Промышленная безопасность: комплексный подход

Разнообразные системы безопасности – от подсистем контроля доступа и видеонаблюдения до ограждений по периметру объекта и системы IT-безопасности – являются в настоящее время неотъемлемой частью стратегии автоматизации производственных предприятий. В статье рассматриваются меры по организации комплексного использования этих средств для эффективной защиты предприятия как в виртуальном, так и в физическом пространстве.

Традиционно различные мероприятия по обеспечению безопасности использовались независимо друг от друга. Например, датчик движущихся объектов, установленный на линии ограждения, подает охраннику сигнал тревоги. Если опасность покажется ему серьезной, охранник по рации предупреждает об этом операторов.

Однако, более совершенный, комплексный подход к обеспечению безопасности предприятия предполагает создание нескольких уровней защиты, позволяющих предупреждать, обнаруживать и предотвращать любые потенциальные угрозы.

Так, в упомянутом случае, при обнаружении системой внешнего видеонаблюдения признаков подозрительного поведения на линии ограждения будет подан сигнал тревоги для предупреждения одновременно и персонала охраны, и операторов. Через считанные секунды и охранник, и оператор смогут наблюдать происходящее на экране видеомонитора. Оператор сможет сразу остановить все критически важные процессы, осуществляемые в зоне предприятия, оказавшейся под угрозой, а охранник – настроить систему контроля допуска для предотвращения несанкционированного проникновения на территорию объекта.

По мере наступления эры "умных" предприятий процесс интеграции между системами управления технологическими процессами и системами безопасности будет расширяться. Это не только позволит оптимизировать производство, но также поможет повысить уровень общей безопасности. В дополнение к функции наблюдения за производственными объектами идеальное решение должно включать следующие возможности:

- идентификацию личности и наблюдение за лицами, входящими на территорию предприятия или ее покидающими;
- отслеживание перемещений всех лиц, находящихся на объекте;
- контроль доступа в закрытые зоны;
- отслеживание и определение местоположения оборудования, объектов производства и иных ресурсов;
- определение, в случае чрезвычайного происшествия, местонахождения всех работников, присутствующих в данный момент на объекте;
- защиту сетей и систем, обеспечивающих автоматизацию технологических процессов, от кибератак;
- упреждающее реагирование на сигналы тревоги и происходящие события;
- коллективный доступ к информации, позволяющий экономить средства предприятия.

Пять шагов к созданию комплексной системы автоматизации предприятия

Долгое время основной задачей системы безопасности завода считалось сокращение количества краж. Однако, сегодня фокус проблем, связанных с безопасностью, сместился в сторону предотвращения последствий внешних угроз и обеспечения безопасности жителей близлежащих микрорайонов.

Чтобы эффективно защитить предприятие, руководство должно придерживаться принципа "от центра к периферии". Система безопасности завода должна начинаться с сердца предприятия (сети, обеспечивающей управление технологическими процессами) и постепенно надстраиваться дополнительными уровнями защиты, простирающимися вплоть до границ объекта. Таким образом, если одна из мер не срабатывает, существуют другие, способные ее подстраховать. Чтобы достичь такой многоуровневой системы защиты, необходимо выполнить следующие пять шагов:

1. провести оценку уязвимости объекта;
2. определить имеющиеся системы безопасности;
3. наметить шаги по уменьшению отрицательных последствий;
4. внедрить систему;
5. провести повторную оценку.

Проведение оценки уязвимости объекта

В области промышленной безопасности, к сожалению, не существует универсального решения. На каждом объекте имеются свои многочисленные переменные, которые необходимо принимать во внимание – от физического местоположения предприятия до вида выпускаемой продукции, так как все они могут повлиять на выбор варианта решения. Поэтому первым шагом в разработке архитектуры любой системы безопасности должна стать оценка возможных уязвимых мест и анализ возникающих в результате рисков. Стратегии, разрабатываемые на основе проведенной оценки, зависят от характерных особенностей конкретных объектов, а также от бизнес-целей компаний, которые их эксплуатируют.

Цель оценки уязвимости объекта (ОУО) состоит в определении возможных слабых мест в общей системе безопасности предприятия и выборе оптимальных путей ее улучшения. На проведение стандартной процедуры ОУО уходит около месяца.

В ходе процедуры ОУО очень важно исследовать взаимосвязь между общей и технической безопасностью, а также безопасностью в физическом и виртуальном пространстве. Нарушение системы защиты представляет угрозу для эксплуатационной безопасности предприятия, поэтому важно рассмотреть шаги, которые может предпринять обслуживающий персонал для уменьшения отрицательных последствий.

Важность кибербезопасности

Процедура оценки уязвимости не должна ограничиваться мерами обеспечения физической безопасности. Она должна установить исходные данные, касающиеся действующих на предприятии процессов, процедур и мер защиты, направленных на обеспечение кибербезопасности и используемых для защиты сети управления технологическими процессами (СУТП) от внешних угроз.

СУТП является одной из самых критически важных зон любого производственного объекта и одновременно может стать одной из самых уязвимых мишеней для атак со стороны нарастающего компьютерного терроризма. Киберугрозы можно подразделить на четыре категории:

- Неспецифические и потенциально деструктивные угрозы. Это наиболее распространенный вид угроз, с которыми сталкиваются промышленные предприятия и индивидуальные пользователи всего мира. Данная категория включает в себя вирусы, троянские программы и компьютерные черви.
- Атаки, направленные на подрыв работоспособности системы, и потенциальные проблемы, связанные с техникой безопасности. Этот вид угроз связан с получением доступа в сеть обманным путем и DOS-атаками, приводящими к отказу от обслуживания, в результате чего сеть может наводниться ложными запросами, не дающими оператору возможности получить подлинный сигнал тревоги.
- Нарушение конфиденциальности. Еще один из наиболее распространенных видов киберугроз – перехват информации и взлом пароля, что позволяет хакерам добираться до конфиденциальных данных, например показателей деловой активности или рабочих параметров.
- Нарушение целостности и достоверности. Эта опасность возникает в том случае, если незваный визитер проникает на объект с целью умышленного искажения данных, действуя под видом законного пользователя.

Аналогично проводимой во время процедуры ОУО оценке рисков физической безопасности можно ранжировать уязвимые элементы СУТП, исходя из связанного с ними потенциального риска. Большинство объектов будут в этом случае рассматриваться как комбинация зон с низким и средним уровнем риска, и лишь ограниченное число зон будет иметь высокий уровень риска. Повышенная уязвимость некоторых объектов обусловлена слабой политикой в отношении безопасности или ее полным отсутствием. Проблемы, как правило, заключаются в плохом управлении паролями, отсутствии антивирусной программы или использовании устаревших ее версий, отсутствии обновлений системы безопасности для ОС, а также в неэффективности процессов, используемых в рамках политики обмена данными.

Определение шагов по уменьшению отрицательных последствий

После обнаружения уязвимых мест и определения их приоритетов необходимо наметить шаги по уменьшению отрицательных последствий потенциальных атак. Для каждого объекта меры будут разными, однако существует большое количество стандартных методов, которые доказали свою способность повышать уровень

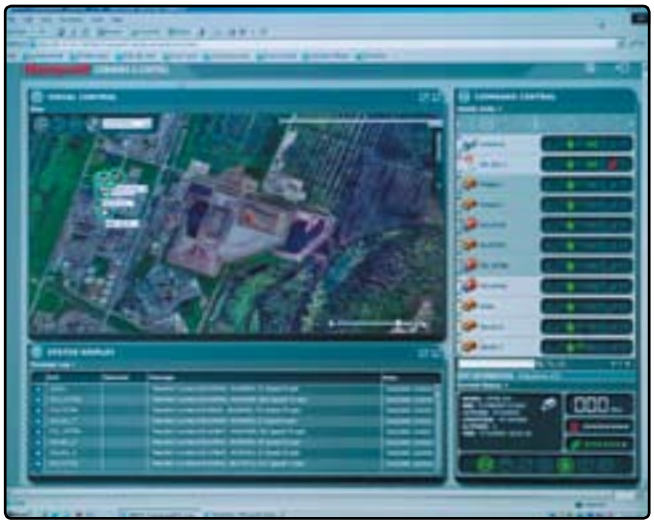
безопасности. Удачным примером использования таких средств может служить организация системы безопасности на заводе по производству спецматериалов в городе Джейсмар, штат Луизиана. Внедренная на этом предприятии система объединяет модернизированные системы безопасности с управлением технологическими процессами. Передовые методы, примененные на заводе в Джейсмаре, включают:

- многоуровневую систему защиты, которая обеспечивает использование замещающих средств безопасности, если один уровень подвергается риску. При таком подходе оказываются задействованными разные элементы технической защиты, например обнаружение проникновения по всему периметру территории объекта, контроль доступа, камеры наблюдения и радары, осуществляющие мониторинг приближающихся судов;
- сокращение количества и обеспечение постоянного режима безопасности всех входов. Если говорить о внешнем ограждении, то это может означать, что вход и выход людей осуществляется через один-единственный контрольно-пропускной пункт. На территории завода эта концепция может быть распространена на диспетчерское помещение, что будет гарантировать доступ в эту важную зону только лицам, обладающим соответствующим уровнем допуска;
- объединенные системы безопасности и управления технологическими процессами, что позволяет эффективно отслеживать все перемещения персонала. В случае нарушения безопасности или возникновения опасных производственных ситуаций оператор, управляющий технологическим процессом, может воспользоваться средствами радиочастотной идентификации, камерами и устройствами считывания информации с персональных карточек для определения местонахождения сотрудников, которым грозит опасность.

Внедрение системы

Комплексные системы позволяют обслуживающему персоналу лучше ориентироваться на территории предприятия, а также предоставляют возможности для более эффективного взаимодействия и реагирования на внештатные ситуации, что помогает уменьшить риски, связанные с угрозой безопасности. Для беспрепятственного процесса внедрения на этапе объединения системы безопасности и производственных систем необходимо использовать распределенную архитектуру сервера (Distributed Server Architecture, DSA). На заводе в Джейсмаре системы контроля зданий и системы управления технологическими процессами используют один и тот же сервер DSA, что позволяет системам управления технологическими процессами, системам контроля зданий и системам безопасности иметь объединенный доступ к данным, сигналам тревоги и изображениям, получаемым с камер видеонаблюдения.

Одним из важнейших требований для успешной интеграции является способность объединить системы сторонних производителей. Без такого стандарта, каким является архитектура DSA, практически невозможно добиться эффективного взаимодействия, позволяющего персоналу объекта лучше ориентироваться в вопросах безопасности.



Помимо интеграции данных и сигналов тревоги архитектура DSA позволяет осуществлять свободную стыковку. Это означает, что заказчики могут свободно обновлять какую-либо систему без необходимости модернизации всего оборудования. Таким образом, архитектура DSA не только служит коммуникационным механизмом для совместного анализа информации всеми системами, но и позволяет предприятиям гибко планировать модернизацию этих систем.

Расчет комплексной эффективности инвестиций

Обычно обоснование затрат на такой сложный объект, как комплексная система обеспечения управления технологическими процессами и безопасности, входит в сферу компетенции руководителей предприятия.

Один из результатов, который можно проверить путем проведения повторной оценки, – уменьшение риска. В некоторых случаях предприятие может получить более низкую страховую ставку, если докажет, что ему удалось значительно снизить риски, связанные с вопросами безопасности. Если говорить с этой точки зрения о предприятиях химической промышленности, то они должны гарантировать, что их системы не отстают от постоянно эволюционирующих угроз и что их системы кибернетической и физической безопасности находятся под надлежащим контролем.

Объединение систем управления технологическими процессами и систем безопасности позволит уменьшить риск больше, чем это сделали бы независимые друг от друга системы, поскольку в чрезвычайной ситуации объединение обеспечивает более эффективное взаимодействие между службой безопасности и службой оперативного управления. Своевременное получение большего объема информации поможет предприятию повысить быстроту реагирования. Такое совместное владение информацией создает основу для превращения объекта в "умное" предприятие, все элементы которого находятся под надежной защитой.

Джон Хармон, Степан Гвоздик,
Honeywell Process Solutions

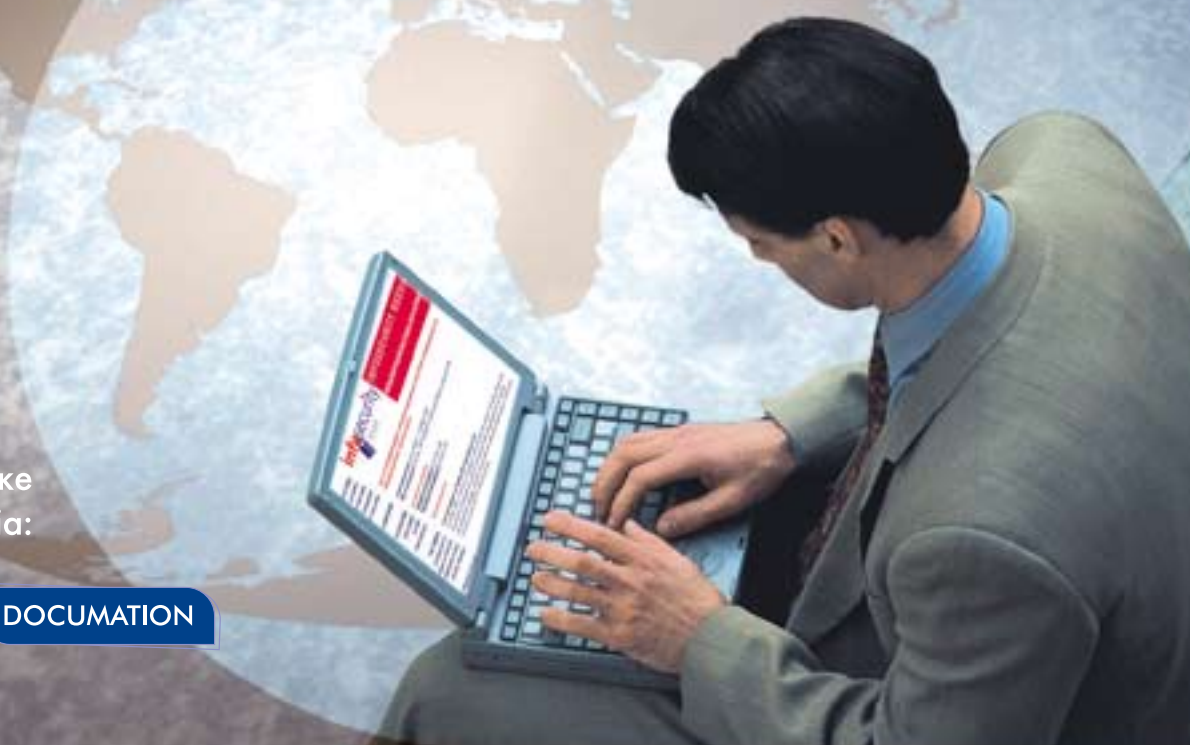
www.infosecuritymoscow.com

2009 infosecurity RUSSIA

6-я международная специализированная выставка-конференция по информационной безопасности

29 сентября – 1 октября 2009

МОСКВА, Экспоцентр на Красной Пресне
Павильон №7



Одновременно на одной площадке с Infosecurity Russia:

STORAGE EXPO

DOCUMATION

РАЗДЕЛЫ ВЫСТАВКИ

- Антиспам
- Антивирусы
- Безопасность приложений
- Биометрические системы
- Непрерывность бизнеса/восстановление бизнеса после катастроф
- Соответствие требованиям регуляторов и стандартам
- Системы мониторинга и фильтрации контента
- E-mail безопасность / Безопасность средств оперативной пересылки сообщений или Безопасность мгновенного обмена сообщениями (систем типа ICQ)
- Шифрование, PKI (инфраструктура открытых ключей), Цифровые сертификаты
- Межсетевые экраны (брандмауэры)
- Управление идентификацией и доступом
- Безопасность Интернет/сетевая безопасность
- Выявление и предупреждение вторжений
- Расследование компьютерных инцидентов
- Техническая поддержка/системы helpdesk
- Законодательство и стандарты/BS7799/Сертификация
- Сертификационные центры
- Управление внесением исправлений
- Тестирование безопасности системы путем имитации атак / Оценка риска и уязвимости
- Физическая безопасность
- Удаленный доступ
- Безопасность хранения данных
- Политика безопасности
- Маркеры доступа
- Обучение и повышение осведомленности в области безопасности
- Безопасность Веб-сервисов
- Система «Доступ за один шаг» (Single Sign-On)
- Смарт-карты
- Системы унифицированного управления защитой от угроз
- Безопасность IP телефонии
- VPN (виртуальные частные сети)
- Безопасность мобильных/беспроводных систем

ВЫСТАВОЧНОЕ ОБЪЕДИНЕНИЕ РЕСТЭК™

Reed Exhibitions®

Дирекция выставки:
Санкт-Петербург, Петрозаводская ул., д.12
Тел.: +7 (812) 320-8098, факс: +7 (812) 320-8090, E-mail: itcom@restec.ru