Threats of systems of video surveillance

Belozerova A.[1], Martynov, L.[2], Kovalev S.[3], Nazarova K.[4], Kozhevnikova I.[5], Ananyin E.[6], Popkov S.[7], Lysenko A.[8]

Угрозы систем видеонаблюдения

Белозёрова А. А.[1], Мартынова Л. Е.[2], Ковалев С. А.[3], Назарова К. Е.[4], Кожевникова И. С.[5], Ананьин Е. В.[6], Попков С. М.[7], Лысенко А. В.[8]

[1]Белозёрова Ангелина Андреевна / Belozerova Angelina – студент;
[2]Мартынова Лариса Евгеньевна / Martynova Larisa – студент;
[3]Ковалев Станислав Андреевич / Kovalev Stanislav – студент;
[4]Назарова Кристина Евгеньевна / Nazarova Kristina – студент,
кафедра информационной безопасности;
[5]Кожевникова Ирина Сергеевна / Kozhevnikova Irina – магистрант,
кафедра телекоммуникационных систем;
[6]Ананьин Евгений Викторович / Ananyin Evgeny – студент,
кафедра информационной безопасности;
[7]Попков Сергей Михайлович / Popkov Sergey – студент;
[8]Лысенко Александр Вячеславович / Lysenko Aleksandr – студент,
кафедра информационной безопасности,
Волгоградский государственный университет, г. Волгоград

Аннотация: *системы видеонаблюдения, по своей сути, это один из аспектов системы безопасности. CCTV на предприятиях могут достигать таких размеров, что часто представляют собой уникальные решения, разработанные для конкретного заказчика, и выполняют широкий спектр задач по контролю за процессами на производстве. Современные предприятия сталкиваются с самыми серьезными угрозами безопасности. Эти угрозы имеют как внутренние, так и внешние источники и по характеру делятся на умышленные нарушения и катастрофы и дестабилизирующие факторы случайного характера.*

Abstract: *systems of video surveillance, in essence, it is one of aspects of a security system. CCTV at the enterprises can reach such sizes that often represent the unique decisions developed for the specific customer and carry out a wide range of tasks of control of processes on production. The modern enterprises face the most serious threats to security. These threats have both internal, and external sources and on character are divided into deliberate violations and accidents and the destabilizing factors of casual character.*

Ключевые слова: *система видеонаблюдения, безопасность, отказоустойчивость, угрозы.*
Keywords: *system of video surveillance, safety, fault tolerance, threats.*

Системы видеонаблюдения, по своей сути, это один из аспектов системы безопасности. Видеонаблюдение – представляет собой систему визуального контроля за событиями, происходящими на охраняемой территории, с использованием специального оборудования. Следовательно, система видеонаблюдения (CCTV англ. TCOH – телевизионные системы охранного наблюдения), это комплекс, состоящий из специализированного оборудования (видеокамеры, видеорегистраторы, мониторы, всевозможные монтажные материалы и др.), а также программного обеспечения для комфортного подключения и просмотра.

CCTV на предприятиях могут достигать таких размеров, что часто представляют собой уникальные решения, разработанные для конкретного заказчика, и выполняют широкий спектр задач по контролю за процессами на производстве. При этом любая система видеонаблюдения состоит из следующих основных элементов:

- Сетевые видеокамеры.
- Сеть передачи данных.
- Линии передачи данных или СКС.
- Подсистема отображения.
- Электропитание.
- Подсистема обработки и хранения данных.
- Вспомогательное оборудование (кабели, кронштейны, кожухи).

Архитектура системы видеонаблюдения, в зависимости от размеров объекта, требований к видеонаблюдению и выделенного бюджета, может быть следующая:

1) «Камера – монитор». В такой системе видеокамера получает и передает аналоговый видеосигнал на монитор. Никакой цифровой обработки сигнала не происходит, так как в этом нет необходимости. Соединение осуществляется по коаксиальному (антенному) кабелю.

2) «Камера – цифровой регистратор – монитор». В данной системе происходит оцифровка видеосигнала. Эту задачу выполняет видеорегистратор. Оцифровка делается для: сжатия изображения для последующей записи и хранения; одновременной работы с несколькими видеокамерами, реализации дополнительных

функций (детекция движения, распознавание автомобильных номеров). Камера и цифровой регистратор соединяются также по коаксиальному кабелю.

3) «IP-камера – [ЛВС, Интернет] – [регистратор, ПК, сервер] – монитор». Данная схема позволяет создать распределенную цифровую систему видеонаблюдения (IP-видеонаблюдения) на базе стандартной сетевой архитектуры. Для анализа и обработки данных применяются современные информационные технологии. Подключение осуществляется по медному кабелю.

Правильно спроектированная и грамотно инсталлированная система видеонаблюдения должна обеспечивать достаточную степень отказоустойчивости и возможность незамедлительного восстановления нормального режима эксплуатации после устранения причины отказа. Тем не менее, как свидетельствует реальность, злоумышленные действия над информацией не только не прекращаются, а имеют достаточно устойчивую тенденцию к росту [1].

Забавно, что камеры наблюдения, которые служат первой линией безопасности в реальном мире, стали слабым звеном в виртуальном. Современные предприятия сталкиваются с самыми серьезными угрозами безопасности. Эти угрозы имеют как внутренние, так и внешние источники и по характеру делятся на умышленные нарушения и катастрофы и дестабилизирующие факторы случайного характера [2]. Последствия таких воздействий на систему видеонаблюдения могут быть весьма печальны, начиная с утечки персональной информации и нарушения коммерческой тайны и заканчивая нарушением работы систем жизнеобеспечения, что, в свою очередь, ставит под угрозу жизнь и здоровье граждан. Ведь сейчас достаточно часто система видеонаблюдения является частью единой системы автоматизации и безопасности объекта.

Большое количество угроз безопасности видеонаблюдения возникают ещё на этапе проектирования. Ошибки на этом этапе могут повлечь за собой серьезные материальные потери и прочие трудноразрешимые проблемы, причем их исправление часто становится просто невозможным, приходится создавать систему безопасности практически с нуля. Систематизировать типичные ошибки при проектировании CCTV предлагаю по следующим показателям:

1. установка камер:
2. линии связи;
3. приемно-контрольная аппаратура;
4. программное обеспечение.

При переходе с традиционных аналогово-цифровых систем на современное IP-видеонаблюдение основной угрозой может считаться возможность удаленного подключения, поскольку она не исключает риска проведения хакерских атак. Поэтому стоит уделить особое внимание безопасности локальной сети. Системы видеонаблюдения выбираются, разрабатываются и внедряются департаментами физической безопасности, которые обычно достаточно далеки от анализа современных IT-угроз. Департаменты IT и IT-безопасности в лучшем случае привлекаются на этапах подключения систем в сеть предприятия. Иногда даже для видеонаблюдения строятся отдельные каналы связи и отдельный выход в Интернет, которые тоже редко обеспечивают защиту в соответствии со стандартами безопасности предприятия.

Также к источникам угроз систем видеонаблюдения можно отнести антропогенные, техногенные и стихийные носители угроз.

1. Антропогенные источники угроз

Антропогенными источниками угроз безопасности выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорит о причинении ущерба. В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты, действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним можно отнести:

1) криминальные структуры;
2) потенциальные преступники и хакеры;
3) недобросовестные партнеры;
4) технический персонал поставщиков телематических услуг;
5) представители надзорных организаций и аварийных служб.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов. К ним относятся:

1) представители службы безопасности;
2) вспомогательный персонал (уборщики, охрана);
3) технический персонал.

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты.

2. Техногенные источники угроз

Данная группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако, последствия, вызванные такой деятельностью, вышли из-под контроля

человека и существуют сами по себе. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в современных условиях. Технические средства, являющиеся источниками потенциальных угроз безопасности, также могут быть внешними:

1) средства связи;
2) сети инженерных коммуникаций (водоснабжения, канализации);

и внутренними:

1) некачественные технические средства;
2) некачественные программные средства;
3) вспомогательные средства (сигнализации, телефонии).

3. Стихийные источники угроз

Эта группа источников угроз объединяет обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. Такие источники совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда. Стихийные источники потенциальных угроз безопасности видеонаблюдения, как правило, являются внешними по отношению к защищаемому объекту и под ними понимаются, прежде всего, природные катаклизмы:

1) пожары;
2) землетрясения;
3) наводнения;
4) ураганы;
5) различные непредвиденные обстоятельства;
6) необъяснимые явления.

Литература

1. *Цыбулин А. М.* Подход к построению автоматизированной системы управления информационной безопасностью предприятия // Вестник Волгоградского государственного университета. Инновационная деятельность ,2011. № 5. 86 с.
2. *Аткина В. С.* Оценка эффективности катастрофоустойчивых решений // Вестник Волгоградского государственного университета. Серия 10: Инновационная деятельность, 2012. № 6. С. 86-92.