических решений [12]:
 ограничение доступа на охраняемую территорию;
 идентификация лица, осуществляющего проход на охраняемую территорию;
 ведение статистического учета по посетителям и сотрудникам;
 возможность интеграции с системами безопасности, например:
 с системами видеонаблюдения при совмещении архивов данных с информацией о посещениях охраняемой территории, извещениях о необходимости начала записи, поворота камеры для записи активности посетителей (например, известно, что системы видеонаблюдения имеют отграничения на предельный объем хранимой информации. интеграция с системой СКУД даст возможность экономии дискового пространства за счет автоматических остановок записи при отсутствии активированных учетных данных при посещениях охраняемой территории и автоматическом ее старте при проходе посетителей через видеосистемы, интегрированные со СКУД);
 с системами пожарной сигнализации (СПС) при необходимости получения данных о функционировании пожарных извещателей, автоматической разблокировки аварийных выходов и закрывания противопожарных дверей при возникновении пожарной тревоги.
При этом интеграция СКУД с другими информационными системами несколько снижает общую защищённость системы. Если необходимы особые меры защищенности помещений, то все перечисленные системы должны функционировать независимо друг от друга.
Основными компонентами систем контроля управления доступом являются:
- система пропуска, турникеты, шлюзовые кабины (устройства контроля и блокировки прохода людей и транспорта на охраняемую территорию);
- пульт охраны, позволяющий управлять системой пропуска;
- программное обеспечение (выполняет различные функции – учет прохода людей и транспорта на объект, протоколирование произведенных действий со стороны поста охраны, учет фактического прибытия сотрудников и транспорта на объект и отправки с объекта);
- считыватели идентификаторов;
- сетевые контроллеры.
Внедрение СКУД для решения задач контроля доступа:
- выполнить требования стандартов безопасности за счет интеграции системы контроля пропуска с системами безопасности, в т.ч. охранной сигнализацией и системой видеонаблюдения;
- исключить влияние человеческого фактора при контроле прохода посетителей.
Для всех систем видеонаблюдения, которые входят в состав аппаратно-программного комплекса,

необходимо обеспечивать следующие характеристики надежности:
• Параметры сохранения работоспособности;
• Технологии обеспечения сохранности данных.
Параметры надежности должны обеспечивать возможности по выполнению функциональных задач с помощью комплекса средств автоматизации.
К параметрам надежности относятся:
• средний временной промежуток между выходом из строя отдельных компонентов системы видеонаблюдения;
• средняя продолжительность обслуживания, ремонта или замены вышедших из строя компонентов;
• средняя продолжительность процесса восстановления работоспособности системы видеонаблюдения.
Параметры надежности системы должны достигаться посредством применения ряда организационно-технических мероприятий по обеспечению доступности ресурсов, их управляемости и обслуживаемости.
Технические меры по обеспечению надежности должны предусматривать:
• возможность резервирования критически важных составляющих видеосистемы СКУД и данных, а также отсутствие единой точки отказа;
• использование технических средств, имеющих избыточные компоненты и возможность проведения их горячей замены;
• возможность конфигурирования используемых средств и использования специализированных программных систем, обеспечивающего высокий уровень доступности.
Организационные мероприятия по обеспечению надежности должны быть направлены на сокращения рисков в работе АПК, а также рисков, связанных с работой персонала службы эксплуатации при проведении работ по обслуживанию комплекса технических средств АПК, минимизацию времени ремонта или замены вышедших из строя составляющих за счет:
• регламентации выполняемых работ и процедур, связанных с обслуживанием и восстановлением системы;
• своевременностью оповещения должностных лиц при возникновении х нештатных ситуаций при работе системы;
• своевременностью диагностики неисправностей;
• заключением договоров по сервисному обслуживанию и поддержке компонентов комплекса технических средств системы видеонаблюдения.
Необходимо обеспечивать следующие значения параметров надежности:
• Возможность круглосуточной работы системы;
• Гарантийный срок службы системы – не менее 3-х лет;
• Параметры наработки на отказ – не менее 6000 часов;
• Наработка на сбой – не менее 2500 часов.
Иные количественные характеристики надежности должны учитываться в процессе проектирования для каждого из компонентов КСА АПК.
Работоспособность должны сохраняться при локальных отказах компонентов СКУД:
• отказ оборудования;
• сбои в работе серверных, клиентских операционных систем;
• возникновении сбоев в работе СУБД при выполнении пользовательских задач;
• отказах в работе каналов связи;
• возникновении импульсных помех, сбоев или перебоях в электропитании.
В случае возникновения нарушений или возникновении разрывов в каналах связи система должна переходить на резервные каналы, а при его отсутствии продолжать работу в автономном режиме, который подразумевает выполнение функций, предусматривающих использование режима периодического обмена данными.
В случае возникновения сбоев или при выходе из строя одного из накопителей система должна работать в штатном режиме, должно быть предусмотрено резервирование данных. Должна обеспечиваться возможность «горячей» замены сбойных или вышедших из строя жестких дисков без остановки работы интегрированной в СКУД системы видеонаблюдения. При возникновении импульсных помех, сбоев или прекращении подачи электропитания не должна нарушаться функциональность СКУД.
Определим перечень требований к надежности технического и
программного обеспечения
Обеспечение надежности функционирования системы видеонаблюдения должно производиться за счет:
• наличия в системе видеонаблюдения СКУД технических средств, имеющих повышенные характеристики

отказоустойчивости с возможностью их структурного резервирования;
• наличия системы защиты системы видеонаблюдения от перебоев в системе электропитания через использование источников бесперебойного питания;
• топология ЛВС, к которой подключена СКУД и система видеонаблюдения, должна предполагать вариантность маршрутизации потоков данных;
• реализации технологий по автоматическому обнаружению и локализации неисправных модулей и видеокамер;
• использования средств мониторинга и оповещения о возникновении аварийных ситуаций.
• наличия систем автоматического оповещения администраторов системы о возникновении нештатных ситуаций, как с помощью средств электронной почты, так с использованием других коммуникационных технологий.

1. Система видеонаблюдения Nest Cam Indoor. [Электронный ресурс]. Режим доступа: https://tech-house.su/obzor-kamery-videonablyudeniya-nest-cam-opravdana-li-ee-stoimost/
2. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: Горячая линия - Телеком, 2012. – 272 с.
3. Задорожный, В.Н. Информационные технологии и автоматизация управления. - Омск : Изд-во ОмГТУ, 2016. - 269 с.
4. Идентификация по смартфону - URL: https://www.aamsystems.ru/mobile-access/ (дата обращения: 20.02.2021)
5. V.D. Cunsolo, S. Distefano, A. Puliafito and M.L. Scarpa, ’’Achieving Information Security in Network Computing Systems”, 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
6. Горев А. И., Симаков А. А. Обработка и защита информации в компьютерных системах: учебно-практическое пособие / А. И. Горев, А. А. Симаков. - Омск : ОмА МВД России, 2016. - 87 с.
7. Калачев А. Для мобильных стражей: беспроводной стандарт Bluetooth Low Energy в системах безопасности - URL: https://www.compel.ru/lib/ne/2013/1/3-dlya-mobilnyih-strazhey-besprovodnoy-standart-bluetooth-low-energy-v-sistemah-bezopasnosti (дата обращения: 20.06.2019)
8. Крахмалев А.К. Средства и системы контроля и управления доступом. Учебное пособие. М.: НИЦ «Охрана» ГУВО МВД России, 2011.
9. Мировой рынок СКУД http://www.techportal.ru/access-control/market/
10. Михайлова Е. М., Анурьева М. С. Организационная защита информации [Электронный ресурс]/ Михайлова Е. М., Анурьева М. С. - Тамбов: ФГБОУ ВО "Тамбовский государственный университет имени Г. Р. Державина", 2017.
11. Мобильная идентификация. Технологии. Чек-лист по выбору системы. Обзор решений. URL: http://www.techportal.ru/review/mobile-access/how-to-choose/ (дата обращения: 20.06.2019)
12. Обзор российского рынка СКУД http://www.s-director.ru/i/tree/101/7_2010.1.pdf
13. Рынок СКУД. URL: http://sio.su/ (дата обращения: 06.06.2019)
14. Системы безопасности http://www.bolid.ru/soft/object/object_5.html
15. Сравнение СКУД. URL: http://biometricsecurity.ru/ (дата обращения: 10.06.2019).
16. J. Harauz, L.M. Kaufman and B. Potter, ”Data Security in the World of Cloud Computing”, IEEE Security and Privacy, 2009.
17. C. Wang, Q. Wang, K. Ren and W. Lou, ’’Privacy-Preserving Public Auditing for Data Storage Security in Could Computing”, Proceedings of IEEE INFOCOM, 2010.
18. Такатлы Д. А. Защита персональных данных / Д. А. Такатлы. - Петропавловск-Камчатский: Дальневосточный филиал Федерального государственного бюджетного образовательного учреждения высшего образования "Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации", 2016. - 92 с.
19. Melnyk A. O. Multilevel base platform of cyber-physics systems // Cyber-physical systems: achievements and challenges // Materials of the first scientific seminar, Lviv, 2015. – P. 5–15.
20. Jason R. Indoor WiFi Location and Beacons: Better Together. URL: http://blogs.cisco.com/ wireless/ indoor-wifi-location-and-beacons-better-together/ (дата обращения: 10.02.2021).
21. Базовые характеристики СКУД. URL: https://www.inarm.ru/solutions/skud (дата обращения: 28.02.2021)
22. Официальный сайт ФСТЭК России [Электронный ресурс] / Банк данных угроз безопасности информации – Режим доступа: http://bdu.fstec.ru/threat / Дата обращения: 09.02.2021 г.
23. Официальный сайт ФСТЭК России [Электронный ресурс] / Руководящий документ Автоматизированные

системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации – Режим доступа: https://fstec.ru/component/attachments/download/296 / Дата обращения: 09.02.2021 г.
24. Аникин Д. В. Информационная безопасность и защита информации: учебное пособие / Д.В. Аникин. - Барнаул: Изд-во Алтайского государственного университета, 2018. - 196 с.
25. Ахметов И. В., Карабельская И. В., Губайдуллин И. М., Сафин Р. Р. Моделирование бизнес-процессов: учебное пособие. - Уфа: Уфимский государственный университет экономики и сервиса, 2015. - 67 с.
26. Бабиева Н. А., Раскин Л. И. Проектирование информационных систем: учебно-методическое пособие / Н. А. Бабиева, Л. И. Раскин. - Казань: Медицина, 2014. – 200с.