зав. кафедрой, Т.Н. Беляцкой была предпринята попытка оценить уровень грамотности населения Республики Беларусь в сфере ИБ.

Для этого был проведено масштабное исследование населения Беларуси, в котором приняло участие 1500 человек; репрезентативность выборки контролировалась по региональным пропорциям численности населения, пропорциями между городским и сельским населением, пропорциями между мужчинами и женщинами, а также пропорциями между возрастными группами. В спектр задач исследования входили как самооценка респондентов по базовым знаниям в сфере ИКТ, так и базовые вопросы по обеспечению безопасности платежей, выборе паролей, скачивания файлов. Отдельный блок вопросов был посвящен безопасности в социальных сетях. Анализ показал, что в целом уровень грамотности в сфере ИБ не слишком высок. Так, из числа респондентов, которые постоянно пользуются компьютером и сетью Интернет, только 32% респондентов правильно ответили на вопрос: «Вы хотите скачать песню Beatles «Yesterday» и нашли несколько вариантов в Интернете. Какие из них скачаете?». Варианты ответа были: Yesterday-Beatles-Song.scr; Beatles_All_songs.zip; Beatles_Yesterday.mp3.exe; Betles-Yesturday.wma.

Повышение грамотности населения в сфере ИБ является одной из основных задач в свете достижения целей в области информатизации. Для ее решения предлагается создать портал, посвященный основам знаний в данной области.

АСПЕКТЫ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

Р.В. Берёзкин, Г.А. Власова

В настоящее время наибольшее распространение получили сетевые системы видеонаблюдения (IP-протокол) по сравнению с аналоговыми (протокол CCTV). Сетевое позволяет обеспечить быструю передачу данных, лучшее качество сигнала и помехозащищенность, такую систему проще масштабировать и интегрировать в существующие системы безопасности крупных и мелких объектов. Базовым методом защиты данных в локальных сетях является аутентификация по имени пользователя и паролю. Этого достаточно, когда сеть видеонаблюдения отделена от локальной основной сети, и посторонние физически не могут получить доступ к ней. В других случаях для повышения безопасности данные должны шифроваться, чтобы посторонние не имели возможность чтения или использования передаваемой информации.

Известно много алгоритмов шифрования. Однако не все они удовлетворяют требованиям, предъявляемым к алгоритмам для систем видеонаблюдения. В современных системах видеонаблюдения требуемая скорость передачи данных от 0,6 до 12 Мбит/с. Поскольку алгоритмы шифрования снижают скорость передачи данных, для видеонаблюдения следует использовать симметричные алгоритмы.

Массовое использование систем видеонаблюдения обусловлено развитием IoT (Internet of things – Интернет вещей). В связи с этим, возникают новые требования к алгоритмам шифрования, а именно: ограниченные вычислительные ресурсы, ценовые ограничения, определенные ограничения на энергозатратность реализации.

Среди известных алгоритмов наиболее подходящими для систем видеонаблюдения являются хорошо изученные DES, AES и ГОСТ 28147-89, а также легковесные алгоритмы PRESENT и CLEFIA. Пропускная способность при использовании алгоритма PRESENT более чем в 4 раза превосходит алгоритм CLEFIA при одинаковой сложности устройства (количестве условных логических элементов, GE). Однако PRESENT менее криптостойкий (длина ключа – 80 или 128 бит), в сравнении с CLEFIA (длина ключа – 128, 192 или 256 бит).

Поскольку в современных условиях длина ключа 128 бит не обеспечивает долговременную безопасность, предпочтительнее использовать алгоритм CLEFIA. Алгоритм PRESENT применим только для обеспечения краткосрочной безопасности.