МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «МИСиС»**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**История развития средств защиты информации**

Москва, 2024

# **Содержание**

[**Содержание** 2](#_Toc167270166)

[**Введение** 3](#_Toc167270167)

[Глава 1. Первый этап: начало 20 века - 1950е 4](#_Toc167270168)

[Нидерланды (1915) 4](#_Toc167270169)

[Шифр Вернама (1917) 4](#_Toc167270170)

[Шифровальная машина B-21 (1925) 4](#_Toc167270171)

[“Энигма” (1927) 5](#_Toc167270172)

[Первая советская шифровальная машина (1932) 5](#_Toc167270173)

[Вокодер Гомера Дадли (1930e) 5](#_Toc167270174)

[Первая Американская дисковая шифровальная машина (1936) 6](#_Toc167270175)

[SZ-40 (1940) 6](#_Toc167270176)

[NEMA (1946) 6](#_Toc167270177)

[Клод Шеннон (1949) 7](#_Toc167270178)

[Фиалка-M (1963) 7](#_Toc167270179)

[Глава 2. 2 Этап: 1960 - середина 2000е 8](#_Toc167270180)

[1 Период: Начало 1960-х – 1970-е 8](#_Toc167270181)

[Уязвимости, ARPANET и первые компьютерные вирусы 8](#_Toc167270182)

[Телефонные фрикеры 9](#_Toc167270183)

[Защита информации в период 1960-х – середины 1970–х годов 9](#_Toc167270184)

[2 Период: Вторая половина 1970–х – начало 1990–х годов 10](#_Toc167270185)

[Криптографические методы защиты информации в этот период 10](#_Toc167270186)

[3 Период: 1990-е – начало 2000–х 13](#_Toc167270187)

[Криптографические методы защиты информации в период с 1994 года до начала 2000–х 14](#_Toc167270188)

[4 Период: Вторая половина 2000–х – настоящее время 15](#_Toc167270189)

[Направления развития криптографических систем информационной и кибербезопасности 15](#_Toc167270190)

[Криптографические методы защиты информации в этот период 15](#_Toc167270191)

[Список литературы 17](#_Toc167270192)

# **Введение**

Век за веком шифрование информации становилось актуальным в различных сферах человеческого бытия: от сферы сакрального до сферы бытового. Развитие криптографии и области ее применения обусловлены развитием коммуникационных средств. Широкая доступность телекоммуникационных средств изменила ценность информации, делая ее сверхценной, одновременно повышая значимость криптографических решений, способствующих ее защите. Криптографические методы применяются повсюду и миллиардами людей пользуются ими по всему миру ежедневно. К примеру, они являются неотъемлемой частью стандартных протоколов, что делает относительно легким внедрение сильного шифрования в широкий спектр приложений, для защиты личной информации в интернете.

Научные исследования в сфере информационной безопасности ведутся постоянно, с каждым годом совершенствуя используемые методы для более надежной защиты информации. В истории существует не мало инцидентов связанный со взломом и кражей ценной информации, которые приводили к серьезным последствиям. Но если, раньше под угрозой были в основном государственные организации и большие корпорации, то сейчас этому подвержены и обычные пользователи, которые могут столкнуться с этой проблемой. Поэтому растущая сложность компьютерных сетей, увеличение числа уязвимых пользователей, вовлечение все большего числа документов в электронный документооборот форсируют рост потребности в разработке все более надежных методов защиты. Научные исследования в сфере информационной безопасности ведутся постоянно, с каждым годом совершенствуя используемые методы.

Подводя итог, очевидно, что для более детального понимания важности этого вопроса, стоит ознакомится с историей разработки и использования разного рода шифровальных методов. Понимание того, как и почему были разработаны определенные методы защиты, позволяет оценить их эффективность, а также лучше понимать современные угрозы и способы от их защиты.

**Цель:** рассмотреть историю развития методов защиты информации и повлиявшие на этот процесс факторы.

**Объект исследования:** методы защиты информации

**Предмет исследования:** криптографические и информационные методы защиты информации в период с начала 20 века до настоящего времени.

**Задачи:**

1. Провести обзор и анализ исторических методов защиты информации, таких как шифровальные машины.
2. Проследить история развития технологий криптографической защиты в информационном обществе.
3. Оценить роль криптографических и информационных методов и алгоритмов защиты в современном мире.

# Глава 1. Первый этап: начало 20 века - 1950е

Новая глава развития криптографии началась в начале 20 века. Технические достижения конца ХІХ века, такие как телеграф, телефон и радио, позволяли оставаться на связи даже в самых сложных условиях и обмениваться голосовыми или текстовыми сообщениями по радиоволнам. Для повышения безопасности передачи секретной информации был создан и модифицирован ряд шифровальных машин и шифров, которые позволяли кодировать и декодировать информацию, делая её непонятной для посторонних. Такие шифровальные системы стали важным инструментом военной связи и разведки. Они помогали сохранять конфиденциальность коммуникаций и обеспечивать безопасность передаваемых данных.

### Нидерланды (1915)

Первая дисковая шифровальная машина была разработана офицерами Королевского флота Нидерландов Тео ван Хенгелем и Рудольфом Питером Корнелисом Шпенглером для связи между Вест-Индией и Нидерландами во время Первой мировой войны.

### Шифр Вернама (1917)

Шифр Вернама — это система автоматического шифрования телеграфных сообщений, разработанная в 1917 году американским инженером Гилбертом Вернамом. Он предложил при передаче сообщений электромеханически складывать «импульсы» знаков открытого (незашифрованного) текста с «импульсами» гаммы, которая представляла собой последовательность знаков, предварительно нанесенных на перфоленту, и была секретным ключом.

Система Вернама позволяла автоматически зашифровывать сообщение, введенное с помощью клавиатуры телеграфного аппарата, и одновременно передавать его по каналу связи. Эта система, названная Вернамом «Методом длинной ленты для телетайпов», стала основой для создания системы шифрования «Одноразовый блокнот», абсолютную стойкость которой в 1940-х годах доказали американский криптоаналитик и математик Клод Шеннон и советский ученый Владимир Котельников.

### Шифровальная машина B-21 (1925)

Шифровальная машина В-21, созданная изобретателем Борисом Хагелином, стала первым устройством с нерегулярным шагом шифровальных дисков, которым управляли настраиваемые пины на дисках и штифтовой барабан.

### “Энигма” (1927)

В 1917 году немецкий инженер Артур Шербиус запатентовал роторную шифровальную машину, положив основы для "Энигмы". Его разработка, изначально предназначавшаяся для коммерческих целей, привлекла внимание военных. Шербиус, в сотрудничестве с Фридрихом Риттером и Боргесом Хехтом, усовершенствовал свою машину, адаптировав ее для военных нужд.

Важные технические особенности:

1. Система вращающихся роторов: Сердцем "Энигмы" стала инновационная система из трех вращающихся роторов, каждый из которых был зашифрован своим алфавитом.
2. Коммутационная панель: Дополнительный уровень секретности обеспечивала коммутационная панель, где можно было вручную переназначать соединения между буквами алфавита.
3. Секретный ключ: Безопасность кода гарантировалась секретным ключом, который менялся с определенной периодичностью.

Чтобы расшифровать сообщение Энигмы, получателю необходимо было иметь Энигму с теми же подключениями плагборда, роторами, настройками кольца, позициями левого/центрального/правого роторов и начальными настройками. Это позволяло току пройти по тому же пути в обратном направлении и результатом была подсветка буквы открытого текста на панели освещения. Немцы, имея опубликованные списки ключей, обладали необходимой информацией. У альянсов не было такой информации. Энигма устраняла любые тонкости языка, которыми могли воспользоваться предыдущие методы криптоанализа.

В 1932 году немецкая армия и флот приняли "Энигму" на вооружение, осознав ее огромный потенциал в защите секретных сообщений.

"Энигма" быстро стала основным шифровальным инструментом Германии, обеспечивая небывалый уровень секретности военных планов, дипломатических переговоров и разведданных.

### Первая советская шифровальная машина (1932)

Первая советская шифровальная машина ШМВ-1 («Шифровальная машина Волоска»), разработанная под руководством инженера-конструктора Ивана Волоска, работала по принципу гаммирования: наложение гаммы одноразового ключа на комбинацию знаков открытого текста.

### Вокодер Гомера Дадли (1930e)

В 1930-х годах рост числа абонентов телефонной связи привел к дефициту частотных ресурсов сети, необходимых для передачи широкого диапазона устной речи. Чтобы предоставить услуги телефонной связи всем желающим, нужно было либо прокладывать Новые каналы, либо искать способы экономии частотных ресурсов уже существующих линий. Благодаря революционному устройству вокодеру, разработанному в середине 1930-х годов инженером-акустиком из американской компании Bell Labs Гомером Дадли, такой способ был найден.

Вокодер позволил не только сэкономить частотные ресурсы линий связи, заметно увеличив их пропускную способность, но и нашел применение в секретной телефонии, а позднее - в музыкальной индустрии для создания звуковых эффектов.

### Первая Американская дисковая шифровальная машина (1936)

Первая американская дисковая шифровальная машина для правительственной связи M-325 (Sigfoy), созданная криптографом Уильямом Фридманом, была принята на вооружение американской армии только в 1944 году.

### SZ-40 (1940)

Одна из первых машин для линейного шифрования телеграфного трафика - SZ-40, созданная компанией Lorenz, - была оборудована шестью дисками с нерегулярным шагом, которые генерировали гамму для шифрования. Для взлома этого устройства в 1944 году в Блетчли-Парке, главном шифровальном подразделении Великобритании, был создан «Колоссус» - первый в мире электронный программируемый компьютер.

### NEMA (1946)

NEMA (Neu Enigma Maschine) была разработана сотрудниками Бернского университета (Швейцария) под руководством профессора математики, капитана Артура Адлера к концу Второй мировой войны. Новая машина заменила немецкую Enigma K, которую использовала швейцарская армия до и во время войны. Несмотря на то, что принципы работы этих устройств были схожи, конструкция NEMA имела несколько усовершенствований. В частности, количество дисков швейцарской машины было увеличено до десяти: пять из них были шифрующими, а остальные пять управляли нерегулярным шагом дисков.

Текст из машины мог выводиться не только на ламповую панель, но и на прямую линию телетайпа или на электронную пишущую машинку. С 1946 года было выпущено 640 экземпляров шифровальной машины NEMA в трех несовместимых друг с другом модификациях: учебной, дипломатической и военной (здесь представлена военная модификация машины). Устройство использовалось в швейцарской армии и в Министерстве иностранных дел вплоть до 1970-х годов. В 1991 году шифровальная машина NEMA была рассекречена.

### Клод Шеннон (1949)

Работа Клода Шеннона «Теория связи в секретных системах», выпущенная в 1949 г., является еще одной переходной точкой, когда утвердились новые теоретические принципы криптографической защиты информации. Криптография провозглашается математической наукой.

### Фиалка-M (1963)

«Фиалка» - кодовое название самой популярной советской дисковой электромеханической шифровальной машины, которая оставалась засекреченной до недавнего времени и никогда ранее не была показана широкой публике. Первая модель М-125 была разработана в 1950-х годах на ленинградском заводе Nº 209 (сейчас завод им. А.А. Кулакова) под руководством главного конструктора Николая Гырдымова по заказу Вооруженных сил СССР. Машина была названа «Фиалкой», вероятно, из-за ее небольших размеров. Это кодовое слово использовалось при обсуждениях и в переписке во время ее разработки. А позднее так стали называть и алгоритм шифрования. Использование разборных шифровальных дисков со специальным вкладышем повышало устойчивость машины к взлому. Всего было создано несколько модификаций машины, в том числе для стран - участниц Варшавского договора.

# Глава 2. 2 Этап: 1960 - середина 2000е

## 1 Период: Начало 1960-х – 1970-е

В 1951 году появились первые коммерческие серийные компьютеры в Европе – Ferranti Mark 1 и в США – UNIVAC–I. К 1970 году в мире насчитывалось уже порядка 120 000 ЭВМ.

Криптография решала задачи аутентификации, верификации и безопасности военной и правительственной коммуникации. К этому периоду относится период т.н. научной криптографии, начавшийся в 1930–е годы, характеризующийся созданием криптосистем со строгим математическим обоснованием криптостойкости. В 1960–е годы ведущие криптографические школы подошли к созданию блочных шифров, реализация которых была возможна только в виде цифровых электронных устройств.

**Этот этап обладает следующими характерными особенностями:**

1. Появление и распространение первых ЭВМ
2. Появление первых хакеров и соответственно первых компьютерных преступлений
3. Большое число случаев мошенничества с телефонными сетями – фрикинга.
4. Основные угрозы: утечки по техническим каналам, угрозы сбоев в электропитании и угрозы электронного перехвата
5. Появление первых систем и стандартов компьютерной защиты информации.
6. Появление компьютерной криптографии.
7. Появление систем разграничения доступа (СРД) в компьютерных системах, основанных на парольной идентификации.

### Уязвимости, ARPANET и первые компьютерные вирусы

В 1965 году появилась информация о первой уязвимости в ЭВМ. Её обнаружил Вильям Д. Мэтьюс, когда нашел возможность несанкционированного чтения файла с паролями доступа.

В 1969 году в США появилась сеть ARPANET (разработана в агентстве (Advanced Research Projects Agency) Министерства обороны США) – первая глобальная сеть, связавшая крупнейшие научные центры, исследовательские лаборатории и компании, выполняющие оборонный заказ. В последующие несколько лет ARPANET начала быстро расширяться, объединяя все новые и новые центры. Важным для обеспечения безопасности было то, что сеть была основана на идее разделения времени доступа к ресурсам вычислительных центров.

В 1972 году была написана первая программа для отправки и получения текстовых сообщений, которую создатель Рэй Томлинсон назвал e–mail. Появление электронной почты стало новым этапом развития возможностей общения и связи людей, появилась новая модель взаимодействия пользователей. Помимо e–mail, ARPANET поддерживала удаленное подключение (Telnet) и удаленную загрузку файлов (ftp). Новые технологии связи вычислительных машин спровоцировали появление большого количества компьютерных преступлений.

### Телефонные фрикеры

В то же время, если компьютеры еще не были так популярны, и доступ имели только ограниченное число людей, то телефонные сети были уже достаточно распространены и достаточно прочно вошли в повседневную жизнь.

В 1960–х годах начало появляться достаточно большое число телефонных фрикеров, которые занимались взломом телефонных сетей. Рост числа подобных преступлений был в том числе обусловлен халатностью сотрудников одного из телефонных операторов, опубликовавших в своей статье «Signaling Systems for Control of Telephone Switching» детальную информацию о частотах, используемых для междугородней связи.

В 1971 году Джон Дрэйпер, считающийся «отцом фрикинга», обнаружил, что подарочный свисток из коробки кукурузных хлопьев выдает сигнал определенной частоты, которая использовалась AT&T для осуществления административного доступа к коммутирующим системам. Однако это не было случайностью – Джон Дрэйпер обладал глубокими знаниями в радиоэлектронике и пониманием устройства телефонных аналоговых сетей.

Дрэйпер служит хорошим примером, иллюстрирующим истинную природу хакерства: чтобы взломать какую–то систему, необходимы серьезные знания и понимание того, как система устроена и функционирует.

Фрикеры того времени изготавливали и пользовались специальными устройствами, т.н. "Multi Frequency box" (позже «blue box»), для генерации сигналов различных частот. Bluebox – это довольно простые устройства, состоящее из динамика и кнопочной панели. Вместе с этим, они обладали довольно широким диапазоном действий: бесплатные междугородние переговоры, создание конференций, прорыв сигнала «занято», прослушивание разговоров, разрыв чужого соединения, дозвон на недоступные обычному человеку номера и даже контроль над АТС. В 1971 году вышла статья Рона Розенбаума "Secrets of the Little Blue Box", в которой рассказывалось о фрикерах, существующих уязвимостях и устройстве blue box. Статья привела к популяризации фрикерства и росту числа такого рода преступлений.

Фрикинг оставался распространенным явлением вплоть до появления первых персональных компьютеров. Но в начале 1980–х это «увлечение» или этот вид хакерства заменился актуальным сегодня компьютерным взломом. Многие известные хакеры вышли именно из этой среды (Lex Luthor, Cheshire Catalyst, Nightstalker, Кевин Митник и Кевин Поулсен).

### Защита информации в период 1960-х – середины 1970–х годов

Примерно во второй половине 1960 годов с развитием проекта ARPANET появилось осознание опасности потенциальных угроз компьютерной безопасности. Её родоначальником считается Виллис Вейр (Willis Ware). Активные работы по исследованию проблем безопасности он начал в 1960 годах, подчеркивая необходимость защиты компьютеров и компьютерной информации в связи с ростом зависимости от них государства.

Сложившиеся правила организации работы с конфиденциальными документами стали неэффективны с появлением и внедрением подхода разделения рабочего времени в ARPANET. В существующей системе не было возможности разделения данных и предоставления доступа в соответствии с полномочиями. Первые попытки создания систем разграничения доступа относятся именно к этому этапу – середина 1960 годов – и были предприняты совместно Вейром и Бернардом Питерсом.

## 2 Период: Вторая половина 1970–х – начало 1990–х годов

Появление персональных компьютеров и развитие протокола TCP/IP открыло новый этап в развитии компьютерных преступлений. Сообщество хакеров перестало быть закрытым, новые технологии привели к тому, что ряды «научных или профессиональных» хакеров пополнились хакерами–любителями, появились первые специализированные электронные форумы (Bulletin Board Systems, BBS) и хакерские объединения.

Появление протокола TCP/IP в середине 1970–х, адаптированного для применения в персональных компьютерах, и начало продаж первых относительно недорогих общедоступных модемов создали новые возможности по объединению ПК в локальные сети, которые в свою очередь существенно расширили глобальную сеть ARPANET.

В 1983 году ARPANET полностью перешла на использование протокола TCP/IP, что послужило точкой отсчета для начала трансформации ARPANET в Интернет. Без наличия единого стандарта связи распространение сетей попросту было невозможно. В течение 1980–х глобальные сети прочно вошли в жизнь пользователей по всему миру, уже в 1987 году в сети насчитывалось более 10000 хостов по всему миру.

Появление Интернета, повсеместное распространение компьютеров и сетей, развитие клиент–серверных технологий привели к тому, что вопросы обеспечения компьютерной безопасности в 1990–х стали вопросами, требующими безотлагательного и качественного решения для обеспечения существования и развития любой коммерческой организации.

### Криптографические методы защиты информации в этот период

#### Ассиметричные шифры и системы с открытым ключом

В конце 1970–х годов у коммерческих организаций возникла острая необходимость встроить шифрование в только что появившуюся новую технологию – электронную почту, в основном запрос был сформирован нефтяными и банковскими компаниями.

Этот факт и послужил причиной создания Уитфилдом Диффи и Мартином Хеллманом ассиметричных шифров и систем с открытым ключом (1975 год). Диффи, работая в одной из компаний подрядчиком МО США, заинтересовался вопросами повышения безопасности компьютерных вычислений и возможностью применения математических и криптографических методов в частных коммуникациях.

Открытие Диффи и Хеллмана сделало криптографию доступной обычным людям и позволило применять ее для защиты частной информации. Для широкого практического применения криптографии необходимо было решить проблему обмена ключами без участия центра и без обмена самим секретным ключом. Проблема порождала две сложные задачи: обеспечение целостности и аутентичности информации – надежное шифрование и подтверждение подлинности отправителя. Однако алгоритм Диффи–Хеллмана не мог решить задачу аутентификации сторон.

В 1978 была опубликована работа, содержащая описание новой криптосистемы RSA (Великобритания, авторы Рон Ривест, Ади Шамир и Леонард Адлеман), в которой решалась проблема взаимной идентификации.

Алгоритм RSA обеспечивал необходимую стойкость и надежность. В 1982 году была основана компания RSA Data Security, которая в том числе занималась выдачей лицензий на использование алгоритма RSA в программных продуктах других фирм. В частности он был встроен в продукты Microsoft, Apple и в IBM Lotus Notes.

Ассиметричная криптография, помимо того, что позволила решить свою первую прикладную задачу – шифрование частных коммуникаций (электронной почты), открыла несколько перспективных направлений применения – системы электронной цифровой подписи и электронной коммерции.

#### Биометрические системы (1969)

Первые полуавтоматические системы распознавания лиц появились в 1960–х годах. Тогда же были начаты активные исследования по автоматизации распознавания и идентификации по другим биометрическим характеристикам (отпечатки пальцев, голос, подпись).

* В 1969 году ФБР внедрила первую автоматическую систему идентификации по отпечаткам.
* В 1974 появились первые коммерческие систем биометрической идентификации по геометрии руки.

В течение 1970–1980–х годов продолжались исследования, направленные на совершенствование систем биометрической идентификации: создание сканеров, алгоритмов сравнения, поиск лучших признаков. Были созданы первые системы идентификации по голосу человека. В это же время была доказана возможность идентификации по сетчатке глаза, были получены первые результаты и патенты, и вскоре был обнаружен достаточно эффективный алгоритм идентификации (Dr. John Daugman), на него также был получен патент (владелец компания Iridian Technologies). Сегодня эта разработка и патент лежат в основе всех коммерческих разработок по распознаванию сетчатки глаза.

* В 1991 году появилась первая система распознавания лиц в реальном времени.

Начиная с 1900х биометрические сканеры стали применяться для обеспечения доступа к ПК. Позже, в начале 2000–х годов, развитие технологий биометрической идентификации позволило внедрить ее в переносные устройства. Так, в 2004 году в ноутбуках впервые появились сканеры отпечатков, а в смартфонах – в 2013 (Apple iPhone).

#### FTP (1971)

Протокол передачи файлов FTP (File Transfer Protocol) был разработан для обмена документами по сети между группами ученых. Он позволяет пользователю гарантированно получать файл целиком, без ошибок. Если во время передачи возникает ошибка, процесс копирования останавливается и для пользователя выводится сообщение. Сегодня используют криптографически защищенные версии протокола FTP: SFTP, FTPS.

#### TCP (1974)

Протокол управления передачей данных ТСР (Transmission Control Protocol) был разработан американскими учеными Винтоном (Винтом) Серфом и Робертом (Бобом) Каном для установления соединения и обмена информацией между разными компьютерами и локальными сетями. Протокол позволил решить проблему отсутствия гарантированной доставки пакетов, с которой ученые столкнулись к середине 1970-х годов, обеспечив надежную доставку пакетов без ошибок в том же порядке, в каком они были отправлены. В июле 1976 года Серф и Кан впервые провели эксперимент по передаче данных с использованием ТСР по трем различным сетям. Пакет прошел по маршруту: Сан-Франциско - Лондон - Университет Южной Калифорнии, преодолев 150 000 километров и не потеряв ни одного бита.

#### DES (1977)

Симметричный алгоритм блочного шифрования DES был разработан фирмой ВМ и в 1977 году утвержден правительством США как официальный стандарт шифрования. Он предназначался для защиты важной, но несекретной информации в государственных и коммерческих организациях США. DES осуществляет шифрование блоков данных размером 64 бита.

#### UDP (1980)

Протокол UDP (User Datagram Protocol) позволяет обмениваться данными с другими компьютерами в сети быстрее, чем с помощью протокола ТСР. UDP не требует получения подтверждения о приеме всех пакетов данных, поэтому компьютер-отправитель просто продолжает пересылать информацию. Протокол используется для потоковых приложений, например, в IP-телефонии, в сетевых компьютерных играх, а также на нем построена работа многих современных VPN-клиентов.

#### SMTP (1981)

К началу 1980-х годов существовало несколько почтовых протоколов, например, FTP Mail, где письмо посылалось как файл. Но они не позволяли обмениваться почтой компьютерам разных моделей с разными операционными системами. Чтобы решить эту проблему, американский инженер Джон Постел предложил простой протокол передачи почты SMTP (Simple Mail Transfer Protocol). Он поддерживал возможность пересылки сообщений через промежуточные компьютеры, то есть узлы сетей, находящиеся между отправителем и получателем. Кроме того, SMTP «следил» за доставкой писем и сообщал об ошибке, если часть данных терялась по дороге. Письмо считалось доставленным и оказывалось доступным получателю в почтовой программе только в том случае, если все промежуточные узлы подтверждали успешность доставки.

#### Разработка системы DNS (1983)

Идея давать узлам сети понятные и запоминающиеся имена вместо их числовых адресов была реализована еще в ARPANET. Узел в Стэнфордском университете хранил текстовый файл HOSTS.TXT с записью названий всех узлов. Файл вели вручную.

Чтобы сделать новую запись или запросить название какого-то узла, нужно было позвонить по телефону в Сетевой информационный центр (Network Information Center). В начале 1980-х годов из-за быстрого роста сети перед учеными встала задача автоматизировать процесс. В 1983 году американский ученый Пол Мокапетрис создал систему доменных имен. А через год студенты Университета в Беркли представили первый DNS-сервер BIND (Berkeley Internet Name Domain). Разработанная ими система автоматически преобразовывала DNS-имя в IP-адрес и наоборот. BIND по-прежнему остается одной из самых популярных реализацией DNS-сервера. В 1985 году, когда DNS были внедрены в ARPANET, сразу шесть организаций зарегистрировали свои домены.

## 3 Период: 1990-е – начало 2000–х

Настоящий переворот в использовании Интернета произошел в результате появления новой технологии WWW (World Wide Web). В 1991 году Тим Бернерс–Ли создал первые веб–страницы, положив начало новой технологии www, также им были созданы URI, URL, HTTP, HTML. До этого Интернет служил для передачи файлов, отправки электронной почты и ряда других сервисов. Веб–страницы полностью изменили возможности коммуникации и получения информации, каждый пользователь из любой точки мира мог обратиться по некоторому адресу и получить информацию. Интернет стал доступным, это была новая концепция доступа – «все для всех». Вместе с тем возникли новые угрозы и произошел резкий скачкообразный рост компьютерных или киберпреступлений.

Считается, что 1990–е – это период массового безнаказанного хакерства, в первую очередь обусловленного отсутствием и несовершенством механизмов безопасности, наличием огромного числа уязвимостей в ОС (Windows и UNIX), а также возможностью получить доступ к компьютерным системам, благодаря подключению их к Интернету и массовым использованием одинакового ПО и ОС (Windows и Unix–подобных систем).

В 1993 году прошла первая конференция DefCon. Она сразу же выделилась своей массовостью и разнообразностью тематик. Сегодня это крупнейший съезд хакеров, объединяющий не только тех, кто взламывает сети, но и тех, кто их защищает и поддерживает. DefCon привлекает огромное внимание мировой общественности и является одним из ключевых мероприятий в области защиты информации.

### Криптографические методы защиты информации в период с 1994 года до начала 2000–х

#### Стандарт S/MIME (Secure Multipurpose Internet Mail Extensions)

Разработан компанией RSA Security. Применяется в обеспечении криптографической безопасности электронной почты.

#### Стандарт шифрования SSL (1995)

Криптографический протокол SSL (Secure Sockets Layer) был разработан в тот момент, когда стало понятно, что протокол НТТР, который использовали веб-сайты, не может обеспечить должный уровень безопасности.

SSL-протокол позволил создать защищенный канал связи между браузером пользователя и веб-сайтом, и информация пользователя передавалась на сайт уже строго в зашифрованном виде.

Протокол SSL (позднее TLS) использует два принципа шифрования: симметричное (ключи шифрования и расшифрования одинаковые) для защиты трафика и асимметричное (используется два ключа: открытый и секретный) для аутентификации и создания общего ключа. Подтверждением владения открытого ключа являются SSL-сертификаты, которые надолго стали основой доверия и безопасности при обмене информации в интернете. Алгоритм AES (Advanced Encryption Standard)

#### Captcha (1996)

В 1996 году прообраз капчи разработал израильский криптограф Мони Наор.

Он предложил решение для борьбы со спамом — задание, основанное на тесте Тьюринга. Одна из его идей — просить пользователя определить пол человека по фотографии.

Вскоре разработчики Digital Equipment Corporation заметили, что системы распознавания текста не могут «прочитать» буквы, если они растянуты или повернуты, хотя для людей такие искажения несущественны. Так появилась известная всем капча, после внедрения которой количество спам-запросов значительно снизилось.

#### Криптографический алгоритм шифрования AES

AES – это алгоритм блочного симметричного шифрования. Сегодня алгоритм AES применяется для защиты данных в правительственных и банковских организациях, для защиты беспроводных соединений, а также для защиты государственных данных США уровня «совершенно секретно».

## 4 Период: Вторая половина 2000–х – настоящее время

Последний этап развития компьютерных преступлений и программно-аппаратных средств защиты информации начался примерно в середине 2000–х годов. Его начало связано с повсеместным распространением Интернета и социальных сетей, появлением доступных мобильных устройств (смартфоном, планшетов), развитием технологий мобильной и беспроводной связи.

Новые технологии порождают как новые виды угроз, так и ведут к трансформации и актуализации старых.

### Направления развития криптографических систем информационной и кибербезопасности

1. Адаптация криптографических примитивов для использования в производственных и киберфизических системах.
2. Разработка методов аудита киберфизических систем.
3. Разработка эффективных реализаций легковесной криптографии для новых технологий.
4. Разработка системы обеспечения целостности и конфиденциальности данных в распределенных системах хранения и обработки информации.

### Криптографические методы защиты информации в этот период

2004:

* Революция в финансах: появляется Bitcoin, первая криптовалюта, использующая криптографию для обеспечения безопасности и защиты от подделок. Bitcoin не только меняет правила игры в мире финансов, но и стимулирует развитие новых технологий, таких как блокчейн, которые имеют широкий спектр применения.

2008:

* Укрепление защиты: Разработан новый алгоритм шифрования SHA-256, который более устойчив к взлому, чем его предшественники. SHA-256 используется для защиты программного обеспечения, цифровых подписей и других важных данных, повышая уровень безопасности в цифровом мире.

2013:

* Конфиденциальность под угрозой: Раскрытие программы слежки PRISM вызывает озабоченность по поводу конфиденциальности в интернете и стимулирует интерес к более надежным методам шифрования. Это событие подчеркивает важность криптографии для защиты информации от несанкционированного доступа.

2017:

* Защита от квантовых компьютеров: Создан алгоритм CRYSTALS-Kyber, устойчивый к взлому квантовыми компьютерами. Квантовые компьютеры потенциально могут взломать многие современные методы шифрования, поэтому разработка устойчивых к ним алгоритмов имеет критическое значение.

2018:

* Квантовая связь: Запущен проект QCrypt, направленный на создание абсолютно защищенных каналов связи с использованием квантовых эффектов. QCrypt может революционизировать способ передачи конфиденциальной информации, делая ее недоступной для взлома.

2019:

* Вычисления над зашифрованными данными: Разработан алгоритм HElib, позволяющий выполнять вычисления над зашифрованными данными без их расшифровки. HElib может иметь широкий спектр применений, таких как защита медицинских данных и обеспечение конфиденциальности финансовых транзакций.

2020:

* Блокчейн набирает обороты: Технология блокчейн, использующая криптографию для обеспечения безопасности и прозрачности, становится все более популярной. Блокчейн используется в различных областях, таких как криптовалюты, логистика и управление цепочками поставок.

# Список литературы

* 1. Гатченко Н.А., Исаев А.С., Яковлев А.Д. Криптографическая защита информации// СПб: Университет ИТМО, 2012.
  2. Воробьев А.А., Пантюхин И.С. История развития программно-аппаратных средств защиты информации// СПб: Университет ИТМО, 2017.
  3. Джонатан Катц. Введение в современную криптографию. Второе издание// Издательство «СиЭрСи» «Тэйлор энд Фрэнсис Груп», 2016. 2Глава
  4. Henk C.A. van Tilborg. Encyclopedia of Cryptography and Security// Eindhoven University of Technology The Netherlands, 2005.
  5. Dan Bohner, Victor Shoup. A Graduated course in Applied Cryptography//Stanford, 2017
  6. Назаров А.П. Криптографические методы защиты информации// Перспективы развития информационных технологий, 2014.
  7. Литература музея