Принципы построения системы:

1. Необходимость **применения операционной системы (ОС) с открытыми исходными кодами** (Linux и др.)

Исходный код таких программ доступен для просмотра, изучения и изменения, что позволяет пользователю контролировать работу программы, принять участие в доработке самой открытой программы, использовать код для создания новых программ и исправления в них ошибок. Операционная система с открытым исходным кодом делает невозможной установку шпионского программного обеспечения и прослушку и исключает возможность утечки информации. Отличие подобной операционной системы заключается в том, что открытый исходный код исключает наличие закладок.

ОС с закрытыми исходными кодами (зарубежные производители как Windows, MS-Office, Android, iOS и др.) автоматически подразумевает возможность удаленного управления данными или снятия какой-то информации, делая систему незащищенной и уязвимой со стороны обладателей исходного кода.

(Распоряжение Правительства Российской Федерации от 17 декабря 2010 г. № 2299-р.; Федеральный закон от 29.06.2015 г. № 188 – ФЗ, подписанный В.В. Путиным, согласно которому с 1 января 2016 г. на всей территории РФ запрещено использование иностранного ПО).

2. Использование открытых протоколов обмена данными устройств и программных продуктов.

Это позволяет интегрировать ПО и оборудование разных производителей в единый Аппаратно-программный комплекс. В противном случае объединить разрозненные устройства и подсистемы в единый АПК невозможно.

3. Визуализация состояния объектов и территорий в 3D ГИС исполнении с привязкой всех компонентов системы мониторинга (видеокамер, датчиков, приборов и др.) к географическим координатам и времени.

(Распоряжение Правительства РФ от 17.11.2008 № 1662-р «О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года», Рекомендации МЧС РФ № 2-4-60-3-28 от 25 февраля 2009 г.)

Это позволяет вести мониторинг объектов размещенных на различных уровнях от земли, в том числе и под землей (коммуникации, тоннели, метро), получая на экране привычное для глаз человека изображение, вызывать отображение нужной точки местности или помещения не выбором камер, направленных на требуемую точку, а простым клик-приказом на точку карты-схемы, по которому выводятся на экран изображения всех камер, в чьей зоне действия находится интересующее место. Поворотные камеры, в этом случае, автоматически разворачиваются в нужном направлении (на указанные координаты). В свою очередь при возникновении

критической ситуации или тревожного события естественное восприятие обстановки ускоряет и обеспечивает адекватное принятие решения и его корректное воплощение.

Привязка всех компонентов системы безопасности на 3D-плане объекта с отражением их функционального состояния повышает оперативность устранения возможных технических отклонений в работе системы.

4. Шифрование передаваемых данных до степени секретности объекта

(в соответствии с требованием о защите передаваемых данных и Постановлению РФ от 5 января 2004 г. № 3-1 «Об утверждении Инструкции по обеспечению режима секретности в РФ»).

Это обеспечивает:

- Недоступность информации для сторонних лиц;
- Подлинность информации (то есть информации поступит в неискаженном виде);
- Целостность информации (данные, которые передаются останутся целыми в процессе передачи).

5. Применение электронной подписи (ЭП) для обеспечения санкционированного доступа к информации (Закон об электронной подписи от 6 апреля 2011 г. № 63-ФЗ, Приказ № 107 от 13.04.2012 г. Об утверждении Положения о федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»).

Электронная подпись идентифицирует владельца сертификата ЭП, а также защищает от несанкционированных изменений информации в электронном документе. Применение ЭП в системах безопасности обеспечивает надежную защиту от несанкционированного доступа, персональную ответственность за передаваемую информацию и ее искажение (дезинформацию).

6. Полицентрическое построение системы безопасности.

То есть передача информации осуществляется не в единый центр, где обрабатывается и далее передается пользователю, а анализируется и обрабатывается, а также хранится локально на объектах (распределенные центры) и передает события одновременно всем пользователям в соответствии с их правами доступа по любым каналам передачи информации. Нарушение работы части системы или отдельных ее каналов не приводит к потере информации и потере работоспособности всей системы, что обеспечивает ее устойчивость и надежность жизнедеятельности.