



**Цифровые технологии в управлении рисками
возникновения чрезвычайных ситуаций.
Модель комплексной системы безопасности
современного вуза**



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 3 декабря 2014 г. № 2446-р

МОСКВА

1. Утвердить прилагаемую Концепцию построения и развития аппаратно-программного комплекса "Безопасный город".

2. Рекомендовать органам исполнительной власти субъектов Российской Федерации и органам местного самоуправления руководствоваться положениями Концепции, утвержденной настоящим распоряжением, при решении задач в сфере обеспечения комплексной безопасности среды обитания, а также при разработке и утверждении региональных и муниципальных программ построения и развития аппаратно-программного комплекса "Безопасный город".

Председатель Правительства
Российской Федерации



Д.Медведев

Проект «Безопасный город» – совокупность КСА существующих и перспективных автоматизированных систем различного уровня, объединенных для решения задач в сфере обеспечения защиты населения и территорий от ЧС природного и техногенного характера, общественной безопасности, правопорядка и безопасности среды обитания



Основные понятия

1

Безопасность – это состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз статья 1 Закона РФ "О безопасности"

2

Комплексная безопасность вуза – состояние защищенности охраняемых субъектов и объектов от реальных и прогнозируемых угроз социального, техногенного и природного характера

3

Комплексная безопасность является сочетанием организационных мероприятий и технических средств обеспечения безопасности



Мероприятия КСБ

- Организация физической охраны
- Обеспечение инженерно-технической укреплённости
- Организация инженерно-технического оборудования
- Плановая работа по антитеррористической защищённости
- Организация внутриобъектового и пропускного режимов
- Выполнение норм пожарной безопасности
- Соблюдение норм охраны труда и электробезопасности
- Плановые работы по гражданской обороне
- Комплекс мер по антитеррористической защищённости, противодействию терроризму и экстремизму
- Взаимодействие с правоохранительными органами и другими структурами
- Обучение и формирование культуры безопасности
- Защита материальных и информационных ценностей
- Защита собственных ресурсов и технических средств при попытках несанкционированного доступа к ним
- Организация доступа студентов, работников и посетителей на территорию вуза
- Обнаружение и регистрация фактов несанкционированного проникновения нарушителя на территорию вуза
- Оповещение охраны и/или службы безопасности о нештатных ситуациях
- Наблюдение за прилегающей территорией к зданиям вуза
- Компьютерный анализ работоспособности элементов КСБ, управление техническими средствами подсистем с автоматизированного рабочего места (АРМ)



Организационные и технические компоненты КСБ

Комплекс технических средств, обеспечивающих комплексную безопасность вуза включает в себя:

- Системы охраны периметра
 - система охранного телевидения
 - система охранно-тревожной сигнализации
 - система охранного освещения
 - система экстренной связи
 - система противопожарной безопасности
- Система контроля и управления доступом (СКУД)
- Инженерные (SCADA) системы
- Система видеонаблюдения и видеоаналитики
- ИТ инфраструктура и системы управления ИТ, включая средства виртуализации, архивного копирования, мониторинга инфраструктуры
- Системы информационной безопасности
- Ситуационный и информационно-аналитические центры
 - система диспетчеризации и управления ТОИР
 - аналитическая система с возможностью прогнозирования нештатных ситуаций на основе технологий машинного обучения
 - система визуализации информации – ситуационный центр
- Мультимедиа, интернет системы, мобильные ассистенты как средства оповещения и информации



Мультимедиа



ИТ-инфраструктура



Сеть



Мультимедиа
хранилище



Интернет
и мобильные ресурсы



Навигация
и IoT



Инженерные
системы



Видеонаблюдение



СКУД



ОПС



Ситуационный
центр



Аналитический
центр



Модель комплексной системы безопасности вуза

1. ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

1.1 Охрана периметра

- подсистема охранного телевидения, охранной сигнализации внешнего и внутреннего периметра (реализуется классическими способами – путем мониторинга информации, поступающей с размещенных на территории вуза проводных и беспроводных датчиков);
- подсистема охранного освещения;
- подсистема экстренной связи.

1.2 СКУД (система контроля и управления доступом в помещения вуза), реализующая функции идентификации и контроль доступа

1.3 Система мониторинга и позиционирования, в составе которой:

- подсистема видеонаблюдения
- подсистема учета и маршрутизации обучающихся и сотрудников вуза
- подсистема контроля физического состояния лиц

2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Вся IT инфраструктура вуза и доступ к сервисам единого информационно-образовательного пространства должен быть реализован на основе применения технологии Virtual Desktop Infrastructure (VDI). Система виртуализации рабочих мест пользователей представляет собой комплексную систему, предназначенную для организации работы пользователей (студентов и работников) с информационными системами вуза, путем виртуализации рабочих мест и предоставления доступа к ним по защищенному терминальному протоколу, в том числе по открытым каналам связи.

3. ЗАЩИТА при ВОЗНИКНОВЕНИИ ЧС

- 3.1 Защита при возникновении ЧС природного характера.
- 3.2 Защита при возникновении ЧС техногенного характера.

4. ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ

5. ПРОТИВОДЕЙСТВИЕ КОРРУПЦИИ



Возможности системы позиционирования

Дать возможность студенту или посетителю заявить о нештатной ситуации

- без потребности звонить по телефону
- быстро, на том же месте, не привлекая внимания
- передача сигнала в локальную СБ

Контроль местонахождения источника

- СБ получает местоположение источника вызова относительно карты здания
- сигнал сопоставляется с данными о студенте или госте ВУЗа

Оповещения ГО/ЧС

- информирование всех присутствующих о ЧС
- контроль исполнения планов эвакуации и оставшихся в здании людей на карте в реальном масштабе времени

