3. *Гусаров Ю. А.* Европа и становление нового миропорядка // РАНИНИОН – М., 2006 – 203с.
4. *Журкин В.* Военные структуры ЕС: цель 2010 // Современная Европа. – 2005 №3 – с. 5–12
5. *Зайцев Б.* ЕС на пути к созданию новой «архитектуры» безопасности// Компас. – 2001 № 2 – с.38-43
6. *Уткин С. В*. Основные инструменты общей внешней политики и политики безопасности ЕС // Мировая экономика и международные отношения – 2005 № 11 – с.44–54
7. *Erhard Cziomer* Udział USA w systemie bezpieczeństwa europejskiego // Wydawnictwo «Meritum» – Kraków 2000 – 125s.
8. *Hastedt G.* American foreign policy: past, present and future. New York: Prentice Hall, 2000 – 283 p.

СИСТЕМАТИЗАЦИЯ ЗНАНИЙ О КРИПТОСИСТЕМАХ

Е. Н. Скопинова

ВВЕДЕНИЕ

Желание иметь тайны волновало людей со времен их появления. Еще Сенека писал: «Если Вы хотите сохранить секрет, не доверяйте его никому». Я же заинтересовалась данной проблемой после прочтения, как ни странно, художественной книги «Цифровая крепость» Дэна Брауна. Автор повествует о создании шифра, над взломом которого пришлось изрядно поработать криптографическому отделу АНБ (агентства национальной безопасности) США, настолько секретного, что один из героев в шутку расшифровал аббревиатуру АНБ «агентство, которого никогда не было» [1].

Несмотря на то, что описанные в книге события – художественный вымысел, я отчетливо осознала, что именно криптография является одним из немногих способов защитить человека в ситуации, когда он вдруг обнаруживает, что живет в тоталитарном государстве, которое может контролировать каждый его шаг.

В данной работе была сделана попытка выделить основные этапы развития криптографии как науки и оценить уже сложившиеся схемы периодизации этой науки.

АНАЛИЗ УЖЕ ИЗВЕСТНЫХ ПЕРИОДИЗАЦИЙ ИСТОРИИ КРИПТОГРАФИИ

Традиционно развитие криптосистем разделяется на 3 этапа: *докомпьютерный* (до 1949 года), *шенноновский* (до 1976 года) и *компьютерный* (до настоящего времени). На мой взгляд, это то же самое, что считать яблоней грушевое дерево, только здесь не деревья, а подходы: компьютерный и докомпьютерный *уровни развития технологии*, в то время как шенноновский математический *метод исследования* криптологии.

Кроме того, первый этап характеризуется временным отрезком, который в несколько раз больше, чем у второго и третьего вместе взятых.

Поиски были продолжены книгой С.Г.Баричева и Р.Е.Серова [2]. Авторы в своей работе разделили историю на этапы в соответствии с уровнями развития технологических методов шифрования. Они выделили 4 этапа: *наивная* криптография (до начала 16 века), *формальная* (конец 15 – начало 20 века), *научная* (30 – 60-е 20 века) и *компьютерная* (с 70-х 20 века). Но они не учли появления качественно нового этапа науки – квантовой криптографии, о которой на момент написания книги (2002 год) уже давно говорили.

КРИТЕРИИ ПОСТРОЕНИЯ ПЕРИОДИЗАЦИОННЫХ МОДЕЛЕЙ

Для построения новых моделей периодизации, на основании выше изложенного предлагается несколько принципов, которым я сама впоследствии и следовала:

1. В названиях этапов должна четко прослеживаться логическая связь, впрочем, как и между самими этапами.
2. Заголовки не должны выглядеть синонимично.
3. Периоды должны охватывать приблизительно одинаковые отрезки времени.
4. Максимальная описательность, разносторонность, стремление избегать излишней обобщенности.

К чему же привел меня этот «квартет»?

МОИ ВАРИАНТЫ ПЕРИОДИЗАЦИЙ ИСТОРИИ КРИПТОГРАФИИ

Таблица 1

Принцип – объединение средств и способов шифрования

№	Этапы (ключевое слово – криптография)	Временные рамки	Примеры
1	Примитивная	Древнее время – начало 16 века	Цезарь, Полибий
2	«Граммная»	Возрождение – начало 20 века	Виженер, Плейфер
3	Механическая	Начало 20 века – 60-е годы	Создатели Энигмы
4	Компьютерная	60е – 80е годы 20 века	Создатели блочных шифров
5	Квантовая	С 90-х 20 века	Компании IBM, GAP...

Таблица 2

Принцип – что шифрует (ся)

№	Этапы (ключевое слово – модель)
1	Предметно-ориентированная
2	Алфавитно-ориентированная
3	Алгоритмическая
4	Фотонная

Таблица 3

Принцип – отношение к науке

№	Этапы (ключевое слово – позиция)
1	Развития письменности и языка
2	Механики и математики
3	Физики и кибернетики
4	Оптики и квантовой физики (квантовой оптики)

Примечание. Хронологические рамки для 2 и 3 таблиц совпадают, только продолжительность этапа под номером 3 таблицы 2 соответствует объединению временных отрезков этапов 3 и 4 таблицы 1, а продолжительность этапа под номером 1 таблицы 3 соответствует времени периодов 1 и 2 таблицы 1.

ЗАКЛЮЧЕНИЕ

Отмечу тот факт, что, подобно тому, как невозможно создать невзламываемые шифры, невозможно и с идеальной точностью выделить и описать этапы их развития, так как в своем большинстве эти периоды просто переплетаются.

С полной версией моей работы, включающей подробное описание всех упомянутых мною криптографических шифров в виде презентации, пояснений к ней, а также с симулятором шифровальной машины «Энигма», можно ознакомиться по ссылкам, указанным в списке литературы [3], [4], [5].

Литература

1. *Браун Д.* Цифровая крепость // Москва: АСТ, АСТ Москва, Транзиткнига. 2005
2. *Баричев С. Г., Серов Р. Е.* Основы современной криптографии // М.: Горячая линия – Телеком. 2002
3. Интернет-адрес: http://narod.ru/disk/10382917000/Presentation.rar.html.
4. Интернет-адрес: http://narod.ru/disk/10383198000/%D0%9F%D0%BE%D1%8F%D1%81%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F.rar.html.
5. Интернет-адрес: http://narod.ru/disk/10383055000/EnigmaSim.zip.html.