Электроника
системы управления
безопасностью

ELECTRONIKA SECURITY MANAGER (ESM)

Инструмент повышения эффективности

Система управления безопасностью ELECTRONIKA SECURITY MANAGER, как основное средство повышения эффективности системы физической защиты потенциально опасных и критически важных объектов

Одной из основных задач, решаемых системой безопасности, является обнаружение нарушителя, и затруднение его продвижения к защищаемым объектам с целью дать силам охраны запас времени для своевременного прибытия к месту перехвата и оказания эффективного противодействия нарушителю.

Способность интегрированной системы безопасности (ИСБ) обнаруживать нарушителя зависит:

- от правильности проектных решений и качества реализации проекта;
- от качества обслуживания системы;
- от уровня подготовки оператора системы по оценке тревожных сигналов и его добросовестного отношения к своим обязанностям.

При расследовании фактов несанкционированного проникновения на территорию зачастую выясняется, что система охранной сигнализации периметра выдала тревожный сигнал, на записи системы видеонаблюдения виден нарушитель, но при этом оператор технических средств охраны (ТСО) не выполнил свои обязанности по проверке тревожного сигнала, а просто сбросил сигнал тревоги. Это может происходить по следующим причинам:

1. Система дискредитировала себя в глазах оператора ТСО недопустимо большим числом ложных тревог. (**Ложные тревоги являются причиной снижения эффективности системы физической защиты**).
2. Оператор с недобросовестным отношением к работе не выполняет свои обязанности, зная, что начальство не может полностью проконтролировать качество его работы.
3. Оператор не обладает необходимыми личностными качествами и (или) профессиональными навыками для выполнения обязанностей оператора ТСО. (по п. 2 и 3 **Низкое качество информации, сохраняемое в системе, не обеспечивает контроль работы оператора ТСО и является причиной снижения эффективности ИСБ**).

Другими важными задачами ИСБ, направленными на повышение эффективности системы физической защиты, являются:

- поддержка процесса принятия решений при выборе наилучшей тактики реагирования на угрозы;
- своевременное извещение об угрозах должностных лиц, подразделений и организаций.

В рамках поддержки процесса принятия решений при выборе наилучшей тактики реагирования на угрозы система управления безопасностью ESM обеспечивает:

1. Возможность одновременной обработки нескольких инцидентов несколькими операторами или последовательной обработки нескольких инцидентов одним оператором с учетом их уровня критичности. В рамках решения данной задачи система обеспечивает:
   - возможность автоматического переключения для приоритетного реагирования на более критичный инцидент;
   - возможность мгновенного переключения оператора между инцидентами;
   - сбор и вывод от всех систем информации и сигналов, принадлежащих этому инциденту, без перемешивания с информацией принадлежащей другим инцидентам (в каждый момент времени оператору поступает только та информация, которая необходимая для выполнения текущей задачи);
   - мгновенный доступ не только к «живой», но и записанной по данному инциденту видеоинформации и фонограммам переговоров;
   - отображение уже выполненных мер и мер, которые необходимо выполнить в рамках реагирования по данному инциденту (нет необходимости запоминать какие меры выполнены, а какие еще нет при переключении между инцидентами);
   - возможность передачи задачи более опытному или вышестоящему сотруднику при возникновении трудностей с ее выполнением.
2. Вывод по тревожному сигналу пошаговых инструкций по первоочередным мерам по реагированию на данный тип угрозы, что позволяет повысить оперативность и точность реагирования, а также снизить требования к уровню подготовки операторов и обеспечить контроль качества их работы.
3. Автоматизированную регистрацию инцидентов выявленных силами охраны в ходе выполнения своих должностных обязанностей (в ходе видеонаблюдения, патрулирования, получения информации об угрозах анонимно или от очевидцев), с выводом пошаговых инструкций по реагированию на угрозы из разных предметных областей (антикриминальная и антитеррористическая безопасность, противопожарная безопасность, промышленная безопасность, экологическая безопасность, экономическая безопасность, охрана труда и т.п.).
4. Регистрацию дополнительно поступающих сведений об угрозе с обеспечением динамической корректировки пошаговых инструкций с целью выбора ответных мер, адекватных угрозе.

В рамках извещения должностных лиц, подразделений и организаций об угрозах система управления безопасностью ESM обеспечивает:

1. Автоматический дозвон и передачу голосового сообщения на сотовые и стационарные телефонные номера, а также абонентам оперативной радиосвязи.
2. Автоматическое СМС оповещение должностных лиц о наиболее серьезных инцидентах (угрозах).

3. Автоматизацию набора сотовых и стационарных телефонных номеров, а также абонентов оперативной радиосвязи в рамках выполнения пошаговых инструкций по реагированию на инцидент (извещение как один из шагов инструкции по реагированию).
4. Автоматическое формирование и пересылка отчетов по инцидентам по электронной почте.
5. Запись телефонных разговоров с привязкой фонограмм к инцидентам.

В последние годы прослеживается тенденция передачи потенциально опасных и критически важных объектов под охрану частным охранным предприятиям или ведомственной охране. Помимо достоинств передача охраны на аутсорсинг имеет и негативные факторы:

1. предприятие лишается влияния на кадровую политику организации осуществляющей охрану объекта;
2. ротация кадров, применяемая охранными организациями, может привести к ситуации, когда сотрудник охраны, заступивший на дежурство, не владеет инструкциями по действиям в различных нештатных ситуациях на данном предприятии.

Перечисленные выше функции системы управления безопасностью ESM обеспечат вывод на каждую нештатную ситуацию пошаговой инструкции по ее эффективному разрешению, что снижает требования к уровню подготовки персонала охраны. А наличие системы регистрации действий операторов ТСО по реагированию на инциденты обеспечит:

- выявление отклонений в действиях операторов ТСО от инструкции в режиме реального времени, что позволит вовремя вмешаться и не допустить выхода ситуации из-под контроля;
- выявление операторов ТСО с недобросовестным отношением к работе, пытающихся упростить себе работу предоставляя системе заведомо ложные сведения с созданием доказательной базы их профнепригодности.

Ложные тревоги, как одна из причин снижения эффективности системы физической защиты

По статистике в системах охраны коммерческой и частной недвижимости до 90% тревожных событий являются ложными. В системе охраны крупного предприятия имеющего систему защиты периметра протяженностью несколько километров процент ложных тревог еще больше.

Ниже приведены некоторые причины возникновения ложных тревог:

1. ложные тревоги, связанные с несовершенством средств обнаружения (низкая помехозащищенность);
2. ложные тревоги, связанные с некачественным монтажом (плохой контакт, выбор неправильного места установки извещателей);
3. ложные тревоги, связанные с условиями эксплуатации (разбитые окна, насекомые, грызуны);
4. ложные тревоги периметральной охранной сигнализации, работающей в условиях естественных помех (усиливается неправильным подбором средств обнаружения);
5. ложные тревоги охранной сигнализации, вызванные забывчивостью или невнимательностью персонала (открытие не снятых с охраны помещений, сдача под охрану помещений с животными);
6. ложные тревоги, вызванные неправильными действиями сотрудников охраны (несвоевременное снятие с охраны или ошибочное взятие под охрану помещений с людьми);
7. ложные тревоги видеодетекторов движения и средств видеоанализа;
8. удержание персоналом дверей, оборудованных системами контроля и управления доступом;
9. ложные срабатывания пожарной сигнализации по причине запыленности дымовых извещателей и по причине электромагнитных помех;
10. ложные тревоги, вызванные отключением электроснабжения или скачками напряжения.

Указанные выше причины приводят к тому, что количество ложных тревог достигает критического уровня, при котором бдительность сотрудников охраны снижается настолько, что они перестают реагировать на тревожные сообщения, обычно реагирование ограничивается беглым взглядом на монитор системы видеонаблюдения (при наличии в этой зоне камер) и сбросом тревоги.

Как не парадоксально звучит, но выполнение требований по антитеррористической защищенности объектов, приведет к снижению эффективности системы защиты, вызванному резким увеличением процента ложных тревог. Увеличение процента ложных тревог происходит по следующим причинам:

1. за счет увеличения количества средств обнаружения, которые являются источниками ложных тревог (если раньше периметр объекта не был защищен, то от него не поступало ложных тревог, при оборудовании периметра в 2 рубежа можно ожидать, что количество ложных тревог будет вдвое больше, по сравнению с однорубежной охраной);
2. за счет уменьшения количества несанкционированных проникновений с целью хищения и других правонарушений, по причине создания образа высокой защищенности объекта.

Если раньше на каждые 100 тревожных событий фиксировалось два несанкционированных проникновения, то процент ложных тревог составлял 98/(98+2) или 98%. Если при выполнении антитеррористических мероприятий количество технических средств обнаружения, а, следовательно, и ложных тревог увеличится вдвое, а количество нарушений криминального характера снизиться в 5 раз, то процент ложных тревог будет составлять 196/(196+0,4) или 99,7%.

Приведенный пример доказывает, что реализация антитеррористических мероприятий для галочки (без применения мероприятий, направленных на повышение эффективности системы безопасности) приведет к повышению как количества, так и процента ложных тревог до недопустимого уровня, что в итоге станет причиной дискредитации системы в глазах сотрудников охраны.

Снижение количества ложных тревог

Помимо выбора средств обнаружения с высокой помехоустойчивостью снижение количества ложных тревог достигается за счет:

1. корреляции данных и оценки уровня достоверности сигналов;
2. автоматической компенсации погодных явлений для периметральных средств обнаружения различных производителей;
3. автоматического оповещения сервисных служб о необходимости технического обслуживания и активации инцидентов, связанных с неисправностью или низким качеством работы системы.

Корреляция данных и оценка уровня достоверности сигналов

Использование принципа корреляции данных позволяет за счет повышения количества технических средств не только значительно (не менее чем на порядок) снизить количество ложных тревог, но и повысить обнаруживающую способность всех технических средств.
Это достигается за счет средств поиска в системе взаимосвязанных событий путем сопоставления информации из разных источников и объединения последовательности событий, принадлежащих одной ситуации в учетную карточку инцидента.

В алгоритме корреляции информации участвуют следующие данные:

- сигналы от технических средств обнаружения;
- сигналы от видеодетекторов движения и средств ситуационного видеоанализа;
- информация о погодных условиях с метеостанции;
- информация от оператора ТСО о подтверждении/опровержении информации, полученной с использованием средств видеонаблюдения или сообщений от группы быстрого реагирования.

Корреляция данных обеспечивает оценку достоверности информации путем комплексного анализа сигналов от указанных источников. Достоверность информации влияет на вид отображаемой информации и возможности оператора по реагированию на данную тревогу.

В таблице представлена информация по корреляции данных системы защиты периметра.

Данные участвующие в корреляции	**Достоверность/ вид вывода информации**	**Возможности оператора по реагированию на тревогу**
Любой сигнал подтвержденный оператором	Высокая/ тревожное событие	Реагирование по сценарию «пресечение действий нарушителя»
Срабатывание двух рубежей охранной сигнализации, погодные условия в норме, по видео подтвердить не возможно	Высокая/ тревожное событие	Реагирование по сценарию «выезд тревожной группы для проверки ситуации»
Срабатывание одного рубежа и средств видеоанализа, погодные условия в норме, по видео подтвердить не возможно	Выше средней/ тревожное событие	Реагирование по сценарию «выезд тревожной группы для проверки ситуации»
Срабатывание двух рубежей охранной сигнализации либо одного рубежа и средств видеоанализа, плохие погодные условия которые могли стать причиной тревоги, по видео подтвердить не возможно	средняя/ тревожное событие	Реагирование по сценарию «выезд тревожной группы для проверки ситуации»
Срабатывание одного рубежа, плохие погодные условия которые могли стать причиной тревоги, по видео подтвердить не возможно	Ниже средней/ эмуляция срабатывания видеодетектора движения	Реагирование по сценариям: 1. «выезд тревожной группы для проверки ситуации» (при условии, что на видео не видны явные причины ложной тревоги) 2. регистрация ложной тревоги с обязательным указанием причины ложной тревоги, выявленной по видеоизображению
Срабатывание средств видеоанализа, погодные условия в норме, по видео подтвердить не возможно либо срабатывание одного рубежа, имеющего низкую достоверность сигнала	Низкая/ срабатывания видеодетектора движения	Реагирование по сценариям: 1. «выезд тревожной группы для проверки ситуации» (при условии, что на видео не видны явные причины ложной тревоги) 2. регистрация ложной тревоги указание причины ложной тревоги не обязательно
Срабатывание средств видеоанализа, плохие погодные условия которые могли стать причиной тревоги	Крайне низкая/ срабатывания видеодетектора движения	Реагирование по сценариям: 1. «выезд тревожной группы для проверки ситуации» (при условии, что на видео не видны явные причины ложной тревоги) 2. регистрация ложной тревоги указание причины ложной тревоги не обязательно

По событиям, имеющим достоверность от средней и выше, автоматически активируются инциденты с запуском пошаговых инструкций по их разрешению, оператор не имеет возможности их сбросить без реагирования. События с достоверностью ниже средней отображаются в виде видеоокна с кнопками принятия решения «Тревога», «Ложная тревога», «Требуется проверка», активация инцидента

производится в зависимости от принятого оператором решения, при этом сохраняется информация достаточная для проверки правильности принятого решения.
Мы создали систему, в которой человек является дополнительным источником данных (датчиком), которые могут в определенных пределах влиять на уровень достоверности событий, но если данные полученные от технических средств имеют высокую достоверность, то негативное влияние «человеческого фактора» исключается.

Автоматическая компенсация погодных явлений для системы охраны периметра

Компенсация погодных явлений используется для исключения ложных тревог при неблагоприятных погодных условиях и обеспечения высокой обнаруживающей способности при благоприятной погоде.

Иногда приходится слышать мнения специалистов, что компенсация погодных условий неприемлема для систем охраны. Но на деле подобные алгоритмы адаптивной подстройки уже применяются в технических средствах обнаружения с той лишь разницей, что они оперируют лишь силой помехи и не имеют понятия вызвана ли она погодой или ухищренными действиями нарушителя. Так, например, ограждение, оборудованное вибрационным средством обнаружения можно преодолеть без вызова сигнала тревоги если пособник нарушителя будет раскачивать сетчатое ограждение с нарастающей силой (раскачка ограждения с нарастающей силой приведет к тому, что алгоритмы адаптивной подстройки снизят чувствительность). Мы же предлагаем ввести обратную связь именно с силой ветра, дождя, града, что приведет к тому, что раскачивание ограждение в безветренную погоду приведет к выдаче сигнала тревоги.

Настройка технических средств обнаружения на объектах проводится таким образом, чтобы оно не выдавало ложных тревог при неблагоприятных условиях эксплуатации и, к сожалению, делается это за счет снижения чувствительности в благоприятных условиях. Так, например, радиоволновое однопозиционное средство настраивается таким образом, чтобы не выдавало ложных тревог в сильный ветер при высоте травы, допустим 30 см, но это приводит к тому, что нарушитель преодолевающий рубеж слишком медленно может остаться незамеченным. Введение компенсации в этом случае позволит повысить чувствительность в периоды когда сила помехи незначительна (при условии регулярного покоса травы или в безветренную погоду).

Другими словами мы предлагаем ввести обратную связь, назначение которой не снижать чувствительность при неблагоприятных условиях, а наоборот **повышать чувствительность при благоприятных условиях** эксплуатации.

Предлагаемая нами система предназначена для компенсации погодных явлений для технических средств обнаружения различных производителей. В состав системы защиты периметра, могут входить следующие средства измерения внешних помеховых факторов:

1. Метеостанция

Предназначена для измерения температуры, направления и силы ветра (м/с), интенсивности дождя (мм/ч), интенсивность града (удар/см2/ч). Участвует в корреляции данных от технических средств обнаружения, на которые оказывают влияние погодные факторы, такие как: вибрационные и сейсмические извещатели, радиолучевые и радиоволновые извещатели в сочетании с доплеровским измерителем помех от

растительности, видеодетекторы движения и средства видеоанализа. Также участвует в сезонной подстройке вибрационных извещателей для компенсации изменения жесткости кабельных чувствительных элементов.

2. Термоизмерительный зонд

Предназначен для измерения глубины промерзания почвы. Участвует в сезонной подстройке сейсмических извещателей.

3. Доплеровский измеритель помех от растительности

Предназначен для измерения силы помех от растительности (травы, кустарников и т.п.). Участвует в корреляции данных от технических средств обнаружения, на которые оказывают влияние колебания травы под действием ветра, таких как радиолучевые и однопозиционные радиоволновые извещатели. Дополнительно может использоваться для активации задачи (инцидента) «необходимость покоса травы».

Другие меры снижения количества ложных тревог для системы охраны периметра

Система охраны периметра наиболее сильно подвержена дестабилизирующим факторам внешних условий эксплуатации и является наиболее значимым источником ложных тревог в ИСБ. В данном разделе мы опишем другие меры снижения количества ложных тревог, которые могут применяться в системе управления безопасностью ESM.

В последнее время появляется значительное число технических средств обнаружения обеспечивающих точную локализацию места вторжения нарушителя, к числу таких систем относятся:

1. Волоконно-оптические вибрационно-сейсмические системы обнаружения, Сокол и др.
2. Вибрационные системы обнаружения на основе кабельного чувствительного элемента, INTREPID MicroPoint
3. Вибрационные системы обнаружения на основе адресных вибродатчиков, Peridect и др.
4. Однопозиционные радиоволновые извещатели, Зебра.
5. Средства ситуационного видеоанализа.

Отличительной особенностью данных технических средств обнаружения помимо выдачи точного места проникновения нарушителя, что позволяет более эффективно использовать управляемые видеокамеры и тепловизоры для оценки тревожных сигналов, также является более высокая помехоустойчивость. Высокая помехоустойчивость достигается за счет того, что сигнал анализируется отдельно для каждого короткого участка протяженностью от 1 до 10 м, а, следовательно:

- Отсутствует эффект усиления помехи, когда помехи от каждого контролируемого метра суммируются.
- Повышается помехоустойчивость от широкофронтовых помех, таких как ветер, дождь, град, ЖД транспорт, автомагистрали, которые действуют одновременно на протяженные участки. Помехоустойчивость достигается за счет

сопоставления сигналов с соседних участков, сигнал тревоги формируется только если обнаружено точечное воздействие. (Реализуется внутренними алгоритмами извещателя или алгоритмами корреляции информации системы).

Система управления безопасности ESM обеспечивает поддержку технических средств обнаружения с точной локализацией места вторжения различных производителей.

Низкое качество информации, как одна из причин низкой эффективности системы физической защиты

Сигналы от систем безопасности являются неоднозначными. Тревога на периметре может быть связана с действиями нарушителя, а может быть связана с плохими погодными условиями. Тревога охранной сигнализации может быть связана с проникновением нарушителя, а может быть связана с забывчивостью сотрудника вошедшего в не снятое с охраны помещение. Сигналы от видеодетекторов движения и ситуационной видеоаналитики имеют значительно меньший уровень достоверности по сравнению с системами сигнализации.

Все это позволяет сделать вывод о том, что сигналы от ИТСО, без дополнительной обработки не несут достаточной и достоверной информации для анализа ситуации на объекте и эффективности принятых мер по реагированию на нештатные ситуации.

В основной массе интегрированных систем безопасности информация от систем безопасности направлена на оператора ТСО, действия которого практически невозможно проконтролировать. От оператора ТСО требуется лишь вовремя принять сигнал тревоги, а дальнейшие действия по оценке ситуации и реагированию на тревогу отдаются ему на откуп.

При помощи отчета типовой интегрированной системы безопасности можно получить информацию, что оператор Иванов в 2 раза быстрее оператора Петрова принимает тревожные сигналы. Но значит ли это, что оператор Иванов выполняет свои обязанности лучше?

При помощи другого отчета можно получить информацию, что система защиты периметра за прошлый месяц срабатывала 157 раз, но при этом в отчетах нет информации о причинах срабатывания, нет информации по каким тревогам на место выдвигалась группа быстрого реагирования, а по каким нет и по каким причинам было принято то или иное решение. Насколько полезна информация о количестве тревожных событий, произошедших по непонятным причинам и с неизвестной реакцией охраны на них?

Очень часто информация о нарушениях появляется в ходе выполнения сотрудниками сил охраны своих должностных обязанностей (в ходе видеонаблюдения, патрулирования, получения информации об угрозах анонимно или от очевидцев). Силы охраны принимают решения о порядке реагирования на данные угрозы. Но отчеты системы безопасности не содержат никакой информации о данных инцидентах и принятых по ним мерам.

Мы создали систему, которая решает все перечисленные недостатки, скачок повышения качества информации достигается за счет:

1. регистрации информации и сигналов от всех систем в единой учетной карточке инцидента, при этом отсутствует перемешивание информации принадлежащих различным инцидентам;
2. записи фонограмм переговоров оператора ТСО с силами охраны;
3. продуманного опроса оператора ТСО о зарегистрированной нештатной ситуации или причинах ложной тревоги;

4. быстрой активации инцидентов оператором ТСО при помощи меню или специализированной клавиатуры, с последующей автоматизацией оперативного реагирования и сбора информации об инцидентах;
5. регистрации выполненных мер, направленных на локализацию и ликвидацию нештатной ситуации и проверку соответствия принятых мер пошаговым инструкциям.

Данные средства делают работу операторов более интеллектуальной, убирают из работы элементы монотонности, но в тоже время имеющиеся средства помощи при принятии решений и качество информации НЕ делают работу оператора чрезмерно сложной.

Интерфейс программного обеспечения устроен таким образом, чтобы максимально упростить (форма с чекбоксами (галочками) и выпадающими списками) и автоматизировать процесс регистрации информации с минимальным отвлечением оператора во время нештатной ситуации.

Система позволяет проводить оценку уровня значимости (срабатывание охранной сигнализации на критическом элементе имеет больший уровень критичности, чем срабатывание охранной сигнализации во второстепенном помещении) и достоверности данных (сигнал охранной сигнализации, подтвержденный срабатыванием видеодетектора, имеет больший уровень достоверности по сравнению со срабатыванием только одного технического средства). При этом активация опроса оператора ТСО может выполняться только по событиям с уровнем значимости (критичности) и уровнем достоверности выше установленного значения.

Наша система позволит сохранить для последующего анализа достаточный объем качественной информации об инциденте и ходе его разрешения, которая, например, позволяет сформировать отчеты:

- по инцидентам, выявленным силами охраны (по которым не было сигналов от технических средств охраны)
- по количеству ложных тревог, вызванных метеоусловиями;
- по количеству тревог, зафиксированных одновременно не менее чем двумя техническими средствами обнаружения, с результатами их проверки;
- по количеству тревог, произошедших по невыясненным обстоятельствам;
- по количеству тревог, по которым на место выдвигалась группа быстрого реагирования с результатами осмотра местности;
- по количеству тревог, вызванных действиями нарушителя;
- по отступлению оператора ТСО от пошаговых инструкций по реагированию;
- по попыткам оператора зарегистрировать тревожную ситуацию с высоким уровнем достоверности как ложную без указания причин.

Данные отчеты могут быть использованы:

1. Для периодической выборочной проверки с целью выявления наиболее подготовленных операторов ТСО, которым можно доверить более ответственное направление, а также выявления операторов с недобросовестным отношением к работе с созданием доказательной базы их профнепригодности.

2. Для своевременной и точной постановки задач по выполнению технического обслуживания и оценки качества технического обслуживания.
3. Для выработки рекомендаций по совершенствованию систем безопасности, а также организационных мероприятий с целью снижения количества ложных тревог.
4. Для выработки рекомендаций по совершенствованию инструкций по реагированию с целью повышения эффективности мер по локализации и ликвидации нештатных ситуаций.

Несвоевременное и некачественное обслуживание, как одна из причин снижения эффективности системы физической защиты

Системы безопасности являются сложными программно-аппаратными комплексами, и для поддержания их в работоспособном состоянии требуется выполнять не только техническое обслуживание элементов системы, но и обслуживание территории на которой расположены технические средства обнаружения (скашивание травы, вырубка кустарника, натяжение АКЛ, ремонт ограждения и т.п.).

Несвоевременное или низкое качество выполнения работ по техническому обслуживанию систем и текущему обслуживанию территории способно снизить эффективность даже самой современной и качественной интегрированной системы безопасности.

Для поддержания технического обслуживания на высоком уровне предлагаемая нашей компанией система управления безопасности ESM имеет следующие функции:

1. Автоматическое вычисление увеличения количества ложных тревог с предложением активировать режим «необходимость технического обслуживания».
2. Доплеровский измеритель помех от растительности с предложением активировать режим «необходимость покоса травы».
3. Использование технологии управления инцидентами для контроля своевременности выполнения технического обслуживания и сохранения отчетов о выполненных в рамках технического обслуживания работах.

Ниже приведен пример алгоритма работы системы контроля качества обслуживания:

1. Количество тревожных сигналов от технического средства обнаружения резко превышает статистические данные.
2. Система предлагает, а ответственное лицо (начальник сектора ИТСО или другое) активирует инцидент «необходимость технического обслуживания» (инцидент имеет низкий уровень приоритета), при необходимости выбирается уровень важности и срочности задачи.
3. Производится оповещение обслуживающей организации по электронной почте с указанием зарегистрированных событий, ставших причиной активации инцидента.
4. Активируется режим ожидания технического обслуживания, например, 3 дня.
5. За один день до окончания срока ожидания производится оповещение о наличии открытого инцидента.
6. После выполнения работ по техническому обслуживанию инциденту присваивается статус «Решен», а после привязки к карточке инцидента акта выполненных работ инцидент закрывается.
7. При просроченном времени формируется соответствующее сообщение.

Оперативная адаптация политик безопасности под уровень угрозы, как одна из причин повышения эффективности системы физической защиты

Добиться повышения безопасности объекта можно за счет введения политики безопасности с жесткими правилами, но подобные меры будут мешать нормальному функционированию и жизнедеятельности объекта, а также приведут к увеличению нагрузки на силы охраны. Наиболее целесообразна реализация такой системы, которая в повседневном режиме будет решать базовые задачи обеспечения безопасности, но при этом не будет мешать нормальному функционированию объекта, но которая в случае необходимости может быть быстро переведена в режим повышенной боевой готовности.

После событий 11 сентября 2001 года в США была разработана система так называемых уровней террористической угрозы. Система состоит из пяти уровней, различающихся по цветам, - зеленого, синего, желтого, оранжевого и красного. Наименьшую степень опасности, соответствующую повседневной норме, обозначает зеленый цвет, наивысшую - красный (синий уровень соответствует призыву быть настороже, желтый характеризуется как серьезный, оранжевый - как критический). Подобные многоуровневые системы террористической угрозы действуют и в других странах таких как Великобритания, Израиль, Индия, Испания, Франция, Япония.

В России установлена 3-х уровневая система террористической опасности, предусматривающая установление уровней террористической опасности: повышенный - "синий", высокий - "желтый", критический - "красный". Во многих странах действуют аналогичные многоуровневые системы террористической опасности

В транспортной безопасности также предусмотрено 3-и уровня безопасности: первый уровень – защита от потенциальных угроз, второй уровень – защита от непосредственных угроз, третий уровень – защита от прямых угроз.

Мировой и отечественный опыт подтверждает то, что правила безопасности должны адаптироваться под действующий в данный момент времени уровень угрозы. Функции управления уровнями безопасности (Security Level Management) представлены в решениях ведущих мировых брендов, представляющих ИСБ, таких как Bosch, Nedap, Siemens.

Система управления безопасностью ESM обеспечивает адаптацию политики безопасности под уровень угрозы объекту (повседневный, высокий, критический) в режиме реального времени, для чего предусмотрена возможность создания нескольких вариантов настроек системы и возможность их быстрой активации.

Изменение уровня безопасности является одной из мер реагирования на критический инцидент или используется для усиления уровня защиты объекта при усилении террористической активности в регионе или наличии сведений об угрозе безопасности объекта или планируемых мероприятиях по проверке антитеррористической защищенности. Изменение уровня безопасности может сопровождаться:

1. Рассылкой должностным лицам извещений об изменении уровня безопасности.
2. Автоматическим изменением алгоритма доступа на объект и(или) его критические элементы (автоматический доступ / доступ после фотоверификации, вход

посетителей с сопровождающим / без сопровождающего, правило двух лиц, ограничение доступа в нерабочее время).

3. Активацией дополнительных рабочих мест операторов ТСО, связанного с возрастанием нагрузки на операторов.
4. Активацией дополнительных эшелонированных рубежей охраны за счет контроля дополнительных охранных средств которые не используются в повседневном режиме по причине большого количества сигналов оказывающих чрезмерно высокую нагрузку на операторов, например, детекторов движения видеокамер, расположенных на подступах к критическим элементам или на предполагаемых маршрутах движения нарушителя.
5. Автоматическим изменением целевого предмета поиска у арочных металлодетекторов, например, пистолет Макарова (повседневный режим), револьвер (высокий уровень угрозы), небольшой револьвер из нержавеющей стали или алюминиевого сплава (критический уровень угрозы). (Подобные возможности по запросу нашей компании реализованы в арочных металлодетекторах Паутина-М6, Паутина-М48, Паутина-М192.)
6. Автоматическим контролем режима охраны критических элементов объекта.
7. Автоматическим изменением чувствительности и алгоритмов обработки сигналов (логическое «И» / «ИЛИ», компенсация погоды) системы защиты периметра с целью перераспределения приоритетов в сторону повышения вероятности обнаружения или снижения количества ложных тревог.
8. Автоматическим изменением графиков и маршрутов патрулирования и автоматическим контролем их соблюдения.

Краткая справка о компании

ООО ПСЦ «Электроника» - российский разработчик и поставщик высокотехнологичных систем безопасности для объектов с повышенными требованиями к защищенности.

Технические решения компании используются для управления безопасностью стратегических объектов различных отраслей экономики: транспортного сектора, ТЭК, промышленности, в том числе оборонной, банковской сферы, сферы торговли и обслуживания, крупных объектов культуры и спорта и др.

За 20 лет работы компанией выполнено свыше 1000 проектов различной сложности в 23 регионах России и зарубежья, для 90 корпоративных заказчиков, многие из которых являются лидерами в своих отраслях.

Направления работы:

- Консалтинг в области комплексной защиты объектов: оценка уязвимости, разработка модели защиты и концепции системы безопасности.
- Проектирование, установка и обслуживание комплексных систем управления безопасностью на объектах с повышенными требованиями к режиму.
- Разработка новейших инженерно-технических решений в области интеграции и управления системами безопасности стационарных и подвижных объектов.

Специализация компании — выполнение комплексных проектов «под ключ»: от разработки концепции системы безопасности до ее внедрения на объекте.

Контактная информация

150001 г. Ярославль, ул. Большая Федоровская, 75
Телефон: + 7 (4852) 66-00-15
marketing@electronika.ru
www.electronika.ru