**Безопасность в сетях**

1. **Первые сети** использовались для обмена файлами или для совместного использования оборудования (принтеров, сканеров и т.п.) и поэтому вопросы безопасности **на этом этапе не привлекали особого внимания**.
2. Большинство проблем безопасности возникает из-за **злоумышленников (злостных или случайных)**, пытающихся извлечь пользу для себя и причинить вред другим. Причем криминальная статистика говорит, что большинство атак на информационные системы возникают изнутри системы (специалистами эксплуатирующими систему).
3. На сегодняшний день **специалист по информационной безопасности – наиболее востребованная профессия**.
4. В первом приближении вопросы безопасности могут быть разделены на 4 пересекающиеся области:

* **секретность (конфиденциальность)**;
* **аутентификация**;
* **обеспечение строгого выполнения обязательств (не возможность отказа от авторства**;
* **обеспечение целостности**.

1. **Конфиденциальность** –предотвращение попадания информации неавторизованным пользователям.
2. **Аутентификация** - проверка принадлежности субъекту предъявленного им идентификатора (подтверждение личности). Процесс аутентификации может осуществляться различным способом:

- логин и пароль;

- электронный сертификат;

- старт-карта;

- идентификация личности по биометрическим данным.

1. **Идентификация** -процесс присвоение субъектам идентификатора и сравнение идентификатора с перечнем идентификаторов.
2. **Авторизация** -процесспроверки прав субъекта на выполнение некоторых действий (говорят: пользователь авторизовался в системе). Иногдапроцесс предоставление прав доступа (говорят: администратор системы авторизует пользователя – наделяет его перечнем прав и полномочий).
3. **Обеспечение строгого выполнения обязательств** - электронная подпись документа, гарантирующая подлинность отправителя.
4. **Обеспечение целостности** – методы защиты электронных документов от модификации в процессе передаче по сети.
5. Безопасность в сетях охватывает **все уровни протоколов**: 1) на **физическом** уровне можно поместить сетевой кабель в специальные герметические трубы наполненные специальным газом (если просверлить, то утечка газа вызывает сигнал тревоги); 2)на **логическом** уровне – аппаратное сжатие, шифрование, перемешивание и пр. данных; 3) на **сетевом** уровне – firewall и brandmauer (отвергаются подозрительные пакеты); 4)на **транспортном** уровне – можно поддерживать зашифрованное соединение между процессами; 5)на **сеансовом** уровне – продолжительность действия ключей для шифров; 6) на **представительском** уровне – методы шифрования; 4) на **прикладном** уровне – процессы аутентификации.
6. На всех уровнях за исключением физического защита информации осуществляется на основе **криптографии**.
7. **Криптография (греч. скрытое письмо)** – наука о методах обеспечения **конфиденциальности (секретности)** и **аутентичности (целостности и невозможность отказа от авторства)**.
8. Родственные понятия для криптографии: **криптосистема** – семейство обратимых преобразований открытого текста; **криптоанализ** – наука, изучающая методы разрушения конфиденциальности и целостности; **криптология** = криптография + криптоанализ; **криптографическая стойкость** - способность криптографического алгоритма противостоять криптоанализу.
9. **Шифр** – побитовое или посимвольное преобразование независимое от лингвистической особенности сообщения. **Ключ** – параметр шифра, определяющий преобразование открытого текста. **Код** – заменяет слово языка другим словом или символом (американцы использовали язык индейского племени навахо (использовали носителей языка) в ходе переговоров на войне с Японией). Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты документа от подделки и позволяющий установить подлинность отправителя.

Назначение и применение ЭЦП

Цифровая подпись предназначена для аутентификации лица, подписавшего электронный документ[1]. Кроме этого, использование цифровой подписи позволяет осуществить:

Контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.

Защиту от изменений (подделки) документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.

Невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом.

Доказательное подтверждение авторства документа: Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец пары ключей может доказать своё авторство подписи под документом. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т. д.

Все эти свойства ЭЦП позволяют использовать её для следующих целей[2]:

Декларирование товаров и услуг (таможенные декларации)

Регистрация сделок по объектам недвижимости

Использование в банковских системах

Электронная торговля и госзаказы

Контроль исполнения государственного бюджета

В системах обращения к органам власти

Для обязательной отчетности перед государственными учреждениями

Организация юридически значимого электронного документооборота

В расчетных и трейдинговых системах

1. Два фундаментальных принципа криптографии**: избыточность** (все пересылаемые данные должны содержать дополнительную информацию не используемую для понимания сообщения); **ограниченный срок действия** - сообщения не должны повторятся (фильм «Игры разума», Джон Нэш (Рассел Кроу), расшифровали предаваемые координаты).
2. Стандарты шифрования: **DES (Data Encryption Standard)** (IBM 56 бит, тройной 168 бит), **AES (Advanced DES)** (NIST,128, 192, 256 бит), **Rijndael**(128-256 бит).

Американский стандарт симметричного шифрования DES (Data Encryption Standard — стандарт шифрования данных) разработан и принят в 1977 г. При разработке считалось, что стандарт выбирается на 10—15 лет, однако решение о смене стандарта было принято только в 1997 г., т.е. через 20 лет. Причем серьезных недостатков в архитектуре алгоритма найдено не было, за исключением одного — чересчур короткого ключа.

Ключ шифрования DES имеет размер 64 бита, из которых 56 бит являются значащими, а остальные используются для контроля четности. DES - симметричная криптосистема, определенная как 16-раундовый [шифр Фейстеля](http://www.racal.ru/rsp/f.htm#Feistel), была первоначально предназначена для аппаратной реализации. Когда DES используется для передачи информации, то чтобы зашифровать и расшифровать сообщение или чтобы создать и проверить код подлинности сообщения, отправитель и получатель должны знать секретный ключ. DES может также использоваться одним пользователем, например, для шифрования файлов на жестком диске. В многопользовательской среде организовать защищенное распределение ключа сложно; идеальное решение этой проблемы предлагает криптография общего ключа.

Национальный институт стандартизации и технологий США (NIST) в 2004г. официально [признал](http://www.infoworld.com/article/04/07/29/HNdesinadequate_1.html) популярный стандарт шифрования DES недействительным и объявил, что государственный патент на его использование будет аннулирован. Причина отмены патента - недостаточная стойкость шифра DES. В 1997 г. такого размера хватало с запасом, но с тех пор компьютерная техника развивалась настолько быстро, что 56-битового ключа стало недостаточно.

Поэтому в 1997 г. было принято решение обновить стандарт, и с этой целью объявили о проведении конкурса AES (Advanced Encryption Standard — «продвинутый» стандарт шифрования) по выбору нового стандарта.

На конкурс могли быть присланы алгоритмы шифрования, разработанные как организациями, так и частными лицами в любой стране. Алгоритм-победитель этого конкурса должен был стать новым стандартом блочного симметричного шифрования США.

Для участия в конкурсе алгоритм шифрования должен был соответствовать всего двум обязательным требованиям:

* 128-битный размер блока шифруемых данных,
* не менее трех поддерживаемых алгоритмом размеров ключей шифрования: 128, 192 и 256 бит.

Кроме того, NIST предъявил большое число требований, носивших рекомендательный характер:

1.     Алгоритм должен быть стойким против криптоаналитических атак, известных на время проведения конкурса.

2.     Структура алгоритма должна быть ясной, простой и обоснованной.

3.     Должны отсутствовать слабые и эквивалентные ключи (т.е. ключи, являющиеся различными, но приводящие к одному и тому же результату шифрования).

4.     Скорость шифрования данных должна быть высокой на всех потенциальных аппаратных платформах – от 8-битных до 64-битных.

5.     Структура алгоритма должна позволять распараллеливание операций в многопроцессорных системах и аппаратных реализациях.

6.     Алгоритм должен предъявлять минимальные требования к оперативной и энергонезависимой памяти.

7.     Не должно быть ограничений для использования алгоритма.

Список участников конкурса оказался весьма разнообразен, но среди них в ходе длительного анализа был выбран победитель - алгоритм Rijndael, который по большинству критериев оказался лучшим и стал называться AES.

1. **Алгоритмы с открытым ключом**: Диффи и Хелман D(E(P))=P, E = f(D) – легко, D = ff(E) – трудно вычислить. Одностороння функция. Открытым ключом можно только зашифровать, а расшифровать сложно, для расшифровки специальный скрытый ключ. Алгоритм RSA. **Ассиметричное шифрование**.
2. **IPsec (RFC 2401-2412) –** набор протоколов длязащиты данных передаваемых с помощью IP.IPsec встроен в **IPv6** и является его неотъемлемой частью. **IPsec** состоит: 1)протоколы для защиты потока - **AH** (**Authentication Header,** гарантируется целостность, но данные не шифруются) и **ESP (Encapsulation Security Payload**, обеспечивает целостность и шифрование**);** 2) протокол обмена криптографическими ключами **IKE** **(Internet Key Exchange)**.

**1.1. Краткая историческая справка появления протокола**

В 1994 году Совет по архитектуре Интернет IAB (<http://www.iab.org/>) выпустил отчет **«Безопасность архитектуры Интернет»**. В этом документе описывались основные области применения дополнительных средств безопасности в сети Интернет, а именно защита от несанкционированного мониторинга, подмены пакетов и управления потоками данных. В числе первоочередных и наиболее важных защитных мер указывалась необходимость разработки концепции и основных механизмов обеспечения целостности и конфиденциальности потоков данных. Поскольку изменение базовых протоколов семейства TCP/IP вызвало бы полную перестройку сети Интернет, была поставлена задача обеспечения безопасности информационного обмена в открытых телекоммуникационных сетях на базе существующих протоколов. Таким образом, начала создаваться спецификация IPSec.

**1.2. Архитектура, функции, режимы работы и стандарты IPSec**

**IPSec** — это комплекс протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов; в его состав на данный момент входят около 20ти предложений по стандартам и 18ти RFC.

Первоначально протоколы IPSec были определены в RFC с номерами от **1825** до **1827**, принятых в **1995 году**. В **1998 году** были приняты новые редакции стандартов (**RFC с 2401** по **2412**), несовместимые с **RFC 1825—1827**. В **2005 году** была принята третья редакция, незначительно отличающаяся от предыдущей.

**Общая архитектура IPsec** описана в **RFC 4301**, **аутентифицирующий заголовок** — в **RFC 4302**, **инкапсуляция зашифрованных данных** — в **RFC 4303**. Ряд других RFC описывает другие детали IPsec, такие как применение различных алгоритмов шифрования, протоколы обмена ключами и т. п.

Большинство современных (**2007 год**) реализаций IPsec основано на **RFC 2401-2412**.

Вот наиболее использующие в настоящее время:

|  |  |  |
| --- | --- | --- |
| **RFC**  **Количество** | **Имя** | **Описание** |
| **2401** | Архитектура безопасности для Интернет-протокола | Основной документ, описывающий архитектуру IPSec. |
| **2402** | Аутентификация IP заголовка | Определяет AH протокол, используется для обеспечения целостности данных. |
| **2403** | Использование HMAC-MD5-96 в пределах ESP и AH | Описывает особенности алгоритма шифрования для использования AH и ESP называемой сообщения Сборник 5 (MD5). |
| **2404** | Использование HMAC-SHA-1-96 в пределах ESP и AH | Описывает особенности алгоритма шифрования для использования AH и ESP призвал Безопасный алгоритм хеширования 1 (SHA-1). |
| **2406** | IP Encapsulating безопасности полезной нагрузки (ESP) | Описывает IPSec Инкапсуляция безопасности полезной нагрузки (ESP) протокол, который обеспечивает шифрование данных для сохранения конфиденциальности. |
| **2408** | Интернет Ассоциация безопасности и управления ключами протокола (ISAKMP) | Определяет методы для обмена ключами и переговорных безопасности ассоциаций. |
| **2409** | IKE | Описывает IKE протокол используется для ведения переговоров безопасности ассоциациями и обмен ключами между устройствами для безопасной связи. Основываясь на ISAKMP и Oakley. |
| **2412** | Oakley ключевые определения протокола | Описывает общий протокол для обмена ключом. |

Средства безопасности для IP описываются семейством спецификаций IPsec. Следовательно, IPSec работает на третьем уровне модели OSI – сетевом, в результате чего защита передаваемых IP-пакетов становится прозрачной для сетевых приложений т.о. IPSec призван обеспечить низкоуровневую защиту.

**Спецификация IPSec** разрабатывается Рабочей группой IP Security Protocol IETF (http://www.ietf.org/).

**Основными функциями IPSec являются:**

* Обеспечение конфиденциальности.

Отправитель должен иметь возможность шифровать пакеты перед тем, как передавать их по сети.

* Обеспечение целостности.

Получатель должен иметь возможность аутентифицировать стороны, учавствующие в процессе обмена информацией, и пакеты IPSec, посылаемые этими сторонами, дабы быть уверенным в том, что передаваемые данные не были изменены в пути.

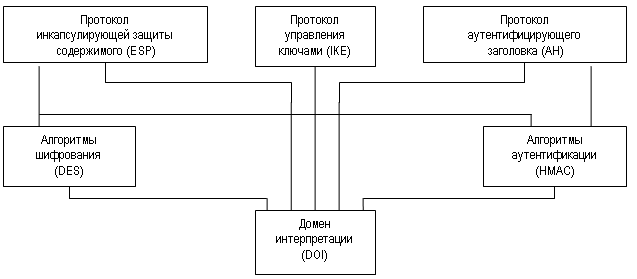
* Обеспечение защиты от воспроизведения пакетов.

Получатель должен иметь возможность обнаруживать и отбрасывать воспроизведенные пакеты, исключая таким образом проведение атак внедрения посредника.

**В комплекс спецификации IPSec входят следующие протоколы и стандарты:**

* **IKE**, обеспечивающий аутентификацию сторон, согласование параметов ассоциаций защиты (SA), а так же выбор ключей шифрования.
* **AH**, обеспечивающий аутентификацию пакетов и выявление их воспроизведения.
* **ESP** - обеспечивает конфиденциальность, аутентификацию источника и целостность данных, а также сервис защиты от воспроизведения пакетов.
* **HMAC** - механизм аутентификации сообщений с использованием хэш- функций.
* **DES**, 3DES – стандарты шифрования данных.

Взаимосвязи между протоколами представлены на рисунке 1:



**Рис 1**. Архитектура IPSec

Архитектура IPSec специфицирована в документе Security Architecture for the Internet Protocol (2401). Ее основные составляющие представлены в соответствии с рисунком 1. Это, прежде всего протоколы обеспечения аутентичности (протокол аутентифицирующего заголовка - AH) и конфиденциальности (протокол инкапсулирующей защиты содержимого - ESP), а также механизмы управления ключами (IKE). На более низком архитектурном уровне располагаются конкретные алгоритмы шифрования и аутентификации. Наконец, роль фундамента выполняет так называемый домен интерпретации (DOI), являющийся, по сути, базой данных, хранящей сведения об алгоритмах, их параметрах, протокольных идентификаторах.

**Режимы работы IPSec**

Существует два режима работы IPsec: **транспортный режим** и **туннельный режим**.

В транспортном режиме шифруется только информативная часть IP-пакета. Заголовок IP-пакета не изменяется (не шифруется). Транспортный режим как правило используется для установления соединения между хостами. Он может также использоваться между шлюзами, для защиты туннелей, организованных каким-нибудь другим способом (IP tunnel и др.).

В туннельном режиме IP-пакет шифруется целиком. Для того чтобы его можно было передать по сети, он помещается в другой IP-пакет. По существу, это защищённый IP-туннель. Туннельный режим может использоваться для подключения удалённых компьютеров к виртуальной частной сети или для организации безопасной передачи данных через открытые каналы связи (например, Интернет).

Режимы IPSec не являются взаимоисключающими. На одном и том же узле некоторые SA могут использовать транспортный режим, а другие — туннельный.

## 1.3. Принципы работы

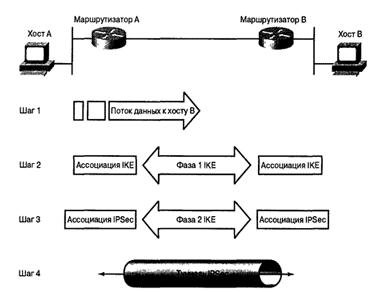
Целостность и конфиденциальность данных посредством IPSec обеспечивается за счет реализации механизмов аутентификации сторон и пакетов, а также шифрования, которые, в свою очередь, требуют предварительного согласования сторонами параметров информационного обмена – так называемого «контекста безопасности»- используемых криптографических алгоритмов, протоколов управления ключами и их параметров.

**Спецификация IPSec** является алгоритмонезависимой, то есть предусматривает возможность использования сторонами нескольких протоколов и параметров аутентификации и шифрования, различных схем распределения ключей. Результатом согласования контекста безопасности является индекс параметров безопасности (SPI), который представляет собой указатель на определенный элемент базы данных политики безопасности (SPD). На основании информации, содержащейся в SPD, для пакета данных может быть выбрано одно из трёх действий: отбросить пакет, обработать пакет без вмешательства IPSec или обработать пакет с помощью IPSec. В последнем случае в SPD также содержится указатель на SA, который необходимо использовать в процессе обмена данными.

В свою очередь SA – это согласованная политика или способ обработки данных, которыми обмениваются стороны. Два устройства с каждой стороны одной ассоциации защиты содержат данные о протоколах, алгоритмах и ключах, используемых в SA. Отдельно взятая ассоциация защиты используется для связи только в одном направлении, для двунаправленной связи их требуется две. Каждый SA реализует один режим и протокол, поэтому в случае, когда для анализа некоторого пакета требуется применить два протокола (например, AH и ESP, хотя этот случай и является очень редким), требуется создание двух различных SA.

**Процесс функционирования IPSec в общем случае можно разбить на следующие шаги:**

1. Инициация IPSec. Приложение, трафику которого требуется защита IPSec, начинает процесс обмена данными IКЕ-протокола.
2. Первая фаза IKE, в которой выполняется аутентификация сторон, и ведутся переговоры о параметрах ассоциаций защиты IKE, в результате чего создается защищенный канал для обмена параметрами защиты IPSec в ходе второй фазы IKE.
3. Вторая фаза IKE, по ходу которой ведутся переговоры о параметрах ассоциации защиты IPSec, создаются соответствующие SA для устройств обеих сторон.
4. Собственно передача данных, т.е. процесс обмена данными, основывающийся на параметрах IPSec и ключах, хранимых в SPD.
5. Завершение работы IPSec. SA IPSec завершают свою работу в результате либо их удаления, либо превышения лимита времени их существования.



**1.4. Оценка IPSec**

Спецификация IPSec получила неоднозначную оценку со стороны специалистов**.**

**С одной стороны**, отмечается, что протокол IPSec является лучшим среди всех других протоколов защиты передаваемых по сети данных, разработанных ранее (включая разработанный Microsoft PPTP).

**По мнению** **другой стороны**, присутствует чрезмерная сложность и избыточность протокола. Так, Niels Ferguson и Bruce Schneier в своей работе "A Cryptographic Evaluation of IPsec" отмечают, что они обнаружили серьезные проблемы безопасности практически во всех главных компонентах IPSec. Эти авторы также отмечают, что набор протоколов требует серьезной доработки для того, чтобы он обеспечивал хороший уровень безопасности.

**ГЛАВА 2. IKE**

**IKE**— протокол обмена Интернет-ключами. Этот протокол предусматривает метод аутентификации для защиты данных и каналов связи и позволяет кодировать заголовки и содержимое пакетов с помощью ключа, обеспечивая практически абсолютную безопасность линии связи. В соответствии с протоколом IKE пакеты шифруются с помощью секретного ключа, заранее известного обеим сторонам, или с помощью стандартного открытого ключа.

**Протокол IKE** является гибридным протоколом, обеспечивающим специальный сервис для IPSec, а именно аутентификацию сторон IPSec, согласование параметров ассоциаций защиты IKE и IPSec, а также выбор ключей для алгоритмов шифрования, используемых в рамках IPSec.

Протокол IKE опирается на протоколы **ISAKMP** (-- протокол управления ассоциациями и ключами защиты в сети Интернет) и Oakley, которые применяются для управления процессом создания и обработки ключей шифрования, используемых в преобразованиях IPSec.

IKE поддерживает набор различных примитивных функций для использования в протоколах. Среди них можно выделить хэш-функцию.

**Хэш-функция** - это функция, устойчивая к коллизиям. Под устойчивостью к коллизиям понимается тот факт, что невозможно найти два разных сообщения m1 и m2, таких, что

H(m1)=H(m2), где H – хэш-функция.

Технология IKE реализована большинством крупнейших производителей (Cisco Systems, Check Point, IBM, Microsoft) и прошла апробацию/внедрение в большом количестве системных проектов.

Электронная Беларусь

С 2003 года действует в Республике Беларусь государственная программа поэтапного перехода к информационному обществу «Электронная Беларусь», которая предполагает создание в республике единой инфраструктуры с широким использованием информационных технологий в государственном управлении, народном хозяйстве, образовании, медицине, торговле и других сторонах жизни общества. В настоящий момент программы состоит из девяти направлений и включает порядка 100 проектов.

Обратной стороной информатизации общества является проблема защиты информации. Утечка, искажение или разрушение информации может негативно отразиться на деятельности государственных органов управления, предприятий и организаций, нарушить права физических лиц и т.п. В условиях информационного общества одной из основных задач стоящих перед государством является построение инфраструктуры национальной информационной безопасности.

**Инфраструктура национальной информационной безопасности.** Инфраструктура национальной информационной безопасности (ИНИБ)представляет собой комплекс взаимосвязанных обслуживающих систем различной природы (организационных, правовых, информационных и т.п.) обеспечивающих основу для решения задачи информационной безопасности (ИБ) в масштабах страны. ИНИБ является составной частью общей системы национальной безопасности страны. На рис. 1 представлена обобщенная схема ИНИБ, исторически сложившаяся в большинстве развитых стран. На рисунке изображены основные элементы ИНИБ (замкнутые фигуры, различной геометрии) и подписанные стрелки, указывающие тип взаимоотношения между парами элементов.

Основой любой ИНИБ является законодательная и нормативно-правовая база обеспечения информационной безопасности (ЗБИБ), являющаяся выражением государственной политики в этой сфере. Государство исходит из того, что информационные ресурсы являются объектами собственности, участвующими в хозяйственном обороте. Законы и правовые акты ЗБИБ наделяют определенные органы государственной власти полномочиями осуществлять государственное регулирование, контроль (мониторинг) и управление в сфере информационной защиты, а также определяют взаимоотношение субъектов информационной деятельности. Технические нормативные акты представляют собой стандарты и технические регламенты, которые могут (или обязаны) использовать субъекты информационной деятельности. Ответственность субъектов информационной деятельности за нарушение законов в сфере информационной безопасности определяется Уголовным и Административным кодексами.

Условно субъекты в сфере информационной безопасности можно разбить на три группы: государственные учреждения, осуществляющие государственное регулирование в этой сфере (группа Г); разработчики технических средств защиты информации (группа Р) и пользователи (группа П). Очевидно, что все эти группы пересекаются.

Полномочия и деятельность субъектов группы Г, определена законом или специальными положениями. Группа Г координирует и лицензирует всю деятельность по технической защите информации, разрабатывает (или участвует в подготовке) нормативных правовых актов, осуществляет экспертизу (сертификацию) технических средств информационной безопасности. Кроме того, субъекты этой группы осуществляют управление государственными информационными системами, связанными с информационной безопасностью (например, удостоверяющие и регистрационные центры).

Основной деятельностью субъекты группы P является разработка технических средств защиты информации. Свою деятельность они осуществляют на основе лицензии, а все созданные ими средства защиты должны пройти сертификацию, прежде, чем они будут применяться пользователями. Сертификация – это процедура подтверждения соответствия продукции определенным техническим нормативным документам (стандартам).

Пользователи информационных систем (группа П) представляют самую многочисленную группу субъектов в сфере информационной безопасности. Субъекты этой группы применяют средства технической защиты информации для защиты собственных информационных ресурсов и взаимодействуют с системами защиты других субъектов. В своей деятельности они могут использовать государственные автоматизированные системы, обеспечивающие сервисные услуги в области технической защиты информации.

Исторически первой ИНИБ сложилась в США. Первый закон о защите информации датируется 1906 годом, а на сегодняшний день ЗБИБ США насчитывает их более 500 [5, 6].

Появление глобальных информационных систем привело к необходимости выработки единого подхода к проблемам информационной безопасности на международном уровне.

Первый важный шаг, который сделан в этом направлении, является разработка международных стандартов по информационной безопасности.

По понятным причинам основой международных стандартов по информационной безопасности стали стандарты, разработанные стандартизирующими организациями ведущих индустриальных стран (прежде всего США и Великобритании). Нормативная документация национальной ЗБИБ, как правило, являются гармонизированными международными стандартами.

**Международные стандарты по информационной безопасности.** Основой для большинства международных стандартов информационной безопасности (таблица 1, столбец «ISO/IEC») служат нормативные документы, разработанные национальными стандартизирующими организациями ведущих индустриальных стран, профессиональными техническими организациями, международными консорциумами или ведущими в области информационных технологий компаниями.

Таблица 1. Основные международные стандарты информационной безопасности

|  |  |  |  |
| --- | --- | --- | --- |
|  | Группы стандартов | ISO/IEC | СТБ |
| 1 | Терминология, общие понятия | 2383-8; 10164-7,8; 10181-1, 2,3,4,5,6,7; 10745; 24767-1; 15443-1, 2,3; 9798-1; 15292; 15816; 18014-1, 2, 3 | 34.101.27, 30 |
| 2 | Требования безопасности,  критерии и методологии оценки, методики испытаний | 15408-1,2.3; 19791; 15446; 18045; 19790; 18045; 24759; 15446 | 34.101.1, 2, 3, 8, 9, 10, 12, 13, 15 |
| 3 | Методы и алгоритмы шифрования, цифровая подпись | 9797-1,2; 10116; 10118-1,2,3,4; 13888-2, 3; 15946-1; 18031, 18032, 18033-1,2,3,4; 9796-2, 3; 9798-2, 3, 4, 5; 14888-1,2,3; 15945; 9594-8 | П 34.101.27, 31; П ISO/IEC 10118-3; П ISO/IEC 18033-1, 3; 34.101.24. 25, 26, 31;  1176-1, 2;  ГОСТ 28147-89 |
| 4 | Управление ключами | 11770-1,2,3, 4 |  |
| 5 | Защита сетевых технологий | 18028-1,2,3,4,5 |  |
| 6 | Организация информационной безопасностью, управление безопасностью, рисками и защитой информации | 13335-1, 27001, 27002, 27005, 27006, 18043,18044, 21827; 24762, 14516; 15447; | П ISO/IEC 27001 |
| 7 | Специализированные стандарты | 9579(SQL), 14762, 29341-13-10,11(UPnP); 15067-4(HES) |  |

Исторически первым (1983 г.) стандартом, сформулировавшим критерии безопасности и получившим широкое распространение, стал стандарт Министерства обороны и Национального комитета компьютерной безопасности США «Критерии оценки доверенных компьютерных систем» (Trusted Computer System Evaluation, TCSEC), чаще всего называемый по цвету обложки «Оранжевой книгой». Стандарт определяет четыре «уровня доверия» к компьютерным системам: D, C , B, A ( перечислены в порядке усиления требований). Уровни С и B подразделяются на классы: C1, C2 и B1, B2, B3. Европейской переработкой этого стандарта является документ «Гармонизированные критерии Европейских стран» (Information Technology Security Evaluation Criteria, ITSEC), опубликованный в 1991 г. от имени соответствующих органов четырех стран: Франции, Германии, Нидерландов и Великобритании.

Часто в литературе упоминается федеральный стандарт США FIPS 140-2 «Требования для безопасности криптографических модулей» (Security requirements for cryptographic modules), опубликованный в 2001 г., заменивший действующий c 1994 г. аналогичный стандарт FIPS 140-1. Для оценки уровня безопасности стандарт использует специальную модель – криптографический модуль, представляющий собой набор программных и (или) аппаратных средств, заключенных в пределах явно определенного и непрерывного периметра.

Наиболее известным международным проектом в области оценки безопасности, результаты которого послужили основой международного стандарта ISO/IEC 15408, является проект «Общие критерии оценки безопасности информационных технологий» (Common Criteria IT Security Evaluation, CC), более известный под коротким наименованием «Общие критерии» [5]. Проект стартовал в 1993 году по инициативе правительственных организаций шести стран: Канады, США, Великобритании, Германии, Нидерландов и Франции. Первоисточниками для проекта авторы называют документы перечисленные выше. Стандарт предусматривает семь уровней безопасности. Все требования к информационной безопасности разбиты на два вида: функциональные и требования доверия. Модель требований представляется в виде иерархии: класс-семейство-компонент элемент. Требования безопасности оформляются в виде специальных документов «Профиля безопасности» (для семейства информационных систем) или «Задания по безопасности» для конкретной системы.

Международный стандарт ISO/IEC 15408: 1999 фактически совпадает с версией 2.1 отчета «Общие критерии».

Стандарты менеджмента, аудита и сертификации информационной безопасности излагаются в международных стандартах ISO/IEC 27001 ISO/IEC 27002, ISO/IEC 27005 и ISO/IEC 27006. Все они являются развитием британского национального стандарта BS 7799. Важным является то, что эти стандарты совместимы с известными стандартами ISO 9000, ISO 9001 и ISO 14001, регламентирующими менеджмент качества на предприятии.

Большое влияние на стандарты безопасности оказывают рекомендации одной старейших стандартизирующих организаций в области телекоммуникаций и радио – Международного союза электросвязи (International Telecommunication Union, ITU). Рекомендации X.800 («Архитектура безопасности для взаимодействия открытых систем»), серия X.500 («Служба директориев») лежат в основе стандартов безопасности распределенных систем.

Стандарты безопасности Интернет разрабатываются группой IETF (Internet Engineering Task Force) сообщества Интернет (ISOC). Наиболее применяемыми являются следующие спецификации:

- IKE/IPSec (RFC 2401-2412, 2451) для протокола IP версий 4 и 6;

-TLS (RFC 2246) для протокола транспортного уровня;

- GSS-API (RFC 2744) – обобщенный прикладной интерфейс службы безопасности;

- протокол Kerberos (RFC 1510, 1964) для аутентификации в разнородной распределенной среде.

Международные стандарты представляют собой исчерпывающую основу для построения систем информационной безопасности. Национальные стандартизирующие организации в основном идут по пути гармонизации (адаптации) в международных стандартов. Процесс гармонизации определяется руководством ISO/IEC 2 и, как правило, сводится к переводу, изменению шифра и (или) формы.

**Инфраструктура национальной информационной безопасности республики Беларусь.** Инфраструктура национальной информационной безопасности республики Беларусь собственное наполнение.

**Законы и правовые акты о защите информации в республике Беларусь**. ЗБИБ Беларуси основывается на двух законах: «Об информатизации» и «Об электронном документе».

Закон «Об информатизации» принят 6 сентября 1995 года, а 9 октября 2008 года Палатой представителей Национального собрания Республики Беларусь был принят проект Закона Республики Беларусь «Об информации, информатизации и защите информации», внесенный Советом Министров Республики Беларусь и предполагающий отмену закона 1995 года [3]. Закон определяет процедуры управления и регулирования в сфере защиты информации.

Закон «Об электронном документе» был принят 10 января 2000 года, а 10 сентября 2008 года в Совет Министров Республики Беларусь представлен проект закона «Об электронном документе и электронной цифровой подписи» [2]. Этот закон «устанавливает правовые основы применения электронных документов, определяет основные требования, предъявляемые к электронным документам, а также права, обязанности и ответственность участников правоотношений, возникающих в сфере обращения электронных документов». Кроме того, закон определяет понятие электронной подписи, как неотъемлемую часть электронного документа.

**Государственное регулирование и управление в сфере защиты информации**. В соответствии со статьей 8 нового закона «Государственное регулирование и управление в сфере информации, информатизации и защиты информации осуществляется Президентом Республики Беларусь, Советом Министров Республики Беларусь, Оперативно-аналитическим центром при Президенте Республики Беларусь, Министерством связи и информатизации Республики Беларусь, Национальной академией наук Беларуси и иными государственными органами в соответствии с компетенцией определенной настоящим Законом и иными актами законодательства Республики Беларусь».

Статьи 9-14 разграничивают полномочия перечисленных государственных органов управления.

Координация и лицензирование деятельности по защите информации, а также организация и проведение работ по технической защите информации в национальном сегменте (BY) возложена на Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ).

В соответствии с Указом Президента от 28.11.2000, № 639 головной научно-исследовательской организацией Республики Беларусь в области защиты информации является Научно-производственное республиканское предприятие «Научно-исследовательский институт технической защиты информации» (НИИ ТЗИ) [4]. Эта организация обеспечивает координацию в области научных, исследовательских, методических и практических работ по технической защите информационных систем в интересах министерств, ведомств и организаций Республики Беларусь.

Государственное научное учреждение «Объединенный институт проблем информатики» Национальной Академии Наук Беларуси привлекается ОАЦ и НИИ ТЗИ для выполнения работ по разработке проектов нормативных актов в сфере защиты информации, а также исследовательских работ в области методологии и оценке эффективности защиты информации.

**Лицензирование в сфере технической защиты информации в Республике Беларусь**. Порядок лицензирования и виды лицензируемой деятельности в сфере защиты информации определяется «Положением о лицензировании деятельности по технической защите информации, в том числе криптографическим методам, включая применение электронной подписи» утвержденным постановлением Совета Министров Республики Беларусь № 1374 от 20.10.2003 [1].

В соответствии с этим Положением выдачу и учет, лицензий на осуществление деятельности по технической защите информации осуществляет ОАЦ. Лицензируемой является практически любая деятельность. связанная с проектированием, разработкой, установкой и оказанием услуг в области технической защиты информации.

**Административная ответственность в сфере защиты информации в Республике Беларусь.** Административный кодекс Республики Беларусь предусматривает ответственность за следующие правонарушения в сфере защиты информации (глава 22 Кодекса):

* самовольное использование сетей электросвязи;
* несанкционированный доступ к компьютерной информации;
* нарушение правил защиты информации;
* незаконная деятельность в области защиты информации.

**Уголовная ответственность в сфере защиты информации в Республике Беларусь**. Уголовный кодекс Республики Беларусь предусматривает уголовную ответственность за следующие преступления против информационной безопасности (Раздел XII Уголовного кодека Республики Беларусь):

* несанкционированный доступ к компьютерной информации;
* модификация компьютерной информации;
* компьютерный саботаж;
* неправомерное завладение компьютерной информацией;
* изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети;
* разработка, использование либо распространение вредоносных программ;
* нарушение правил эксплуатации компьютерной системы или сети.

**Технические нормативные акты в сфере защиты информации в Республике Беларусь**. Основные стандарты в сфере защиты информации являются гармонизированными международными стандартами (столбец «СТБ» таблицы 1) и, судя по всему, эта тенденция будет продолжаться. Исключением является ГОСТ 28147-89, «Система обработки информации. Защита криптографическая. Алгоритм криптографический» успешно применяемый с 1989 года.

**Заключение.** В республике Беларусь планомерно ведется работа, направленная на создание условий информатизации общественной жизни [7].

Важнейшим этапом на этом пути является создание инфраструктуры национальной информационной безопасности. В основном сформирована законодательная основа, определены органы управления и регулирования, созданы механизмы контроля. Ясно, что существующая на сегодняшний день инфраструктура не является совершенной, но предпосылки для ее развития есть.

Существенным тормозом развития информационных технологий является отсутствие национальных стандартов. Но и здесь в последнее время наметился существенный прогресс. Гармонизация международных стандартов в области защиты информации будет способствовать интеграции Республики Беларусь в мировое информационное пространство.

Построение инфраструктуры национальной информационной безопасности формулирует ряд новых требований для автоматизированных систем и, по сути, создает новую среду для их функционирования. Все это потребует переосмысление методологии построения новых автоматизированных систем и реижиниринга уже работающих.

1. **TLS = TLS Record Protocol + TLS Handshake Protocol.** Три фазы: 1)выбор алгоритма шифрования; 2) обмен ключами или аутентификация на основе сертификатов; 3) передача данных на основе симметричного шифрования (AES, DES, ...)
2. **TLS Handshake Protocol** - протокол установки соединения: 1) клиент подключается к серверу и просит защищенное соединение и предоставляет список поддерживаемых им алгоритмов шифрование и хеш-функций; 2)сервер выбирает алгоритм шифрования и сообщает о своем выборе клиенту; 3)сервер отправляет клиенту сертификат (имя сервера, имя доверенного центра сертификации и открытый ключ сервера); 3)клиент связывается (не обязательно) с сервером доверенного центра сертификации и подтверждает аутентичность переданного сертификата (RFC 2459, X.509); 4)клиент шифрует случайную последовательность (ключ для симметричного шифрования) открытым ключом; 5) сервер расшифровывает сообщение скрытым ключом; 6) ключ для симметричного шифрования используется для обмена данными.
3. **TLS Record Protocol –** обмен зашифрованными данными
4. **HTTPS –** расширение HTTP, поддерживающее шифрование; **HTTPS** – это HTTP над SSL/TSL, 443 порт
5. **DNSsec**
6. **Kerberos (RFC 1510, 4210) - протокол аутентификации MIT, DES. GSS-API**

**Kerberos** — [сетевой протокол](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) [аутентификации](http://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F), позволяющий безопасно передавать данные через незащищённые [сети](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) для безопасной [идентификации](http://ru.wikipedia.org/wiki/%D0%98%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F). Также является набором бесплатного [ПО](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) от [Массачусетского технологического института](http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%81%D1%81%D0%B0%D1%87%D1%83%D1%81%D0%B5%D1%82%D1%81%D0%BA%D0%B8%D0%B9_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B8%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%82) (Massachusetts Institute of Technology (MIT)), разработавшего этот протокол. Её организация направлена в первую очередь на [клиент-серверную](http://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_%C2%AB%D0%BA%D0%BB%D0%B8%D0%B5%D0%BD%D1%82-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%C2%BB) модель и обеспечивает взаимную [аутентификацию](http://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) — оба [пользователя](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C) через [сервер](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80) подтверждают [личности](http://ru.wikipedia.org/wiki/%D0%9B%D0%B8%D1%87%D0%BD%D0%BE%D1%81%D1%82%D1%8C) друг друга. [Сообщения](http://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%BE%D0%B1%D1%89%D0%B5%D0%BD%D0%B8%D0%B5), отправляемые через протокол Kerberos, защищены от прослушивания и атак повторного воспроизведения.

Kerberos является одним из вариантов [протокола Нидхема-Шрёдера](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%9D%D0%B8%D0%B4%D1%85%D0%B5%D0%BC%D0%B0%E2%80%94%D0%A8%D1%80%D1%91%D0%B4%D0%B5%D1%80%D0%B0)[[1]](http://ru.wikipedia.org/wiki/Kerberos#cite_note-0), основан на [симметричной криптосистеме](http://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%8B%D0%B5_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B) и требует третье доверенное лицо ([сервер](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80)). Расширение Kerberos позволяет использовать [открытые ключи](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC) в процессе [аутентификации](http://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F).