УДК 621.38:537.86

ЗАЩИТА АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ С КВАНТОВЫМ ПОЛЯРИЗАЦИОННЫМ КОДИРОВАНИЕМ НА ОСНОВЕ ТЕХНОЛОГИИ ПЛАВАЮЩЕГО КОДА

Д. ф-м. н. Р. М. Пелещак[1], А. А. Вельченко[2], С. А. Вельченко[2]

[1]Дрогобычский государственный педагогический университет имени Ивана Франко;
[2]Восточноукраинский национальный университет имени Владимира Даля, г. Луганск
Украина
peleshchak@rambler.ru, anna.velchenko@gmail.com, semmi.vall@gmail.com

В работе предлагается защита автоматизированной информационной системы, с использованием квантового канала передачи сигнала и технологии плавающего кода. Полученная система защиты может быть использована в устройствах контроля и управления доступом, поскольку содержит двойную защиту кода, что делает практически невозможным перехват данных.

Ключевые слова: квантовый канал, поляризация фотонов, плавающий код.

Нынешние современные системы контроля и управления доступом (СКУД) обладают неким подобием интеллекта, поскольку запрограммированы на совершение определенных действий в различных ситуациях. Данные системы чаще всего работают в инфракрасном или радиоканале. Недостатком СКУД является то, что в инфракрасном канале ограничен диапазон действий, а в радиоканале появляется возможность перехвата генерирующего ключа, который затем может быть сгенерирован различными техническими средствами, уже созданными на сегодняшний день.

Поэтому актуальной проблемой является защита автоматизированной информационной системы (АИС) от несанкционированного доступа к информации в корпоративных сетях, на рабочих местах в офисах, в противоугонных средствах, охранных предприятиях, в управлении разграничения доступом по привилегиям к определенному классу информации и базам данных. Жизнь диктует необходимость защиты от несанкционированного доступа как локальных сетей, так и каждого компьютера в отдельности. Особое внимание уделяется серверам базы данных, так как корпоративная сеть предприятия состоит как из проводных, так и беспроводных сетей, точек доступа или просто передает данные через модем. Актуальным становится повышение степени шифрования передаваемых данных по каналам связи. Использование квантовой криптографии открывает большие перспективы, так как она надежна и устойчива к различным видам перехвата информации.

Целью данной работы является разработка защиты АИС от несанкционированного доступа с повышенной взломоустойчивостью и надежностью на основе использования квантового поляризационного кодирования и технологии плавающего кода.

Для защиты АИС предлагается использовать квантовый канал передачи данных [1, 2]. Информация шифруется с помощью поляризационного кодирования по протоколу BB84 (протоколом квантовой криптографии на одночастичных состояниях) с четырьмя состояниями, что делает практически невозможным перехват сигнала передачи, а также позволяет увеличить диапазон действия по сравнению с существующими защитными средствами на инфракрасном канале. В шифровании сигнала, передающегося по квантовому каналу, используется плавающий код (роллинг-код), что позволяет осуществлять двойную защиту кода.

Предлагаемые методы защиты АИС основываются на шифровании как с помощью генератора случайных чисел, так и с использованием поляризационного кодирования. Далее более подробно остановимся на поляризационном кодировании по протоколу BB84, в котором используется для передачи в воздушной среде поляризационное кодирование квантовых состояний фотонов.

На рис. 1 представлена схема передачи сигнала между ключом и блоком защиты.

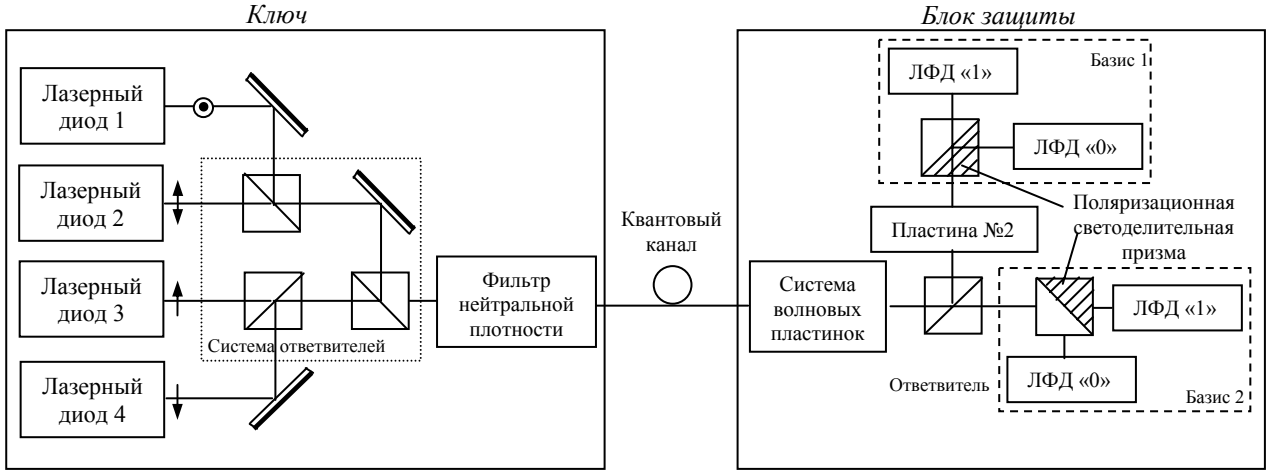

Рис. 1. Схема квантовой криптографической установки с поляризационным кодированием

Ключ, посылающий сигнал по квантовому каналу, состоит из четырех лазерных диодов, которые излучают короткие импульсы света длительностью 1 нс. Поляризация фотонов составляет –45°, 0°, +45° и 90°. Для передачи одного бита активизируется один из лазерных диодов. Затем импульсы ослабляются набором фильтров для обеспечения условия однофотонности, т. е. среднее количество фотонов в импульсе выбирается менее одного $n<1$. После этого фотон излучается по направлению к блоку защиты. Важным условием правильного детектирования информации блока защиты является сохранение поляризации фотонов.

Импульсы, достигая блока защиты, проходят через набор волновых пластинок, используемых для восстановления исходных поляризационных состояний путем компенсации изменений, внесенных волокном. Затем импульсы достигают светоделителя, осуществляющего направление фотона к линейному или диагональному анализатору. Переданные фотоны анализируются в ортогональном базисе при помощи поляризационной светоделительной призмы и двух лавинных фотодиодов (ЛФД). Плоскость поляризации фотонов, прошедших через волновые пластинки поворачивается на 45^0 (с –45° до 0°). В то же время, остальные фотоны анализируются второй системой: «поляризационная светоделительная призма — ЛФД» в диагональном базисе [1].

В протоколе BB84 используются два базиса:

$$\begin{aligned} +&: |x\rangle = |0\rangle, \quad |y\rangle = |1\rangle, \\ \times&: |u\rangle = 1/\sqrt{2}\left(|0\rangle + |1\rangle\right), \quad |\vartheta\rangle = 1/\sqrt{2}\,|0\rangle - |1\rangle. \end{aligned} \tag{1}$$

Внутри обоих базисов состояния ортогональны, но состояния из разных базисов являются попарно-неортогональными (неортогональность необходима для детектирования попыток съема информации) [3, 4]. Данные базисы удовлетворяют условию несмещенности:

$$\begin{aligned} \left|\langle x|u\rangle\right|^2 &= \left|\langle x|\vartheta\rangle\right|^2 = 1/2, \\ \left|\langle y|u\rangle\right|^2 &= \left|\langle y|\vartheta\rangle\right|^2 = 1/2. \end{aligned} \tag{2}$$

Выбирается случайным образом базис, и в соответствии с этим выбором посылается один из четырех сигналов:

— $|x\rangle$, если базис «+», значение бита 0;

— $|y\rangle$, если базис «+», значение бита 1;

— $|u\rangle$, при выпадении базиса «×», значение бита 0;

— $|\vartheta\rangle$, если базис «×», выпал бит 1.

В ключе появляются две случайные битовые строки, т. к. при посылании каждого из этих сигналов запоминается свой набор базиса и выбор бита. Блок защиты, получая сигнал, производит над ним случайным образом одно из двух измерений, каждое из которых способно дать достоверный результат из-за ортогональности состояний внутри каждого базиса ключа:

$$M_0^+ = |x\rangle\langle x|,\ M_1^+ = |y\rangle\langle y|,$$
$$M_0^\times = |u\rangle\langle u|,\ M_1^\times = |\vartheta\rangle\langle\vartheta|. \qquad (3)$$

В результате получаем одну строку с базисами, которые были выбраны для измерения, а вторую строку — с результатами этих измерений.

В квантовой криптографии используются не математические методы, а основы квантовой физики, где для переноса количества информации применяется объект квантовой механики. В данном случае такими объектами выступают электроны в электрическом токе или фотоны в линиях волоконно-оптической связи. Поскольку невозможно измерить хоть один параметр фотона, не нарушив и не исказив другой параметр, то кража информации обнаруживается при попытке измерения переносчика информации – фотона или электрона. Данное явление известно в физике как принцип неопределенности Гейзенберга.

Квантовые явления, используемые в целях криптографии (защиты информации), позволяют создать такую систему защиты, при которой любое подслушивание (попытка произвести нарушение исходного сигнала) обнаруживается с высокой степенью точности и достоверности.

Как бы надежно ни была зашифрована информация, при попадании ключа к перехватчику все усилия шифровальщиков окажутся напрасными. Квантовая рассылка ключей на нынешнее время является самым надежным методом защиты, поскольку невозможно выкрасть часть сигнала с передающей линии, ведь электромагнитный квант неделим.

Квантовый ключ передается в форме фотонов, при этом направление поляризации фотонов выбирается случайным образом. Квантовое состояние фотонов задается отправителем и регистрируется получателем. Чтобы получить достоверный сигнал, отправитель и получатель должны иметь обоюдную договоренность об основе вида поляризации. Поляризация фотонов контролируется при передаче данных. Любое вмешательство при передаче сигнала приводит к изменению поляризации, которое будет замечено адресатом.

Коммерческая система квантовой криптографии состоит из генератора случайных чисел – для создания ключа шифрования и дешифрования, излучающих и регистрирующих устройств квантового сигнала (фотонов света).

Передача данных ведется через встроенные универсальные асинхронные приемопередатчики (UART-Universal Asynchronous Receiver/Transmitter) – микроконтроллеры, которые позволяют упростить программы, исполняемые в ключе и в блоке защиты. Микроконтроллеры в обеих схемах тактируются при помощи встроенного тактового генератора с использованием внешнего кварцевого резонатора на 4 МГц.

Таким образом, принцип работы устройства защиты заключается в следующем: при нажатии на кнопку ключа он отсылает свой серийный номер в блок защиты по квантовому каналу с использованием поляризационного кодирования по протоколу BB84. Если в базе данных блока защиты такой номер фигурирует, то блок защиты высылает ключу четыре пакета с числами (причем каждое число уникально, так как для генерации данных чисел используется ГСЧ). Ключ и блок защиты обрабатывают числа по определенному алгоритму, в котором переменными служат эти числа (в вычислении первого числа фигурирует только первое принятое значение, во втором – первое и второе и т. д.). После завершения математических операций ключ отсылает блоку защиты результат, если результаты вычислений блока защиты и ключа сходятся, то исполнительный механизм разблокирует данную систему на запрограммированное время.

Предложенная система имеет высокую степень защиты за счет того, что по искажению информации видно, что кто-то осуществляет съем информации с квантового канала. Протокол BB84 доста-

точно уязвим для PNS-атак, но ввиду того, что осуществляется математическое шифрование, информация не будет вскрыта. А попытка взлома будет зафиксирована. В дальнейшем можно использовать протокол SARG04 он более устойчив к PNS-атакам.

Таким образом, показано, что защита от современных видов атак несанкционированного доступа к зашифрованной информационной системе путем использования распределения квантовых ключей по протоколу BB84 обеспечивает высокую степень защиты.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Голубчиков Д. М. Применение квантовых усилителей для съема информации с квантовых каналов распределения ключа// Известия ТТИ ЮФУ. — 2008. — №1(78). — С. 19.

2. Холево А. С. Квантовые системы, каналы, информация. — Москва: МЦНМО, 2010.

3. Kurtsiefer C., Zarda P., Halder M. et all. Quantum cryptography: A step towards global key distribution // Nature. — 2002. — Vol. 419. — P. 450.

4. Rarity J.G., Tapster P.R., Gorman P.M., Knight P., Ground to satellite secure key exchange using quantum cryptography // New J. Phys. — N 4.— P. 82 (2002).

———————

R. M. Peleshchak, A. A. Velchenko, S. A. Velchenko

Protection of an automated information system with quantum polarization coding on the basis of the floating code technology.

The authors suggest to protect an automated information system by using the quantum signal transmissing channel and the technology of a floating code. The developed automated information protection system can be used in access monitoring and control devices, because it contains the double protection of the code that makes the interception of data virtually impossible.

Keywords: *quantum channel, photon polarization, floating code.*