

Computerworld Россия №37, 2007

Избирателей на парламентских выборах защитит квантовая механика

На выборах в Швейцарии впервые будет применена квантовая криптография

Эллен Мессмер

Network World, США

Для защиты голосов избирателей на парламентских выборах, которые должны пройти в швейцарском кантоне Женева 21 октября, будут использованы методы квантовой криптографии. Столь передовые методы криптографии впервые применяются в целях защиты избирательного процесса.

Квантовая криптография все еще считается новой областью исследований. Ее методы предусматривают передачу ключей для шифрования связи по оптоволоконным линиям с помощью фотонов. При этом автоматически обнаруживаются попытки подслушивания канала связи.

Оптимальный уровень безопасности

Во время подсчета голосов на выборах в Швейцарии квантово-криптографическая система, разработанная компанией Id Quantique, будет обеспечивать безопасность канала связи между центральной станцией подсчета голосов в центре Женевы и правительственным вычислительным центром, расположенным в пригороде.

"Мы намерены обеспечить оптимальный уровень безопасности для процесса подсчета голосов, - говорится в заявлении канцлера кантона Женева Роберта Хензлера. - В этом смысле ценность методов квантовой криптографии заключается не столько в защите от попыток постороннего вмешательства в процесс, сколько в возможности удостовериться, что данные не были испорчены во время передачи от точки их ввода до точки хранения."

Использование квантовой криптографии в ходе выборов станет наглядной демонстрацией разработанной в Швейцарии технологии. Фирма Id Quantique, расположенная в Каруже, "выросла" на исследованиях, сделанных в середине 90-х годов в Женевском университете группой под руководством профессора Николаса Гисина.

Как сообщил директор Id Quantique Грегуар Риборди, система Serberis, разработанная фирмой совместно с австралийской компанией Senetas, будет использоваться для сквозного шифрования информации об избирательных бюллетенях, пересылаемой по линии коммуникаций от центральной станции подсчета голосов до правительственного вычислительного центра.

Выборы на почте

По словам Риборди, в кантоне Женева проживает примерно 200 тыс. зарегистрированных избирателей (всего в Швейцарии 26 кантонов). На выборах 21 октября избиратели могут проголосовать лично или по почте.

"Все голоса, отправленные по почте, собираются за несколько дней до выборов и будут переданы на центральную станцию подсчета голосов 21 октября", - добавил Риборди.

"Когда голосование закончится - это произойдет в полдень воскресенья 21 октября, опечатанные урны для бюллетеней со всех избирательных участков будут доставлены на центральную станцию подсчета голосов, где их вскроют и поданные бюллетени перемешают с бюллетенями, поступившими по почте. Затем люди на центральной станции вручную произведут подсчет голосов. Результаты подсчета через компьютеры будут переданы в правительственный вычислительный центр кантона Женева", - объяснил Рибоди.

Он считает, что квантово-криптографическая система готова к работе. Риборди не уверен, что в прошлом данный высокоскоростной канал связи вообще был зашифрован, но добавил, что определенные сведения информационно-технологическая служба правительства Швейцарии не разглашает по соображениям безопасности.

Историческое значение

Использование квантовой криптографии на выборах в Швейцарии отмечает начало проекта SwissQuantum, осуществляющегося под руководством профессора Гисина при содействии швейцарского Национального центра поддержки исследований в области квантовой фотоники.

"Участие в защите федеральных выборов имеет историческое значение в том смысле, что после нескольких лет экспериментов и разработок оно станет первым практическим применением гигагерцевого квантового шифратора, прозрачного для пользователя, передающего по обычной оптоволоконной линии актуальные и

важные данные, - сказал в подготовленном заявлении профессор Гисин. - Таким образом, это событие станет настоящим выходом в свет квантовой криптографии."

Целью проекта SwissQuantum является создание в Женеве пилотной коммуникационной сети. Сторонники проекта сравнивают ее с первыми каналами Internet, созданными в США в 70-е годы. Демонстрация проекта квантовой криптографии также ожидается на этой неделе на приеме, посвященном предстоящей выставке ITU Telecom World в Женеве.

Постоянный URL статьи: <http://www.osp.ru/cw/2007/37/4401515/>

© «Открытые системы», 1992-2011. Все права защищены.