



Комплексная система безопасности организации

ПРЕДПОСЫЛКИ ДЛЯ СОЗДАНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ

Антитеррористическая защищенность мест массового пребывания людей и объектов



Обеспечение безопасности – одно из главных требований при подготовке к международному спортивному событию.

Требования законодательства



Отраслевое законодательство и законодательная практика других критически важных отраслей.

Опыт других организаций



Комплексный подход к построению безопасности применяется в вузах, вокзалах, стадионах торговых, развлекательных и бизнес-центрах, предприятиях ТЭК и других организациях.

ОБЗОР ЗАКОНОДАТЕЛЬСТВА

Постановление Правительства РФ № 272 от 25 марта 2015 г.
«Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов».

ТРЕБОВАНИЯ:



Категорирование мест массового скопления людей в зависимости от численности человек, которые могут одновременно находиться в данном месте; составление паспорта безопасности.



Вне зависимости от категории требуется обеспечить антитеррористическую защищенность места массового пребывания людей путем:

- Контроля в едином информационном пространстве в режиме реального времени обстановки, складывающейся в районах расположения мест массового пребывания людей;
- Применения современных информационно-коммуникационных технологий для обеспечения безопасности мест массового пребывания людей;
- Оборудования мест массового пребывания людей необходимыми инженерно-техническими средствами.



Все места массового пребывания людей независимо от установленной категории должны быть оборудованы:

- Системой видеонаблюдения, которая с учетом количества устанавливаемых видеокамер и мест их размещения должна обеспечивать непрерывное видеонаблюдение за состоянием обстановки на всей территории места массового пребывания людей, архивирование и хранение данных в течение 30 дней;
- Системой оповещения и управления эвакуацией;
- Системой освещения.

ЧТО НЕ ОБХОДИМО СДЕЛАТЬ ДЛЯ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ



Модернизировать
СКУД и СВН



Объединить системы
безопасности в единое
инженерно-техническое
решение



Организовать единую службу
(единый центр), который
обеспечивает комплексный
мониторинг безопасности
объекта и повышает
эффективность установленных
технических средств



Разработать
систему
информационной
безопасности

РЕАЛИЗАЦИЯ КОМПЛЕКСНОГО ПОДХОДА НА БАЗЕ ЕДИНОЙ ПЛАТФОРМЫ



ИНТЕГРАЦИОННАЯ ПЛАТФОРМА ELECTRONIKA SECURITY MANAGER (ESM)

Преимущества



Интеграция всех технических решений в единой информационной среде



Сценарный механизм обнаружения угроз; определение достоверности событий и критичности ситуации



Активация пошаговых инструкций, направленных на разрешение инцидента



Адаптация под заданный уровень угроз



Координация сил реагирования, своевременное оповещение всех заинтересованных лиц



Контроль работы оператора с системой, анализ эффективности принятых мер



Сбор доказательной базы и автоматическое формирование отчетов

АВТОМАТИЗИРОВАННОЕ УПРАВЛЕНИЕ УРОВНЯМИ БЕЗОПАСНОСТИ И РЕЖИМАМИ РАБОТЫ ИТСО

В России установлена 3-х уровневая система террористической опасности:

повышенный

высокий

критический

В транспортной безопасности РФ также предусмотрено три уровня безопасности:

1

УРОВЕНЬ

защита
от потенциальных
угроз

2

УРОВЕНЬ

защита
от непосредственных
угроз

3

УРОВЕНЬ

защита
от прямых
угроз



ESM единственная российская система имеющая функцию управления уровнями безопасности и обеспечивающая автоматическую и быструю адаптацию работы технических средств без опасности под уровень угрозы предприятию.



ОБНАРУЖЕНИЕ

ОТРАЖЕНИЕ

ЛИКВИДАЦИЯ
(РЕАГИРОВАНИЕ)

Регламенты оргмероприятий



Технические средства защиты



Силовые подразделения



Видеонаблюдение



Защита периметра



ОПС



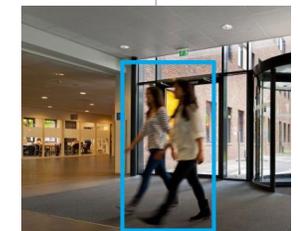
ОТС



СКУД



Дополнительные инженерные решения



Аналитика

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ

1

Работает под управлением открытых и закрытых ОС (кроссплатформенность)

2

Является открытой платформой для интеграции, имеет готовые модули поддержки систем безопасности (СКУД, СВН, СОПС, СОТС и т.д.)

3

Имеет встроенные механизмы аналитики и верификации событий, механизм поддержки принятых решений

4

Поддерживает средства связи и различные способы для оповещения об отклонениях

5

Адаптирует работу всей системы под заданный уровень угроз

6

Контролирует работу операторов с системой, анализирует эффективность принятых мер

7

Собирает доказательную базу и автоматически формирует отчеты

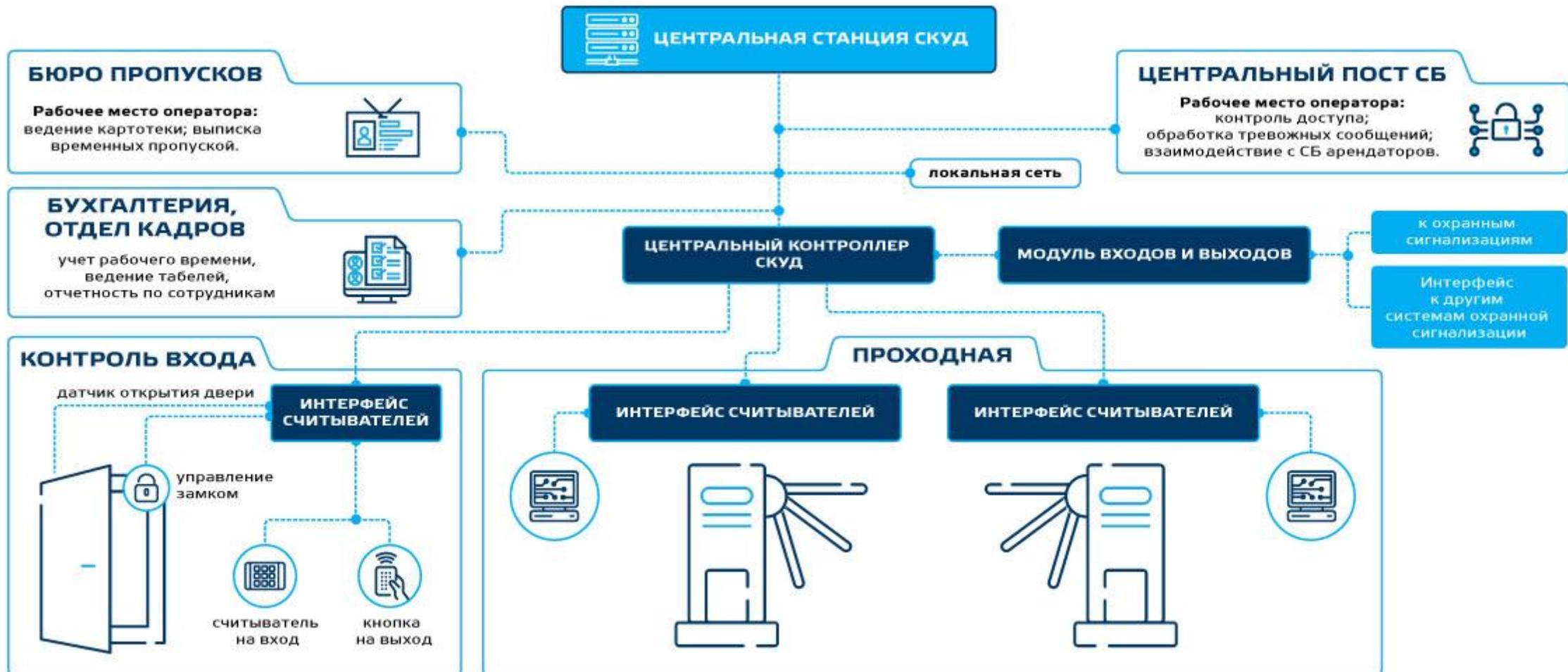
Автоматизация деятельности большого объекта со сложной организационной структурой включает в себя множество процессов, которые должны находиться в тесной связи друг с другом - это работа систем, обеспечивающих безопасность объекта (охранной и пожарной сигнализации, системы контроля и управления доступом (СКУД), видеонаблюдения), систем административного управления, документооборота, бюро пропусков, бухгалтерии и прочих ERP систем, присутствующих на объекте.



ОСОБЕННОСТИ КРУПНЫХ ОРГАНИЗАЦИЙ:

- Большое количество сотрудников
- Большая проходимость
- Значительная территориальная распределенность
- Поддержание в актуальном состоянии постоянно изменяющейся базы данных сотрудников (прием новых, отчисление, перевод в другие подразделения)
- Совместная работа с большим количеством сторонних систем, имеющих на объекте

ИНТЕГРАЦИЯ СКУД С СИСТЕМАМИ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ



ИСПОЛЬЗОВАНИЕ НСПК «МИР» В СКУД.

Согласно Федеральному закону № 161, с 1 января 2018 года все бюджетники должны получать зарплату на карту «Мир», это касается и социальных выплат, в частности, пенсий и пособий.



В целях повышение уровня безопасности существующей системы предлагается использование нефинансового приложения карты национальной системы платежных карт «МИР», при этом обеспечивается:

- обмен данными между картой и считывателем на уровне банковских стандартов безопасности;
- защита от клонирования - при чтении карты применяется специальный трехуровневый алгоритм верификации с использованием криптостойкого шифрования.



«НСПК» МИР проведены переговоры о сотрудничестве с ведущими мировыми платежными системами по выпуску кобейджинговых карт, которые могут использоваться в инфраструктуре других платежных систем как в России, так и за рубежом.

ПРЕДПОСЫЛКИ ДЛЯ ВНЕДРЕНИЯ ЕДИНОЙ КАРТЫ

В настоящее время существует тенденция идентификации персонала в большинстве информационных систем с помощью единой карты, использование которой освобождает от необходимости ношения большого количества различных карт и пропусков, запоминания многочисленных паролей.

СООТВЕТСТВЕННО ЕДИНАЯ КАРТА МОЖЕТ БЫТЬ:

- Банковской картой для зачисления з/п, оплаты питания в столовой и осуществления платежей вне территории организации
- Пропуском на территорию организации, парковки
- Электронным читательским билетом, идентификатором для доступа к другим информационным сервисам организации
- Проездным билетом в общественном транспорте



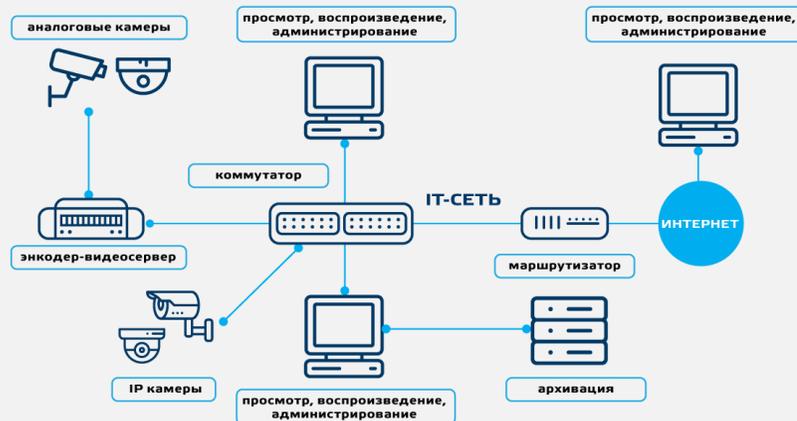
ПРЕИМУЩЕСТВА ВНЕДРЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ:

- Расширенные возможности видеоаналитики
- Постоянный контроль необходимых процессов
- Ведение непрерывного архива, что позволит восстановить информацию и принять правильное решение при рассмотрении спорных ситуаций
- Высокое цифровое разрешение
- Работа в условиях низкой видимости



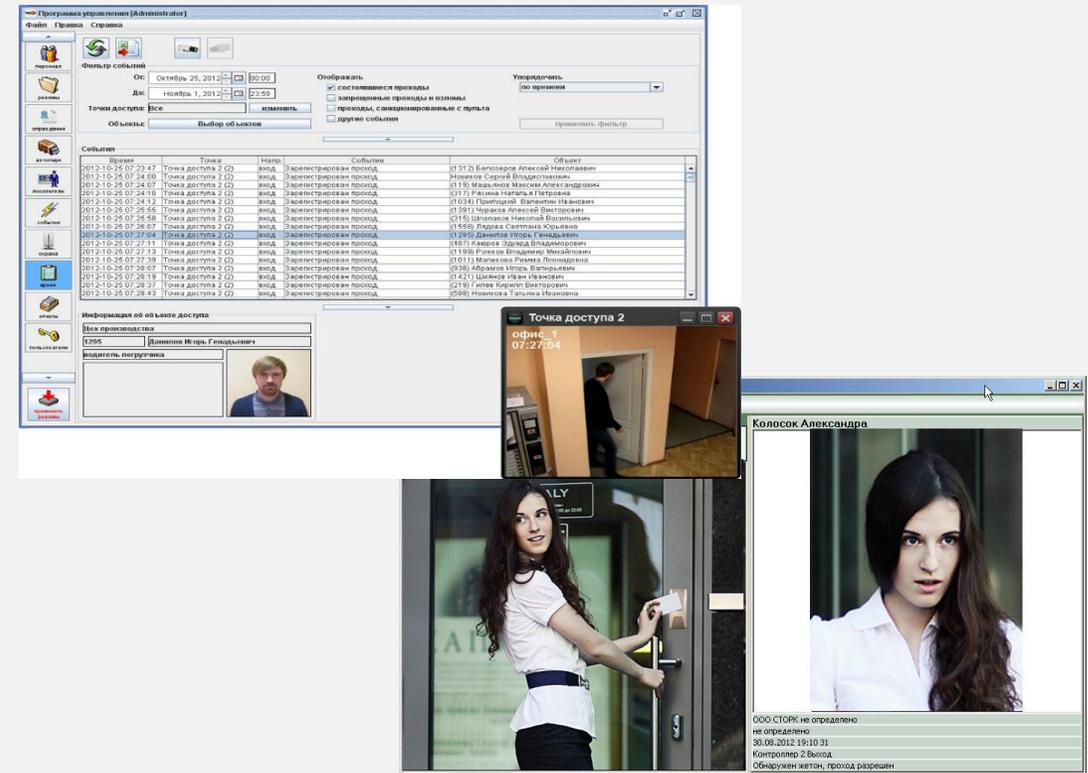
ПРЕИМУЩЕСТВА ВНЕДРЕНИЯ:

- Устойчивость к климатическим воздействиям
- Интерактивные карты показывают расположение камер, давая консолидированное представление о системе безопасности
- Сигнализация интегрирована с картами, благодаря чему пользователи всегда получают уведомления о нежелательных событиях, таких как прохождение людей через охраняемую дверь



ИНТЕГРАЦИЯ СКУД С СИСТЕМОЙ ВИДЕОНАБЛЮДЕНИЯ ПОЗВОЛИТ:

- «Живое» видео на графических планах (для наглядного и удобного отслеживания событий в реальном времени, а также оперативного управления элементами системы)
- «Живое» видео на посту наблюдения (возможность создания индивидуальных видов наблюдения)
- Переход по событию СКУД в видеоархив (обращение СКУД к архиву СВН для визуального сопровождения события)
- Использование распознанных автомобильных номеров (принятие решения о доступе по номеру автомобиля)



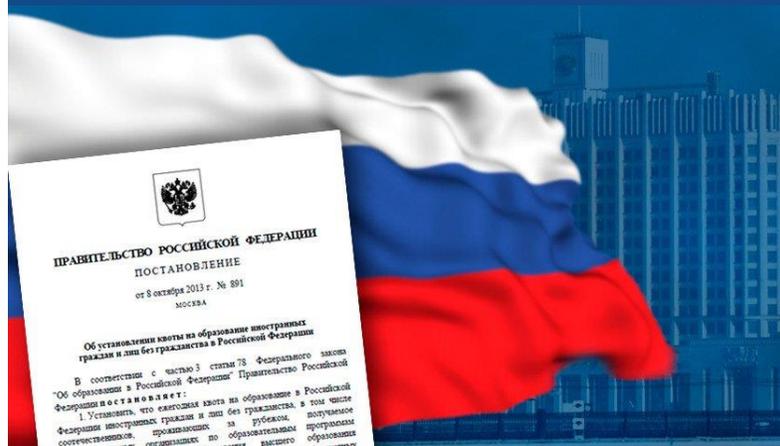
ПРЕДПОСЫЛКИ ДЛЯ СОЗДАНИЯ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ЦИБ)

Сохранение экстремистских и террористических угроз посредством вовлечения молодежи через соцсети



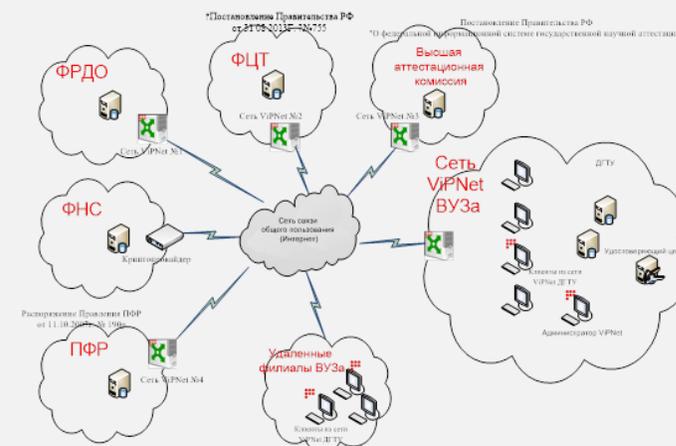
- Обеспечение информационной безопасности - одно из главных требований для полноценной и безопасной жизнедеятельности современного Опорного Университета.

Требования законодательства РФ



- Законодательство в области защиты информации и персональных данных, Комплексный план противодействия идеологии терроризма в Российской Федерации на 2013-2018 годы, утвержденный Президентом РФ.
- Проверки регуляторов (ФСБ, ФСТЭК, Роскомнадзор, Рособранадзор, Прокуратура). Штрафные санкции при невыполнении требований

Постоянный рост узлов взаимодействия со сторонними организациями



- Взаимодействие с вышестоящими организациями, федеральными информационными системами (ЕГИСМ ВАК, ФИС ЕГЭ и тестирования (ФЦТ)), ФИС ФРДО, ИС Контингент учащихся и др.) и сторонними органами исполнительной власти (ПФР) строится через отдельные аттестованные системы или АРМ посредством СЗИ ViPNet.

Постановление Правительства РФ от 01.11.2012 № 1119

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в ИС необходимо выполнение требований:

- а) организация режима обеспечения безопасности помещений, в которых размещена ИС, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- б) обеспечение сохранности носителей персональных данных;
- в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей;
- г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.



ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ ТРЕБУЮЩИЕ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Программное обеспечение СКУД
- Зарплата и кадры
- Бухгалтерия
- Критически значимые информационные системы и ресурсы
- Конфиденциальная информация



Одним из ключевых вопросов является защищенное взаимодействие с различными федеральными и региональными информационными системами (ФИС).



Для подключения к каждой из Систем может использоваться одно или несколько автоматизированных рабочих мест (АРМ).

С учетом того, что организация должна подключаться с помощью сертифицированных ФСБ и ФСТЭК средств защиты информации ViPNet к ряду информационных систем, количество которых постоянно расширяется, предлагается создать собственную ViPNet-сеть, а также выделить и аттестовать отдельный сегмент ЛВС.



Создание Центра информационной безопасности в организации позволит создать масштабируемую систему защиты информации, удовлетворяющую требованиям законодательства, повысить надежность и безопасность хранимой, обрабатываемой и передаваемой сторонним организациям информации, упростить и удешевить дальнейшее взаимодействие с контрагентами по защищенным каналам электронного взаимодействия.

Данные мероприятия будут фактически являться необходимой основой создания Комплексной системы безопасности (КСБ), интегрирующей:

- Систему контроля управления доступом (СКУД);
- Систему видеонаблюдения (СВН);
- Систему информационной безопасности (СИБ) и другие системы по мере их соответствующей модернизации и готовности к интеграции в КСБ.





Компания «CBS»
станет вам надежным
партнером в решение самых
сложных задач.

**Благодарим
за внимание!**

Телефон: 8 (495) 234-68-51
МОСКВА: 123181, ул. Исаковского, д. 33, корп. 3
РОСТОВ-НА-ДОНУ: 344002, пер. Соляной спуск 8-10, 34
E-mail: sales@cbs-group.ru
www.cbs-group.ru