Цель создания системы видеомониторинга и контроля доступа к АРМ **IDmatic -Инсайдер** - противодействие несанкционированным действиям персонала (инсайдерам).

Предполагается, что инсайдерами могут быть сотрудники:

- имеющие легальный доступ в служебные помещения,

- владеющие широкими правами пользователя информационных ресурсов для выполнения своих служебных обязанностей,

- обладающие высокой квалификацией в области технических и программных средств вычислительной техники на уровне разработчиков или системных администраторов.

Принимаются во внимание угрозы умышленного или неумышленного нарушения регламентов работы. В частности:

- передача радиокарточки для доступа в помещения и к АМР,

- передача своих прав пользователя АРМ другим лицам после легального процесса регистрации,

- работы с АРМ в неустановленное время, нарушения правил выполнения рабочих операций требующих присутствие второго сотрудника или контролера,

- несанкционированное вскрытие системных блоков АРМ, аппаратных стоек серверов, сейфов для хранения носителей информации,

- использование своей радио карты для пропуска в рабочие помещения посторонних лиц,

- уход из рабочего помещения без окончания сеанса работы на АРМ.

Предполагается, что задачи защиты информации и авторизированного доступа непосредственно в программных приложениях и операционной среде, решаются другими средствами.

Поставленная задача решается в проекте по нескольким направлениям:

- автоматизация контроля регламентов работы сотрудников;
- регистрация информационного следа действий сотрудников;

- персональная идентификация сотрудников, включая биометрическую;
- охрана и контроль доступа и видеонаблюдение для средств вычислительной техники;
- организация двойного рубежа защиты информации (принцип 4-х глаз).

Автоматизация контроля регламентов работы персонала

Пример автоматизированного контроля работы сотрудников по различным регламентам:

1. Доступ по радиокарте (1 оператор).
2. Доступ по радиокарте с биометрической идентификацией лица (1 оператор).
3. Доступ по радиокарте (2 оператора, принцип 4-х глаз).
4. Доступ по радиокарте с биометрической идентификацией лица (2 оператора, принцип 4-х глаз).

5. Доступ по радиокарте с контролером (1 оператор + контролер).
6. Доступ по радиокарте с контролером и биометрической идентификацией лица (1 оператор + контролер).

Подробнее...

Регистрация информационного следа действий сотрудников

Осуществляется с помощью системы контроля доступа к АРМ, аппаратным стойкам и сейфам, видеомониторинга лиц сотрудников на рабочих местах, видеонаблюдения и системы контроля доступа в рабочих помещениях.
Подобный мониторинг позволяет восстановить историю практически всех действий сотрудников в контролируемых рабочих помещениях.

Подробнее...

Персональная идентификация сотрудников, включая биометрическую

Производится с помощью радиокарт, биометрической процедуры распознавания и видеомониторинга лиц на рабочих местах, точек доступа к сейфам и аппаратным стойкам серверов. Общее видеонаблюдение и система контроля доступа на дверях помогает дежурной службе идентифицировать сотрудников во всех рабочих помещения.

Подробнее...

Охрана и контроль доступа и видеонаблюдение для средств вычислительной техники

С помощью охранных датчиков контролируется вскрытие корпусов АРМ, отсоединение клавиатуры АРМ, вскрытие сейфов для носителей информации и аппаратных стоек серверов.
Специальные контроллеры осуществляют подключение или отключение клавиатуры, мыши и монитора к системным блокам АРМ.
Осуществляется охрана и контроль доступа не только для помещений, где находится техника, но и для каждого устройства в отдельности.

Подробнее...

Организация двойного рубежа защиты информации (принцип 4-х глаз)

Единое информационное пространство, объединяющее различные подразделения компаний, позволяет осуществлять общее администрирование системы и контроль выполнения регламентов работы сотрудниками различных подразделений. Наблюдение за системой на одной площадке осуществляется удаленно, с территории другой площадки. Единая дежурная служба может осуществлять общее видеонаблюдение и контроль доступа в рабочих помещениях.
Таким образом возможно осуществление общего и неформализованного удаленного контроля за работой всех сотрудников в разных подразделениях (на разных площадках) компании. Такое разделение функций между независимыми службами с возможностью выборочного контроля руководства в режиме on-line позволяет организовать два

рубежа защиты информации или принцип 4х глаз. Это существенно снижает потенциальные риски, связанные с инсайдерами. Тот факт, что руководитель может в любую минуту контролировать объект, дополнительно дисциплинирует как сотрудников, так и дежурных.

Особо необходимо отметить, что данная система видеомониторинга и контроля доступа к АРМ IDmatic-Инсайдер может быть установлена, отлажена и введена в эксплуатацию на работающем объекте без остановки технологических процессов.

Подробнее...

Читать подробнее о защите информации и противодействии инсайдерам"

Подробнее об ***IDmatic*** ***-Инсайдер***

Наш сайт insideram.net