- согласование информации (коррекция ошибок) посредством обмена классической информацией через открытый классический канал связи (например, Интернет). Принципиальное отличие этой процедуры от обычных методов коррекции ошибок в классической теории информации состоит в том, что вся информация, передаваемая по открытому каналу связи, считается известной подслушивателю, коррекция проводится между пространственно удаленными пользователями;
- усиление секретности очищенного ключа. После коррекции ошибок и отбрасывания части битов у легитимных пользователей остается битовая строка меньшей длины. Информация подслушивающего может быть уменьшена до экспоненциально малой величины по выбранному параметру секретности путем сжатия (хеширования универсальными хеш-функциями).

Метод квантового шифрования QSC (Quantum Stream Cipher)

Квантовое шифрование — новое направление в квантовой криптографии, которое основывается на квантовом детектировании и теории передачи квантовой информации. Метод был предложен учеными из Северо-Западного университета США в 2000-х годах и известен как шифрсистема AlphaEta [2—3]. С использованием секретного ключа, который определяет квантовые состояния, соответствующие разным битовым последовательностям, пользователи могут применять соответствующие оптимальные квантовые измерения для расшифрования данных. Основная идея квантового шифрования — использование общего ключа для определения набора квантовых сигналов. Общий секретный ключ является неотъемлемой частью протоколов на основе квантового шифрования, результатом работы протоколов могут быть безопасно переданные данные. Таким образом, современные методы квантовой криптографии могут обеспечивать как процедуры распределения ключа, так и процедуру шифрования, тем самым возможно обеспечивать полный цикл защищенного информационного обмена, используя только квантово-механические преобразования.

СПИСОК ЛИТЕРАТУРЫ:

1. *Hirota O., Kato K., Sohma M., Usuda T. S., Harasawa K.* Quantum Stream Cipher Based on Optical Communications. Tokyo: Research Center for Quantum Information Science, Tamagawa University.
2. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. М.: МИР, 2006.
3. *Yuen H. P., Corndorf E., Eguchi T., Kumar P.* Quantum Noise Randomized Ciphers. Evanston: Center for Photonic Communication and Computing Department of Electrical Engineering and Computer Science Northwestern University, 2006.

Е. И. Гончаров

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ШЛЮЗОВ ДЛЯ ВЗАИМОДЕЙСТВИЯ МЕЖДУ СИСТЕМАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАЗНОГО КЛАССА

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказом ФСТЭК России ФСБ России Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» [1] установлены правила в отношении порядка обработки и обеспечения конфиденциальности персональных

данных как собственных работников, так и сторонних физических лиц, персональные данные которых обрабатываются в организации. Также вводится уголовная ответственность за нарушение порядка обработки и хранения персональных данных.

Согласно закону, информационные системы персональных данных, созданные до дня вступления в силу данного Федерального закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 г. Так как на момент вступления в силу данного закона существовали такие ИС федерального и муниципального масштаба, как, например, ИС МГФОМС, МЖД и другие, у которых уже сформировались информационные связи (в том числе и по обмену/обработке персональных данных), то возникает необходимость преобразования этих связей. В случае, когда класс взаимодействующих ИС одинаков, для их связи достаточно использовать соответствующие сертифицированные СЗИ. В противном случае надо гарантировать, что не происходит интеграции информационных систем. Так как если она имеет место быть, то все интегрированные системы должны принадлежать к одному и тому же классу.

Таким образом, чтобы не поднимать класс ИС в случае наличия связи с ИС более высокого класса, необходим механизм, позволяющий производить информационный обмен между ИС разных классов, но при этом гарантирующий отсутствие интеграции между ними. Обеспечение защиты и разделение ИС с помощью таких традиционных средств, как межсетевые экраны, криптографические средства защиты, средства разграничения доступа, не способны полностью решить данную задачу.

Для решения этой задачи предлагается использование информационных шлюзов, которые, благодаря своему устройству и расположению в ИС, можно было бы отнести к такому минимальному классу ИС, что соответствует осуществляемому информационному обмену, в том числе и персональными данными.

Согласно классификации информационных систем обработки персональных данных [1], класс системы может быть понижен следующими способами:

- понижением категории персональных данных, участвующих в обработке,
- уменьшением объема одновременно обрабатываемых данных.

Таким образом, информационный шлюз должен исполнять роль посредника, выполняющего передачу строго определенной категории персональных данных, при этом контролируя и ограничивая объем этих данных.

Для того чтобы шлюз сам не попадал под определение интегрированности в ИС, необходимо выполнение таких требований, как:

- выделение сетевого сегмента шлюза за межсетевой экран соответствующего класса защищенности. Класс межсетевого экрана не может быть ниже класса, необходимого для защиты сети ИС того класса, к которому принадлежит шлюз;
- ограничение на межсетевом экране сервисов и узлов, которые доступны шлюзу, только списком необходимых для информационного обмена сервисов и узлов;
- отключение доступа к шлюзу извне как пользователям, так и обслуживающему персоналу — шлюз должен являться единственным инициатором сетевого взаимодействия;
- использование коммуникационного ПО, которое контролирует категорию передаваемых персональных данных, их объем, целостность;
- обеспечение закрытой программной среды шлюза, которая позволила бы гарантировать целостность ПО и настроек шлюза.

При условии выполнения всех вышеуказанных требований информационный шлюз может быть отнесен к ИС меньшего класса, чем отделяемая им ИС, и гарантировать отсутствие интеграции с ней.

Таким образом, использование подобного шлюза может решить проблему взаимодействия информационных систем разного класса.

Данное решение проблемы взаимодействия информационных систем разного класса было применено в ГУП «Московский социальный регистр». Информационная система данной организации относится к классу К1, так как содержит больше ста тысяч записей персональных данных второй категории [1]. Организация всех информационных потоков с ИС других учреждений, таких как МГФОМС, МЖД и прочие, имеющих класс ниже К1, через шлюз, который в результате проведенных работ был отнесен к классу К3, позволила обеспечить защищенный обмен и полностью выполнить все требования руководящих документов.

СПИСОК ЛИТЕРАТУРЫ:

1. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. № 55/86/20 г. Москва «Об утверждении Порядка проведения классификации информационных систем персональных данных».

В. С. Горбатов, А. П. Дураковский, Ю. Н. Лаврухин, В. А. Петров

УЧЕБНО-МЕТОДИЧЕСКИЕ ТРЕБОВАНИЯ К ЛАБОРАТОРНОМУ ПРАКТИКУМУ В ОБРАЗОВАТЕЛЬНЫХ СТАНДАРТАХ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НОВОГО (ТРЕТЬЕГО) ПОКОЛЕНИЯ

В настоящее время высшая школа находится в состоянии ожидания перехода на многоуровневую подготовку выпускников в системе профессионального образования: среднее специальное образование — бакалавриат — специалитет — магистратура. Для нашего направления «Информационная безопасность» такой переход будет, несомненно, положительным фактором, так как на данный момент для него пока предусматривается сохранение всех указанных выше уровней. Таким образом, расширяется возможность более творческого подхода к организации подготовки широкого спектра выпускников с учетом современных требований науки, техники и промышленности. Однако эффективное решение указанной задачи во многом будет зависеть от качества интенсивно разрабатываемых в настоящее время образовательных стандартов нового (третьего) поколения.

В связи с этим были проанализированы проекты разрабатываемых федеральных государственных образовательных стандартов (ФГОС) высшего профессионального образования нового (третьего) поколения с одной, но, с нашей точки зрения, очень важной позиции: определения требований к уровню знаний, умений и практических компетенций специалистов (бакалавров, магистров) по защите информации в области аттестации объектов информатизации по требованиям безопасности информации. Именно эти требования должны лечь в основу учебно-методического обеспечения такого важного компонента организации учебного процесса, как лабораторные практикумы, а также послужить основой технико-экономического обоснования их дорогостоящей материальной базы.