Современные технологии СКУД развиваются не только в области создания новых карт доступа, усовершенствования турникетов или замков. Расширяется область применения СКУД, переходя на новые сферы бизнеса. Например, контроль доступа к программным и аппаратным средствам вычислительной техники.

Каждый день мы читаем в новостных лентах о хакерских атаках, краже информации и взломе компьютерных систем. А способы защиты от этого уже много лет принципиально не меняются. Все как в известной фразе: «Повторение одних и тех же действий с целью получить иной результат». Десять лет назад нам стало понятно, что иного результата на этом пути не будет, и мы разработали систему контроля доступа к информационным системам - XVmatic, которая объединяет в себе и физическую, и информационную защиту, и контроль выполнения административных правил, основанный на алгоритмах искусственного интеллекта. Именно такие системы могут дать достойный ответ современным вызовам.

Технологии, применяемые в системе контроля доступа к программным и аппаратным средствам вычислительной техники XVmatic

1. Технология работы под контролем
1. Сценарий "4-х глаз"

Одновременная работа на одном АРМ двух сотрудников, один из которых оператор, а другой — контролер. Если контролер или оператор покинет помещение, в котором находится АРМ, сеанс автоматически прерывается.

1.
1. Работа под контролем дежурного службы безопасности

Постоянный мониторинг действий пользователя посредством видеокамеры, расположенной перед оператором, и устройства захвата изображения на экране компьютера. В дежурной службе отображается: текущее изображение экрана, фотография сотрудника из базы данных и реальное изображение, полученное с видеокамеры. Если у оператора дежурной службы возникают какие-либо подозрения или сомнения в правомерности действий пользователя АРМ, он может удаленно отключить компьютер и разобраться в инциденте.

1.

1. Удаленный контроль руководителем

Данный вид контроля может осуществляться как за действиями операторов АРМ, так и за действиями дежурной службы в экстренных ситуациях.

1.

1. Автоматизированный контроль

Используются технические средства IDmatic и XViewsion, в том числе контроль доступа в помещения, биометрическая верификация, видеонаблюдение, управление процессами, регламентами и сценариями.

1. Полное физическое разделение системы доступа к информации и защищаемой вычислительной среды ЦОД

Система XVmatic физически отделена от защищаемого ЦОД. Нет никаких цифровых интерфейсов, связывающих обе системы. При этом осуществляется контроль доступа, биометрическая верификация, мониторинг работы и целостности защищаемых средств вычислительной техники. Такой подход позволяет даже теоретически исключить возможность занесения в защищаемую среду зловредов или вирусов.

1. Технология процессов, регламентов и сценариев

Сертифицированные средства всегда имеют правила их использования. Например, пароль нельзя передавать другому пользователю. Однако эти правила существуют только на бумаге и имеют только административную силу. Управление процессами и регламентами в системе XVmatic позволяет сделать физически невозможным нарушение этих правил.

1. Технология бинарной защиты информации

Защищаемая система разделяется на два или несколько компонентов, каждый из которых не представляет угрозу с точки зрения защиты информации. Для выполнения рабочих процессов эти компоненты объединяются системой XVmatic по заданным регламентам и сценариям на базе алгоритмов искусственного интеллекта.

1. Технология непрерывного мониторинга парольной защиты

Режим распознавания лица применяется в системе XVmatic не только для

биометрической идентификации сотрудника при входе в систему, но и для периодического распознавания лица с целью подтверждения личности оператора. Кроме этого, на рабочее место оператора настроен детектор присутствия подсистемы видеонаблюдения XViewsion. Если оператор покидает рабочее место, через заданный временной интервал АРМ блокируется. При этом не происходит прерывания программы работы ЦОД.

1. Технология объединения процессов управления и контроля доступа в виртуальном и физическом мире

Доступ к АРМ осуществляется подсистемой IDmatic по профилю, в котором учитывается время доступа, номер помещения, номер АРМ, номер радиокарты, пароль, биометрические и личные данные пользователя. Эти параметры однозначно идентифицируют сотрудника в физическом мире по биометрическим признакам и связывают по паролю и логину его действия в виртуальном мире программных кодов.

1. Технологии информационного следа и анализа инцидентов по базе метаданных

В процессе работы системы защиты XVmatic регистрируется огромное количество информации, связанной с работой каждого сотрудника ЦОД. Достаточно сказать, что на крупных объектах базы этих данных имеют объем до 5 Петабайт. Это необходимо для того, чтобы выявлять неправомерные действия сотрудников, которые могут носить и отложенных характер. Фиксируется временной интервал от трех до пяти лет. Для быстрого поиска и анализа применена технология метаданных.

1. Технология физической защиты аппаратных средств вычислительной техники

Контролируется вскрытие корпуса системного блока АРМ, отключение и подключение клавиатуры, мыши и монитора на компьютерах и терминалах. Помимо этого организован физический контроль доступа к аппаратным, коммуникационным стойкам и сейфам хранения носителей информации.

Все аппаратные средства находятся в зонах камер подсистемы видеонаблюдения XViewsion.

1. Технология обеспечения бесперебойной работы системы XVmatic

В системе осуществляется диагностика и мониторинг работоспособности всех компонентов. По заданным сценариям происходит оповещение дежурной службы об авариях и внештатных ситуациях. Система обеспечена отдельными коммуникациями и источниками бесперебойного питания. Установлено кондиционирование помещений аппаратных стоек с непрерывным контролем климатических параметров.

Десятилетний опыт применения XVmatic на практике показал, что этот подход был

выбран правильно, а технологии системы защиты действительно эффективны. В реальной практике на нескольких объектах были выявлены и предотвращены практически все противоправные действия.

В качестве дополнительных «эффектов» системы защиты XVmatic надо отметить повышение производственной дисциплины и контроля рабочего времени сотрудников, что приводило к сокращению производственных издержек.

Валерий Крутских, Генеральный директор ЗАО «МТТ Контрол», д.ф.-м.н.