относительно заданных параметров. Альтернатива X1 (алгоритм DES) имеет максимальное расстояние т.е. имеет наихудшие характеристики.

Выводы

В итоге, приведенный математический аппарат дает возможность более эффективно осуществить задачу выбора алгоритма для данной криптосистемы, тем самым, оптимизируя работу этой системы, целью которой является шифрация информации. Использование предлагаемого подхода выбора алгоритма дает возможность в дальнейшем автоматизировать процесс принятия решения при построении криптосистем и последующего его применения в системах автоматизации проектирования. Возможность накопления базы знаний нечетких альтернатив и формализация процесса принятия решений позволит расширять спектр применения, включая как появление новых алгоритмов шифрования так и новых методов криптоанализа.

Список литературы

1. *Корченко О.Г.* Системи захисту _віязь_раф. Монографія / Корченко О.Г. – К. : НАУ, 2004. – 264 с.

2. *Шнайер Б.* Прикладная Криптография. 2-е изд. Протоколы, Алгоритмы и исходные тексты на языке Си / Шнайер Б. – М., "Триумф", 2002. – 816 с.

3. *Мао, Венбо*. Современная _віязь_рафія: _віязь и практика. Справочник / Мао, Венбо. – М. : Издательский дом «Вильямс», 2005. – 768 с.

4. *Панасенко С.П.* Алгоритмы шифрования. Специальный справочник / Панасенко С.П. – СПб. : БХВ-Петербург, 2009. – 576 с.

5. *Кофман А*. Введение в _віязь нечетких множеств / Кофман А. – М. : Радио и _віязь, 1982. – 432с.

6. Гаенко А.В. Рекомендации и выбор вида шифра для применения в сети доступа / Гаенко А.В., Шестак Н.А. // Вісник Українського будинку економічних та науково-технічних знань. – 2005. – №3. – 50-54 с.

Поступила 24.02.2010

УДК 003.26:621.39+530.145 **Василиу Е.В.**

АНАЛИЗ СТОЙКОСТИ К НЕКОГЕРЕНТНОЙ АТАКЕ ЧЕТЫРЕХ КВАНТОВЫХ ПРОТОКОЛОВ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С КУТРИТАМИ

Современное информационное общество постоянно испытывает необходимость в усовершенствовании методов защиты телекоммуникационных каналов от несанкционированного прослушивания. Предложенная в 80-х годах XX века идея применения принципов квантовой механики к криптографии привела к развитию нового мультидисциплинарного научного направления – квантовой криптографии [1–3]. Одно из направлений квантовой криптографии – квантовые протоколы распределение ключей (КПРК), где две удаленные стороны (Алиса и Боб) с использованием квантового коммуникационного канала могут сгенерировать общую случайную бинарную строку, которую затем используют как ключ для шифрования. При этом законы квантовой механики гарантируют безопасность передачи ключа – при выполнении легитимными сторонами определенных процедур, касающихся как передачи квантовых частиц (фотонов) по каналу связи, так и определенной классической или квантовой пред- и постобработки информации [1–3].

К настоящему времени предложены различные классы КПРК [2,3]. Два основных класса – это протоколы, основанные на передаче одиночных квантовых состояний, относящихся к неортогональным базисам (их называют также протоколами типа «приготовление – измерение») и протоколы, основанные на распределении перепутанных квантовых состояний между пользователями. При этом можно использовать двух-, трех- и т.д. мерные квантовые системы, соответственно каждая такая система позволяет передать один бит, один трит и т.д. информации.

Безопасность протоколов, основанных на передаче двухмерных квантовых систем (кубитов), к настоящему времени исследована теоретически достаточно полно, а их применимость для безопасного распределения ключа между двумя удаленными на большое расстояние пользователями неоднократно продемонстрирована экспериментально [2]. Однако эффективность таких протоколов, определяемая, как отношение количества использованных для создания ключа кубитов к общему количеству переданных кубитов, невелика [2]. Использование для передачи информации многомерных квантовых систем является одним из путей увеличения эффективности протоколов, а соответственно и увеличения скорости генерации ключа.

Были предложены несколько протоколов с передачей трехмерных квантовых систем (кутритов): протокол с передачей одиночных кутритов и использованием двух взаимно несмещенных базисов [4], аналогичный протокол с использованием четырех базисов [5], протокол с перепутанными парами кутритов, состояния которых восстанавливаются методом квантовой томографии – так называемый томографический протокол [6], а также протокол с парами перепутанных кутритов [7], являющийся обобщением на трехмерные квантовые системы протокола Экерта [8]. Были проанализированы также некогерентные атаки с использованием вспомогательных квантовых систем (проб) на эти протоколы [4–7]. В частности, в [7] была рассмотрена симметричная некогерентная атака на предложенный в этой работе протокол, однако оптимизация этой атаки по параметрам квантовых проб не проводилась, поэтому вопрос о стойкости протокола Экерта для кутритов остается открытым.

Целью настоящей работы является анализ и оптимизация симметричной некогерентной атаки на протокол с перепутанными парами кутритов [7], а также сравнение стойкости этого протокола к некогерентной атаке со стойкостью других протоколов с кутритами [4–6]. В качестве меры стойкости протокола используется шенноновская взаимная информация между Алисой и Евой $I_{AE}(D)$, являющаяся функцией среднего уровня ошибок D, вносимых в просеянный ключ вследствие перехвата.

В [7] были получены выражения для взаимной информации между Алисой и Бобом I_{AB} и Алисой и Евой I_{AE}, как функции от параметров F и λ квантовых проб Евы:

$$I_{AB}(F,\lambda) = 2\log_2 3 + \frac{1}{3}(1+F\lambda)\{\log_2(1+F\lambda) - \log_2 9\} + \frac{2}{3}(1-F\lambda)\{\log_2(1-F\lambda) - \log_2 9\}; \quad (1)$$

$$I_{AE}(F,\lambda) = \log_2 3 - 3\langle E'_{00}|E'_{00}\rangle \log_2\langle E'_{00}|E'_{00}\rangle - 6\langle E'_{11}|E'_{11}\rangle \log_2\langle E'_{11}|E'_{11}\rangle -$$
$$- \{-3\langle E'_{00}|E'_{00}\rangle W_1 \log_2(\langle E'_{00}|E'_{00}\rangle W_1) - 6\langle E'_{00}|E'_{00}\rangle(1-W_1)^2 \log_2(\langle E'_{00}|E'_{00}\rangle(1-W_1)^2) -$$
$$- 6\langle E'_{11}|E'_{11}\rangle W_2 \log_2(\langle E'_{11}|E'_{11}\rangle W_2) - 12\langle E'_{11}|E'_{11}\rangle(1-W_2)^2 \log_2(\langle E'_{11}|E'_{11}\rangle(1-W_2)^2)\}, \quad (2)$$

где $|E'_{kl}\rangle$ – состояния проб Евы после измерения,

$$\langle E'_{00}|E'_{00}\rangle = (1+2F\lambda)/9, \qquad \langle E'_{11}|E'_{11}\rangle = (1-F\lambda)/9. \quad (3)$$

В (1), (2) и последующих формулах для взаимной информации единицей измерения является *бит*.

Величины W_1 и W_2 в (2) даются формулами [7]:

$$W_1 = \left(\frac{1}{3}\sqrt{1+2\lambda'_1} + \frac{2}{3}\sqrt{1-\lambda'_1}\right)^2, \qquad W_2 = \left(\frac{1}{3}\sqrt{1+2\lambda'_2} + \frac{2}{3}\sqrt{1-\lambda'_2}\right)^2, \quad (4)$$

где

$$\lambda'_1 = \frac{1}{2}\frac{3F+4F\lambda-1}{1+2F\lambda}, \qquad \lambda'_2 = \frac{1}{2}\frac{3F-2F\lambda-1}{1-F\lambda}. \quad (5)$$

Средний уровень ошибок между Алисой и Бобом [7]:

$$D = 2(1-F\lambda)/3. \quad (6)$$

Чтобы не быть выявленной легитимными пользователями при проверке нарушения неравенств Белла [1,8], Ева должна выбирать параметры F и λ так, чтобы выполнялось условие:

$$F\lambda \ge \left(6\sqrt{3}-9\right)/2 \approx 0{,}69615\,. \qquad (7)$$

Для выяснения степени стойкости этого протокола к некогерентной атаке необходимо найти зависимости взаимной информации (1) и (2) от среднего уровня ошибок D, которые не были получены в [7]. Первое выражение получается подстановкой $F\lambda$ из (6) в (1):

$$I_{AB}(D) = 2\log_2 3 + \left(\frac{2}{3}-\frac{D}{2}\right)\left\{\log_2\left(2-\frac{3}{2}D\right)-\log_2 9\right\} + D\left\{\log_2\left(\frac{3}{2}D\right)-\log_2 9\right\}. \qquad (8)$$

Что касается I_{AE}, то из формул (2) – (6) видно, что эта величина, кроме зависимости от D, будет зависеть также от одного из параметров проб. Это дает Еве возможность максимизировать информацию о ключе выбором одного из параметров своих проб. Для этого Ева должна сначала выбрать средний уровень ошибок D, который она будет создавать при перехвате, так, чтобы он не сильно превышал естественный уровень помех в канале, а затем выбрать один из параметров проб (F или λ) так, чтобы величина I_{AE} была максимальной. Второй параметр при этом будет однозначно определяться из (6) для каждого заданного D, а Ева должна также следить за тем, чтобы параметры ее проб удовлетворяли условию (7).

Зависимость I_{AE} от параметра F представляет собой громоздкое выражение, которое здесь не приводится ввиду того, что, как следует из нашего анализа, I_{AE} зависит от F монотонно. При этом максимальную информацию Ева может получить, выбрав $F = 0{,}69615$, что соответствует $\lambda = 1$. Создаваемый при этом уровень ошибок у легитимных пользователей равен 20,26%.

Получим теперь выражение для $I_{AE}(D\,|\,\lambda)$. Для этого подставим F из (6) в (5), а затем полученные выражения для λ_1' и λ_2' подставим в (4):

$$W_1(D\,|\,\lambda) = \frac{1}{9(1-D)}\left[\frac{1{,}5D-1}{\lambda} - 3D + 4 + 2\sqrt{\left(\frac{2-3D}{\lambda}-6D+4\right)\left(1-\frac{1-1{,}5D}{\lambda}\right)}\right], \qquad (9)$$

$$W_2(D\,|\,\lambda) = \frac{1}{9D}\left[\frac{3D-2}{\lambda} + 3D + 2 + 4\sqrt{\left(\frac{2-3D}{\lambda}+3D-2\right)\left(1-\frac{1-1{,}5D}{\lambda}\right)}\right]. \qquad (10)$$

Подставляя теперь $F\lambda$ из (6) в (3), а затем полученные выражения в (2), получим окончательно:

$$I_{AE}(D\,|\,\lambda) = \log_2 3 - (1-D)\log_2\frac{1-D}{3} - D\log_2\frac{D}{6} + (1-D)W_1(D\,|\,\lambda)\log_2\frac{(1-D)W_1(D\,|\,\lambda)}{3} +$$
$$+ 2(1-D)(1-W_1(D\,|\,\lambda))^2\log_2\frac{(1-D)(1-W_1(D\,|\,\lambda))^2}{3} + DW_2(D\,|\,\lambda)\log_2\frac{DW_2(D\,|\,\lambda)}{6} +$$
$$+ 2D(1-W_2(D\,|\,\lambda))^2\log_2\frac{D(1-W_2(D\,|\,\lambda))^2}{6}, \qquad (11)$$

где $W_1(D\,|\,\lambda)$ и $W_2(D\,|\,\lambda)$ определены в (9) и (10) соответственно.

На рис. 1 приведены зависимости $I_{AE}(D\,|\,\lambda)$ для различных значений параметра λ. Видно, что эта величина зависит от λ не монотонно. Вертикальная штриховая линия на рис. 1 соответствует $D = 0{,}2026$.

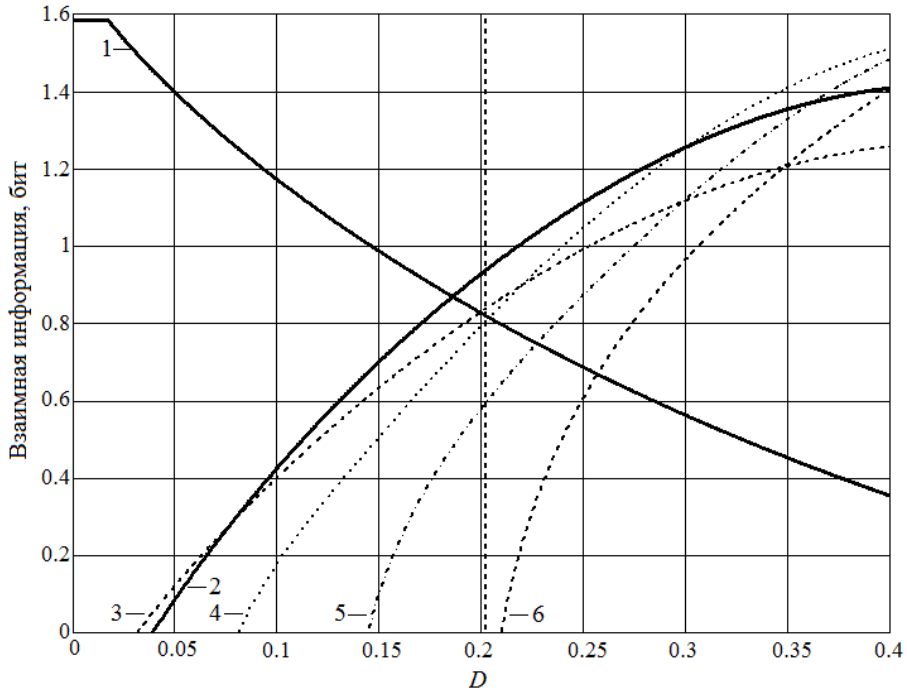

Рис. 1. Взаимная информация $I_{AB}(D)$ (1) и $I_{AE}(D|\lambda)$ для значений параметра λ: 0,9827 (2); 1,0 (3); 0,9 (4); 0,8 (5); 0,7 (6)

Чтобы найти значение параметра λ, оптимальное для Евы, необходимо использовать теорему Цизара и Кёрнера [9], в соответствие с которой Алиса и Боб могут установить секретный ключ, если взаимная информация между ними больше взаимной информации между Алисой и Евой. Таким образом, в квантовой криптографии верхней границей допустимого уровня ошибок считают значение $D_{\max}$, которое получают из уравнения $I_{AB}(D_{\max}) = I_{AE}(D_{\max})$. Следовательно, для определения $D_{\max}$ как функции от λ необходимо приравнять правые части выражений (8) и (11). Решая численно полученное уравнение для различных значений λ, можно найти такое λ, которому соответствует минимальное значение $D_{\max}$. Именно это значение λ и будет оптимальным для Евы.

Численным решением уравнения $I_{AB}(D_{\max}) = I_{AE}(D_{\max})$ было найдено, что минимальному $D_{\max}$, равному 0,186, соответствует $\lambda = 0{,}9827$ (кривая 2 на рис. 1). Как видно, при таком значении параметра λ Ева может получить больше информации, чем при любом другом λ, в широком интервале значений уровня ошибок D. Отметим также, что если Ева при $\lambda = 0{,}9827$ выберет $F \geq 0{,}7083$, что согласно (6) и (7) соответствует $D \leq 0{,}2026$, то неравенства Белла будут нарушаться, и, следовательно, легитимные пользователи не смогут обнаружить атаку проверкой нарушения неравенств Белла.

Выражения для $I_{AB}(D)$ и $I_{AE}(D)$ при оптимальной некогерентной атаке на протокол с одиночными кутритами и использованием двух взаимно несмещенных базисов были получены в [4]:

$$I_{AB}(D) = \log_2 3 + (1-D)\log_2(1-D) + D\log_2(D/2); \tag{12}$$

$$I_{AE}(D) = \log_2 3 + FE(D)\log_2(FE(D)) + (1-FE(D))\log_2\left(\frac{1-FE(D)}{2}\right), \tag{13}$$

где $FE(D) = \frac{1-D}{3} + \frac{2}{3}D + \frac{2}{3}\sqrt{2D(1-D)}$.

$I_{AB}(D)$ для аналогичного протокола с четырьмя базисами совпадает с (12), а $I_{AE}(D)$ имеет вид [5]:

$$I_{AE}(D) = \log_2 3 + (1-D)\left[f(D)\log_2 f(D) + (1-f(D))\log_2\left(\frac{1-f(D)}{2}\right)\right], \quad (14)$$

где $f(D) = \dfrac{3-2D+\sqrt{(3-2D)^2 - 9\cdot(1-2D)^2}}{9\cdot(1-D)}$.

Соответствующие выражения для томографического протокола с кутритами [6]:

$$I_{AB}(D) = \log_2 3 + \beta_0 \log_2 \beta_0 + (1-\beta_0)\log_2 \beta_1; \quad (15)$$

$$I_{AE}(D) = \log_2 3 + \beta_0[\eta_0 \log_2 \eta_0 + (1-\eta_0)\log_2 \eta_1], \quad (16)$$

где $\beta_0 = 1-D$; $\beta_1 = \dfrac{D}{2}$; $\eta_0 = 1-2\eta_1$; $\eta_1 = \dfrac{1}{3}\left(\sqrt{r_0}-\sqrt{r_1}\right)^2$; $r_0 = 1-\dfrac{\beta_1}{\beta_0}+r_1$; $r_1 = \dfrac{\beta_1}{3\beta_0}$.

Путем несложных алгебраических преобразований можно доказать тождественность выражений (12) и (15), а также тождественность выражений (14) и (16). Таким образом, протокол с одиночными кутритами и четырьмя базисами [5] и томографический протокол с кутритами [6] имеют одинаковую стойкость к оптимальной некогерентной атаке.

На рис. 2 приведены зависимости $I_{AB}(D)$ и $I_{AE}(D)$ для четырех протоколов с кутритами, где $I_{AE}(D|\lambda)$ для протокола с перепутанными парами кутритов [7] построено при $\lambda = 0{,}9827$, что соответствует найденному оптимальному значению этого параметра. Кривые 1 и 3 пересекаются в точке $D = 0{,}186$, кривые 2 и 4 – в точке $D = 0{,}211$, а кривые 2 и 5 – в точке $D = 0{,}227$. Таким образом, из теоремы Цизара – Кёрнера следует, что протоколы [5] и [6] наиболее стойки к оптимальной некогерентной атаке, протокол [4] немного менее стоек к такой атаке, а наименьшей стойкостью обладает протокол с перепутанными парами кутритов [7].

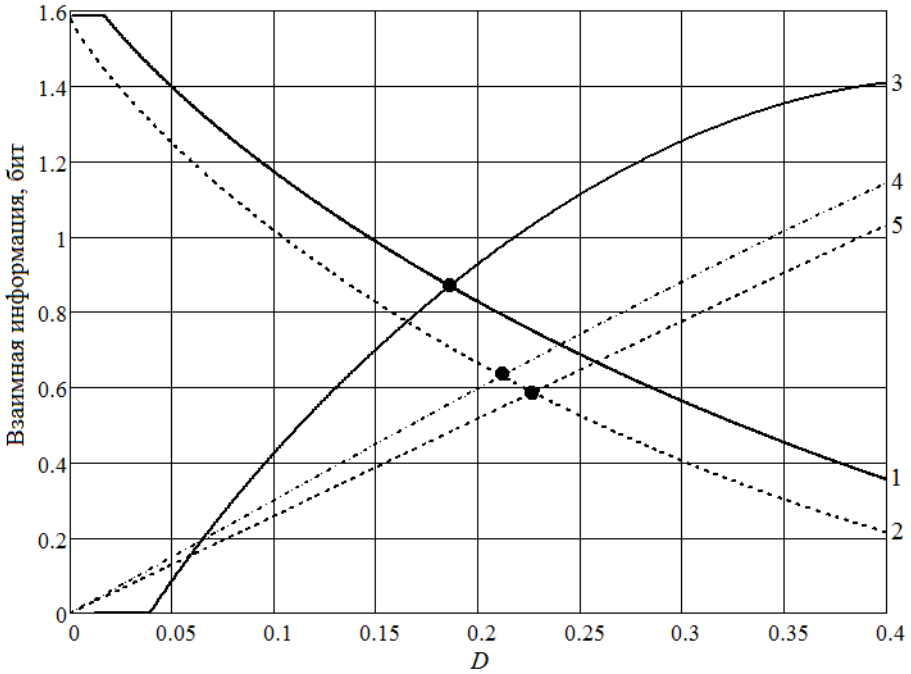

Рис. 2. Взаимная информация $I_{AB}(D)$ и $I_{AE}(D)$ для четырех протоколов с кутритами: 1 – $I_{AB}(D)$ для протокола [7], 2 – $I_{AB}(D)$ для протоколов [4–6], 3 – $I_{AE}(D)$ для протокола [7], 4 – $I_{AE}(D)$ для протокола [4], 5 – $I_{AE}(D)$ для протоколов [5,6]

Рассмотрим теперь эффективность протоколов [4–7]. Будем определять ее при идеальных условиях, т.е. пренебрегать влиянием на эффективность потерь в квантовом

канале, ошибок, создаваемых подслушиванием, а также уменьшением длины полученного ключа после усиления секретности, поскольку все эти факторы зависят от конкретных условий реализации протокола, а не от его схемы. При идеальных условиях эффективность протокола с одиночными кутритами и двумя базисами [4] равна $\frac{1}{2}$ трит/кутрит, протокола с одиночными кутритами и четырьмя базисами [5], как и томографического протокола [6] – равна $\frac{1}{4}$ трит/кутрит, а протокола с перепутанными кутритами [7] – $\frac{1}{9}$ трит/кутрит.

Отсюда следует, что из четырех рассмотренных протоколов наилучшим по критерию эффективности является протокол с одиночными кутритами и двумя базисами, а стойкость этого протокола к оптимальной некогерентной атаке по критерию Цизара – Кёрнера лишь ненамного (~ 7%) меньше стойкости аналогичного протокола с четырьмя базисами. С другой стороны, протокол с перепутанными парами кутритов [7] имеет как наименьшую эффективность, так и наименьшую стойкость к оптимальной некогерентной атаке.

Таким образом, найдены оптимальные параметры квантовых проб для некогерентной атаки на протокол с перепутанными парами кутритов [7], являющийся обобщением на трехмерные квантовые системы схемы Экерта. Показано, что стойкость этого протокола к оптимальной некогерентной атаке наименьшая из всех четырех рассмотренных в работе протоколов. Также показано, что стойкость к такой атаке протокола с одиночными кутритами и четырьмя базисами [5] и томографического протокола с кутритами [6] одинакова и не намного выше стойкости протокола с одиночными кутритами и двумя базисами [4]. Учитывая, что протокол [4] имеет наибольшую эффективность, значительно превышающую эффективность остальных рассмотренных протоколов, а также стойкость к некогерентной атаке, которая незначительно ниже стойкости протоколов [5] и [6], но выше стойкости протокола [7], можно сделать следующий вывод: из четырех рассмотренных в работе протоколов оптимальным является протокол *с одиночными кутритами и двумя взаимно несмещенными базисами* [4]. Этот же протокол является и наиболее простым с точки зрения технической реализации при современном уровне развития технологий квантовой информатики, и, таким образом, его можно признать наилучшим для практического использования.

В заключение необходимо сделать также следующие замечания. Несмотря на то, что протоколы с перепутанными кутритами, как выполняемый по схеме Экерта, так и томографический протокол, обладают меньшей эффективностью по сравнению с протоколом с одиночными кутритами и двумя базисами, они имеют и ряд преимуществ. Одно из главных преимуществ протоколов с перепутанными кутритами состоит в использовании случайности квантовых измерений – это позволяет создать у двух легитимных пользователей одинаковый и полностью случайный криптографический ключ [1,6–8]. При использовании протоколов с одиночными квантовыми системами (кубитами, кутритами и т.д.) ключ должен быть сначала сгенерирован одной из сторон, а затем передан другой стороне с помощью квантового протокола. Другое преимущество протоколов с перепутанными квантовыми состояниями перед протоколами с одиночными состояниями состоит в отсутствии необходимости иметь строго однофотонный источник сигнала. Протоколы с перепутанными состояниями неуязвимы к целому ряду атак, к которым уязвимы протоколы с одиночными состояниями из-за отсутствия в настоящее время однофотонных источников [2]. Поэтому, несмотря на свою невысокую эффективность, а также несколько бльшую сложность технической реализации, протоколы с перепутанными кутритами могут быть использованы в будущих коммерческих системах квантового распределения ключей, наряду с протоколами с передачей одиночных кутритов.

Список литературы

1. *Баумейстер Д., Экерт А., Цайлингер А*. Физика квантовой информации. – М.: «Постмаркет», 2002. – 376 с.
2. *Dusek M., Lutkenhaus N., Hendrych M.* Quantum Cryptography // Progress in Optics. – V. 49. – «Elsevier», 2006. – P. 381–454.
3. *Корченко О.Г., Васіліу Є.В., Гнатюк С.О*. Сучасні квантові технології захисту інформації // Науково-технічний журнал «Захист інформації». – 2010, № 1. – С. 77–89.
4. *Cerf N.J., Bourennane M., Karlsson A., Gisin N*. Security of quantum key distribution using d-level systems // Physical Review Letters. – 2002. – V. 88, №12. – 127902.
5. *Bruss D., Macchiavello C*. Optimal eavesdropping in cryptography with three-dimensional quantum states// Physical Review Letters. – 2002. – V. 88, № 12. – 127901.
6. *Liang Y.C., Kaszlikowski D., Englert B.-G., Kwek L.C., Oh C.H*. Tomographic quantum cryptography // Physical Review A. – 2003. – V. 68, № 2. – 022324.
7. *Kaszlikowski D., Chang K., Oi D.K.L., Kwek L.C., Oh C.H*. Quantum cryptography based on qutrit Bell inequalities // Physical Review A. – 2003. – V. 67, № 1. – 012310.
8. *Ekert A.* Quantum cryptography based on Bell's theorem // Physical. Review Letters. – 1991. – V. 67, № 6. – P. 661–663.
9. *Csiszar I., Korner J*. Broadcast channels with confidential messages // IEEE Transactions on Information Theory. – 1978. – V. IT-24, № 3. – P. 339–348.

Поступила 12.01.2010

УДК 004.056 **Паціра Є.В., Захарова М.С., Корченко А.О.**

ДОСЛІДЖЕННЯ ПРОЦЕСІВ ВПЛИВУ ТА ПОВОДЖЕННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІД ДІЄЮ КІБЕРАТАК

Інформаційні ресурси є одним з обов'язкових елементів, необхідних для здійснення будь-якого виду людської діяльності: виробництва, управління, наукових досліджень, проектування нової техніки і технології. Найважливішим аспектом взаємин споживача і інформаційної системи є по можливості якнайповніше і раціональніше забезпечення ефективного використання інформаційних ресурсів [2]. Саме ефективне використання інформаційних ресурсів таким чином дозволяє мінімізувати витрату усіх інших видів ресурсів при інформаційному забезпеченні споживачів. Тому, відповідно до існуючих підходів, прийнято вважати, що інформаційна безпека системи забезпечена у разі, якщо для будь-яких інформаційних ресурсів (ІР) в системі підтримується певний рівень конфіденційності , цілісності та доступності.

Таким чином, вирішення проблеми вибору ефективних методів забезпечення безпеки інформаційних ресурсів пов'язане з визначенням найбільш небезпечних для конкретних типів ІР класів кібератак, а також з виявленням впливу кібератак на ІР, при якому здійснюється порушення основних характеристик безпеки ресурсів.

При побудові моделі впливу кібератак на ІР необхідно, розглянути саму можливість впливу кожної кібератаки з множини $R = \{R_1, R_2, ..., R_N\}$ на кожен ІР (див. рис. 1). У результаті одержимо інтенсивності $\beta_{nm}(t)$ потоку n-ої кібератаки на m-й ІР. Потік кібератак на ІС описується розподілом імовірностей проміжків часу між сусідніми атаками. Потік кібератак R_n на ІС є ординарним - атаки з'являються поодинці, ординарність потоку атак означає, що імовірність влучення на елементарну ділянку Δt двох або більш атак мала в порівнянні з імовірністю влучення на нього рівно однієї події, тобто при $\Delta t \to 0$ ця імовірність являє собою нескінченно малу вищого порядку; потоком без наслідку - для будь-яких, що не перекриваються, ділянок часу π_1, π_2,..., π_n числа рівні кількості атак, що попадають на ці ділянки, являють собою незалежні випадкові величини, тобто імовірність влучення будь-якого числа атак на одну з ділянок не залежить від того, скільки їх потрапило на інші. Сума потоків атак