

ВИДЫ ТИПОВЫХ ОБЪЕКТОВ И СИСТЕМ ОХРАНЫ ПЕРИМЕТРА

В.М. Алефиренко, Н.В. Яненко

Защита периметра является важной составляющей комплекса мер безопасности объектов различного назначения. Выбор системы охраны периметра и ее компонентов определяется видом объекта и его особенностями [1]. Можно выделить два вида объектов: стационарный и разворачиваемый. Рассмотрим три типовых стационарных объекта и один разворачиваемый.

Таможенный склад. Относится к типу стационарных объектов. Имеет достаточно обширную территорию, расположен за городом вблизи автомобильных дорог и железнодорожных путей, что создает достаточно сильный помеховый фон для датчиков системы охраны периметра. Такой объект будет относиться к категории особо важных объектов, так как содержит достаточно большое количество материальных ценностей и информации. Установлена вибрационная система охраны периметра.

Завод. Относится к типу стационарных объектов. Территория завода расположена в черте города, рядом расположен железнодорожный переезд, который создает помеховый фон. Такой объект будет относиться к категории промышленно-коммерческих, на нем содержится большое количество материальных ценностей, а также документов и чертежей. Установлена емкостная система охраны периметра.

Загородный пансионат. Также относится к типу стационарных объектов. Территория объекта расположена за городом в сосновом бору. Помехи для системы охраны периметра могут создаваться только деревьями и обитателями леса, поэтому уровень помехового фона будет низкий. Объект относится к промышленно-коммерческой категории. Необходимость охраны периметра обусловлена нахождением на объекте людей и их имущества, а также имущества объекта. На объекте установлена инфракрасная система охраны периметра.

Полевой лагерь. Относится к разворачиваемому типу объектов. Для охраны периметра временного лагеря есть жесткое требование: система охраны должна быть легкой, малого объема, должна быстро устанавливаться и быстро сниматься, желательно, без оставления следов своего пребывания. Время работы такой системы от 8 часов до 3 суток в любых погодных условиях. Территория объекта расположена в лесу, помехи для системы охраны могут быть вызваны деревьями или обитателями леса. На объекте установлена радиолучевая система охраны периметра.

Исходя из сравнительной характеристики объектов видно, что выбор типа системы охраны периметра, и, следовательно, ее компонентов, определяется видом объекта и его особенностями.

Литература

1. Введенский Б.С. Современные системы охраны периметров // Специальная техника. 1999. № 3.

СИСТЕМА ЗАЩИТЫ ОТ СПАМ-БОТОВ В СОВРЕМЕННЫХ ВЕБ-СЕРВИСАХ

К.К. Алёхин, А.С. Шеягович

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) – это технология, которая позволяет отличить спам-бота от настоящего пользователя. Их использование позволяет уменьшить поток спама и защитить страницы. Наиболее популярны графические капчи, т.е. в которых пользователю предлагается разобрать текст, который якобы не может прочитать машина, или определить, что изображено на картинке. Однако в последние годы технологии распознавания изображений продвинулись так далеко, что иногда компьютер улавливает зашифрованные смыслы лучше человеческого глаза: пользуясь этим, компьютерам доверяют, например, чтение едва заметных писем на археологических находках или старых картинах. С распознаванием изображений у машин тоже все обстоит довольно неплохо: ученые, правда, до сих пор просят граждан помочь в анализе больших массивов изображений, но с более простыми задачами программы

справляются самостоятельно – Google и другие поисковики давно умеют искать по картинкам, недавно был запущен Shazam для картин, ИИ неплохо разгадывает даже очень плохие рисунки пользователей. В условиях возрастающей мощи компьютера традиционная графическая капча перестает быть помехой для серьезных злоумышленников и целеустремленных спамеров. Поэтому Google отказался от традиционной интерактивной капчи и вместо этого будет анализировать поведение пользователя самостоятельно. В частности, программа будет фиксировать движения мышки и IP-адрес пользователя. Боты, как правило, передвигают курсор кратчайшим путем, что практически невозможно сделать человеку. Новая капча отображается только в виде окошка, в котором программа сама ставит галочку и сообщает пользователю о том, что он не робот.

Литература

1. Коллинс М. Сетевая безопасность по средствам анализа данных. Чикаго: Университет Чикаго, 2014. 202 с.
2. Столингс, У. Основы сетевой безопасности: приложения и стандарты / У. Столингс. Изд. 6-е. М.: Массачусетский технологический институт, 2016. 464 с.

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ

В.В. Артемьева, Н.С. Карпович

Квантовое распределение ключей предоставляет возможность: можно передавать секретную информацию по открытому (незащищенному) каналу и при этом быть уверенным в том, что ее никто не перехватил.

Цель – обеспечить безусловную безопасность коммуникаций, основываясь на законах физики. Установлено, что существует множество квантовых криптографических алгоритмов – защищенные квантовые каналы, квантовое шифрование с открытым ключом, квантовое подбрасывание монеты, квантовое вычисление вслепую, квантовые деньги – но большинство из них требуют для своего осуществления полноценного квантового компьютера.

Предложено использование квантовых алгоритмов для формирования и передачи ключевой информации в симметричных криптосистемах. Это позволило получить «сырой» ключ, далее следует усиление секретности, исправление ошибок и согласование ключевой последовательности с помощью специальных алгоритмов. Этот метод позволяет двум сторонам, соединенным по открытому каналу связи, создать общий случайный ключ, который известен только им, и использовать его для шифрования и расшифрования сообщений. Важным и уникальным свойством квантового распределения ключей является возможность обнаружить присутствие третьей стороны, пытающейся получить информацию о ключе.

ПЕРЕХОД К НЕДВОИЧНЫМ ПОМЕХОУСТОЙЧИВЫМ КОДАМ В БИОМЕТРИЧЕСКИХ СИСТЕМАХ

Б.А. Ассанович, Ю.Н. Веретило, В. Рудалеску

В последнее время в литературе особый интерес вызывает реализация надежных криптографических систем на основе нечетких экстракторов (Fuzzy extractor), использующих ненадежные «зашумленные» данные биометрических измерений.

Известно, что если в таких системах возникающий шум, вызванный нечеткостью биометрических данных, является аддитивным и приводит к ошибкам типа замещений, эффективным решением является применение помехоустойчивых кодов с как можно большим расстояния Хэмминга d . Один из подходов при создании такой системы является использование конструкции с коррекцией кодом (Code-offset) [1], образующей вспомогательный безопасный эскиз (Secure Sketch), хранящийся в базе данных. Он применяется вместе с корректирующим ошибки (n, k, d) кодом и представляет смещение (offset) D , «сдвигающее» кодовый вектор X применяемого помехоустойчивого кода, содержащего пароль пользователя S , на значение биометрического измерения B , т. е. $D = B - X$. При последующем биометрическом измерении B' выполняется вычитание $D - B' = Y$, декодирование Y и получение пароля S' , как правило, совпадающего с S .