Systems and Networks
Security and Resilience
Practicum

I. Zhukovytskyy, D. Ostapets, S. Razgonov, A. Zaets
Edited by V.S. Kharchenko

Modern mechanisms of information security and stability in Internet network

Practical analysis of violations of information security

Resilience mechanisms at systems and networks design

Systems and Networks Security and Resilience. Practicum

PRACTICUM

# SYSTEMS AND NETWORKS

## SECURITY AND RESILIENCE

2017

Co-funded by the Tempus Programme of the European Union

**Министерство образования и науки Украины**
**Днепропетровский национальный университет железнодорожного транспорта имени академика В. Лазаряна**

**И.В. Жуковицкий, Д.А. Остапец, С.А. Разгонов, А.П. Заец**

# Безопасность и резильентность систем и сетей

# System and Networks Security and Resilience

**Практикум**

**Под редакцией И.В. Жуковицкого**

**Проект**
***SEREIN 543968 TEMPUS-1-2013-1-EE-TEMPUS-JPCR Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains***

**2017**

УДК 004.056.5+681.324
Ж86

Викладено матеріали практичної частини навчального курсу «Безпека і стійкість мереж і систем» (System and Networks Security and Resilience), підготовленого для магістрантів в рамках проекту TEMPUS- SEREIN Project Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (543968-TEMPUS-1-2013- 1-EE-TEMPUS-JPCP).

Курс присвячений вивченню сучасних підходів і технологій побудови безпечних і стійких систем і мереж, а також методів і засобів реалізації механізмів захисту систем і мереж. Наводиться навчальна програма курсу, дається опис лабораторних робіт, методичні рекомендації по самостійному вивченню матеріалу курсу.

Для магістрантів університетів, які навчаються за напрямами комп'ютерних наук, комп'ютерної та програмної інженерії, кібербезпеки, а також викладачів відповідних спеціальностей.

**Безопасность и резильентность систем и сетей. Практикум** / И.В. Жуковицкий, Д.А. Остапец, С.А. Разгонов, А.П. Заец - Под ред. Жуковицкого И.В. – Харьков: Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ». – 2017. – 131 с.

Ж86 Изложены материалы практической части учебного курса «Безопасность и резильентность сетей и систем» (System and Networks Security and Resilience), подготовленного для магистрантов в рамках проекта TEMPUS-SEREIN Project Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCP).

Курс посвящен изучению современных подходов и технологий построения безопасных и устойчивых систем и сетей, а также методам и средствам реализации механизмов защиты систем и сетей. Приводится учебная программа курса, дается описание лабораторных работ, методические рекомендации по самостоятельному изучению материала курса.

Для магистрантов университетов, обучающихся по направлениям компьютерных наук, компьютерной и программной инженерии, кибербезопасности, а также преподавателей соответствующих специальностей.

Библ. – 46 наименований, рисунков – 45, таблиц – 2

Рекомендовано к изданию Ученым советом Днепропетровского национального университета железнодорожного транспорта имени академика В. Лазаряна (протокол от 2017 года).

УДК 004.056.5+681.324

© Жуковицкий И.В., Остапец Д.А., Разгонов С.А., Заец А.П.
© Днепропетровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, 2017

This work is subject to copyright. All rights are reserved by the authors, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms, or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

# ПРЕДИСЛОВИЕ

Данное пособие является частью учебно-методического обеспечения курса «Безопасность и резильентность сетей и систем» (System and Networks Security and Resilience), подготовленного для магистрантов в рамках проекта TEMPUS- SEREIN Project Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCP)1.

Курс посвящен изучению современных подходов и технологий построения безопасных и устойчивых систем и сетей, а также методам и средствам реализации механизмов защиты систем и сетей.

В пособии приводятся описание лабораторных работ и семинаров, методические рекомендации по самостоятельному изучению материала курса, в приложении дана учебная программа курса. Практическая часть курса включает лабораторные работы и семинарские занятия, посвященные анализу, разработке и исследованию:

– исследование стойкости многоразовых паролей (лабораторная работа №1);

– исследование систем генерации одноразовых паролей (лабораторная работа №2);

– исследование системы аутентификации s/key (лабораторная работа №3)

– исследование принципов сканирования портов разными методами, анализ и противодействие (лабораторная работа №4);

– настройка пакетных фильтров с использование программы ipfw и наблюдение за результатами их работы (лабораторная работа №5);

– использование Internet Protocol Security (IPSec) для защиты конфиденциальных данных, которые передаются по протоколу TCP/IP (лабораторная работа №6);

– удаленный доступ к сети с использованием виртуального защищенного соединения PPTP и L2TP (лабораторная работа №7);

– использование протокола SSL для безопасного взаимодействия клиентов с веб-сервером IIS (лабораторная работа №8).

Каждая из лабораторных работ включает: цель и задачи;; краткий теоретический материал; программу проведения разработок и исследований; требования к содержанию отчету;

контрольные вопросы.

Семинарские занятия проводятся по темам:

– поиск информационных ресурсов по вопросам Современных механизмов информационной безопасности и устойчивости в сети Internet (семинарское занятие №1);

– практический анализ ситуации нарушения информационной безопасности (семинарское занятие №2);

Механизмы резильентности при проектировании систем и сетей (семинарское занятие №3).

Описание семинарских занятий включает тему, цель, указания по подготовке и проведению семинара, требование к содержанию отчета и презентации, критерии оценки работы.

В пособии использованы материалы магистерских работ студентов специальности «Безопасность компьютерных систем и сетей», выполненные под руководством авторов пособия.

Пособие предназначено для магистров университетов, обучающихся по направлениям компьютерных наук, компьютерной и программной инженерии при изучении вопросов кибербезопасности, а также может быть полезным для преподавателей, ведущих занятия по соответствующим курсам.

Авторы выражают благодарность рецензентам, коллегам по проекту, кафедрам университетов за ценную информацию, методическую помощь и конструктивные предложения, которые высказывались в процессе обсуждения практической части данного курса.

[1] *Этот проект финансируется при поддержке Европейской комиссии. Эта публикация (сообщение) отражает мнения только авторов, и Комиссия не может нести ответственность за любое использование содержащейся в нем информации.*

*This project has been funded with support from the European Commission. This publication (communication) reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*

# 1 ЛАБОРАТОРНЫЕ РАБОТЫ

## 1.1 Исследование стойкости многоразовых паролей

### Цель и задачи работы

Исследовать методы атак на системы аутентификации по многоразовым паролям и выполнить экспериментальную оценку стойкости многоразовых паролей.

### Подготовка к лабораторной работе

При подготовке к лабораторной работе необходимо:

- ознакомиться с целью и задачами работы;
- изучить теоретический материал, приведенный в пособии;
- ознакомиться с принципами работы учебного программного комплекса «Password Work».

### Теоретический материал

Подсистемы аутентификации большинства современных информационных систем используют многоразовые пароли, то есть фактором аутентификации является нечто, известное законному пользователю (пароль). Пользователям или позволяют самостоятельно выбирать пароли, или в системе предусмотрена возможность их генерации.

Необходимо отметить, что сейчас существует достаточно большое количество разнообразных требований как к смысловым паролям, так и к паролям, которые генерируются. Наиболее обобщенными и популярными на данный момент правилами и требованиями по выбору паролей пользователей являются рекомендации по планированию парольной защиты фирмы IBM и советы и рекомендации относительно паролей фирмы Microsoft.

Основным требованием к паролям, которые генерируются, является требование, чтобы пароль представлял собой случайную или практически случайную (псевдослучайную) последовательность символов (или битов). Одним из известных и самых распространенных способов проверки последовательностей символов (чисел) на случайность является использование статистических тестов, разработанных Лабораторией информационных технологий Национального института стандартов и технологий США (НИСТ). Эти тесты определяют меру случайности двоичных последовательностей, которые порождены генерато-

рами случайных чисел. Тесты основаны на разных статистических свойствах, присущих только случайным последовательностям.

Основными видами атак на многоразовые пароли можно считать атаки угадывания (метод проб и ошибок или метод «грубой силы») и атаки со словарем (если пароль смысловой).

В случае атак угадывания злоумышленник последовательно перебирает возможные варианты пароля, пока не получит доступ к системе . Стойкость секретной информации можно оценить путем подсчета общего количества попыток (так называемых предположений), требуемых для выполнения атаки. При расчете стойкости для уменьшения чисел, над которыми проводятся операции, их обычно представляют в виде *битового пространства* (количества двоичных битов, которое необходимо для представления этого числа).

При сравнении эффективности разных методик аутентификации обычно выполняют оценку их стойкости именно к атакам угадывания. При этом можно пользоваться одним из двух унифицированных показателей сложности атаки угадывания – средним пространством атаки или средним временем угадывания.

*Средним пространством атаки* называется битовое пространство, соответствующее количеству попыток, которые должен выполнить злоумышленник:

$$V_{ср} = \log_2 \frac{S}{2} \ , \qquad (1)$$

где $S$ - количество комбинаций базового секрета (для систем парольной аутентификации – количество возможных паролей).

Для оценки фактора времени используется понятие темпа $R$ (попыток за секунду), с которым может выполняться отдельное предположение. Таким образом, среднее время атаки угадывания можно определить по формуле:

$$T_{ср} = \frac{2^{V_{ср}}}{R} \ . \qquad (2)$$

Суть словарных атак заключается в том, что злоумышленник владеет некоторыми словарями и последовательно пытается предоставить слова из этих словарей в качестве пароля. Такие словари обычно содержат известные (уже взломанные) пароли, имена собственные и существительные определенного языка. Для повышения эффективности атаки злоумышленник может также «транспонировать» слова из словарей, то есть менять регистр отдельных или всех символов слова, менять раскладку клавиатуры, проводить транслитерацию, менять буквы

похожими цифрами или символами, добавлять цифры в начале или в конце слова.

В работе для исследования стойкости и генерации многоразовых паролей используется специальный учебный программный комплекс «Password Work» (см. рис. 1), основными функциями которого являются создание (генерация) многоразового пароля и проверка паролей (на случайность, на стойкость к словарным атакам и атакам угадывания).

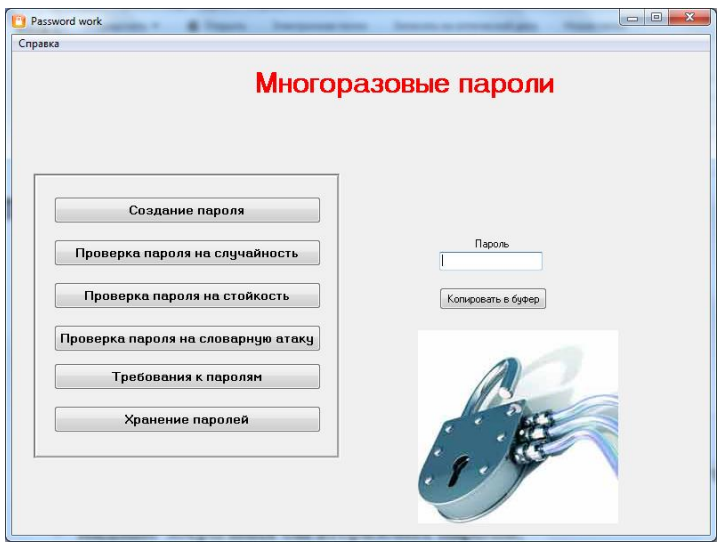



Рис. 1. Вид главного окна учебного комплекса

### Этапы выполнения работы

1. Во внеурочное время ознакомиться со сведениями о многоразовых паролях, принципах и правилах их выбора, генерации, оценки их стойкости и особенностях учебного программного комплекса.

2. С помощью режима генерации паролей учебного программного комплекса, произвольно выбирая длину и алфавит (см. рис. 2) создать псевдослучайный пароль по алгоритму BBS (Блюм-Блюм-Шуба).

С помощью режима проверки паролей на случайность (см. рис. 3), выполнить эксперимент по оценке степени случайности полученного пароля (см. п. 2) статистическими тестами НИСТ. Полученные результаты зафиксировать в отчет.

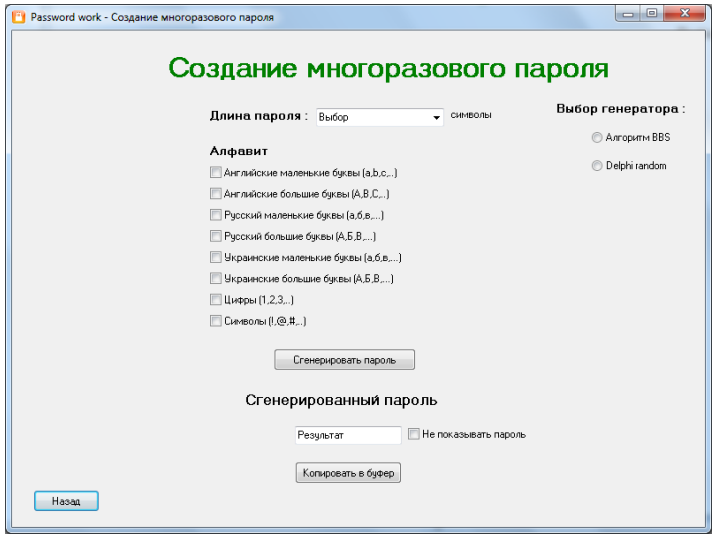



Рис. 2. Окно создания многоразового пароля

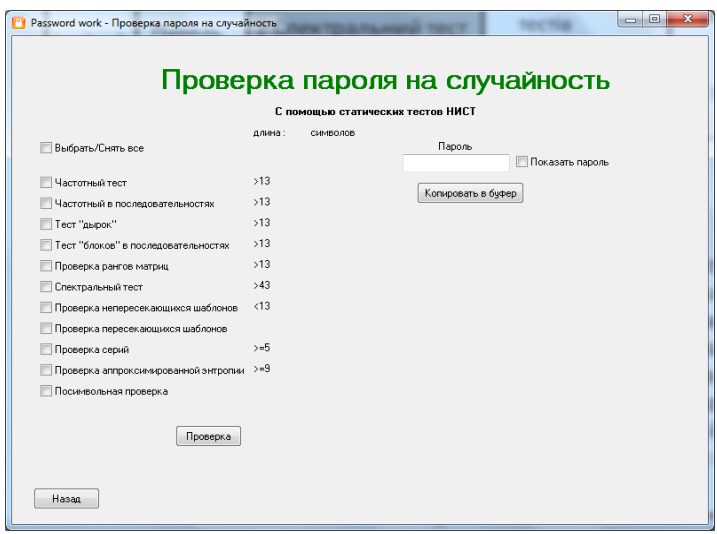



Рис. 3. Окно проверки пароля на случайность

3. С помощью режима проверки стойкости пароля к атакам угадывания методом проб и ошибок (см. рис. 4) для полученного пароля (см. п. 2) провести расчет показателей его стойкости: среднего пространства атаки и среднего времени атаки. Для расчета последнего можно воспользоваться значением темпа угадываний, который определяет учебная программа, или задать собственный. Полученные числовые результаты показателей зафиксировать в отчет.

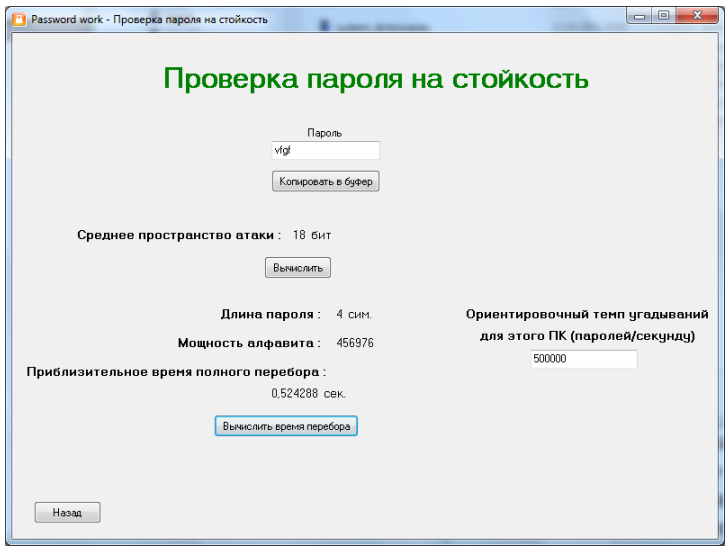



Рис. 4. Окно расчета характеристик атаки угадывания

4. Пользуясь режимом генерации паролей, произвольно выбирая длину и алфавит (см. рис. 2) с помощью генератора Delphi Random получить второй псевдослучайный пароль. Для полученного пароля выполнить проверку его случайности и расчет показателей его стойкости по п. 3 и п. 4 этого порядка, соответственно.

5. Руководствуясь требованиями и правилами по выбору многоразовых паролей, придумать собственный смысловой пароль (такой, который можно относительно легко запомнить).

6. С помощью режима проверки стойкости пароля к словарным атакам (см. рис. 5) для полученного пароля выполнить проверку вхож-

дения (или не вхождения) пароля в словари или «транспонированные» словари. Результаты зафиксировать в отчет.

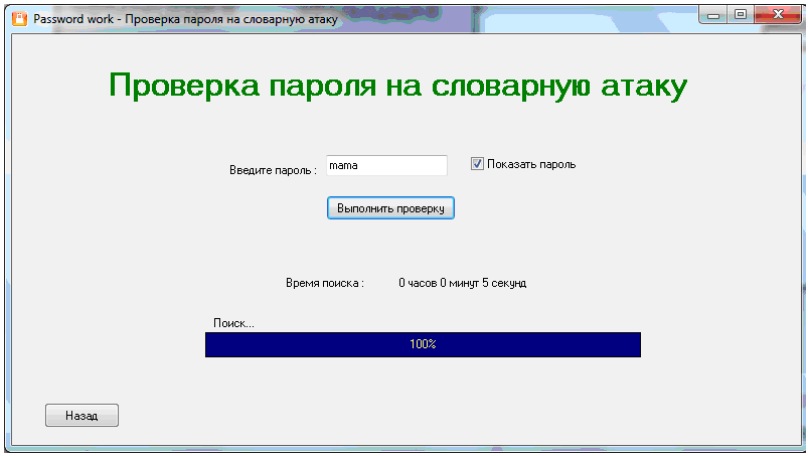



Рис. 5. Окно проверки вхождения пароля в словари

7. Выполнить расчет количественных показателей атак угадывания методом проб и ошибок полученного пароля (см. п. 4 этого порядка). Результаты зафиксировать в отчет.
8. Проанализировать полученные результаты, выводы зафиксировать в отчет.
9. Результаты работы показать преподавателю.
10. Оформить отчет и защитить работу преподавателю.

**Требования к содержанию отчета**

Отчет должен включать:

- номер, тему и цель работы.
- краткие теоретические сведения и описание учебного программного комплекса;
- результаты экспериментов по генерации паролей и проверке их на стойкость (п. 2-8 этапов выполнения работы) с соответствующими пояснениями и выводами, а также схематическим видом соответствующих экранных форм или их распечаток.

## Контрольные вопросы

1. Назовите основные варианты создания многоразовых паролей.
2. Назовите основные требования к многоразовым паролям.
3. Объясните суть и цель статистических тестов НИСТ.
4. Объясните принципы атак угадывания и количественные оценки сложности их реализации.
5. Объясните принципы атак по словарю.

## 1.2 Исследование систем генерации одноразовых паролей

### Цель и задачи работы

Изучить и исследовать работу двухфакторных систем идентификации и аутентификации на базе программных комплексов генерации одноразовых паролей

### Подготовка к лабораторной работе

При подготовке к лабораторной работе необходимо:

- ознакомиться с целью и задачами работы;
- изучить теоретический материал, приведенный в пособии;
- ознакомиться с принципами работы клиентской и серверной частей учебного программного комплекса.

### Теоретический материал

Обычно, методы аутентификации пользователей классифицируют в соответствии с используемой отличительной характеристикой (или фактором): парольные, имущественные и биометрические. Каждый метод аутентификации имеет свои недостатки и во многих случаях отдельно не может обеспечить нужный уровень защиты. Таким образом, в системах аутентификации часто используют механизмы с несколькими (как правило, двумя) факторами. Подобные системы называются многофакторными или системами с сильной аутентификацией.

Наиболее популярными в данное время являются имущественные методы аутентификации (с помощью устройства) и двухфакторные на основе имущественных и парольных (с помощью устройства и PIN-кода). Активные устройства аутентификации, в отличие от пассивных, для каждого сеанса аутентификации используют различную информацию. То есть передается не базовый секрет, а некоторые данные на его основе. Одними из представителей таких устройств являются традиционные устройства генерации одноразовых паролей (такие системы можно отнести и к парольным).

Такие устройства генерируют пароль исходя из начальных, разных для каждого пользователя, настроек. В качестве базового секрета используется некоторая уникальная символьная последовательность, а в качестве хешируемого (шифруемого) блока данных - показания часов или счетчика. В данной работе рассматривается более стойкое устройство часового типа. Часы, которые настраиваются, ведут счет времени, например, от некоторого момента инициализации устройства. Данные

часы должны быть синхронизированы с аналогичными серверными часами. Начальную синхронизацию проводит администратор сервера.

В соответствии со стандартами ANSI X9.9, ANSI X9.19 именно шифр DES является алгоритмом формирования хеш-функций (MAC-кода) в подобных системах. После хеширования (шифрования) получаем пароль в виде символьной (или числовой) последовательности. Этот пароль динамический; в зависимости от организации внутренних часов, он изменяется через определенные интервалы времени. Изменение происходит в силу того, что блок данных, который шифруется, постоянно изменяется, а функция хеширования обеспечивает при наименьшем изменении входных данных на выходе образовывать кардинально различные последовательности, которые не поддаются определенным закономерностям.

В работе для изучения генерации одноразовых паролей используется специальный учебный программный комплекс. Устройство генерации одноразовых паролей пользователей имитируется программно, при этом каждый пользователь будет иметь свою копию данной программы и набор конфигурационных файлов, в которых будут храниться уникальные настройки.

Комплекс состоит из двух частей: клиентской и серверной. Клиентская часть (дальше клиент) находится у пользователя и представляет собой генератор одноразовых паролей. Серверная часть (дальше сервер) представляет собой пользовательский интерфейс, который позволяет имитировать идентификацию и аутентификацию пользователей. Интерфейс сервера позволяет пользователю вводить его идентификатор (логин) и одноразовый пароль. Дальше, на основании проверки пароля, разрешается или запрещается доступ к информационной системе.

Как показано на рис. 1, на основании PIN- кода и базового секрета 1 (БС1) строится ключ – базовый секрет 2 (БС2), а с помощью него происходит шифрование блока данных (показаний внутренних часов). В итоге получаем одноразовый пароль, который для удобства представляется в шестнадцатеричном виде.

В учебной программе вместо хеширования используется шифрование по алгоритму DES, что дополнительно дает возможность ознакомиться с этим шифром. Размер блока у данного шифра составляет 64 бита (56+8). Разрядность ключа также составляет 64 бита, поэтому разрядности базового секрета 2 и показаний внутренних часов соответствуют этой разрядности. Настройку внутренних часов выполняет администратор системы и синхронизирует его с внутренними часами сервера. Также администратор выдает пользователю базовый секрет 1.

Серверная часть комплекса построена аналогично клиентской, за исключением того, что на сервере хранятся уже сформированные базовые секреты 2 пользователей.

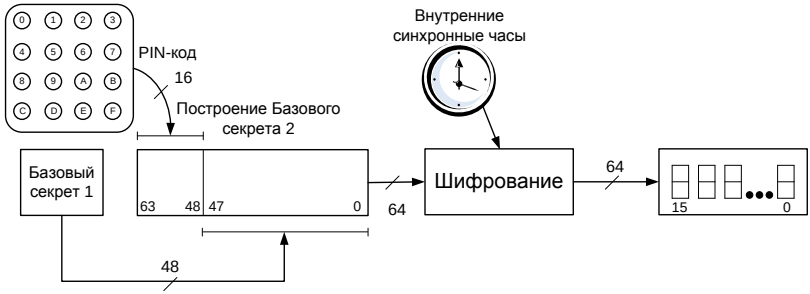
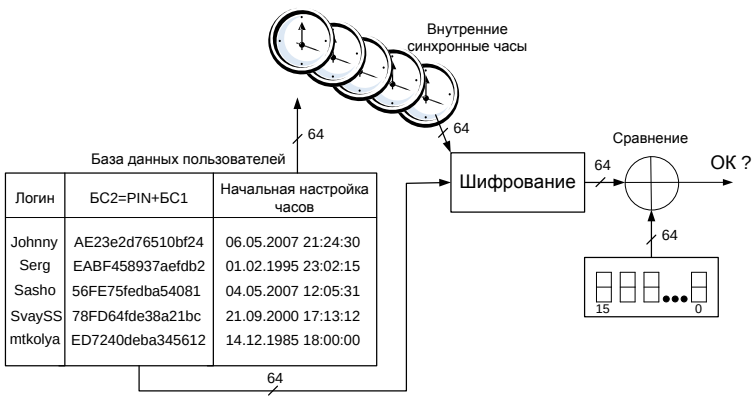



Рис. 1. Схема организации клиентской части комплекса

В состав серверной части, как показано на рис. 2, входит база данных пользователей. База данных содержит в себе идентификатор (логин) и уже сформированный базовый секрет 2 каждого пользователя, а также начальную настройку внутренних часов для каждого пользователя. Пользователь сам выбирает себе логин и PIN- код, а администратор вносит их в базу данных.




| Логин | БС2=PIN+БС1 | Начальная настройка часов |
|---|---|---|
| Johnny | AE23e2d76510bf24 | 06.05.2007 21:24:30 |
| Serg | EABF458937aefdb2 | 01.02.1995 23:02:15 |
| Sasho | 56FE75fedba54081 | 04.05.2007 12:05:31 |
| SvaySS | 78FD64fde38a21bc | 21.09.2000 17:13:12 |
| mtkolya | ED7240deba345612 | 14.12.1985 18:00:00 |

Рис. 2. Схема организации серверной части комплекса

**Этапы выполнения работы**

1. Во внеурочное время ознакомиться со сведениями о системах многофакторной аутентификации, генерации одноразовых паролей и особенностями учебного программного комплекса.

2. Выполнить настройку клиентской части учебного программного комплекса, имитируя действия пользователя системы. Для этого сформировать два конфигурационных файла *bs1.txt* и *bs3.txt* (папка *Client*) с личными настройками пользователя. В файл *bs1.txt* поместить базовый секрет 1 – это 48-битное число в шестнадцатеричном виде (например, e2d76510bf24), а в файл *bs3.txt* – начальную настройку внутренних часов в формате дата-время (например, 06.05.2007 21:24:30). Полученные файлы настроек зафиксировать в отчет.

3. Выполнить настройку серверной части учебного программного комплекса, имитируя действия администратора системы. Для этого сформировать один файл конфигурации – файл базы данных пользователей *database.txt* (папка *Server*), каждая строка которого отвечает определенному пользователю и содержит следующие поля: фамилия и инициалы пользователя, его логин, базовый секрет 2, начальная настройка внутренних часов в формате дата-время (например, Барчук_Л.Д. Johnny AE23e2d76510bf24 06.05.2007 21:24:30). Полученный файл настроек зафиксировать в отчет.

4. Запустить программу клиентской части (клиент) учебного комплекса – файл *Client.exe*, папка *Client* (на экране появится окно, которое изображено на рис. 3).

5. Запустить программу серверной части (сервер) учебного комплекса – файл *Server.exe*, папка *Server* (на экране появится окно, которое изображено на рис. 4).

6. Сгенерировать одноразовый пароль пользователя с помощью клиента. Для этого в клиентской части в поле ввода 1 (см. рис. 3) нужно ввести PIN-код пользователя, который состоит из 4-х шестнадцатеричных цифр и нажать на кнопку 2 «Получить пароль». В поле 3 отобразится сгенерированный одноразовый пароль.

7. Убедиться в корректности служебной информации о начальных параметрах для генерирования пароля, которая выводится в нижней части окна клиентской программы (см. рис. 3): в поле 4 отображается базовый секрет 1 пользователя, в поле 5 отображается сформированный базовый секрет 2, который служит ключом при шифровании, в поле 6 отображается начальная настройка внутренних часов, которая также является личным секретом для каждого пользователя, в поле 7 отображается блок данных, который шифруется и представляет собой

разность в секундах между текущей датой-временем и начальной настройкой внутренних часов, представленную в шестнадцатеричном виде, поле 8 и кнопка 9 «Расшифровать» являются технологическими и предназначены для проверки корректности алгоритма шифрования.

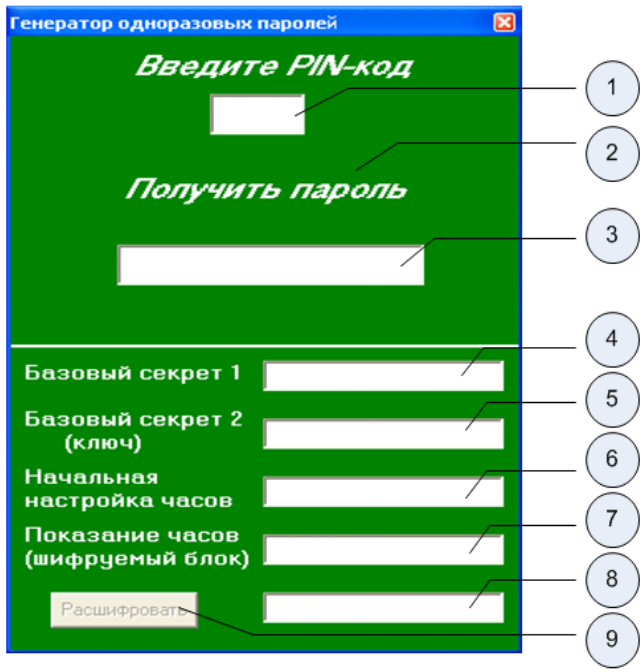



Рис. 3. Окно клиентской части комплекса

8. Выполнить попытку аутентификации пользователя на сервере по полученному в клиентской части одноразовому паролю. Для этого в серверной части в поле 1 (см. рис. 4) нужно ввести логин пользователя, а в поле 2 – сгенерированный пароль (см. рис. 3, поле 3) и нажать кнопку 3 («Получить доступ»). В поле 4 отобразится сообщение с результатом получения доступа для данного пользователя: «Доступ разрешен» или «Доступ запрещен», а в поле 5 – время ответа сервера пользователю в миллисекундах. При этом в поле 6 задается временой интервал, в течение которого пользователь должен ввести пароль, иначе ему будет отказано в доступе (так называемое «временное окно»).

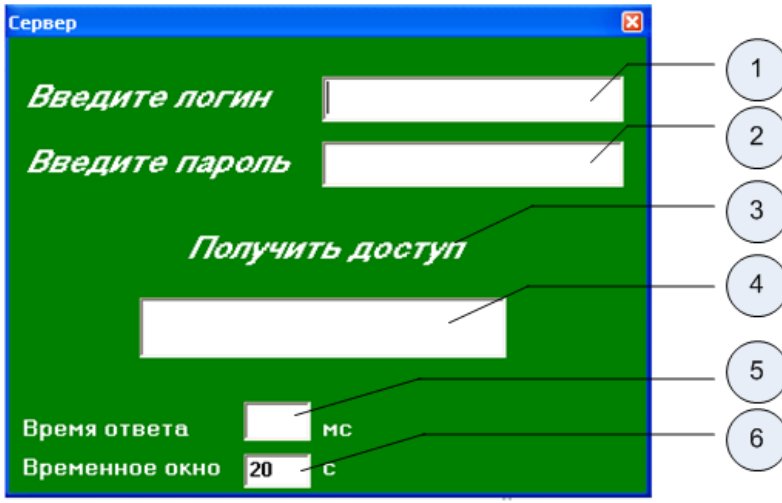



Рис. 4. Окно серверной части комплекса

9. Выполнить эксперименты по аутентификации пользователя на сервере с помощью нескольких одноразовых паролей клиента, повторяя п. 6-8 этого порядка. Результаты экспериментов зафиксировать в отчет.

10. Экспериментально выяснить влияние величины временного окна на возможность аутентификации легитимных пользователей. Для этого провести аутентификацию пользователя на сервере с помощью нескольких одноразовых паролей (см. п. 6-8 этого порядка) с разным значением временного окна и выдерживая при этом соответствующую временного паузу. Результаты эксперимента зафиксировать в отчет.

11. Определить экспериментально величину временного окна, которое отвечает времени реакции сервера приблизительно равной 1 с. Для этого проводить проверку одноразового пароля на сервере с постепенным увеличением значения временного окна (см. п. 10 этого порядка), пока полученное время ответа не будет находиться в пределах 980-1020 мс (диапазон корректных значений временного окна 1-65535 мс). Результаты эксперимента и основные технические характеристики ПЭВМ рабочего места зафиксировать в отчет.

12. Результаты работы показать преподавателю.

13. Оформить отчет и защитить работу преподавателю.

**Требования к содержанию отчета**

Отчет должен включать:

1. Номер, тему и цель работы.
2. Краткие теоретические сведения и описание учебного программного комплекса.
3. Распечатки файлов конфигурации клиентской и серверной частей учебного программного комплекса (п. 2-3 порядка выполнения работы).
4. Результаты экспериментов по аутентификации пользователей и с временным окном (п. 9-11 порядка выполнения работы) с соответствующими пояснениями и схематическим видом соответствующих экранных форм.

**Контрольные вопросы**

1. Что такое одноразовый пароль?
2. Назовите основные варианты организации генераторов одноразовых паролей.
3. Поясните работу устройства генерации одноразового пароля по схеме.
4. Поясните работу устройства проверки одноразового пароля по схеме.
5. Поясните содержание файлов конфигурации клиентской части учебного программного комплекса.
6. Поясните содержание файла конфигурации серверной части учебного программного комплекса.
7. Поясните порядок регистрации нового пользователя в учебном программном комплексе.

## 1.3 Исследование системы аутентификации s/key

### Цель и задачи работы

Изучить и исследовать работу системы S/Key, организацию базы данных сервера и настроек клиента на примере учебного комплекса программ.

### Подготовка к лабораторной работе

При подготовке к лабораторной работе необходимо:

- ознакомиться с целью и задачами работы;
- изучить теоретический материал, приведенный в пособии;
- ознакомиться с принципами работы клиентской и серверной частей учебного программного комплекса.

### Теоретический материал

Одной из самых распространенных и давно известных систем аутентификации на основе одноразовых паролей является система S/Key. Концепция системы была предложена еще в 1981 г. Лесли Лемпортом, а сама система разработана компанией Bell Communications Research (Bellcore) в 1990 г. для использования при регистрации в UNIX- подобных системах. Сейчас система S/Key имеет статус Интернет – стандарта, опубликованного Инженерным советом Интернет (Internet Engineering Task Force, IETF) в RFC 1760.

Главным отличием подхода Лемпорта от других систем аутентификации по принципу «запрос-ответ» является отсутствие базы данных секретных ключей на сервере. В системе S/Key используется последовательность значений хеш, вычисленных из исходного пароля (см. рис. 1). Сервер хранит лишь последнее хеш – значение (пароль 0). Таким образом, даже его знание не дает возможность злоумышленнику получить базовый секрет.

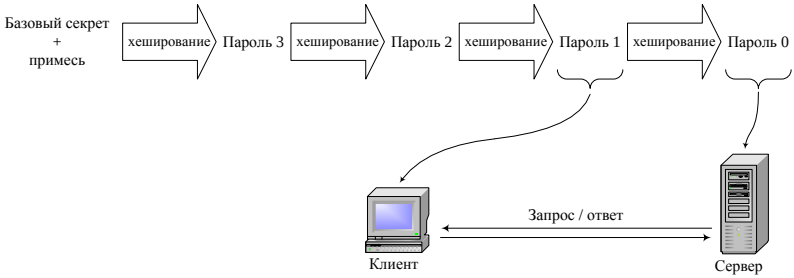



Рис. 1. Общая схема формирования одноразовых паролей в системе S/Key

В качестве сеансового (одноразового) пароля, пользователь передает предпоследнее значение из последовательности (на рис. 1 это пароль 1). Сервер выполняет хеширование полученного пароля и сравнивает результат со значением своего хранимого пароля (на рис. 1 это пароль 0). Если эти значения совпали, то сервер заменяет свое значение пароля (пароль 0) на принятое от клиента (пароль 1). При следующем сеансе аутентификации клиент должен предоставить уже другой по порядку одноразовый пароль (пароль 2), а сервер проведет с ним аналогичную процедуру. Таким образом, последовательность паролей, которая показана на рис. 1 рассчитана на проведение трех сеансов аутентификации.

Для удобства пользователя, сервер S/Key предоставляет порядковый номер ожидаемого им одноразового пароля и, кроме того, так называемую «примесь» или «зерно» (англ. seed). Таким образом, S/Key принято относить к системам класса «запрос-ответ». Примесь объединяется с исходным базовым секретом и дает возможность пользователю использовать тот же базовый секрет повторно. Система S/Key имеет программную реализацию.

В работе для изучения системы аутентификации по одноразовым паролям S/Key используется специальный учебный программный комплекс, который состоит из двух программ: клиентской (калькулятор одноразовых паролей) и серверной (имитатор аутентификации пользователей по одноразовому паролю).

**Этапы выполнения работы**

1. Во внеурочное время ознакомиться со сведениями об одноразовых паролях по принципу «запрос-ответ», системой аутентификации S/Key и особенностями учебного программного комплекса.

2. Выполнить настройку клиентской части учебного программного комплекса, имитируя действия пользователя системы. Для этого сформировать конфигурационный файл *client.txt* (папка *SKey*) с личными настройками пользователей. Файл организован по принципу файла инициализации (*INI*- файла). В качестве названия раздела (в квадратных скобках) следует задать имя (логин) пользователя (например, *[user]*) и, кроме того, два параметра, которые ему соответствуют: базовый секрет (например, *BaseSecret=OTP's are good*) и его описание (например, *Description=some user info*). Полученный файл настроек зафиксировать в отчет.

3. Запустить программу клиентской части (клиент) учебного комплекса – файл *Client.exe*, папка *SKey* (на экране появится окно, которое изображено на рис. 2).

4. Запустить программу серверной части (сервер) учебного комплекса – файл *Server.exe*, папка *Server* (на экране появится окно, которое изображено на рис. 3).

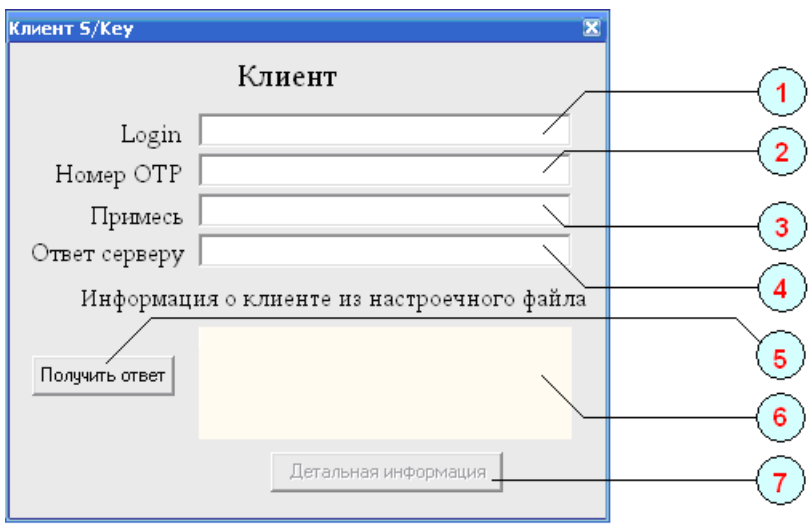



Рис. 2. Окно клиентской части комплекса

5. Произвольно выбрать примесь (например, *correct*) или сгенерировать ее на сервере. Для этого на сервере нажать кнопку 3 («Сгенерировать примесь»).

6. С помощью клиентской части для данного пользователя (*user*) задать количество возможных одноразовых паролей (соответствует количеству возможных сеансов аутентификации, например, *15*) и полученную примесь (*correct*) и вычислить ответ, который представляет собой последний одноразовый пароль (например, *2152f1696796759f*). Для этого в поле ввода 1(см. рис. 2) нужно ввести логин пользователя, в поле ввода 2 «Номер OTP» - его порядковый номер, в поле ввода 3 «Примесь» - значение примеси и нажать кнопку 5 «Получить ответ». В поле 4 «Ответ серверу» отобразится ответ – вычисленный одноразовый пароль, который администратор системы должен позже сохранить на сервере.

7. Убедиться в корректности служебной информации о начальных параметрах для генерирования пароля клиента, которые выводятся в нижней части окна клиентской программы (см. рис. 2, поле 6 «Информация о клиенте из настроечного файла») и просмотреть детали процесса хеширования пароля по алгоритму MD5 (нажатие кнопки 7 «Детальная информация»).

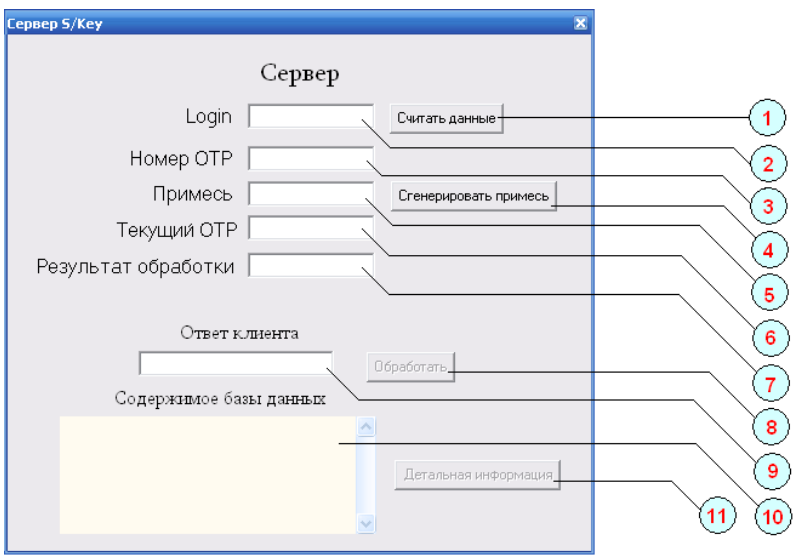



Рис. 3. Окно серверной части комплекса

8. Выполнить настройку серверной части учебного программного комплекса, имитируя действия администратора системы. Для этого сформировать файл базы данных пользователей *server _ db.txt* (папка *SKeyServer*), каждая строка которого отвечает определенному пользователю и содержит следующие поля: логин пользователя, текущий номер одноразового пароля сервера, одноразовый пароль сервера, примесь (например, *user 15 2152f1696796759f correct*). Полученный файл настроек сервера зафиксировать в отчет.

9. Проверить работоспособность системы, сгенерировав одноразовый пароль пользователя в клиентской части и сымитировав попытку аутентификации по нему в серверной части. Для этого в серверной части в поле 2 (см. рис. 3) ввести логин пользователя, нажать кнопку 1 «Считать данные» для считывания информации пользователя из базы данных сервера (в полях 3, 5 и 6 появятся значения последнего номера одноразового пароля, примеси и самого пароля, соответственно). Далее, задать значения соответствующих полей в клиентской части (см. рис. 2, п. 6 этого порядка), учитывая, что номер пароля клиента должен быть на единицу меньше номера пароля сервера и вычислить ответ (сеансовый одноразовый пароль). Полученный ответ ввести в поле 9 «Ответ клиента» серверной части и нажать кнопку 8 «Обработать». В поле 7 «Результат обработки» отобразится результат хеширования паролю, а ниже поля 7 – также и сообщение о результате получения доступа пользователем: «Доступ разрешен» или «Доступ запрещен».

10. Выполнить эксперименты по аутентификации пользователя с помощью нескольких одноразовых паролей (см. п. 9 этого порядка). Результаты зафиксировать в отчет.

11. Результаты работы показать преподавателю.

12. Оформить отчет и защитить работу преподавателю.

**Требования к содержанию отчета**

Отчет должен включать:

- номер, тему и цель работы.
- краткие теоретические сведения и описание учебного программного комплекса.
- распечатки файлов конфигурации клиентской и серверной частей учебного программного комплекса (п. 2, п. 8 порядка выполнения работы).
- результаты экспериментов по аутентификации пользователей (п. 10 порядка выполнения работы) с соответствующими пояснениями и схематическим видом соответствующих экранных форм.

**Контрольные вопросы**

1. В чем заключаются общие принципы формирования одноразовых паролей по принципу «запрос-ответ»?
2. Назовите основное достоинство системы S/Key.
3. Поясните принципы формирования одноразовых паролей в системе S/Key по схеме.
4. Поясните работу системы аутентификации S/Key по схеме.
5. Поясните содержание файла конфигурации клиентской части учебного программного комплекса.
6. Поясните содержание файла конфигурации (базы данных) серверной части учебного программного комплекса.
7. Поясните порядок регистрации нового пользователя в учебном программном комплексе.
8. Какое назначение имеет примесь?
9. Назовите основные варианты ввода (передачи) одноразовых паролей в реальных реализациях S/Key по RFC 1760.

## 1.4 Исследование принципов сканирования портов разными методами, анализ и противодействие

### Цель и задачи работы

Цель работы - изучение сканирования сетевых портов.

Учебные задачи: изучение принципов сканирования сетевых портов.

Практические задачи: получение навыков сканирования сетевых портов при помощи утилиты namp в ОС FreeBSD.

Исследовательские задачи: исследование методов противодействия сканированию сетевых портов.

### Подготовка к лабораторной работе

При подготовке к лабораторной работе необходимо:

- ознакомиться с целью и задачами исследования;
- изучить теоретический материал, приведенный в учебном пособии;
- ознакомиться с типами сканирования сетевых портов;
- ознакомиться с основными командами и ключами утилиты nmap.

### Краткие теоретические сведения

На транспортном уровне TCP/IP сети работают протоколы UDP и TCP. Используя протокол IP для взаимодействия между узлами сети они организуют взаимодействие между приложениями, которые выполняются на этих узлах. Для адресации приложений используется понятие «порт» – номер очереди сообщений, входящих/выходящих из приложения. Всего можно адресовать $2^{16}$-1 портов TCP и столько же портов UDP (порт 0 зарезервирован).

Протокол UDP обеспечивает быструю, но ненадежную передачу данных (дейтаграмм) между приложениями.

Протокол TCP решает задачу надежной передачи данных между любой парой прикладных процессов, выполняющихся в сети. Надежность обеспечивается установлением логического соединения между портом-источником и портом-получателем – это позволяет ему, в отличие от UDP, гарантировать доставку пакетов.

Набор данных, передаваемых протоколом TCP, называется сегментом. К этому набору данных добавляется заголовок TCP. Поле данных и заголовок TCP также называются сегментом. Сегмент TCP помещается в поле данных пакета IP.

В заголовке TCP имеется поле флагов (служебных бит), которые используются для управления работой протокола. Часто по имени взведенных флагов в заголовке TCP-сегмента называют пакет IP, в котором помещен этот TCP-сегмент .

Формирование логического соединения между двумя узлами реализуется специальной последовательностью, называемой handshake (рукопожатия). В упрощенном описании эта последовательность следующая:

- узел A посылает узлу B специальный пакет SYN (взведен флаг SYN в заголовке сегмента TCP) – приглашение к соединению;
- узел B отвечает пакетом SYN-ACK (взведены флажки SYN, ACK) – согласием об установлении соединения;
- узел A посылает пакет ACK – подтверждение, что согласие получено.

После этого TCP соединение считается установленным и приложения, работающие в этих узлах, могут посылать друг другу пакеты с данными.

«Соединение» означает, что узлы помнят друг о друге, нумеруют все пакеты, идущие в обе стороны, посылают подтверждения о получении каждого пакета и перепосылают потерявшиеся по дороге пакеты.

Для узла A это соединение называется исходящим, а для узла B – входящим.

Отметим, что эти термины не имеют никакого отношения к входящему или исходящему трафику. Они показывают только инициатора соединения, то есть направление самого первого пакета (SYN). Любое установленное TCP соединение симметрично, и пакеты с данными по нему всегда идут в обе стороны.

Когда один из узлов решает, что пора заканчивать соединение, он посылает специальный пакет FIN, после этого узлы разрывают соединение.

Сетевой порт – условное число от 1 до 65535, указывающее, какому приложению предназначается пакет.

Если прибегнуть к аналогии, то IP адрес - почтовый адрес дома, а порт - номер квартиры конкретного жильца.

Согласно стандарту IP, в заголовке каждого пакета присутствуют IP адрес узла-источника и IP адрес узла-назначения. В заголовке TCP-сегмента дополнительно указываются порт источника и порт назначения.

Узел назначения, получив пакет, извлекает оттуда сегмент TCP, определяет (по полю TCP-заголовка) порт назначения и передает сегмент соответствующему приложению.

Использование портов позволяет независимо использовать TCP протокол сразу многим приложениям на одном и том же компьютере.

Клиентом называют приложение, которое пользуется каким-то сервисом, предоставляемым другим приложением – Сервером, обычно на удаленном компьютере. Практически всегда клиент начинает исходящие соединения, а сервер ожидает входящих соединений (от клиентов), хотя бывают и исключения.

Сервер при запуске сообщает Операционной Системе (ОС), что хотел бы «занять» определенный порт (или несколько портов). После этого все пакеты, приходящие на компьютер к этому порту, ОС будет передавать этому серверу. Говорят, что сервер «слушает» этот порт.

Клиент, начиная соединение, запрашивает у своей ОС какой-нибудь незанятый порт во временное пользование и указывает его в посланных пакетах как порт источника. Затем на этот порт он получит ответные пакеты от сервера.

***Утилита Nmap***

Nmap (“Network Mapper”) это утилита с открытым исходным кодом для исследования сети и проверки безопасности. Она была разработана для быстрого сканирования больших сетей, хотя прекрасно справляется и с единичными целями. Nmap использует IP пакеты с вложенными заголовками TCP-сегментов оригинальными способами, чтобы определить, какие хосты доступны в сети, какие службы (название приложения и версию) они предлагают, какие операционные системы (и версии ОС) они используют, какие типы пакетных фильтров/брандмауэров используются и еще дюжины других характеристик. В тот время как Nmap обычно используется для проверки безопасности, многие сетевые и системные администраторы находят ее полезной для обычных задач, таких как контролирование структуры сети, управление расписаниями запуска служб и учет времени работы хоста или службы.

Синтаксис запуска программы следующий:

Nmap [Scan type(s)] [options] {target specification},

где вместо [Scan type(s)] указывается тип сканирования (по умолчанию, если это место оставить пустым, Nmap будет открыто сканиро-

вать доступные порты). В качестве [options] вводятся всевозможные ключи и параметры сканирования, а вместо {target specification} – либо IP-адрес компьютера, либо диапазон IP-адресов (который определяется маской подсети), либо название хоста.

***Описания типов сканирования***

-sT – сканирование TCP портов в обычном режиме. Сканирование происходит на основе функции connect(), присутствующей во всех полноценных ОС. Если соединение с удалённым портом установлено, то данный порт открыт, иначе порт закрыт либо фильтруется.

-sS – использование метода TCP SYN. Это – так называемое стелс сканирование. Nmap отправляет на удалённый порт SYN-пакет и ожидает ответа. В зависимости от ответа определяется состояние порта. При этом полноценное соединение не устанавливается. Благодаря этому определить факт сканирования очень сложно. Для запуска этого метода требуются привилегии администратора на Вашем компьютере.

-sF,-sX,-sN (scan FIN, scan Xmas, scan NULL) – эти совместные методы используется, например, если не помогло -sS или -sT сканирование.

-sU – сканирование UDP портов. На удалённый порт отправляется UDP-пакет и ожидается ответ. Если ответ содержит ICMP-сообщение «порт недоступен» значит порт закрыт либо защищен файрволом, иначе порт открыт.

-sR – использование RPC-сканирования (RPC – удаленный вызов процедуры). Этот метод позволяет определить программу, обслуживающую RCP-порт и её версию. При этот, если на удалённом сервере установлен файрвол, Nmap может его «пробить», не оставляя логов.

-sP – ping-сканирование. Данный метод позволяет узнать все адреса активных хостов в сети. Nmap отправляет на указанный IP ICMP-запрос, если в сети есть активные хосты, они отправят нам ответ, тем самым указав на свою активность. Если Вы пингуете сети лучше не указывать больше никаких методов сканирования.

***Описания некоторых опций***

Опции служат для тонкой настройки сканирования и задания дополнительных функций. Опции не обязательны, работа сканера будет нормальной и без них. Но все они будут полезны в том или ином случае.

Основные опции:

-O – так называемый режим «снятия отпечатков» TCP/IP для определения удалённой ОС (OS fingerprints). Работает это следующим образом: Nmap отправляет удалённой системе запросы и в зависимости от ответов («отпечатков» стека) определяется ОС и её версия.

-p [диапазон] – сканирование определённого диапазона портов. Например: '-p 21, 22, 25, 80, 31337'. Это уменьшает время сканирования за счёт уменьшения диапазона портов.

-F – сканирование стандартных портов (1-1024) записанных в файл services. Это, так называемое, быстрое сканирование.

-P0 – отмена ping-опросов перед сканированием портов хоста. Полезна в тех случаях, если Вы сканируете сети типа microsoft.com, так как в них ICMP-запрос запрещен файрволом.

-6 – сканирование через протокол IPv6. Работает значительно быстрее чем через IPv4.

-T «Paranoid|Sneaky|Polite|Normal|Aggressive|Insane» – настройка временных режимов. При «Paranoid» сканирование будет длиться очень долго, но тогда у Вас больше шансов остаться не обнаруженными скан-детекторами. И, наоборот, «Insane» используется при сканировании быстрых либо слабо защищённых сетей.

-oN/-oM «logfile» – вывод результатов в logfile в нормальном (-oN) или расширенном (-oM) виде.

-D «host_1, host_2,…,host_n» – это очень полезная функция. Она позволяет запутать удалённую систему и сделать видимость что её сканируют с нескольких хостов («host_1, host_2,…,host_n»), тем самым стараясь скрыть Ваш реальный адрес.

***Состояния портов распознаваемых Nmap***

***Открыт (open)***

Приложение принимает запросы на TCP соединение или UDP пакеты на этот порт. Обнаружение этого состояния обычно является основной целью сканирования. Люди, разбирающиеся в безопасности, знают, что каждый открытый порт это прямой путь к осуществлению атаки. Атакующие хотят использовать открытые порты, а администраторы пытаются закрыть их или защитить с помощью брандмауэров так, чтобы не мешать работе обычных пользователей. Открытые порты также интересны с точки зрения сканирования, не связанного с безопасностью, т.к. они позволяют определить службы доступные в сети.

***Закрыт (closed)***

Закрытый порт доступен (он принимает и отвечает на запросы Nmap), но не используется каким-либо приложением. Они могут быть

полезны для установления, что по заданному IP адресу есть работающий хост (определение хостов, ping сканирование), или для определения ОС. Т.к. эти порты достижимы, может быть полезным произвести сканирование позже, т.к. некоторые из них могут открыться. Администраторы могут заблокировать такие порты с помощью брандмауэров. Тогда их состояние будет определено как фильтруется, что обсуждается далее.

***Фильтруется (filtered)***

Nmap не может определить, открыт ли порт, т.к. фильтрация пакетов не позволяет достичь запросам Nmap этого порта. Фильтрация может осуществляться выделенным брандмауэром, правилами роутера или брандмауэром на целевой машине. Эти порты бесполезны для атакующих, т.к. предоставляют очень мало информации. Иногда они отвечают ICMP сообщениями об ошибке, такими как тип 3 код 13 (destination unreachable: communication administratively prohibited (цель назначения недоступна: связь запрещена администратором)), но чаще встречаются фильтры, которые отбрасывают запросы без предоставления какой-либо информации. Это заставляет Nmap совершить еще несколько запросов, чтобы убедиться, что запрос был отброшен фильтром, а не затором в сети. Это очень сильно замедляет сканирование.

***Не фильтруется (unfiltered)***

Это состояние означает, что порт доступен, но Nmap не может определить, открыт он или закрыт. Только ACK сканирование, используемое для определения правил брандмауэра, может охарактеризовать порт этим состоянием. Сканирование не фильтруемых портов другими способами, такими как Window сканирование, SYN сканирование или FIN сканирование может помочь определить, является ли порт открытым.

***Открыт|Фильтруется (open|filtered)***

Nmap характеризует порт таким состоянием, когда не может определить открыт порт или фильтруется. Это состояние возникает при таких типах сканирования, при которых открытые порты не отвечают. Отсутствие ответа также может означать, что пакетный фильтр не пропустил запрос или ответ не был получен. Поэтому Nmap не может определить наверняка открыт порт или фильтруется.

***Закрыт|Фильтруется (closed|filtered)***

Это состояние используется, когда Nmap не может определить, закрыт порт или фильтруется.

**Этапы выполнения работы**

Каждой команде выделяется 2 компьютера – хост A и хост B.

1) Загрузить ОС FreeBSD. Задать адреса сетевых интерфейсов (байт x – указывает преподаватель):

A: #ifconfig rl0 10.x.1.1/24

B: #ifconfig rl0 10.x.1.2/24

2) На хосте B необходимо настроить файрвол закрытого типа следующим образом:

| | протокол | порт | действие |
|---|---|---|---|
| * | tcp | 7(echo) | reset |
| * | tcp | 13(daytime) | allow |
| * | tcp | 19(chargen) | deny |
| * | udp | --- | reject |

***Часть 1. Методики сканирования***

3) Компьютер A сканирует компьютер B различными методами. Результаты сканирования сохранить в файле.

#nmap -O -v -n 10.x.1.2 - определение типа ОС;

#nmap -sO -v -n 10.x.1.2 - определение списка протоколов, которые поддерживаются;

#nmap -sT -v -n 10.x.1.2 -p 1-25 - сканирование способом «TCP-connect»;

#nmap -sS -v -n 10.x.1.2 -p 1-25 - сканирование способом полуоткрытых соединений;

#nmap -sF -v -n 10.x.1.2 -p 1-25 - «невидимое» сканирование (или -sX или -sN).

***Часть 2. Противодействие сканированию***

4) Компьютер B настраивает файрвол для порта 13 (daytime), тем самым пытаясь противодействовать сканированию.

***Сканирование открытого порта***

5) Хосту A необходимо убедиться, что работа хоста B по порту 13 разрешена файрволом. Хост A выполняет сканирование разными способами (сохранить результат nmap и tcpdump):

```
#tcpdump -i rl0 -n -v net 10.x
#nmap -sT -v -n 10.x.1.2. -p 13

#tcpdump -i rl0 -n -v net 10.x
#nmap -sS -v -n 10.x.1.2. -p 13

#tcpdump -i rl0 -n -v net 10.x
#nmap -sF -v -n 10.x.1.2. -p 13          (или -sX или -sN)
```

***Сканирование порта закрытого опцией deny***

6) Хост B закрывает порт 13 с помощью файрвола правилом:

```
#ipfw add 100 deny tcp from any to me 13
```

Хост A выполняет сканирование разными способами (сохранить результат nmap и tcpdump).

***Сканирование порта закрытого опцией reset***

7) Хост B закрывает порт 13 с помощью файрвола правилом:

```
#ipfw delete 100
#ipfw add 100 reset tcp from any to me 13
```

Хост A выполняет сканирование разными способами (сохранить результат nmap и tcpdump).

***Сканирование порта закрытого опцией reject***

8) Хост B закрывает порт 13 с помощью файрвола правилом:

#ipfw delete 100
#ipfw add 100 reject tcp from any to me 13

Хост А выполняет сканирование разными способами (сохранить результат nmap и tcpdump).

**Требования к содержанию отчета**

Отчет должен включать:

- номер, тема и цель работы, программа проведения исследований;
- краткие теоретические сведения;
- листинги или скриншоты выполненных команд;
- результаты экспериментов (дамп пакетов и результаты сканирования);
- выводы по работе.

**Контрольные вопросы**

1. Отличие протокола TCP от протокола UDP?
2. Последовательность формирования TCP-соединения?
3. Цели сканирования портов?
4. Какие состояния портов может распознать Nmap?
5. Методы сканирования портов? В чем их отличие?
6. Поясните настройки файрвола, которые используются для защиты от сканирования портов.

## 1.5 Настройка пакетных фильтров с использование программы ipfw и наблюдение за результатами их работы.

### Цель и задачи работы

Цель работы - изучение принципов работы и настройки межсетевого экрана (файрвола).

Учебные задачи:

- изучение принципов фильтрации сетевого трафика при помощи межсетевого экрана (файрвола);
- изучение основных правил настройки межсетевого экрана (файрвола).

Практические задачи:

- получение навыков установки и настройки файрвола IPFW в ОС FreeBSD.

Исследовательские задачи:

- исследование корректности настройки файрвола IPFW при помощи анализатора трафика tcpdump.

### Подготовка к лабораторной работе

При подготовке к лабораторной работе необходимо:

- ознакомиться с целью и задачами исследования;
- изучить теоретический материал, приведенный в учебном пособии;
- ознакомиться с синтаксисом построения правил файрвола IPFW в среде ОС FreeBSD.

### Теоретический материал

Межсетевой экран или файрвол (от англ. firewall - "стена огня") или брандмауэр - программный или программно-аппаратный элемент в компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Основным назначением данных элементов является защита подсетей или отдельных узлов от несанкционированного доступа.

Фильтрация трафика осуществляется на основе набора предварительно сконфигурированных правил. При фильтрации пакетов каждый сетевой пакет, поступающий в систему, сверяется со списком правил. Когда соответствующее правило найдено, ядро действует, исходя из этого правила. Правила могут пропустить, удалить или видоизменить пакет

Наиболее распространенным видом межсетевых экранов являются пакетные фильтры. Пакетные фильтры функционируют на сетевом уровне модели OSI и контролируют прохождение трафика на основе информации, содержащейся в заголовке пакетов. Многие межсетевые экраны данного типа могут оперировать заголовками протоколов и более высокого, транспортного, уровня (например, TCP или UDP).

При анализе заголовка сетевого пакета используются следующие параметры:

- IP-адреса источника и получателя;
- тип транспортного протокола;
- поля служебных заголовков протоколов сетевого и транспортного уровней;
- порт источника и получателя.

Для ОС FreeBSD разработан ряд пакетных фильтров: IPFW, IP Filter и PF.

IPFW (IP firewall) - представляет собой межсетевой экран, написанный и поддерживаемый добровольными участниками проекта FreeBSD. Он использует stateless правила, т.е. правила без учета состояния, и наследование техники кодирования правил для получения того, что называется простой логикой с сохранением состояния (stateful).

IPFW поддерживает протоколы IPv4 и IPv6. IPFW может быть подгружен как модуль, а может быть встроен в ядро операционной системы.

Настроенный IPFW представлен упорядоченным списком правил с номерами из диапазона 1-65535. Каждый пакет приходит с различных уровней стека протоколов, и попадая на фильтрацию поочередно сравнивается с критерием каждого правила в списке. Если совпадение найдено, то выполняется действие, закрепленное за данным правилом.

IPFW всегда содержит правило по умолчанию (с номером 65535) которое не может быть ни изменено, ни удалено. Это правило является терминальным, т.е. оно применяется к пакетам, не попавшим во все предыдущие. В зависимости от конфигурации ядра это правило может выполнять действия «запретить» или «разрешить». Это правило определяет тип файрвола как «закрытый» или «открытый». Все остальные правила могут редактироваться администратором системы.

Существует несколько основных действий, которые IPFW может применять к пакетам:

allow (син. — pass, accept, permit) — разрешить прохождение пакета. После этого действия другие правила не рассматриваются.

deny (син. drop) — запретить (сбросить) пакет. Пакет прекращает движение по списку правил и система полностью про него забывает.

unreach — запретить пакет. В отличие от deny, отправителю отправляется сообщение об ошибке по протоколу ICMP. После этого действия другие правила не рассматриваются.

reject — запретить пакет, и послать отправителю ICMP-сообщение «Заданный узел не найден».

skipto — перейти к правилу с заданным номером, минуя все промежуточные (используется для того, чтобы избежать просмотра списка правил, условия которых заведомо не выполняются).

fwd (син. forward) — перенаправление пакета (используется для организации «transparent-proxy»; а также для маршрутизации пакетов по IP-адресу источника или любым другим признакам, не обрабатываемым обычной маршрутизацией).

divert — передать пакет на анализ пользовательскому приложению, которое может изменить пакет и вернуть его в firewall (возвращённый пакет будет передан следующему правилу) либо уничтожить пакет.

tee — аналогичен divert, за исключением того, что на анализ передается копия пакета (чаще всего используют для подсчета трафика).

pipe, queue — прохождение пакета через «канал» или «очередь» dummynet (shaping). Используется для ограничения пропускной способности и внесения задержек в прохождение пакетов.

Редактирование правил файрвола IPFW выполняется с помощью утилиты командной строки ipfw.

Общий синтаксис построения правил командой ipfw такой:

ipfw [-N] команда [номер] действие [log] протокол адреса [параметры]

Здесь N – флаг разрешения адресов и имен сервисов при отображении.

Доступные команды:

add – добавление правила к списку фильтрации/учета

delete – удаление правила из списка фильтрации/учета

Если указано значение номер, оно используется для помещения правила на определенную позицию в цепочке. Иначе правило помещается в конец цепочки с номером на 100 больше, чем у предыдущего правила (сюда не включается правило по умолчанию с номером 65535).

С параметром log соответствующие правила выводят информацию на системную консоль, если ядро собрано с опцией IPFIREWALL_VERBOSE.

Существующие действия:

reject – отбросить пакет и отправить в адрес источника ICMP пакет, сообщающий о недостижимости хоста или порта;

allow – пропустить пакет как обычно (синонимы: pass, permit, и accept);

deny – отбросить пакет, источнику не выдается ICMP сообщение (как если бы пакет вообще не достиг цели);

count – обновить счетчик пакета, но не применять по отношению к нему правила allow/deny, поиск продолжится со следующего правила в цепочке.

Могут быть определены следующие протоколы:

all – соответствует всем IP пакетам;

icmp – соответствует ICMP пакетам;

tcp – соответствует TCP пакетам;

udp – соответствует UDP пакетам.

Поле адреса формируется следующим образом:

источник адрес/маска [порт] цель адрес/маска [порт] [via интерфейс]

Вы можете указать port только вместе с протоколами, поддерживающими порты (UDP и TCP).

Параметр via опционален и может содержать IP адрес или имя домена локального IP интерфейса, или имя интерфейса (например ed0), он настраивает правило на соответствие только тем пакетам, которые проходят через этот интерфейс. Номера интерфейсов могут быть заменены на опциональную маску. Например, ppp* будет соответствовать PPP интерфейсам ядра.

Для утилиты ipfw доступны также команды просмотра правил:

– последовательный список всех правил

ipfw list

– список всех правил, с меткой времени, когда правило последний раз совпадало

ipfw -t list

Имеется команда сброса счетчиков:

ipfw zero.

**Задание для выполнения**

Каждой команде выделяется 2 компьютера (хосты A и B).

На хосте A необходимо настроить файрвол, который обеспечит следующую политику доступа к его ресурсам:

| | протокол | порт | действие |
|---|---|---|---|
| * | tcp | 7(echo) | reset |
| * | tcp | 13(daytime) | allow |
| * | tcp | 19(chargen) | deny |
| * | udp | --- | reject |

Настройку выполнить в двух вариантах: 1 – все остальные ресурсы, кроме указанных выше открыты (файрвол открытого типа); 2 – все остальные ресурсы, кроме указанных выше закрыты (файрвол закрытого типа).

**Этапы выполнения работы**

1) Загрузить ОС FreeBSD. Задать адреса сетевых интерфейсов для хостов A и B (байт x – указывает преподаватель):

A: #ifconfig rl0 10.x.1.1/24

B: #ifconfig rl0 10.x.1.2/24

***Часть 1. Настройка файрвола открытого типа***

2) Проверить правила файрвола на каждом из хостов:

#ipfw list

Убедиться, что все пакеты разрешены (пропускаются). При необходимости добавить правила для разрешения всех пакетов. Таблица таких правил файрвола может иметь варианты:

65535 allow ip from any to any

или

65534 allow ip from any to any (номер этого правила может быть другим)
65535 deny ip from any to any

3) На хосте А добавить правила файрвола, которые обеспечивают политику доступа, указанную в задании, для файрвола открытого типа.

4) Убедиться в правильности работы файрвола. Для этого выполнить следующее:

На хосте В проверить соединение по TCP-протоколу с портами 7, 13, 19, проанализировать результаты (дамп пакетов, и вывод telnet), сохранить результаты в файлы (перенаправления вывода). Для работы с портом 7 такая проверка может выглядеть, например, следующим образом:

```
#tcpdump –i  rl0 –n –v net 10.x > file.txt
#telnet -4 10.x.1.1 7
```

На хосте В проверить работу протокола UDP, проанализировать результаты (дамп пакетов, и вывод traceroute) таким, например, образом:

```
#tcpdump –i  rl0 –n –v net 10.x > file_udp.txt
#traceroute 10.x.1.1
```

5) На хосте А сохранить правила файрвола в файл таким, например, образом:

```
#ipfw list > file_list.txt
```

***Часть 2. Настройка файрвола закрытого типа***

6) Сбросить все правила файрвола на хосте А:

7) Проверить правила файрвола на хосте А:

```
#ipfw list
```

8) Добавить правила в файрвол на хосте А для запрещения всех пакетов. Правила файрвола для запрещения могут иметь такие варианты:

```
65535 deny ip from any to any
```

или

```
65534 deny ip from any to any
```

(номер этого правила может быть другим)

65535 allow ip from any to any

9) На хосте A добавить правила файрвола, которые обеспечивают политику доступа, указанную в задании, для файрвола открытого типа.

10) Выполнить действия, изложенные в пункте 4).

11) На хосте A сохранить правила файрвола в файл таким, например, образом:

#ipfw list > file_list2.txt

**Требования к содержанию отчета**

Отчет должен включать:

- цели и программу проведения исследований;
- листинги или скриншоты выполненных команд;
- результаты экспериментов (дамп пакетов и вывод утилит telnet и traceroute);
- выводы по работе.

**Контрольные вопросы**

1. Что такое межсетевой экран и для чего он применяется?
2. Принципы функционирования пакетного фильтра.
4. Какой основной принцип настройки файрвола?
5. Для чего предназначено правило по умолчанию?
6. Какие действия может применять к пакетам файрвол IPFW?
7. При помощи каких команд работает утилита ipfw?
8. Синтаксис построения правила для утилиты ipfw.
9. Каким образом можно проверить возможность TCP-соединения?
10. Каким образом можно проверить работу UDP протокола?

## 1.6 Использование Internet Protocol Security (IPSec) для защиты конфиденциальных данных, которые передаются по протоколу TCP/IP

### Цель и задачи работы

1. Изучить архитектуру стека протоколов IPSec.
2. Настроить политики IPSec в ОС семейства Windows для организации защиты передаваемых данных между двумя компьютерами в сети.
3. Провести эксперименты для проверки работоспособности настроек политик IPSec.

### Подготовка к лабораторной работе

При подготовке к лабораторной работе необходимо:

- ознакомиться с целью и задачами исследования;
- изучить теоретический материал, приведенный в учебном пособии;
- бесплатно скачать с официального сайта: http://www.microsoft.com/en-us/download/details.aspx?id=4865 утилиту Microsoft Network Monitor 3.4, инсталлировать ее на компьютерах лаборатории, ознакомиться с правилами ее использования.

### Теоретический материал

Стек протоколов IPSec обеспечивает защищенную передачу данных в IP-сетях с использованием служб шифрования, а также защиту сетевого доступа в окружении Windows. Протоколы IPSec обеспечивают защиту информации на сетевом уровне, что делает их работу прозрачной для приложений. Архитектура IPSec совместима с протоколами IPv4 и IPv6.

Архитектура средств безопасности IPSec представлена на рис. 1.

На верхнем уровне расположены три протокола, составляющих ядро IPSec:

а) протокол согласования параметров виртуального канала и управления ключами IKE (Internet Key Exchange), определяющий способ инициализации защищенного канала, включая согласование используемых алгоритмов криптозащиты, а также процедуру обмена и управления секретными ключами в рамках защищенного соединения;

б) протокол аутентифицирующего заголовка AH (Authentication Header), обеспечивающий аутентификацию источника данных, проверку их целостности и подлинности после приема, а также защиту от навязывания повторных сообщений;

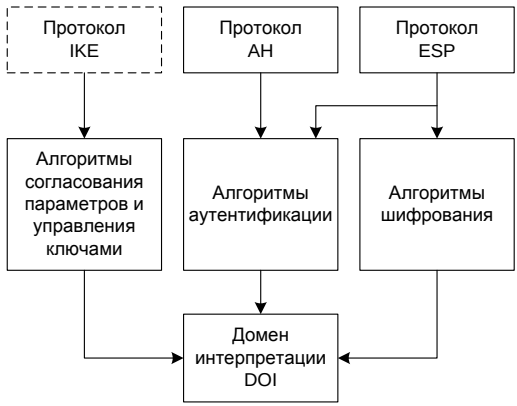



Рис. 1. Архитектура стека протоколов IPSec

в) протокол инкапсулирующей защиты содержимого ESP (Encapsulation Security Payload), обеспечивающий криптографическое закрытие, аутентификацию и целостность передаваемых данных, а также защиту от навязывания повторных сообщений.

Средний уровень образуют алгоритмы согласования параметров и управления ключами, применяемые в протоколе IKE, а также алгоритмы аутентификации и шифрования, используемые в протоколах AH и ESP. Для шифрования данных в IPSec (в протоколе ESP) может быть использован любой симметричный алгоритм шифрования с секретными ключами, такие как DES, 3Des, AES. Для обеспечения целостности и аутентификации данных (в протоколах AH и ESP) применяется шифрование с использованием односторонней хеш-функции, например, MD5 или SHA-1.

Нижний уровень образует домен интерпретации DOI (Domain of Interpretation). DOI в качестве БД хранит сведения об используемых в IPSec протоколах и алгоритмах, их параметрах, протокольных идентификаторах и т.п. Этот модуль обеспечивает совместную работу всех применяемых и вновь подключаемых протоколов и алгоритмов.

Протокол IPSec работает следующим образом:

1) агент политик считывает политики безопасности из SPD в реестре;

2) если политика указывает на использование IPSec, то агент посылает уведомление драйверу;

3) затем агент использует службы Security Association (SA) и IKE для обмена секретным ключом;

4) IKE создает защищенный канал между двумя компьютерами;

5) драйвер IPSec использует открытый ключ для создания SA-идентификаторов каждому из компьютеров для передачи данных;

6) при шифровании (ESP) и/или подписи (AH) пакетов, драйвер IPSec использует SA-key для создания ключа на входящее и исходящее соединение, а также Security Parameters Index (SPI), который будет вставлен в заголовок IPSec пакета;

7) после чего пакет передается на транспортный уровень;

8) на принимающей стороне происходят обратные процедуры.

Важным параметром безопасной ассоциации является так называемый ключевой материал, то есть секретные криптографические ключи, которые используются в работе протоколов AH и ESP. В целях безопасности, эти ключи никогда не пересылаются по сети, а передаются данные, необходимые каждому конечному узлу для локальной генерации ключей.

Параметры SA должны устраивать обе конечные точки защищенного канала. Поэтому при использовании автоматической процедуры установления безопасной ассоциации протоколы IKE, работающие по разные стороны канала, выбирают параметры на основании взаимных согласований. Для каждой задачи, которые решаются протоколами AH и ESP, предлагается несколько схем аутентификации и шифрования.

Безопасная ассоциация является однонаправленным логическим соединением, поэтому при двустороннем обмене данными необходимо установить две ассоциации SA (одну для входящих пакетов, другую – для исходящих). Для идентификации каждой SA предназначен индекс параметров безопасности SPI.

Протоколы AH и ESP могут работать в туннельном или транспортном режимах.

Для выполнения своих задач по обеспечению безопасной передачи данных протоколы AH и ESP включают в пакеты, которые обрабатываются ими, дополнительную служебную информацию, оформляя ее в виде заголовков.

На рис. 2 представлена структура IP-пакета после применения протокола AH в транспортном и туннельном режимах.

В транспортном режиме заголовок исходного IP-пакета становится внешним заголовком, за ним следует заголовок AH, а затем все данные защищаемого пакета (т.е. пакет протокола верхнего уровня). Протокол AH защищает весь полученный таким образом пакет, включая заголовок IP и собственно сам заголовок AH. Таким образом, любое изменение данных в пакете или заголовков будет обнаружено. Следует также заметить, что в этом режиме данные пакета отсылаются открытыми, т.е. данные пакета защищены от изменений, но не защищены от просмотра. В частности, не удается скрыть IP-адреса источника и назначения от возможного просмотра посторонними лицами, поскольку эти поля всегда присутствуют в незашифрованном виде и соответствуют действительным адресам хостов.


Рис. 2. IP-пакет после применения протокола AH в транспортном и туннельном режимах

В туннельном режиме в качестве заголовка внешнего IP-пакета создается новый заголовок IP. IP-адреса посылающей и принимающей сторон могут отличаться от адресов в заголовке исходного IP-пакета. В защищенном IP-пакете внутренний (первоначальный) IP-заголовок содержит целевой адрес пакета, а внешний IP-заголовок содержит адрес конца туннеля. За новым заголовком внешнего IP-пакета следует заголовок AH, а затем весь исходный пакет (заголовок IP и сами данные). Как и в случае транспортного режима, протокол AH защищает весь созданный пакет (два заголовка IP, заголовок AH и данные), что также позволяет обнаружить любые изменения в пакете. Как и в транспортном режиме, сам пакет не защищен от просмотра.

Не зависимо от режима работы, протокол AH предоставляет меры защиты от атак, направленных на нарушение целостности и подлинно-

сти пакетов сообщений. С помощью этого протокола аутентифицируется каждый пакет, что делает программы, пытающиеся перехватить управление сеансом, неэффективными. Протокол AH обеспечивает аутентификацию не только содержимого, но и заголовков IP-пакетов. Однако следует иметь в виду, что аутентификация по протоколу AH не допускает манипулирования основными полями IP-заголовка во время прохождения пакета. По этой причине данный протокол нельзя применять в среде, где используется механизм трансляции сетевых адресов NAT (Network Address Translation), поскольку для его работы необходимо манипулирование IP-заголовками.

Протокол AH может применяться как отдельно, так и в комбинации с протоколом ESP или даже с пакетом, который уже содержит AH-заголовок (вложенное применение).

Протокол инкапсулирующей защиты содержимого ESP обеспечивает конфиденциальность, аутентичность, целостность и защиту от повторов для пакетов данных. Следует отметить, что конфиденциальность данных протокол ESP обеспечивает всегда, а целостность и аутентичность являются для него опциональными требованиями. Конфиденциальность данных обеспечивается путем шифрования содержимого отдельных пакетов. Целостность и аутентичность данных обеспечиваются на основе вычисления дайджеста.

Функциональность протокола ESP шире, чем у протокола AH. Протокол ESP поддерживает все функции протокола AH по защите зашифрованных потоков данных от подлога, воспроизведения и случайного искажения, а также обеспечивает конфиденциальность данных.

В протоколе ESP функции аутентификации и криптографического закрытия могут быть задействованы либо вместе, либо отдельно друг от друга. При выполнении шифрования без аутентификации появляется возможность использования механизма трансляции сетевых адресов NAT, поскольку в этом случае адреса в заголовках IP-пакетов можно модифицировать.

На рис. 3 представлена структура IP-пакета после применения протокола ESP в транспортном и туннельном режимах.

В транспортном режиме зашифрованные данные транспортируются непосредственно между хостами. В транспортном режиме протокола ESP заголовок исходного IP-пакета остается внешним. Заголовок ESP помещается в передаваемый пакет между заголовками протоколов третьего (IP) и четвертого (например TCP) уровней. Следует заметить, что поля протокола ESP следуют после стандартного IP-заголовка, а это означает, что такой пакет может маршрутизироваться в сети с помощью обычного оборудования, поддерживающего IP.

Шифрованию подвергаются только данные исходного IP-пакета (пакет верхнего уровня) и заключительная часть ESP-заголовка (ESP trailer). В этом режиме ESP не шифрует заголовок IP-пакета, иначе маршрутизатор не сможет прочитать поля заголовка и корректно осуществить продвижение пакета между сетями.


Рис. 3. IP-пакет после применения протокола ESP в транспортном и туннельном режимах

В отличие от протокола AH, контроль целостности и аутентичности данных в протоколе ESP не распространяется на заголовок исходного пакета, и по этой причине имеет смысл применять оба протокола совместно – ESP для шифрования, а AH – для контроля целостности.

Таким образом, адресная информация (IP-адреса отсылающей и принимающей сторон) видна при пересылке пакета по сети и несанкционированное изменение этих IP-адресов не будет замечено.

В туннельном режиме основная роль отводится шлюзам безопасности, поскольку предполагается, что клиентские станции (или серверы) могут не поддерживать IPSec и отправляют в сеть обычный IP-трафик. Перед тем, как достичь каналов глобальной сети, каждый исходный IP-пакет сначала попадает в шлюз, который помещает этот пакет целиком в оболочку IPSec, зашифровывая его содержимое вместе с исходным IP-заголовком. Чтобы обеспечить возможность маршрутизации получившегося пакета, шлюз снабжает его новым IP-заголовком и только после этого отправляет в сеть. Шлюз, находящийся на противоположном конце соединения, расшифровывает этот пакет и передает его на

оконечное устройство в первоначальном виде. Описанная процедура называется туннелированием.

В туннельном режиме в качестве внешнего заголовка создается новый заголовок IP. Весь исходный IP-пакет (и данные и заголовок) и заключительная часть заголовка ESP (ESP trailer) шифруются. Поэтому адресная информация исходного IP-пакета не доступна для просмотра. Заголовок внешнего IP-пакета протоколом ESP не защищается.

Туннелирование позволяет распространить действие средств защиты на сетевой уровень модели OSI и, в частности, скрыть истинные адреса источника и получателя. При этом уменьшается риск атак, основанных на детальном анализе трафика.

Сравнивая протоколы ESP и AH можно заметить, что они дублируют функциональность друг друга в области обеспечения аутентификации данных. Главным отличием протокола AH от ESP в данном вопросе является, то что протокол AH обеспечивает аутентификацию всего пакета, в то время как протокол ESP аутентифицирует только данные из пакета. При шифровании в протоколе ESP используется симметричный секретный ключ, т.е. передаваемые данные зашифровываются и расшифровываются с помощью одного и того же ключа. Протокол ESP также определяет перечень обязательных алгоритмов шифрования – DES, MD5 и SHA-1.

Протокол ESP может применяться как отдельно, так и совместно с протоколом AH.

**Этапы выполнения работы**

1. Организация соединения компьютеров в локальной сети.
2. Настройка политики IPSec для компьютера с именем Host-A с операционной системой Windows 7.
3. Настройка политики IPSec для компьютера с именем Host-B с операционной системой Windows XP.
4. Проведение экспериментов для проверки работоспособности настроек политик IPSec.
5. Возобновление обычного режима связи между компьютерами.

Для выполнения лабораторной работы необходимо наличие двух компьютеров, физически объединенных в единую сеть с ОС Windows XP или Windows 7. На рис. 4 показана логическая структура такой сети.

На хостах A и B будет настроена политика IPSec для защищенной передачи данных. Если имеется третий хост (не обязательно), то с помощью него можно проверить возможность перехвата данных путем

сканирования сети или прямого взаимодействия с защищаемыми компьютерами. Данные будут передаваться в транспортном режиме работы протоколов.

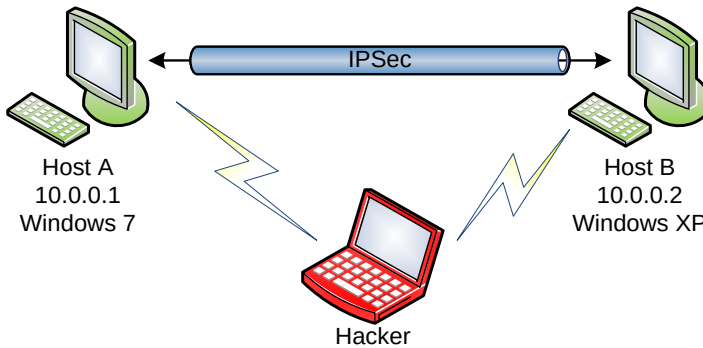



Рис. 4. Логическая структура сети

***Этап 1 – Организация соединения компьютеров в локальной сети***

*Примечание.* Если локальная сеть между компьютерами уже настроена, то этап настройки можно пропустить и перейти к шагу 3 данного подраздела для определения установленных IP-адресов и имен компьютеров.

*а) Настройка сети на хосте А с ОС Windows 7:*

1) войти в систему с правами администратора;
2) Пуск ⇨ Панель управления ⇨ Центр управления сетями и общим доступом ⇨ Изменение параметров адаптера;
3) кликнуть правой кнопкой мыши на «Подключение по локальной сети» ⇨ выбрать Свойства;
4) в окне «Подключение по локальной сети» во вкладке Сеть выбрать «Протокол Интернета версии 4 (TCP/IPv4)» ⇨ Свойства;
5) установить значения, показанные на рис. 5 и нажать ОК;
6) закрыть окно «Подключение по локальной сети»;
7) если состояние иконки «Подключение по локальной сети» – «отключено», включить его двойным кликом мыши.

*б) Изменение рабочей группы на хосте А:*

1) Пуск ⇨ Компьютер ⇨ Свойства системы;

2) в разделе «Имя компьютера, имя домена и параметры рабочей группы», кликнуть на «Изменить параметры» ⇨ в окне «Свойства системы» во вкладке «Имя компьютера» ⇨ Изменить;

3) в данной работе используется: «Имя компьютера» – Host-A, «Является членом рабочей группы» – WORKGROUP;

4) после закрытия окна свойств, необходимо перезагрузить ОС.

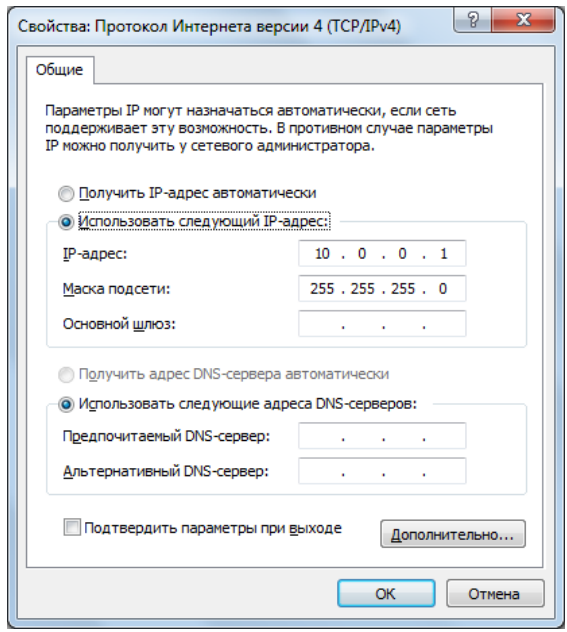



Рис. 5. Настройка TCP/IP на хосте A

*в) Настройка сети на хосте B с ОС Windows XP:*

1) войти в систему с правами администратора;

2) Пуск ⇨ Настройки ⇨ Панель управления ⇨ Сетевые подключения;

3) кликнуть правой кнопкой мыши на «Подключение по локальной сети» ⇨ выбрать Свойства;

4) в окне «Подключение по локальной сети – свойства» во вкладке Общие выбрать «Протокол Интернета TCP/IP» ⇨ Свойства;

5) установить значения, показанные на рис. 6 и нажать ОК;

6) закрыть окно «Подключение по локальной сети»;

7) если состояние иконки «Подключение по локальной сети» – «отключено», включить его двойным кликом мыши.

*г) Изменение рабочей группы на хосте B:*

1) Мой компьютер ⇨ Свойства ⇨ Перейти во вкладку «Имя компьютера» ⇨ Изменить;

2) в данной работе используется: «Имя компьютера» – Host-B, «Является членом рабочей группы» – WORKGROUP;

3) после закрытия окна свойств, необходимо перезагрузить ОС.

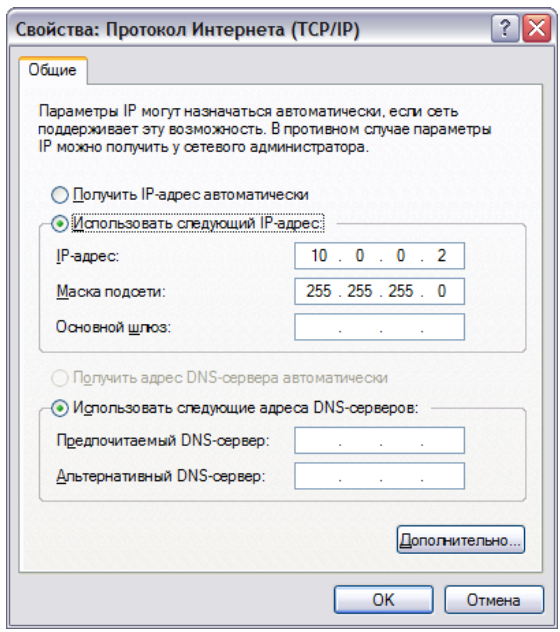



Рис. 6. Настройка TCP/IP на хосте B

*д) Проверка локального соединения.* Для определения установленных имен компьютеров и IP-адресов, на каждой машине необходимо выполнить следующее:

1) Пуск ⇨ Выполнить (либо сочетанием клавиш Win+R);

2) ввести cmd.exe и нажать на клавишу Enter;

3) выполнить команду ipcongfig /all – среди отображенной информации есть установленное ранее «Имя компьютера» и «IP-адрес адаптера подключения по локальной сети»;

4) в окне утилиты cmd.exe на компьютере А выполнить команду: ping 10.0.0.2.

Полученные ответы от хоста 10.0.0.2 свидетельствуют об успешном прохождении ICMP-пакетов и правильно выполненной настройке.

***Этап 2 – Настройка политики IPSec для компьютера Host-A с Windows 7***

*а) Создание файла консоли:*

1) Пуск ⇨ Выполнить (либо сочетанием клавиш Win+R);
2) ввести mmc.exe и нажать на клавишу Enter;
3) пункт меню Файл ⇨ Добавить или удалить оснастку;
4) в списке доступных оснасток выделить «Управление политикой IP-безопасности» ⇨ Добавить ⇨ оставить флажок «Локальный компьютер» ⇨ Готово;
5) среди оснасток Добавить «Монитор IP-безопасности»;
6) аналогично добавить «Службы» и «Просмотр событий» для локального компьютера;
7) закрыть окно «Добавление и удаления оснасток» кнопкой OK;
8) Файл ⇨ Сохранить как... ⇨ выбрать путь к рабочей папке и сохранить файл консоли управления ipsec.msc ⇨ OK.

В результате получается четыре оснастки, что показано на рис. 7.

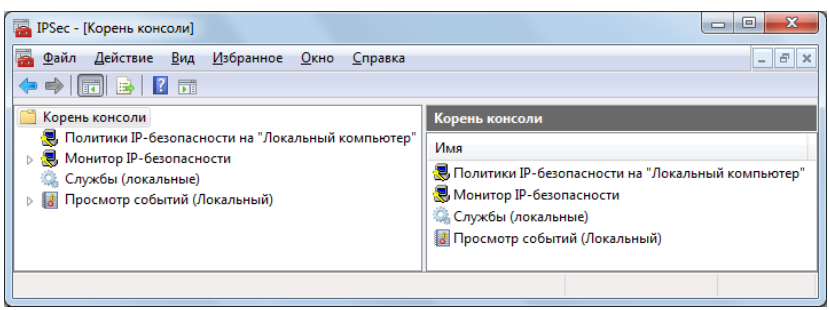



Рис. 7. Консоль mmc с файлом ipsec.msc

*б) Запуск службы:*

1) в корне консоли выбрать Службы;

2) в области описания окна найти службу «Агент политики IPSec» ⇨ запустить службу двойным кликом.

*в) Создание политики безопасности и настройка IP-фильтров:*

1) в корне консоли кликнуть правой кнопкой мыши на «Политики IP-безопасности»;

2) выбрать «Создать политику безопасности»;

3) в открывшемся мастере нажать Далее ⇨ ввести имя «Политика IPSec» ⇨ Далее ⇨ оставить снятым флажок «Использовать правило по умолчанию» ⇨ Далее ⇨ оставить установленным флажок «Изменить свойства» ⇨ Готово;

4) в открывшемся окне Свойства ⇨ зайти во вкладку Общие ⇨ открыть Параметры ⇨ Методы;

5) в открывшемся окне «Методы безопасности при обмене ключами» (IKE) установить параметры, показанные на рис. 8 ⇨ нажать ОК и вернуться в окно Свойств во вкладку Правила.

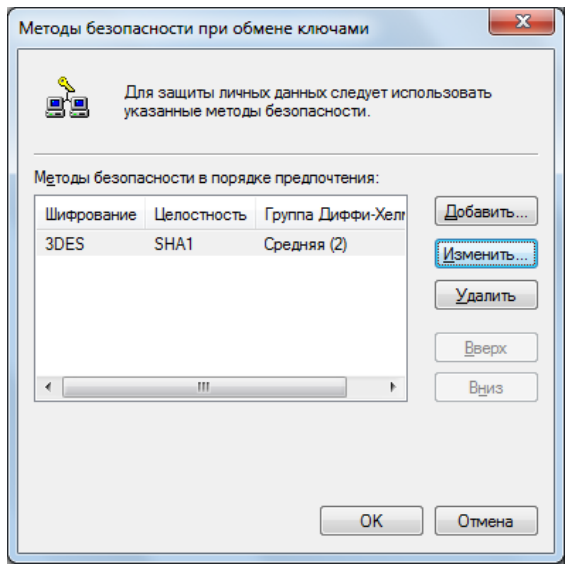



Рис. 8. Методы безопасности при обмене ключами в Windows 7

6) Добавить ⇨ в «Мастере создания новых правил» нажать Далее;

7) установить флажок «Это правило не определяет туннель» ⇨ Далее (таким образом, устанавливается транспортный режим работы стека протоколов IPSec);

8) тип сети «Все сетевые подключения» ⇨ Далее ⇨ Добавить;

9) в открывшемся окне «Список IP-фильтров» ввести имя «Защищенный IP-трафик с хостом B» ⇨ Добавить;

10) во вкладке Адреса выбрать опции показанные на рис. 9;

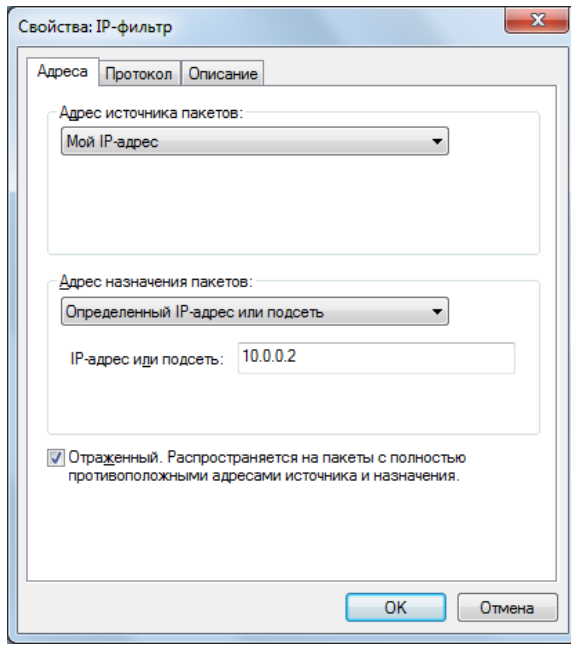



Рис. 9. Свойства IP-фильтра компьютера с именем Host-A

11) во вкладке Протокол указать «Тип протокола: Любой» ⇨ ОК;

12) в списке IP-фильтров выбрать созданный «Защищенный IP-трафик с хостом B» ⇨ Далее;

13) в окне «Действие фильтра» оставить флажок «Использовать мастер» ⇨ Добавить ⇨ Далее ⇨ Имя: Шифровать ⇨ Далее ⇨ Согласовать безопасность ⇨ Далее ⇨ Запретить небезопасное соединение ⇨ Далее ⇨ Другой ⇨ Параметры;

14) установить настройки соответствующие рис. 10 ⇨ ОК ⇨ ДА ⇨ Далее ⇨ Готово;

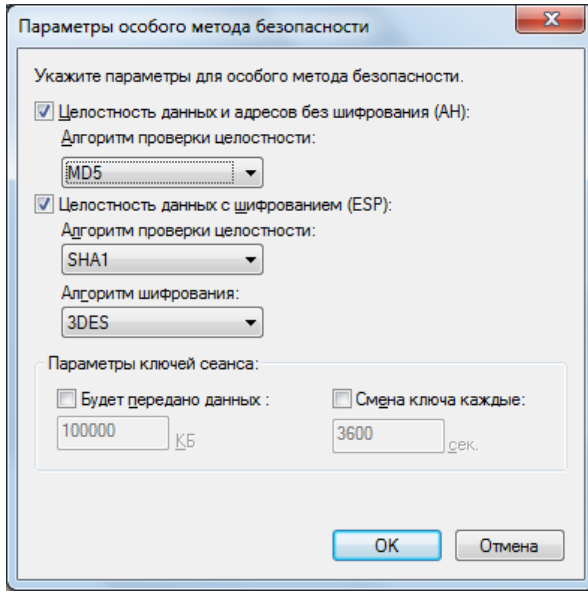



Рис. 10. Параметры метода безопасности

15) Действие фильтра: Шифровать ⇨ Далее;

16) в окне «Метод проверки подлинности» выбрать «Использовать данную строку для защиты обмена ключами» и набрать: Pre-Shared Key ⇨ Далее ⇨ Готово ⇨ закрыть окно ОК;

17) нажать правой кнопкой на «Политика IPSec» ⇨ Назначить.

*г) Добавление нового фильтра:*

1) открыть свойства Политики IPSec через контекстное меню;

2) выполнить аналогичные действия описанные выше по добавлению нового фильтра со следующими параметрами:

- Тип сети: Все сетевые подключения;
- Имя фильтра: Полный IP-трафик;
- Адрес источника пакетов: Мой IP-адрес;
- Адрес назначения пакетов: Любой IP-адрес;
- Отраженный; Протокол: Любой;
- Действие фильтра: Блокировать.

Таким образом создается фильтр закрывающий весь трафик для компьютера А, кроме защищенного взаимодействия с компьютером В.

***Этап 3 – Настройка политики IPSec для компьютера Host-B с Windows XP***

*Примечание*. Для защиты передаваемых данных, оба компьютера должны иметь согласованные методы безопасности при обмене ключами и шифровании данных.

*а) Создание файла консоли:*

1) Пуск ⇨ Выполнить (либо сочетанием клавиш Win+R);
2) ввести mmc.exe и нажать на клавишу Enter;
3) меню Консоль ⇨ Добавить или удалить оснастку ⇨ Добавить;
4) в списке доступных оснасток выделить «Управление политикой IP-безопасности» ⇨ Добавить ⇨ оставить флажок «Локальный компьютер» ⇨ Готово ⇨ Закрыть ⇨ ОК;
5) Консоль ⇨ Сохранить как... ⇨ выбрать путь к рабочей папке и сохранить файл консоли управления ipsec.msc нажав ОК;

*б) Запуск службы IPSec:*

Пуск ⇨ Выполнить ⇨ cmd.exe ⇨ Enter ⇨выполнить команду: net start PolicyAgent;

*в) Создание политики безопасности и настройка IP-фильтров:*

1) кликнуть правой кнопкой мыши на «Политики IP-безопасности»;
2) Создать политику безопасности;
3) в открывшемся мастере нажать Далее ⇨ ввести имя «Политика IPSec» ⇨ Далее ⇨ снять флажок «Использовать правило по умолчанию» ⇨ Далее ⇨ оставить установленным флажок «Изменить свойства» ⇨ Готово.
4) в открывшемся окне Свойства ⇨ зайти во вкладку Общие ⇨ Дополнительно ⇨ Методы;
5) в окне «Методы безопасности при обмене ключами» (IKE), установить параметры, аналогичные рис. 8;

Примечание. В ОС Windows XP по умолчанию задано четыре метода безопасности при обмене ключами, что изображено на рис. 11.

6) нажать ОК и вернуться в окно Свойств во вкладку Правила;
7) Добавить ⇨ в «Мастере создания новых правил» нажать Далее;
8) установить флажок «Это правило не определяет туннель» ⇨ Далее.
9) выбрать тип сети «Все сетевые подключения» ⇨ Далее;
10) использовать данную строку для защиты обмена ключами, набрать: Pre-Shared Key ⇨ Далее;

11) нажать на кнопку Добавить, в открывшемся окне «Список IP-фильтров», ввести имя «Защищенный IP-трафик с хостом B» ⇨ Добавить;

12) во вкладке Адреса выбрать значения, как на рис. 12;

13) во вкладке Протокол выбрать тип протокола: Любой ⇨ ОК;

14) в списке IP-фильтров выбрать созданный «Защищенный IP-трафик с хостом B» ⇨ Далее;

15) в окне «Действие фильтра» оставить флажок «Использовать мастер» ⇨ Добавить ⇨ Далее ⇨ Имя: Шифровать ⇨ Далее ⇨ Согласовать безопасность ⇨ Далее ⇨ Не соединяться с компьютерами, не поддерживающими IPSEC ⇨ Далее ⇨ Другой ⇨ Параметры;

16) установить настройки соответствующие рисунку 2.9 ⇨ ОК ⇨ ДА ⇨ Далее ⇨ Готово;

17) выбрать действие фильтра: Шифровать ⇨ Далее ⇨ Готово ⇨ Применить ⇨ ОК;

18) нажать правой кнопкой на «Политика IPSec» ⇨ Назначить.

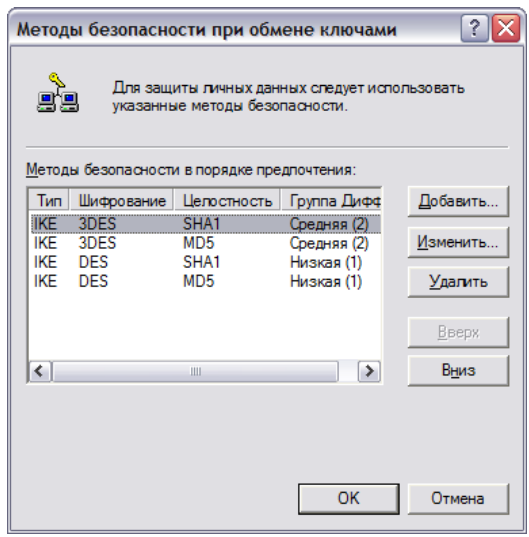



Рис. 11. Методы безопасности при обмене ключами в Windows XP

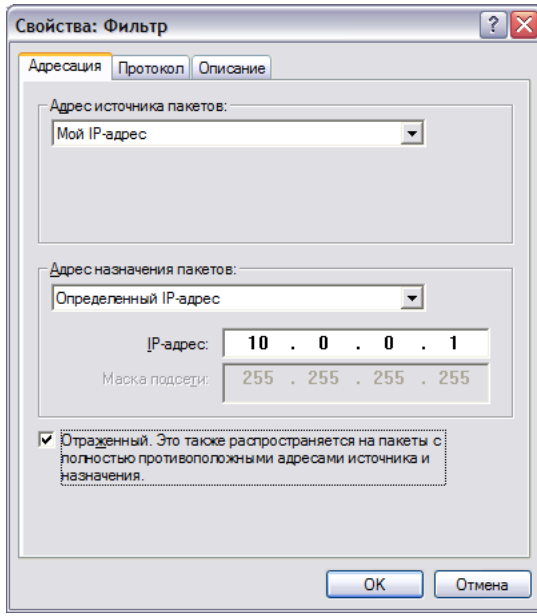



Рис. 12. Свойства IP-фильтра компьютера с именем Host-B

***Этап 4. Проведение экспериментов для проверки работоспособности настроек политик IPSec***

***Эксперимент 1 – Просмотр журнала безопасности:***

Открыть общий доступ к рабочей папке на хосте A (действие выполняется через контекстное меню);

Выполнить вход с хоста B на хост A по адресу \\10.0.0.1, который вводится в проводнике – данное событие фиксируется в журнале безопасности Windows;

На компьютере с именем Host-A:

1) развернуть ветвь «Просмотр событий (локальный)» в консоли;
2) Журналы Windows ⇨ Безопасность;
3) просмотреть общие сведения последних по времени событий, зафиксировать результат.

***Эксперимент 2 – Проверка достижимости узла с включенными политиками:***

На компьютере Host-B:

1) запустить утилиту cmd.exe;

2) выполнить команду: ping 10.0.0.1;

3) убедиться в успешном прохождении ICMP-пакетов, получив ответы от хоста 10.0.0.1.

Провести аналогичный тест с любым хостом в глобальной сети Интернет, например с google.com, получить ответ;

Повторить аналогичные действия на компьютере Host-A.

Зафиксировать результаты. При попытке осуществить выход в Интернет Host-B имеет такие возможности, а Host-A – нет (с чем это связано?).

***Эксперимент 3 – Проверка достижимости узла с отключенной политикой:***

Отключить политику IPSec на компьютере A (правая клавиша мыши ⇨ Снять);

На компьютере B выполнить команду: ping 10.0.0.1;

На компьютере A выполнить команду: ping 10.0.0.2;

Ззаново запустить политику IPSec на компьютере A.

Зафиксировать и объяснить полученные результаты.

***Эксперимент 4 – Просмотр событий в «Мониторе IP-безопасности»:***

На компьютере с именем Host-A развернуть ветвь «Просмотр событий (локальный)» в корне консоли;

Развернуть ветвь HOST-A;

В подпапках находятся статистические данные по IP-безопасности.

Зафиксировать и объяснить полученные результаты.

*Примечание.* Оснастка «Монитор IP-безопасности» может быть использована для просмотра и наблюдения за статистическими данными и политикой IPSec. Эта информация может быть полезна при устранения неполадок в IPSec и тестировании создаваемых политик. Эти статистические данные могут использоваться при обнаружении возможных атак на данный компьютер или другие компьютеры, добавленные к оснастке. При просмотре сопоставлений безопасности данного компьютера можно определить, какие компьютеры с ним соединены, какой тип целостности данных и шифрации используется в этих соединениях, а также получить другую информацию.

***Эксперимент 5 – Сканированием сети анализатором трафика:***

*Примечание.* Для данного эксперимента на одном из компьютеров устанавливается утилита Microsoft Network Monitor 3.4, которую можно бесплатно скачать с официального сайта:

http://www.microsoft.com/en-us/download/details.aspx?id=4865 (для 32- и 64-разрядных систем).

*Сканирование трафика при выполнении команды ping с отключенной политикой безопасности:*

1) отключить политику IPSec на обоих компьютерах;
2) запустить программу Microsoft Network Monitor 3.4;
3) создать новый захват: File ⇨ New ⇨ Capture или Ctrl+N;
4) нажать на кнопку Capture Settings на панели инструментов;
5) в открывшемся окне параметров захвата установить флажок напротив имени «Подключение по локальной сети» для текущего сетевого адаптера (IPv4 = 10.0.0.1 или 10.0.0.2), остальные снять ⇨ Close;
6) запустить сканирование кнопкой Start на панели инструментов;
7) провести ping со второго хоста;
8) по завершении ping нажать на Pause (F6);
9) раскрыть ветвь All Traffic и кликнут мышью на ветке My Traffic в окне Network Conversations;
10) в окне Display Filter ввести ICMP и нажать Apply.

Изучить содержимое окон Frame Summary и Frame Details, объяснить и сохранить полученные результаты.

*Перехват данных, передаваемых в открытом виде:*

1) сбросить фильтр нажав Remove Filter и запустить сканирование отжав кнопку Pause (F6);
2) передать с одного хоста на другой предварительно созданный txt-файл, содержимое которого составляют пару сотен «1» (единиц), по завершении передачи нажать на паузу;
3) создать и применить новый TCP-фильтр;
4) поочередно выбирая фреймы в окне Frame Summary и просматривая содержимое окна Hex Details, обнаружить переданные «1».

*Сканирование трафика при выполнение команды ping с включенной политикой безопасности:*

1) сбросить фильтр ⇨ остановить сканирование Stop! ⇨ Start!;
2) включить политики безопасности на обоих компьютерах;
3) выполните ping с одного хоста на другой;
4) создать и применить ICMP-фильтр, объяснить результат;
5) создать и применить ESP-фильтр, объяснить результат.

*Просмотр сообщений IKE-согласований:*

1) создать и примените IKE-фильтр;

2) изучить содержимое окон Frame Summary и Frame Details, объяснить и сохранить полученные результаты;

3) повторить эксперимент с передачей файла, содержащего «1», объяснить полученный результат.

***Этап 5. Возобновление обычного режима связи между компьютерами***

1. На обоих компьютерах в консоли mmc, вызвав контекстное меню, снять ранее назначенные политики IPSec.

2. Закрыть окна программ mmc.exe, cmd.exe, MS Network Monitor.

3. Возобновить первоначальные значения настроек сетевого интерфейса.

4. Выйти из системы, завершив сеанс работы от имени администратора.

**Требования к содержанию отчета**

Отчет должен включать:

- номер, тема и цель работы;
- краткие теоретические сведения по работе;
- ход выполнения работы со скриншотами основных окон настроек;
- распечатки результатов экспериментов с комментариями к ним;
- выводы по работе.

**Контрольные вопросы**

1. Какие три протокола представляют ядро IPSec и какое назначение каждого из них?

2. Какова последовательность работы протокола IPSec?

3. Какая структура IP-пакета после применения протокола AH в транспортном и туннельном режимах?

4. Какая структура IP-пакета после применения протокола ESP в транспортном и туннельном режимах?

5. Чем отличаются транспортный и туннельный режимы работы IPSec?

6. Какие методы проверки подлинности (IKE) обеспечиваются ОС Windows? Опишите их отличительные особенности.

7. Назовите алгоритмы проверки целостности и шифрования используемые в ОС Windows для обеспечения безопасности при обмене ключами и передачи данных.

8. Из каких полей состоят заголовки AH и ESP?

9. Структура IKE-сообщения.

## 1.7 Удаленный доступ к сети с использованием виртуального защищенного соединения PPTP и L2TP

### Цель и задачи работы

1. Изучить протоколы туннелирования PPTP и L2TP.
2. В лабораторных условиях ознакомиться с процессом организации удаленного доступа к сети с использованием виртуального защищенного соединения.
3. Провести эксперименты для проверки работы протоколов.

### Подготовка к лабораторной работе

При подготовке к лабораторной работе необходимо:

- ознакомиться с целью и задачами исследования;
- изучить теоретический материал, приведенный в учебном пособии;
- бесплатно скачать с официального сайта: http://www.microsoft.com/en-us/download/details.aspx?id=4865 утилиту Microsoft Network Monitor 3.4, инсталлировать ее на компьютерах лаборатории, ознакомиться с правилами ее использования.

### Теоретический материал

Средства VPN, применяемые на канальном уровне модели OSI, позволяют обеспечить инкапсуляцию различных видов трафика третьего уровня (и выше) и построение виртуальных туннелей типа «точка-точка» (от маршрутизатора к маршрутизатору или от персонального компьютера к шлюзу ЛС) (рис. 1). Туннелирование само по себе не решает задачи обеспечения безопасности передачи данных. Специальные пакеты предназначены всего лишь для маршрутизации данных в точку назначения.

Протоколы PPTP (Point-to-Point Tunneling Protocol) и L2TP (Layer-2 Tunneling Protocol) – это протоколы туннелирования канального уровня модели OSI. Протокол PPTP осуществляет туннелирование и шифрование передаваемых данных. Протокол L2TP поддерживает только функцию туннелирования, поэтому для защиты данных необходимо использовать дополнительный протокол IPSec.

Протоколы PPTP и L2TP основываются на стандартном протоколе канального уровня PPP (Point-to-Point Protocol) и являются его расширениями.

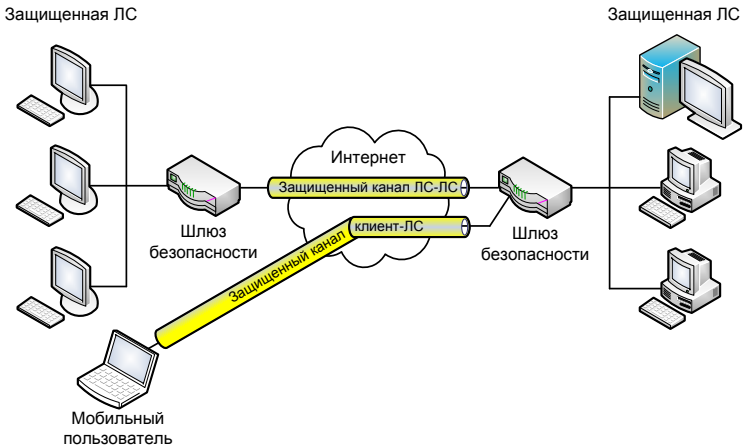



Рис. 1. Виртуальные защищенные каналы типа ЛС-ЛС и клиент-ЛС

В набор PPP входят протокол управления соединением LCP (Link Control Protocol), ответственный за конфигурацию, установку, работу и завершение соединения «точка-точка», и протокол управления сетью NCP (Network Control Protocol), способный инкапсулировать в PPP протоколы сетевого уровня для транспортировки через соединение «точка-точка».

Процесс доставки конфиденциальных данных:

1) инкапсуляция данных с помощью протокола PPP;

2) шифрование и собственная инкапсуляция протоколами PPTP и L2TP;

3) упаковка в протокол IP;

4) продвижение пакета в сетях TCP/IP из начальной точки в конечную;

5) проверка и деинкапсуляция пакетов в точке приема.

Пакеты, передаваемые в рамках сессии PPTP, имеют структуру показанную на рис. 2.

| Заголовок кадра передачи | IP-заголовок | GRE-заголовок маршрутизации | PPP-заголовок | Данные PPP | Концевик кадра передачи |
|---|---|---|---|---|---|

Рис. 2. Структура пакета для пересылки по туннелю PPTP

По протоколу PPTP при создании защищенного виртуального канала производится аутентификация удаленного пользователя и шифрование передаваемых данных (рис. 3).

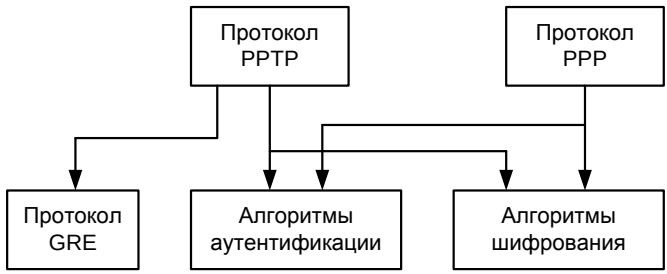



Рис. 3. Архитектура протокола PPTP

Для аутентификации может использоваться один из перечисленных протоколов: распознавание по паролю PAP (Password Authentication Protocol), распознавание при рукопожатии MSCHAP (Microsoft Challenge-Handshaking Authentication Protocol) и распознавание EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).

Для шифрования используется протокол MPPE (Microsoft Point-to-Point Encryption), который совместим только с MSCHAP (версии 1 и 2) и EAP-TLS. Протокол MPPE поддерживает работу с ключами длиной 40, 56 и 128 бит, он изменяет значение ключа шифрования после каждого принятого пакета.

Для установления соединения по протоколу PPTP между удаленным пользователем и локальной сетью необходимо наличие:

- на компьютере пользователя – установленная клиентская часть сервиса удаленного доступа RAS (Remote Access Service) и драйвер PPTP, которые входят в состав ОС Windows;
- на сервере удаленного доступа локальной сети (функции которого может выполнять пограничный маршрутизатор с поддержкой используемых протоколов или компьютер с ОС Windows Server) – сервер RAS и драйвер PPTP.

Недостатки протокола PPTP:

- возможность создания туннеля только поверх TCP/IP сетей;
- уязвимости протоколов аутентификации;
- слабая аутентификация пользователя (по паролю) и отсутствие аутентификации компьютера;

- протокол шифрования MPPE не поддерживается большинством сетевого оборудования.

Протокол L2TP разработан в организации IETF (Internet Engineering Task Force) при поддержке компаний CISCO Systems и Microsoft, как альтернатива протоколу PPTP.

В отличие от PPTP, протокол L2TP не привязан к протоколу IP, поэтому он может быть использован в сетях с коммутацией пакетов (например ATM) или в сетях с ретрансляцией кадров (Frame Relay). Кроме того, в протокол L2TP добавлена функция управления потоками данных и дополнительных функций защиты, в частности, включена возможность работы с протоколами AH и ESP стека протоколов IPSec (рис. 4).

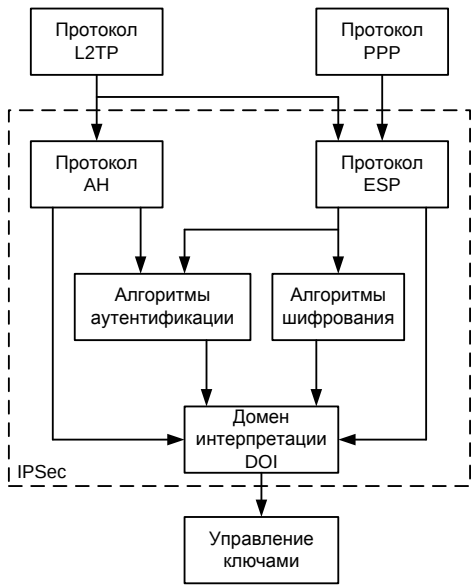



Рис. 4. Архитектура протокола L2TP

Протокол L2TP (поверх IPSec) выполняет аутентификацию на уровнях «компьютер» и «пользователь», а также шифрование данных надежнее, чем PPTP. В отличие от протокола PPTP, L2TP предоставляет возможность открывать между конечными абонентами сразу несколько туннелей, каждый из которых может быть выделен для отдельного приложения.

Согласно спецификации протокола L2TP роль сервера удаленного доступа выполняет концентратор LAC (L2TP Access Concentrator), который обеспечивает удаленному пользователю доступ к его ЛС через Интернет. В качестве сервера удаленного доступа ЛС выступает сетевой сервер LNS (L2TP Network Server), функционирующий на совместимых с протоколом PPP платформах.

Три этапа формирования VPN-канала:

1) установление соединение с сервером удаленного доступа ЛС;
2) аутентификация пользователя;
3) конфигурирование защищенного туннеля.

Недостатки протокола L2TP:

- для его реализации необходима поддержка Интернет-провайдеров;
- ограничивает трафик рамками выбранного туннеля и лишает пользователей доступа к другим частям Интернета;
- спецификация обеспечивает шифрование только в IP-сетях с IPSec.

**Этапы выполнения работы**

1. Настройка VPN-сервера с ОС Windows Server 2008 R2.
2. Настройка VPN-клиента с ОС Windows XP.
3. Настройка компьютера в локальной сети.
4. Тестирование виртуального защищенного соединения.
5. Восстановление начального состояния компьютеров.

Для выполнения лабораторной работы необходимо наличие трех компьютеров, физически объединенных в единую сеть. На компьютере, выполняющего роль VPN-сервера должно быть две сетевые карты и установленная Windows Server 2008 R2, на двух других – Windows XP/7. На рис. 5 показана структура рабочей схемы сети.

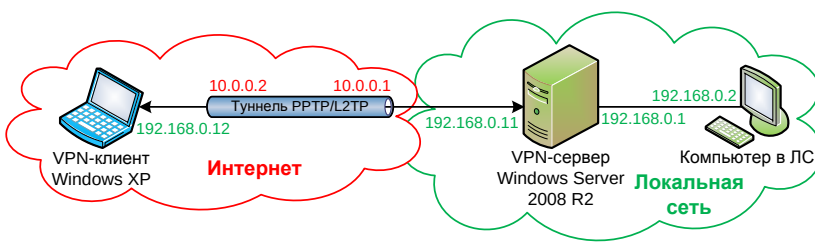



Рис. 5. Структура рабочей схемы сети

***Этап 1 – Настройка VPN-сервера с ОС Windows Server 2008 R2:***

*а) Настройка сетевого интерфейса с сетью 10.0.0.0:*

1) Пуск ⇨ Панель управления ⇨ Сеть и Интернет ⇨ Центр управления сетями и общим доступом ⇨ Изменение параметров адаптера (или Win+R ⇨ ncpa.cpl ⇨ Enter);

2) правой кнопкой мыши на «Подключение по локальной сети» ⇨ Свойства ⇨ Протокол Интернета версии 4 ⇨ Свойства;

3) установить следующие параметры:

- выбрать опцию «Использовать следующий IP-адрес»,
- IP-адрес: 10.0.0.1,
- Маска подсети: 255.0.0.0,
- Предпочитаемый DNS-сервер: 127.0.0.1;

4) ОК ⇨ Закрыть;

5) включить «Подключение по локальной сети» двойным кликом.

*б) Настройка сетевого интерфейса с сетью 192.168.0.0:*

1) Пуск ⇨ Панель управления ⇨ Сеть и Интернет ⇨ Центр управления сетями и общим доступом ⇨ Изменение параметров адаптера;

2) правой кнопкой мыши на «Подключение по локальной сети 2» ⇨ Свойства ⇨ Протокол Интернета версии 4 ⇨ Свойства;

3) установить следующие параметры:

- выбрать опцию Использовать следующий IP-адрес,
- IP-адрес: 192.168.0.1,
- Маска подсети: 255.255.255.0,
- Предпочитаемый DNS-сервер: 127.0.0.1;

4) ОК ⇨ Закрыть;

5) включить «Подключение по локальной сети 2» двойным кликом.

*в) Установка роли «Службы политики сети и доступа»:*

1) Пуск ⇨ Администрирование ⇨ Диспетчер сервера;

2) в дереве консоли кликнуть правой кнопкой мыши на Роли ⇨ Добавить роли;

3) установить флажки напротив «Службы политики сети и доступа» ⇨ Далее ⇨ Далее;

4) установить флажок «Службы маршрутизации и удаленного доступа» ⇨ Далее ⇨ Установить ⇨ Закрыть.

*г) Настройка службы «Маршрутизация и удаленный доступ»:*

1) Пуск ⇨ Администрирование ⇨ Маршрутизация и удаленный доступ;

2) кликнуть правой кнопкой мыши на имени сервера WINSRV-2008-R2 (если его нет, то добавить через контекстное меню) ⇨ Настроить и включить маршрутизацию и удаленный доступ;

3) в открывшемся Мастере нажать Далее ⇨ выбрать опцию «Особая конфигурация» ⇨ Далее;

4) установить флажок «Доступ к виртуальной частной сети (VPN)» ⇨ Далее ⇨ Готово;

5) запустить службу – значок рядом с именем сервера должен принять вид зеленой стрелки направленной вверх (рис. 6).

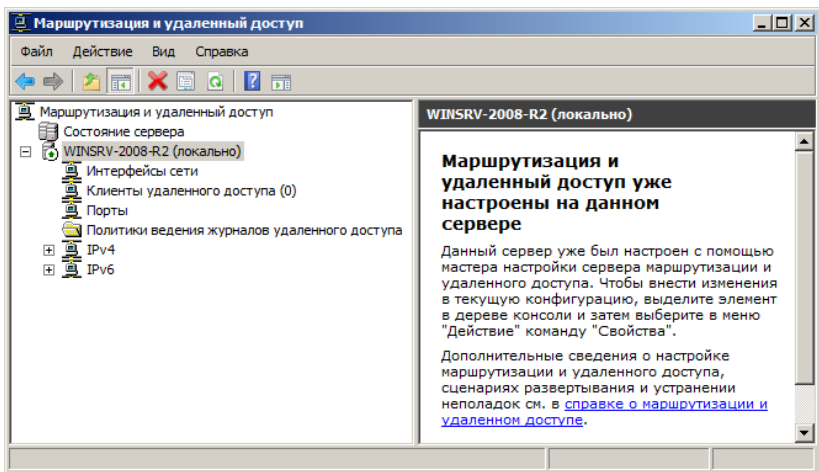



Рис. 6. Служба маршрутизации и удаленного доступа

*д) Настройки безопасности и назначение IP-адресов для удаленных VPN-клиентов:*

1) кликнуть правой кнопкой мыши на «Маршрутизация и удаленный доступ» ⇨ Свойства;

2) перейти во вкладку Безопасность ⇨ Методы проверки подлинности;

3) установить флажок напротив «Шифрованная проверка (Microsoft, версия 2, MS-CHAP v2)» (рис. 7) ⇨ OK;

4) установить флаг «Разрешать пользовательские IPSec-политики»;

5) ввести предварительный ключ: Pre-Shared Key;

6) перейти во вкладку IPv4;
7) выбрать опцию статический пул адресов ⇨ Добавить;

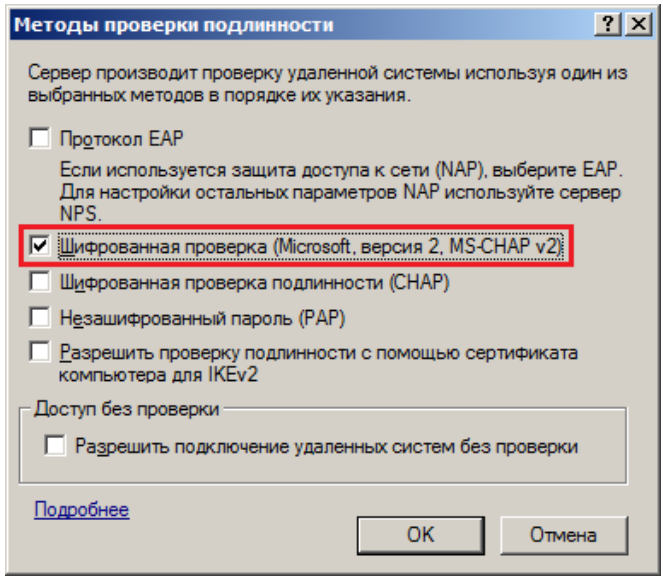



Рис. 7. Методы проверки подлинности

8) ввести значения:
- Начальный IP-адрес: 192.168.0.11,
- Конечный IP-адрес: 192.168.0.12,

⇨ ОК;

9) выбрать адаптер «Подключение по локальной сети», через который подключаются VPN-клиенты (если включен только один адаптер, то данный список не отображается);

10) перейти во вкладку PPP ⇨ снять флажок «Многоканальные подключения»;

11) перейти во вкладку «Ведение журнала» ⇨ выбрать опцию «вести журнал всех событий»;

12) закрыть окно свойств нажав ОК.

*е) Создание и настройка виртуальных портов для приема VPN-подключений:*

1) в ветви «Маршрутизация и удаленный доступ» кликнуть правой кнопкой мыши на Порты ⇨ Свойства;

2) в новом окне выделить WAN Miniport (L2TP) ⇨ Настроить;

3) оставить только флажок «Подключения удаленного доступа (только входящие)» (рис. 8);

4) задать «Максимальное число портов» равное 1 ⇨ ОК ⇨ Да;

5) вернувшись в окно Свойства, аналогично настроить порты PPTP;

6) отключить порты «WAN Miniport (IKEv2)» и «WAN Miniport (SSTP)» сняв флажки всех подключений в их настройках;

7) закрыть окно Свойства нажав ОК.

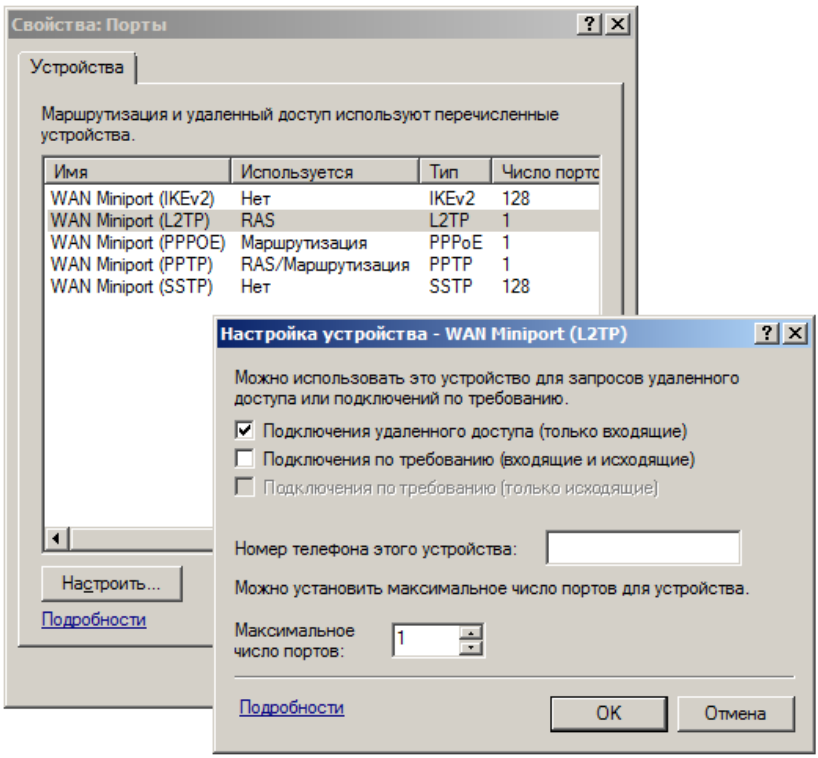



Рис. 8. Настройка VPN-портов

*ж) Установка роли Active Directory и настройка сервера контроллером домена:*

1) Пуск ⇨ Администрирование ⇨ Диспетчер сервера;

2) в Дереве консоли кликнуть правой кнопкой мыши на Роли ⇨ Добавить роли;

3) установить флажок «Доменные службы Active Directory»;

4) Далее ⇨ Далее ⇨ Установить ⇨ Закрыть.

5) нажать на клавиатуре сочетание Win+R ⇨ напечатать dcpromo.exe ⇨ Выполнить;

6) в «Мастере установки доменных служб Active Directory» нажать Далее;

7) Далее ⇨ Создать новый домен в новом лесу ⇨ Далее;

8) ввести доменное имя: testlab.net ⇨ Далее;

9) выбрать режим работы леса: Windows Server 2008 R2 ⇨ Далее;

10) оставить флажок «DNS-сервер» ⇨ Далее ⇨ Да ⇨ Далее;

11) ввести пароль: pa$$w0rd ⇨ Далее ⇨ Далее;

12) установить флажок «Перезагрузка по завершении», дождаться завершения настроек и перезагрузки компьютера.

Результат проведенных настроек представлен на рис. 9.

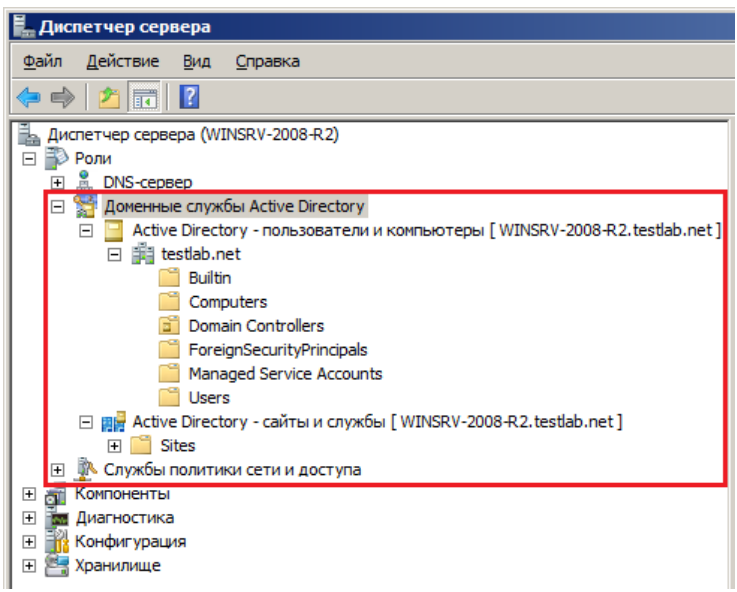



Рис. 9. Доменные службы Active Directory

*и) Создание пользователей с правами на удаленное подключение к локальной сети 192.168.0.0:*

1) Пуск ⇨ Администрирование ⇨ Active Directory – Пользователи и компьютеры;

2) раскрыть ветвь testlab.net ⇨ кликнуть правой кнопкой мыши на Users ⇨ Создать ⇨ Пользователь;

3) в окне «Новый объект – Пользователь» ввести:

- Имя: vpn-user,
- Имя входа пользователя: vpn-user ⇨Далее
- установить флажок «Срок действия пароля не ограничен» и ввести:
- Пароль: pa$$w0rd,
- Подтверждение: pa$$w0rd,
- Далее ⇨ Готово;

4) в основном окне «Active Directory – Пользователи и компьютеры» найти созданного vpn-user и кликнуть по нему правой кнопкой мыши ⇨ Свойства;

5) перейти во вкладку «Входящие звонки»;

6) установить опцию «Разрешить доступ» ⇨ OK;

7) закрыть окно «Active Directory – Пользователи и компьютеры».

***Этап 2 – Настройка VPN-клиента с ОС Windows XP***

*а) Настройка сетевого интерфейса:*

1) Пуск ⇨ Настройка ⇨ Панель управления ⇨ Сетевые подключения;

2) кликнуть правой кнопкой мыши на «Подключение по локальной сети» ⇨ Свойства;

3) выбрать «Протокол Интернета TCP/IP» ⇨ Свойства;

4) ввести следующие параметры:

IP-адрес: 10.0.0.2,

Маска подсети: 255.0.0.0,

OK ⇨ Закрыть;

включить «Подключение по локальной сети» двойным кликом.

*б) Проверка соединения:*

1) на клиентской машине нажать Win+R ⇨ cmd.exe ⇨ Enter;

2) ввести команду: ping 10.0.0.1 ⇨ Enter;

3) убедиться в успешности обмена пакетами с VPN-сервером при простом локальном соединении.

*в) Создание PPTP-подключения:*

1) открыть «Сетевые подключения»;

2) Файл ⇨ Новое подключение ⇨ Далее;
3) выбрать «Подключить к сети на рабочем месте» ⇨ Далее;
4) выбрать «Подключение к виртуальной частной сети» ⇨ Далее;
5) ввести имя подключения: PPTP ⇨ Далее;
6) ввести IP-адрес VPN-сервера: 10.0.0.1 ⇨ Далее ⇨ Готово;
7) в окне «Подключение: PPTP» ввести:
Пользователь: vpn-user,
Пароль: pa$$w0rd,
установить флажок «Сохранять имя пользователя и пароль»;
8) зайти в Свойства ⇨ открыть вкладку Безопасность;
9) выбрать опцию «Дополнительные (выборочные параметры)» ⇨ Параметры;
10) задать шифрование данных – обязательное;
11) установить флажок «Протокол проверки пароля Microsoft (MS CHAP v2)» ⇨ ОК;
12) перейти во вкладку Сеть ⇨ Тип VPN: PPTP VPN (рис. 10);

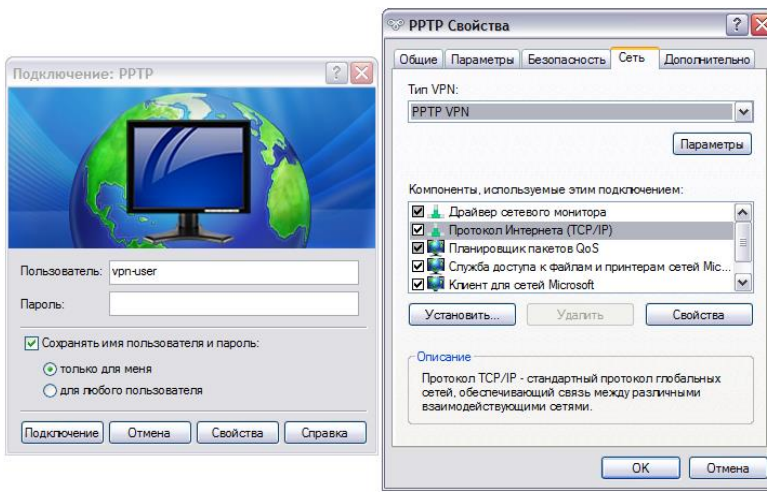



Рис. 10. PPTP-подключение на компьютере клиента

13) «Протокол Интернета TCP/IP» ⇨ Свойства ⇨ оставить включенной опцию «Получить IP-адрес автоматически»;
14) кнопка Дополнительно ⇨ снять флажок «Использоватьосновной шлюз в удаленной сети» (это нужно для того, чтобы на клиенте работало Интернет-соединение);

15) закрыть все окна: ОК ⇨ ОК ⇨ ОК.

*г) Создание L2TP-подключения:*

1) открыть «Сетевые подключения»;
2) Файл ⇨ Новое подключение ⇨ Далее;
3) выбрать «Подключить к сети на рабочем месте» ⇨ Далее;
4) выбрать «Подключение к виртуальной частной сети» ⇨ Далее;
5) ввести имя подключения: L2TP ⇨ Далее;
6) выбрать «Не набирать номер для предварительного подключения» ⇨ Далее;
7) ввести IP-адрес VPN-сервера: 10.0.0.1 ⇨ Далее ⇨ Готово;
8) в окне Подключение: L2TP ввести:
Пользователь: vpn-user,
Пароль: pa$$w0rd,
установить флажок «Сохранять имя пользователя и пароль»;
9) зайти в Свойства ⇨ открыть вкладку Безопасность;
10) выбрать опцию «Дополнительные (выборочные параметры)» ⇨ Параметры;
11) задать шифрование данных – обязательное;
12) установить флажок «Протокол проверки пароля Microsoft (MS CHAP v2)» ⇨ ОК;
13) нажать на кнопку «Параметры IPSec»;
14) установить флажок «Для проверки подлинности использовать предварительный ключ» ⇨ ввести: Pre-Shared Key ⇨ ОК (рис. 11);

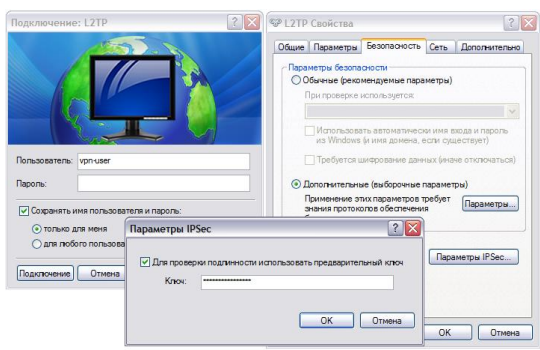



Рис. 11. L2TP-подключение на компьютере клиента

15) перейти во вкладку Сеть ⇨ Тип VPN: L2TP IPSec VPN;

16) Протокол Интернета TCP/IP ⇨ Свойства ⇨ оставить включенной опцию «Получить IP-адрес автоматически»;

17) кнопка Дополнительно ⇨ снять флажок «Использовать основной шлюз в удаленной сети» (это нужно для того, чтобы на клиенте работало Интернет-соединение);

18) закрыть все окна: ОК ⇨ ОК ⇨ ОК.

***Этап 3 – Настройка компьютера в локальной сети 192.168.0.0:***

*а) Настройка сетевого интерфейса:*

1) Пуск ⇨ Настройка ⇨ Панель управления ⇨ Сетевые подключения;

2) кликнуть правой кнопкой мыши на «Подключение по локальной сети» ⇨ Свойства;

3) выбрать «Протокол Интернета TCP/IP» ⇨ Свойства;

4) ввести следующие параметры:

IP-адрес: 192.168.0.2,

Маска подсети: 255.255.255.0,

ОК ⇨ Закрыть;

5) включить «Подключение по локальной сети» двойным кликом.

*б) Проверка соединения:*

1) на компьютере в ЛС нажать Win+R ⇨ cmd.exe ⇨ Enter;

2) ввести команду: ping 192.168.0.1 ⇨ Enter;

3) убедиться в успешности обмена пакетами с сервером.

***Этап 4. Тестирование виртуального защищенного соединения***

***Эксперимент 1 – Установка PPTP-соединения:***

*На машине VPN-клиента:*

1) зайти в сетевые подключения (Win+R ⇨ ввести: ncpa.cpl ⇨ Enter);

2) двойной клик по значку PPTP ⇨ Подключение ⇨ дождаться установления соединения;

3) кликнуть правой кнопкой мыши по значку PPTP ⇨ Состояние;

4) изучить информацию во вкладках Общие и Сведения (обратить внимание на IP-адреса сервера и клиента) ⇨ Закрыть.

*На машине VPN-сервера:*

1) открыть Маршрутизация и удаленный доступ;

2) открыть ветвь Клиенты удаленного доступа;

3) в основном окне отобразится информация о клиенте удаленного доступа vpn-user ⇨ произвести двойной клик по этой записи;

4) изучить информацию о состоянии текущего подключения;

5) перейти в ветвь Порты ⇨ найти в списке открытый PPTP-порт и дважды кликнуть по нему;

6) изучить сведения о состоянии порта;

7) нажать кнопку Отключить ⇨ Закрыть.

Зафиксировать и проанализировать полученные сведения.

***Эксперимент 2 – Установка L2TP-соединения:***

Повторить действия *Эксперимента 1* с L2TP подключением на машинах VPN-клиента и VPN-сервера. Зафиксировать и проанализировать полученные результаты.

***Эксперимент 3 – Просмотр журнала безопасности:***

События, происходящие в системе, фиксируются в журнале безопасности Windows Server. Открыть журнал:

1) Пуск ⇨ Администрирование ⇨ Просмотр событий;

2) развернуть ветвь Журналы Windows ⇨ Безопасность;

3) просмотреть общие сведения последних по времени событий.

***Эксперимент 4 – Анализ трафика PPTP-соединения:***

*Примечание.* Для данного эксперимента на компьютере пользователя должна быть установлена утилита Microsoft Network Monitor 3.4, которую можно бесплатно скачать с официального сайта: http://www.microsoft.com/en-us/download/details.aspx?id=4865 (для 32- и 64-разрядных систем).

1) запустить программу MS Network Monitor 3.4 на машине VPN-клиента;

2) создать новый захват: File ⇨ New ⇨ Capture или Ctrl + N;

3) нажать на кнопку Capture Settings (F4) на панели инструментов;

4) в открывшемся окне параметров захвата установить флажок напротив имени «Подключение по локальной сети» для текущего сетевого адаптера (IPv4 = 10.0.0.2), остальные снять ⇨ Close;

5) запустить сканирование кнопкой Start (F5) на панели инструментов;

6) установить PPTP-соединение в сетевых подключениях (ncpa.cpl);

7) по завершении подключения нажать на Pause (F6); изучить какие протоколы использовались при установлении PPTP-соединения в окне Frame Summary;

8) в окне Display Filter ввести PPTP и нажать Apply, в окне Frame Summary останется 7 PPTP-кадров; последовательно изучить PPTP-заголовки каждого кадра в окне Frame Details, обратить особое внимание на значение поля ControlMessageType;

9) в окне Display Filter ввести и применить новый фильтр – LCP; изучить заголовки протокола управления соединением (LCP), обратить внимание на порядок инкапсуляции данных;

10) создать новый фильтр для CHAP; изучить процесс проверки подлинности при «рукопожатии» между сервером и клиентом;

11) отключить фильтр кнопкой Remove;

12) перезапустить сканирование кнопками Stop (F7) и Start (F5);

13) с помощью утилиты cmd.exe запустить команду ping 192.168.0.11;

14) остановить сканирование Pause (F6); изучить трафик в окнах Frame Summary и Frame Details;

15) возобновить сканирование ⇨ разорвать соединение PPTP в Сетевых подключениях ⇨ остановить сканирование ⇨ создать PPTP-фильтр; последовательно изучить PPTP-заголовки каждого кадра в окне Frame Details, обратить особое внимание на значение поля ControlMessageType;

16) сбросить фильтр, программу Network Monitor оставить открытой.

***Эксперимент 5 – Анализ трафика L2TP-соединения:***

1) Запустить сканирование кнопкой Start (F5) на панели инструментов;

2) установить L2TP-соединение в сетевых подключениях (ncpa.cpl);

3) по завершении подключения нажать на Pause (F6); изучить какие протоколы использовались при установлении L2TP-соединения в окне Frame Summary. Изучить заголовки протоколов IKE и ESP в окне Frame Details;

4) перезапустить сканирование кнопками Stop (F7) и Start (F5);

5) с помощью утилиты cmd.exe запустить команду ping 192.168.0.11;

6) остановить сканирование Pause (F6); изучить исходящий и входящий трафик в окнах Frame Summary и Frame Details;

7) возобновить сканирование ⇨ разорвать соединение L2TP в Сетевых подключениях ⇨ остановить сканирование; просмотреть заголовки протоколов, участвующих при разрыве соединения (IKE и ESP);

8) закрыть программу Network Monitor.

***Эксперимент 6 – Удаленный доступ к компьютеру локальной сети:***

*На компьютере в ЛС 192.168.0.0:*

1) в рабочей директории создать папку test, в ней создать файл data.txt, заполнить его текстом (например всеми «1»);

2) нажать правой кнопкой мыши на папке test ⇨ Общий доступ и безопасность;

3) установить флажок Открыть общий доступ к папке ⇨ ОК.

*На VPN-клиенте:*

1) установить PPTP-соединение с сервером;

2) проверить доступность удаленного хоста в ЛС с VPN-клиента, для этого запустить cmd.exe ⇨ ввести и запустить команду: ping 192.168.0.2, убедиться в успешности обмена пакетами с хостом локальной сети;

3) открыть проводник: правой кнопкой на Пуск ⇨ Проводник;

4) в адресной строке ввести: \\192.168.0.2 ⇨ Enter;

5) в основном окне открыть папку test ⇨ скопировать data.txt;

6) запустить сканирование (F5) в Network Monitor;

7) вставить скопированный ранее файл в рабочую директорию на компьютере VPN-клиента;

8) остановить сканирование (F7) и просмотреть результаты. Изучить поле данных в окне Hex Details, убедиться, что они зашифрованы;

9) повторить передачу данный и сканирование трафика при L2TP-соединении, зафиксировать результат.

***Этап 5. Восстановление начального состояния компьютеров***

1. На компьютере ЛС 192.168.0.0:

- снять общий доступ к папке test и удалить ее;
- восстановить первоначальные настройки сетевого интерфейса.

2. На компьютере VPN-клиента:

- удалить виртуальные частные подключения PPTP и L2TP;
- восстановить первоначальные настройки сетевого интерфейса.

3. На компьютере VPN-сервера:

- восстановить первоначальные настройки сетевых интерфейсов на обеих сетевых адаптерах;
- отключить службу маршрутизации и удаленного доступа;
- удалить роли: Службы политики сети и доступа, Доменные службы Active Directory и DNS-сервер.

4. Закрыть все открытые окна.

5. Выйти из систем, завершив сеанс работы от имени администратора.

**Требования к содержанию отчета**

Отчет должен включать:
- номер, тема и цель работы;
- краткие теоретические сведения по работе;
- ход выполнения работы со скриншотами основных окон настроек;
- распечатки результатов экспериментов с комментариями к ним;
- выводы по работе.

**Контрольные вопросы**

1. Какой процесс доставки конфиденциальных данных по VPN-туннелю?
2. Архитектура протокола PPTP.
3. Архитектура протокола L2TP.
4. Опишите сходства и различия протоколов PPTP и L2TP. Достоинства и недостатки каждого из них.
5. Перечислите основные шаги настройки VPN-сервера.

## 1.8 Использование протокола SSL для безопасного взаимодействия клиентов с веб-сервером IIS

### Цель и задачи работы

1. Изучить протокол формирования защищенных каналов SSL/TLS.
2. Научиться разворачивать автономный центр сертификации и веб-сервер IIS в Windows Server 2008 R2, создавать и выдавать сертификаты, настраивать защищенный доступ к сайту по протоколу SSL.
3. Провести эксперименты для проверки работы настроек SSL.

### Подготовка к лабораторной работе

При подготовке к лабораторной работе необходимо:

- ознакомиться с целью и задачами исследования;
- изучить теоретический материал, приведенный в учебном пособии;
- бесплатно скачать с официального сайта: http://www.microsoft.com/en-us/download/details.aspx?id=4865 утилиту Microsoft Network Monitor 3.4, инсталлировать ее на компьютерах лаборатории, ознакомиться с правилами ее использования.

### Теоретический материал

При построении защищенных виртуальных сетей на сеансовом уровне появляется возможность криптографической защиты информационного обмена, включая аутентификацию, а также реализации ряда функций посредничества между взаимодействующими сторонами.

Однако, на сеансовом уровне начинается непосредственная зависимость от приложений, реализующих высокоуровневые протоколы. Поэтому реализация протоколов защиты информационного обмена, соответствующих этому уровню, в большинстве случаев требует внесения изменений в высокоуровневые сетевые приложения.

Для защиты информационного обмена на сеансовом уровне широкое распространение получил протокол SSL (Secure Sockets Layer – протокол защищенных сокетов) и его более новая версия – стандарт TLS (Transport Layer Security – протокол защиты транспортного уровня). Первая версия стандарта TLS в своей основе очень близка к SSLv3, с которой имеет обратную совместимость. Эти протоколы используют криптографию для обеспечения безопасности информационного обмена.

Протокол SSL выполняет все функции по созданию защищенного канала между двумя узами сети, включая их взаимную аутентификацию, обеспечение конфиденциальности, целостности и аутентичности передаваемых данных.

Взаимная аутентификация обеих сторон в SSL выполняется путем обмена цифровыми сертификатами открытых ключей пользователей (клиента и сервера), заверенными цифровой подписью специальных сертификационных центров. Протокол SSL поддерживает сертификаты, соответствующие общепринятому стандарту X.509, а также стандарты инфраструктуры открытых ключей PKI (Public Key Infrastructure), с помощью которой организуется выдача и проверка подлинности сертификатов.

Конфиденциальность обеспечивается шифрованием передаваемых сообщений с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении соединения. Сессионные ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей, извлеченных из сертификатов абонентов.

Подлинность и целостность циркулирующей информации обеспечивается за счет формирования и проверки электронной цифровой подписи.

В качестве алгоритмов асимметричного шифрования используются RSA, а также алгоритм Диффи-Хеллмана. Допустимыми алгоритмами симметричного шифрования являются RC2, RC4, DES, 3DES и AES. Для вычисления хэш-функций могут применяться стандарты MD5 и SHA-1.

Протокол SSL обеспечивает возможность надежной защиты сквозной передачи данных с использованием протокола TCP и представляет собой не один протокол, а два уровня протоколов, как показано на рис. 1.

Протокол записи SSL (SSL Record Protocol) обеспечивает базовый набор средств защиты, применяемых протоколами более высоких уровней. В частности, может использоваться протокол передачи гипертекстовых файлов (HTTP), обеспечивающий обмен данными при взаимодействии клиентов и веб-серверов. Частью SSL считаются и три протокола более высокого уровня: протокол квитирования установления связи (Handshake Protocol), протокол изменения параметров шифрования (Change Cipher Spec Protocol) и протокол извещения (Alert Protocol). Эти протоколы служат для управления обменом данными SSL.


Рис. 1. Архитектура стека протоколов SSL

Работа протокола SSL описывается в терминах двух важных понятий – соединения и сеанса.

*Соединение SSL* – транспорт (в терминах модели OSI), обеспечивающий сервис некоторого подходящего типа. В случае SSL такие соединения представляют равноправные отношения между узлами. Соединения являются временными и ассоциируется только с одним сеансом.

*Сеанс SSL* – это связь между клиентом и сервером. Сеансы создаются протоколом квитирования. Сеанс определяет набор параметров криптозащиты, которые могут использоваться несколькими соединениями.

На рис. 2 показана общая схема работы протокола записи после установления соединения. Этот протокол обеспечивает конфиденциальность и целостность сообщений.

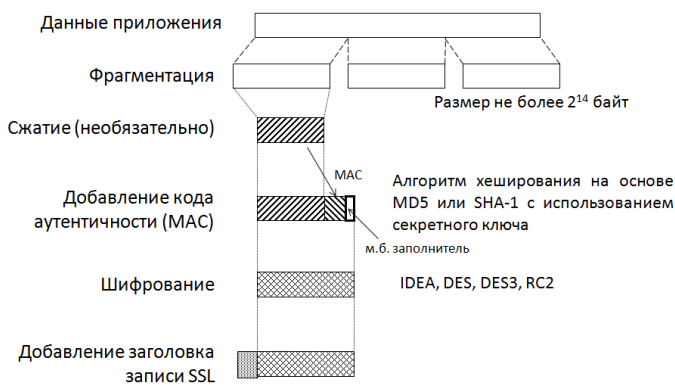



Рис. 2. Общая схема работы протокола записи SSL

Формат записи, получаемой на выходе SSL, показан на рис. 3.


Рис. 3. Формат записи SSL

*Протокол изменения параметров шифрования* является самым простым из трех протоколов высшего уровня. Он генерирует однобайтовое сообщение. Задачей этого сообщения является указание начать копирование параметров состояния ожидания в текущее состояние, что приводит к обновлению комплекта шифров, используемых для данного соединения.

*Протокол извещения* предназначен для передачи другой стороне, участвующей в обмене данными, извещений, касающихся работы SSL. Любое сообщение, генерируемое данным протоколом, состоит из двух байтов:

- первый байт содержит значение, обозначающее уровень предупреждения или уровень неустранимой ошибки;
- второй байт содержит код, уточняющий смысл данного извещения.

*Протокол квитирования* позволяет серверу и клиенту выполнить взаимную аутентификацию, а также согласовать алгоритмы шифрования, алгоритмы аутентификации сообщений и криптографические ключи, которые будут служить для защиты данных, пересылаемых в рамках протокола записи SSL. Протокол квитирования должен использоваться до начала пересылки данных прикладных программ.

Согласно протоколу SSL криптозащищенные туннели создаются между конечными точками виртуальной сети. Инициаторами каждого защищенного туннеля являются клиент и сервер, функционирующие на компьютерах в конечных точках туннеля.

Протокол SSL предусматривает следующие этапы взаимодействия клиента и сервера при защищенном соединения:

1) установление SSL-сессии;

2) защищенное взаимодействие.

В процессе установления SSL-сессии решаются следующие задачи:

- аутентификация сторон;
- согласование криптографических алгоритмов и алгоритмов сжатия;
- формирование общего секретного мастер-ключа;
- генерация на основе сформированного мастер-ключа общих секретных сеансовых ключей для криптозащиты информационного обмена.

Процедура установления SSL-сессии, называемая также процедурой рукопожатия, отрабатывается перед непосредственной защитой информационного обмена и выполняется по протоколу начального приветствия (Handshake Protocol), входящему в состав протокола SSL.

При установлении повторных соединений между клиентом и сервером стороны могут, по взаимному соглашению, формировать новые сеансовые ключи на основе «старого» общего «секрета» (данная процедура называется «продолжением» SSL сессии).

Протокол SSL 3.0 поддерживает три режима аутентификации:

- взаимную аутентификацию сторон;
- одностороннюю аутентификацию сервера без аутентификации клиента;
- полную анонимность.

При использовании последнего варианта обеспечивается защита информационного обмена без каких-либо гарантий относительно подлинности сторон. В этом случае взаимодействующие стороны не защищены от атак, связанных с подменой участников взаимодействия.

В реализациях протокола SSL для аутентификации взаимодействующих сторон и формирования общих секретных ключей обычно используют алгоритм RSA.

Соответствие между открытыми ключами и их владельцами устанавливается с помощью цифровых сертификатов, выдаваемых специальными центрами сертификации.

SSL для аутентификации и шифрования использует одинаковые ключи, что при определенных условиях может привести к потенциальной уязвимости. Подобное решение дает возможность собрать больше статистического материала, чем при аутентификации и шифровании разными ключами.

**Этапы выполнения работы**

1. Установка веб-сервера и автономного центра сертификации.

2. Проверка работы установленных сервисов.

3. Создание сертификата сервера и получение сертификата веб-браузера клиентом.

4. Создание сайта и настройка SSL на веб-сервере IIS.

5. Проведение экспериментов для проверки работоспособности.

6. Восстановление начального состояния компьютеров.

Для выполнения лабораторной работы необходимо наличие двух компьютеров, объединенных в единую сеть с настроенными сетевыми интерфейсами. На компьютере-сервере необходимо установить Windows Server 2008 R2, на клиентском – Windows XP/7 и утилиту MS Network Monitor.

На рис. 4 показана логическая структура данной схемы.

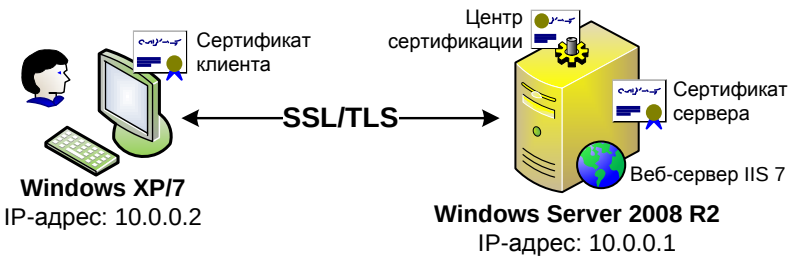



Рис. 4. Логическая структура схемы

***Этап 1 – Установка веб-сервера и автономного центра сертификации:***

*а) Установить роли:*

1) Пуск ⇨ Администрирование ⇨ Диспетчер сервера;

2) кликнуть правой кнопкой на ветви Роли ⇨ Добавить роли;

3) установить флажки напротив «Веб-сервер (IIS)», «Сервер приложений» и «Службы сертификации Active Directory»;

4) мастер предложит «Добавить необходимые компоненты для сервера приложений» (если ранее они не были установлены) ⇨ Далее ⇨ Далее;

5) выбрать службы ролей для «Сервера приложений»: «Поддержка веб-сервера (IIS)», «Общий доступ к TCP-портам», «Активация по HTTP» ⇨ Далее ⇨ Далее;

6) выбрать службы ролей для «Службы сертификации Active Directory»: «Центр сертификации» и «Служба регистрации в центре сер-

тификации через Интернет» ⇨ Добавить требуемые службы роли ⇨ Далее;

7) Автономный ЦС ⇨ Далее;

8) Корневой ЦС ⇨ Далее;

9) Создать новый закрытый ключ ⇨ Далее;

10) оставить настройки шифрования для ЦС по умолчанию ⇨ Далее;

11) ввести общее имя для ЦС: testlab-WINSRV-2008-R2-CA ⇨ Далее;

12) срок действия сертификата, оставить без изменений: 5 лет ⇨ Далее;

13) расположение БД сертификатов оставить без изменений ⇨ Далее;

14) для веб-сервера выбрать службу «FTP-сервер» ⇨ Далее ⇨ Установить.

***Этап 2 – Проверка работы установленных сервисов:***

*а) Проверка работоспособности веб-сервера:*

1) в адресной строке браузера Internet Explorer набрать: http://localhost (или его IP-адрес 127.0.0.1);

2) в результате отображается стандартная страница приветствия IIS 7 (рис. 5);

3) для доступа к странице приветствия с компьютера пользователя, ввести в адресной строке браузера IP-адрес сервера: http://10.0.0.1.

Работа с веб-сервером осуществляется через «Диспетчер служб IIS», который запускается в меню Пуск ⇨ Администрирование (рис. 6).

*Примечание.* IP-адрес сервера можно узнать с помощью команды ipconfig /all в утилите cmd.exe с пометкой «Основной». Изменить IP-адрес можно в свойствах протокола TCP/IP сетевого адаптера в сетевых подключениях (ncpa.cpl).


Рис. 5. Страница приветствия IIS

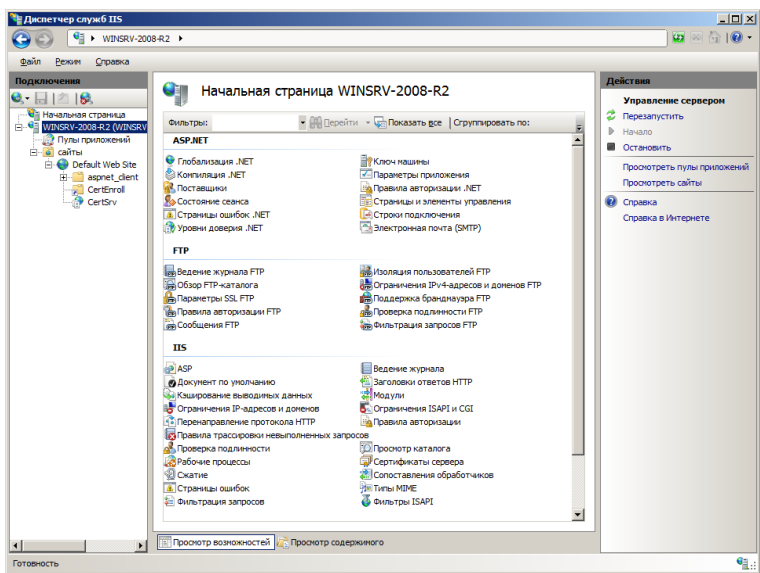



Рис. 6. Диспетчер служб IIS

*б) Проверка работоспособности центра сертификации:*

1) Пуск ⇨ Администрирование ⇨ запустить оснастку «Центр сертификации» (рис. 7);

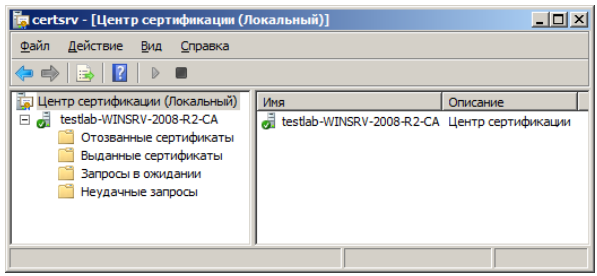



Рис. 7. Оснастка «Центр сертификации»

2) перейти на главную страницу службы сертификации – в адресной строке набрать: http://10.0.0.1/certsrv (рис. 8).

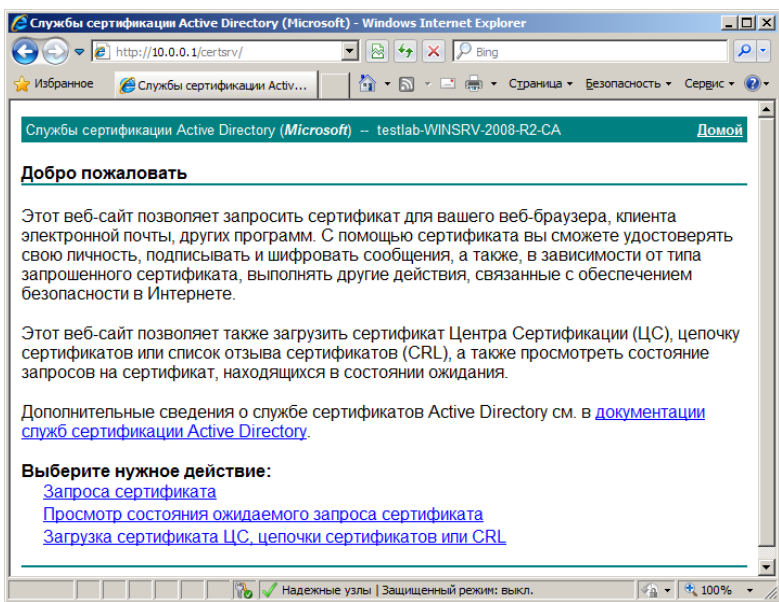



Рис. 8. Главная страница службы сертификации

***Этап 3 – Создание сертификата сервера и получение сертификата веб-браузера клиентом:***

*а) Создание сертификата сервера:*

1) на серверном компьютере запустить браузер Internet Explorer;

2) перейти на страницу: http://10.0.0.1/certsrv;

*Примечание.* Для устранения различный предупреждений безопасности, необходимо добавить данный узел в «Надежные узлы» и установить «низкий уровень безопасности для этой зоны», а также разрешить загрузку «неподписанных ActiveX» в параметрах безопасности (кнопка «Другой»).

3) выбрать действие «Запрос сертификата» ⇨ «расширенный запрос сертификата» ⇨ «Создать и выдать запрос к этому ЦС»;

4) при получении предупреждения о выполнении операций с цифровыми сертификатами, разрешить их, нажав кнопку Да;

5) заполнить форму, следующим образом:

Идентифицирующие сведения:

Имя: Сертификат веб-сервера,

Организация: ДИИТ,

Подразделение: Тестовая лаборатория ЭВМ,

Город: Днепропетровск,

Тип требуемого сертификата:

Сертификат проверки подлинности сервера,

Параметры ключа:

оставить опцию Создать новый набор ключей,

CPS оставить по умолчанию,

Использование ключей: оба,

Размер ключа: 1024,

оставить опцию Автоматическое имя контейнера,

Пометить ключ как экспортируемый,

Дополнительный параметры оставить без изменений;

6) нажать кнопку Выдать;

7) вернуться на страницу http://10.0.0.1/certsrv;

8) открыть «Просмотр состояния ожидаемого запроса сертификата» ⇨ выбрать сертификат для просмотра;

9) запустить оснастку «Центр сертификации» (Пуск ⇨ Администрирование) ⇨ развернуть ветвь «Запросы в ожидании»;

10) в основном окне нажать правой кнопкой мыши на запросе ⇨ «Все задачи» ⇨ Выдать – заявка перейдет в раздел «Выданные сертификаты»;

11) вернуться в окно браузера с ожидаемым сертификатом ⇨ обновить F5 ⇨ нажать на Повтор для отображения страницы;

12) Установить этот сертификат.

*б) Создание сертификата клиента:*

1) на клиентском компьютере запустить браузер Internet Explorer;

2) перейти на страницу: http://10.0.0.1/certsrv;

3) необходимо загрузить сертификат ЦС и поместить его в хранилище доверенных сертификатов, для этого выбрать действие «Загрузка сертификата ЦС, цепочки сертификатов или CRL» ⇨ «Загрузка сертификата ЦС» ⇨ Открыть файл;

4) нажать на кнопку «Установить сертификат», откроется мастер;

5) Далее ⇨ «Поместить все сертификаты в следующее хранилище» ⇨ Обзор ⇨ выбрать «Доверенный корневые центры сертификации» ⇨ ОК ⇨ Далее ⇨ Готово ⇨ В окне предупреждения нажать Да.

6) открыть страницу: http://10.0.0.1/certsrv;

7) выбрать действие «Запрос сертификата» ⇨ «расширенный запрос сертификата» ⇨ «Создать и выдать запрос к этому ЦС»;

8) заполнить форму:

Идентифицирующие сведения:

Имя: User

Организация: ДИИТ

Подразделение: Тестовая лаборатория ЭВМ

Город: Днепропетровск

Тип требуемого сертификата:

Сертификат проверки подлинности клиента

Параметры ключа:

оставить опцию Создать новый набор ключей

CPS оставить по умолчанию

Использование ключей: оба

Размер ключа: 1024

оставить опцию Автоматическое имя контейнера

Дополнительный параметры оставить без изменений

9) нажать кнопку Выдать;

10) запустить Центр сертификации на компьютере сервера и Выдать сертификат;

11) вернуться на страницу http://10.0.0.1/certsrv на машине клиента;

12) открыть «Просмотр состояния ожидаемого запроса сертификата» ⇨ выбрать сертификат для просмотра;

13) Установить этот сертификат ⇨ Да.

***Этап 4 – Создание сайта и настройка SSL на веб-сервере IIS:***

*а) Создание тестового сайта:*

1) создать на серверном компьютере папку testsite в директории C:\inetpub\wwwroot;

2) в папке test создать файл index.htm (для отображения расширений файлов: Alt ⇨ Сервис ⇨ Параметры папок ⇨ Вид ⇨ снять флажок «Скрывать расширения для зарегистрированных типов файлов» ⇨ ОК);

3) файл index.htm наполнить содержимым:

```
<html>
    <head>
                    <title>Тестируем SSL</title>
    </head>
    <h1>Добро пожаловать на сайт!</h1>
</html>
```

4) закрыть и сохранить файл.

*б) Экспорт сертификата из хранилища сервера в файл:*

1) запустить консоль: Win+R ⇨ mmc.exe ⇨ Enter;

2) Файл ⇨ Добавить или удалить оснастку ⇨ выбрать оснастку Сертификаты ⇨ Добавить ⇨ ОК;

3) развернуть ветвь Личное ⇨ кликнуть правой кнопкой на «Сертификат веб-сервера» ⇨ Все задачи ⇨ Экспорт;

4) в открывшемся мастере: Далее ⇨ Да, экспортировать закрытый ключ ⇨ Далее;

5) установить флажки: «Включить по возможности все сертификаты в путь сертификации» и «Экспортировать все расширенные свойства» ⇨ Далее;

6) ввести пароль: 12345 ⇨ Далее ⇨ указать путь к рабочей папке и имя файла с сертификатом ⇨ Далее ⇨ Готово ⇨ ОК.

*в) Импорт сертификата из файла в веб-сервер IIS:*

1) Пуск ⇨ Администрирование ⇨ Диспетчер служб IIS (или Win+R ⇨ inetmgr.exe ⇨ Enter);

2) выделить ветвь с именем сервера WINSRV-2008-R2 ⇨ в основном окне «Начальная страница» в группе IIS открыть «Сертификаты сервера»;

3) в правой колонке Действия кликнуть на Импорт;

4) ввести путь к файлу сертификата и пароль (12345) ⇨ ОК.

*г) Добавление сайта в диспетчере IIS:*

1) в боковом меню диспетчера IIS щелкнуть правой кнопкой мыши на пункте Сайты ⇨ Добавить веб-сайт;
2) в открывшемся окне ввести данные, как на рис. 9 ⇨ ОК.

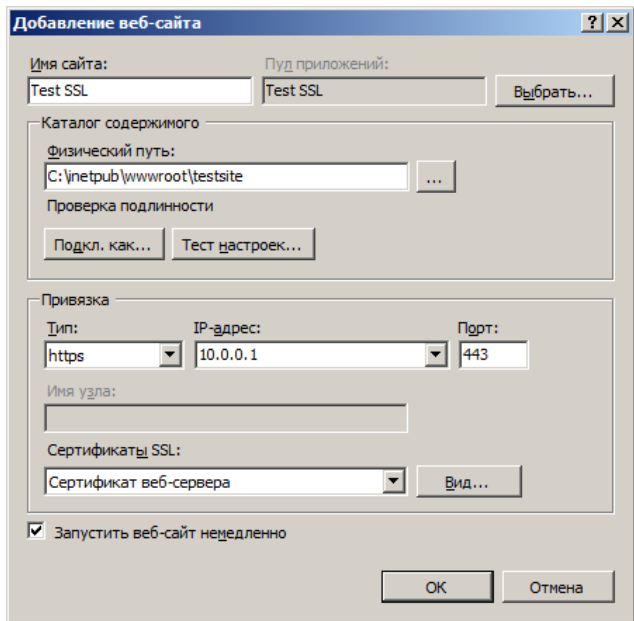



Рис. 9. Добавление веб-сайта в IIS

*д) Включение аутентификации клиента:*

*Примечание*. При создании сайта с использованием SSL аутентификация клиента по сертификату по умолчанию не производится. Для использования двухсторонней проверки подлинности, необходимо:

1) в Диспетчере служб IIS кликнуть на имени сайта «Test SSL»;
2) в основном окне открыть «Параметры SSL»;
3) установить параметры, показанные на рис. 10;
4) сохранить изменения нажав кнопку Применить в правом столбце Действий.

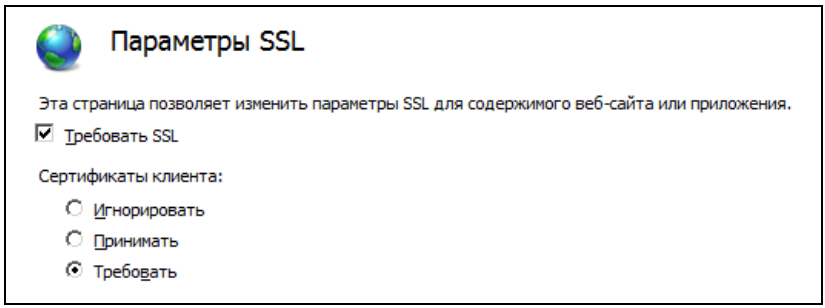



Рис. 10. Включение аутентификации клиента

***Этап 5. Проведение экспериментов для проверки работоспособности***

***Эксперимент 1 – Проверка запуска сайта с компьютера пользователя:***

1) в адресной строке браузера на клиентском компьютере ввести: https://10.0.0.1;

2) проигнорировать ошибку безопасности «Сертификат безопасности этого веб-узла был выпущен для веб-узла с другим адресом» нажав на Продолжить;

*Примечание*. Ошибка вызвана тем, что при создании сертификата в имени было прописано «Test SSL», а доступ происходит через IP-адрес 10.0.0.1. Необходима привязка IP-адреса к доменному имени, которое совпадает с именем в сертификате, что для учебных целей некритично.

3) выбрать сертификат клиента ⇨ OK;

Сохранить результат запущенного сайта.

***Эксперимент 2 – Проверка запуска сайта с компьютера сервера***

1) в адресной строке браузера на серверном компьютере ввести: https://10.0.0.1;

2) проигнорировать ошибку безопасности нажав на Продолжить.

При попытке доступа к сайту через браузер на компьютере сервера появляется Ошибка HTTP 403.7. Чем это вызвано? Какие действия необходимо предпринять для устранения этой ошибки?

***Эксперимент 3 – Просмотр сведений о сертификатах:***

*Сертификат сервера:*

1) на сервере открыть Центр сертификации;

2) зайти в раздел Выданные сертификаты;

3) открыть Сертификат веб-сервера.

Изучить данные вкладок «Общие» и «Состав». Обратить внимание на данные об использовании ключа. Результаты зафиксировать.

*Сертификат пользователя:*

1) на сервере открыть Центр сертификации;

2) зайти в раздел Выданные сертификаты;

3) открыть Сертификат пользователя.

Изучить данные вкладок «Общие» и «Состав». Обратить внимание на данные об использовании ключа. Результаты зафиксировать.

*Сертификат центра сертификации:*

1) на компьютере сервера или пользователя запустить консоль: Пуск ⇨ Выполнить ⇨ mmc.exe ⇨ Enter;

2) Добавить или удалить оснастку (ctrl+M) ⇨ добавить Сертификаты ⇨ моей учетной записи пользователя ⇨ Готово ⇨ ОК;

3) зайти в раздел Доверенные корневые центры сертификации;

4) в списке сертификатов найти testlab-WINSRV-2008-R2-CA (общее имя для ЦС, которое вводилось при установке роли).

Изучить сведения о сертификате, кому и кем он выдан, размер ключа, его использование. Результаты зафиксировать.

***Эксперимент 4 – Просмотр сведений о соединении в браузере:***

1) перейти на тестовый сайт https://10.0.0.1 с компьютера пользователя;

2) в браузере Internet Explorer открыть Свойства в контекстном меню содержимого страницы, изучить полученный результат;

3) в браузере Google Chrome кликнуть по пиктограмме в виде замочка(в начале адресной строки), изучить полученный результат.

***Эксперимент 5 – Анализ работы протокола SSL путем сканирования сетевого трафика***

*Примечание.* Для проведения данного эксперимента установить утилиту Microsoft Network Monitor 3.4, которую можно бесплатно скачать с официального сайта: http://www.microsoft.com/en-us/download/details.aspx?id=4865 (для 32- и 64-разрядных систем).

1) запустить программу MS Network Monitor ⇨ New Capture;

2) Capture Settings ⇨ установить флажок напротив Подключение по локальной сети для сети 10.0.0.0, остальные снять ⇨ Close;

3) запустить захват трафика Start (F5);

4) открыть браузер на клиентской машине ⇨ перейти по адресу: https://10.0.0.1 ⇨ проигнорировать предупреждение и, при необходимости, выбрать сертификат пользователя;

5) развернуть окно программы Network Monitor ⇨ Pause (F6);

6) для исследования работы протокола TLS (SSL) необходимо создать фильтр: в окне Display Filter ввести TLS ⇨ Apply.

Изучить в окне Frame Details какими параметрами обмениваются клиент и сервер по протоколу квитирования (HandShake), какие алгоритмы шифрования и хеширования используются, данные сертификата передаваемые сервером, содержимое при обмене данными прикладного уровня.

***Этап 6. Восстановление начального состояния компьютеров***

1. На компьютере пользователя:

- удалить сертификат клиента (через консоль mmc.exe ⇨ оснастка Сертификаты ⇨ ветвь Личные сертификаты);
- восстановить первоначальные настройки сетевого интерфейса (если такие изменения проводились);
- закрыть браузер, MS Network Monitor и другие открытые окна.

2. На компьютере сервера:

- отозвать сертификат клиента и сервера в Центре сертификации;
- удалить сертификат сервера (через консоль mmc.exe ⇨ оснастка Сертификаты ⇨ ветвь Личные сертификаты);
- удалить тестовый сайт в Диспетчере служб IIS;
- удалить папку с сайтом C:\inetpub\wwwroot\testsite;
- удалить роли: Диспетчер служб IIS, Сервер приложений, Службы сертификации Active Directory через диспетчер сервера;
- восстановить первоначальные настройки сетевого интерфейса (если такие изменения проводились).

3. Выйти из систем, завершив сеанс работы от имени администратора.

**Требования к содержанию отчета**

Отчет должен включать:

- номер, тема и цель работы.
- краткие теоретические сведения по работе.
- ход выполнения работы со скриншотами основных окон настроек.
- распечатки результатов экспериментов с комментариями к ним.
- выводы по работе.

**Контрольные вопросы**

1. Какие функции выполняет протокол SSL?
2. Архитектура стека протоколов SSL. Назначение каждого протокола.
3. Что такое соединение и сеанс связи в SSL?
4. Какова общая схема работы протокола записи SSL?
5. Что такое цифровой сертификат?

## 2 СЕМИНАРЫ

### 2.1 Поиск информационных ресурсов по вопросам информационной безопасности в сети Internet

**Цель семинара:** В ходе семинара выполняется анализ информационных ресурсов по тематике информационной безопасности, приобретение навыков самостоятельного поиска информационных ресурсов в сети Internet и их анализа, а также публичного доклада о результатах поиска.

**Задачи:** по указанной преподавателем тематике найти и просмотреть соответствующие веб-сайты по информационной безопасности, определить информационные ресурсы, расположенные на нем, проанализировать их и составить отчет по лабораторной работе. По результатам работы подготовить устное информационное сообщение.

**Подготовка к семинару**

***Получение (определение) темы работы***

Темы работы согласовываются с преподавателем исходя из ориентировочного перечня, представленного в табл. 1.

Таблица 1. Тематика информационного поиска

| № | Тема | Примечания | Фамилия |
|---|---|---|---|
| 1 | Технические средства защиты информации | | |
| 2 | Криптография | | |
| 3 | Стеганография | | |
| 4 | Парольная защита | | |
| 5 | Организационные меры по защите информации | | |
| 6 | Взлом электронной почты | | |
| 7 | Политика информационной безопасности | | |
| 8 | Информационные войны | | |
| 9 | Психологические аспекты защиты информации | | |

**Содержание работы**

1. Создать свою рабочую папку в директории “Students”.

2. Открыть веб-браузер.

3. В поисковике указать тему из табл.1, указанную преподавателем.

4. Ознакомиться с информационными ресурсами, расположенными на веб-сайтах, в том числе, на англоязычных сайтах. Поиск информации производится по ключевым словам из выданного задания.

5. Для анализа необходимо просмотреть и сохранить в своей рабочей папке следующую информацию по каждому сайту:

- главную страницу веб-сайта;
- информацию об авторах сайта;
- информацию об организации, которую он представляет, ее реквизиты;
- страницы, содержащие перечень информационных ресурсов;
- полный текст одной из статей (с рисунками, если они есть) по своему выбору.

6. Составить отчет.

7. Подготовить краткое сообщение о веб-сайтах, посвященных данной тематике и доложить его студентам в порядке обмена информацией на заключительном занятии.

**Содержание отчета**

1. Наименование семинара, цель и задачи.

2. Информация по каждому сайту:

- адрес сайта в Интернете;
- название сайта;
- кто поддерживает сайт (имена авторов, названия организаций, проектов, в рамках которых создавался сайт и т.д.);
- аннотация назначения и содержания сайта (не более 10-20 предложений);
- иллюстрацию главной страницы сайта;
- перечень информационных ресурсов по тематике информационной безопасности;
- текст выбранной статьи.

В том случае, если на данном сайте отсутствуют статьи, а находятся только книги или программные продукты – привести оглавлении книги или краткое описание программного продукта.

3. Краткое обоснование своего выбора именно данного информационного ресурса (не более 5-10 предложений).

4. Свое мнение о данных сайтах (не более 5-10 предложений).

**Разработка плана отчета и презентации**

1. План отчета (и презентации) включает подготовку следующих разделов:

– введение (актуальность, вызовы практики, краткий анализ состояния вопроса – цель и основные тематического поиска, структура отчета и содержание, план поисковых работ);

– систематизированное изложение основных частей отчета;

– выводы (констатация достижения поставленной цели, практические результаты);

– список литературы;

– приложения.

2. Написание отчета. Отчет имеет объем 10-15 страниц формата А4 (шрифт 14, интервал полуторный, поля 2 см), включая титульный лист, содержание, основной текст, литература, приложения. Семинарские отчеты, подготовленные путем простой компиляции Интернет-материалов, без тщательного структурирования, с некорректной терминологией и без выводов не рассматриваются.

Обязательным приложением к отчету являются презентационные слайды и электронный вариант всех материалов.

3. Подготовка презентации. Презентация разрабатывается в PowerPoint и соответствует плану отчета (10-15 слайдов) исходя из времени на презентацию – 10 мин.

Презентация должна включать следующие слайды:

– титульный слайд (с указанием темы доклада, автора, даты презентации);

– содержание (структура) доклада;

– актуальность рассматриваемых вопросов, цель и задачи доклада исходя из этого анализа;

– слайды с раскрытием содержания поставленных задач;

– выводы по докладу;

– список использованных источников.

Каждый из слайдов должен содержать колонтитул с указанием темы и авторов доклада.

**Защита работы**

Защита работы осуществляется на семинаре, занимает 15 мин и включает собственно доклад с презентацией (10 мин) и обсуждение (5 мин).

**Оценка работы**

Оценка выполненной работы учитывает качество текста отчета (форма и содержание), презентации (содержание и дизайн), собственно доклад (структура, содержание и выводы), полноту, глубину и правильность ответов на вопросы.

Оценка за выполненную работу выставляется каждому студенту из группы авторов доклада индивидуально в соответствии с результатами и распределением ответственности.

## 2.2 Практический анализ ситуации нарушения информационной безопасности

**Цель:** В ходе семинара выполняется практическая проверка знаний, полученных студентами в ходе самостоятельного изучения международного стандарта ISO/IEC 17799. Также, студенты приобретают навыки по публичному докладу результатов анализа по тематике информационной безопасности.

### Подготовка к семинару

1) Самостоятельно изучить международный стандарт ISO/IEC 17799-2005 "Информационные технологии - Методы обеспечения безопасности – Практические правила управления информационной безопасностью".

2) Просмотр фрагмента художественного фильма «Хранители сети», заданный преподавателем.

3) Анализ ситуаций, показанных в фильме, с точки зрения нарушения требований стандарта ISO/IEC 17799 в письменном виде согласно предлагаемой форме (см. табл.1).

4) Подготовить отчет и доклад.

Таблица 1. Отчетная форма

| № | Краткое описание обнаруженного фрагмента фильма | Раздел стандарта ISO/IEC 17799 | Краткое описание нарушения требований стандарта | Примечания |
|---|---|---|---|---|
| **1** | | | | |
| | | | | |
| | | | | |

### Содержание отчета

1. Наименование семинара, цель и задачи.

2. Информация по каждой ситуации, показанной в фильме, с точки зрения нарушения требований стандарта.

3. Краткое обоснование своего выбора именно данной ситуации нарушения стандарта (не более 5-10 предложений).

4. Выводы по результатам анализа.

**Разработка плана отчета и презентации**

1. План отчета (и презентации) включает подготовку следующих разделов:

– введение (актуальность, вызовы практики, краткий анализ состояния вопроса – цель и основные тематического поиска, структура отчета и содержание, план поисковых работ);

– систематизированное изложение основных частей отчета;

– выводы (констатация достижения поставленной цели, практические результаты);

– приложения.

2. Написание отчета. Отчет имеет объем 10-15 страниц формата А4 (шрифт 14, интервал полуторный, поля 2 см), включая титульный лист, содержание, основной текст, литература, приложения. Семинарские отчеты, подготовленные путем простой компиляции, без тщательного структурирования, с некорректной терминологией и без выводов не рассматриваются.

Обязательным приложением к отчету являются презентационные слайды и электронный вариант всех материалов.

3. Подготовка презентации. Презентация разрабатывается в PowerPoint и соответствует плану отчета (10-15 слайдов) исходя из времени на презентацию – 10 мин.

Презентация должна включать следующие слайды:

– титульный слайд (с указанием темы доклада, автора, даты презентации);

– содержание (структура) доклада;

– актуальность рассматриваемых вопросов, цель и задачи доклада исходя из этого анализа;

– слайды с раскрытием содержания поставленных задач;

– выводы по докладу;

– список использованных источников.

Каждый из слайдов должен содержать колонтитул с указанием темы и авторов доклада.

**Защита работы**

Защита работы осуществляется на семинаре, занимает 15 мин и включает собственно доклад с презентацией (10 мин) и обсуждение (5 мин).

**Оценка работы**

Оценка выполненной работы учитывает качество текста отчета (форма и содержание), презентации (содержание и дизайн), собственно доклад (структура, содержание и выводы), полноту, глубину и правильность ответов на вопросы.

Оценка за выполненную работу выставляется каждому студенту из группы авторов доклада индивидуально в соответствии с результатами и распределением ответственности.

## 2.3 Механизмы резильентности при проектировании систем и сетей.

**Цель семинара**

Приобретение знаний и практических навыков по подготовке и презентации выполненного проекта (реферата, аналитического обзора) по вопросам современных и перспективных разработок в области создания механизмов резильентности.

**Подготовка к семинару**

***1. Получение (определение) темы работы***

Темы работ могут формироваться обучаемыми самостоятельно и согласовываться с руководителями исходя из ориентировочного перечня:

Дисциплины, составляющие резильентность

Инициатива ResiliNets (аксиомы, стратегия).

Принципы проектирования ResiliNets

Примеры структур, построенных на принципах ResiliNets

Оценки показателей резильентности систем.

Проект ResumeNet

Возможности использования методов искусственного интеллекта при проектировании механизмов резильентности систем.

***2. Разработка плана работ и распределение ответственности между участниками целевой группы.***

Целевая группа состоит из 3 человек. Примерный ресурс времени на подготовку 9 часов (+ 15 мин презентации).

Распределение ответственности определяют участники группы.

***3. Поиск информации по теме работы*** (библиотека, Интернет) и ее предварительный анализ.

Список рекомендуемой литературы приведен в данном практическом пособии и может быть дополнен индивидуально (по группам).

***4. Разработка плана отчета и презентации проекта.***

План отчета (и презентации) включает подготовку следующих разделов:

– введение (актуальность, вызовы практики, краткий анализ состояния вопроса – литературы, цель и основные задачи реферата, структура и характеристика содержания, план работ и распределение ответственности);

– систематизированное изложение основных частей реферата (классификационные схемы, характеристика моделей, методов, средств, технологий по группам, выбор показателей и критериев для оценки, сравнительный анализ);

– выводы (констатация достижения поставленной цели, основные теоретические и практические результаты, их значимость, направления дальнейших работ);

– список литературы;

– приложения.

***5. Написание отчета.*** Отчет имеет объем 15-20 страниц формата А4 (шрифт 14, интервал полуторный, поля 2 см), включая титульный лист, содержание, основной текст, литература, приложения. Рефераты, подготовленные путем простой компиляции Интернет-материалов, без тщательного структурирования, с некорректной терминологией и без выводов не рассматриваются.

Обязательным приложением к реферату является презентационные слайды и электронный вариант всех материалов.

***6. Подготовка презентации.*** Презентация разрабатывается в PowerPoint и соответствует плану реферата (10-15 слайдов) исходя из времени на презентацию – 10 мин.

Презентация должна включать следующие слайды:

– титульный слайд (с указанием темы доклада, автора, даты презентации);

– содержание (структура) доклада;

– актуальность рассматриваемых вопросов, цель и задачи доклада исходя из этого анализа;

– слайды с раскрытием содержания поставленных задач;

– выводы по докладу;

– список использованных источников.

Каждый из слайдов должен содержать колонтитул с указанием темы и авторов доклада.

Содержание слайдов не должно представлять собой части текста из отчета, а включать ключевые слова, рисунки, формулы.

Возможно представление реферата и презентации на английском языке, что повысит оценку за семинар.

**Защита работы**

Защита работы осуществляется на семинаре, занимает 15 мин и включает собственно доклад с презентацией (10 мин) и обсуждение (5

мин).

**Оценка работы**

Оценка выполненной работы учитывает качество текста отчета (форма и содержание), презентации (содержание и дизайн), собственно доклад (структура, содержание и выводы), полноту, глубину и правильность ответов на вопросы. Оценка за выполненную работу выставляется каждому обучаемому из группы авторов доклада индивидуально в соответствии с результатами и распределением ответственности.

# 3 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ

## 3.1 Пояснения к учебной программе

Самостоятельную работу над дисциплиной «Безопасность и резильентность сетей и систем» следует начинать с изучения учебной программы, которая приведена в Приложении А.

*Отчетность по дисциплине* включает отчеты по каждой из лабораторных работ и семинарам, а также экзамен, который включает типовые вопросы и задачи.

## 3.2 Подготовка к занятиям и экзамену

Подготовка к занятиям по дисциплине детально описана в разделе 2.

При подготовке к лабораторным работам следует обратить внимание на уяснение целей и задач (учебных или теоретических, практических и исследовательских) и знаний, которые нужны для их выполнения. При выполнении разработок и исследований необходимо строго руководствоваться описанием и попытаться найти ответы на вопросы, приведенные в конце каждой работы. Особое внимание следует уделить формулировке выводов по результатам исследований при оформлении отчета.

При подготовке к семинарам важно правильно спланировать свою работу в составе группы проекта, организовать отбор и анализ необходимой литературы, подготовку качественной презентации и подготовку к ответам на возможные вопросы.

Кроме того, следует обратить внимание на вопросы, вынесенные на самостоятельное изучение, которые приводятся в программе и уточняются преподавателем.

## ЛИТЕРАТУРА

## ДЛЯ ПОДГОТОВКИ К ЛАБОРАТОРНЫМ РАБОТАМ


1. Смит Ричард Э. Аутентификация: от паролей до открытых ключей [Текст] / Ричард Э. Смит – М.: Издательский дом «Вильямс», 2002. – 432 с.

2. Планирование защиты паролей [Электрон. ресурс] / Информационный центр IBM DB2 Content Manager Version 8.3 – 2006. – Режим доступа: http://publib.boulder.ibm.com/infocenter/cmgmt/v8r3m0/index.jsp?topic=%2Fcom.ibm.installingcm.doc%2Ficmpgmst39.htm.

3. Надежные пароли [Электрон. ресурс] / Библиотека Microsoft TechNet – 2011. – Режим доступа: http://technet.microsoft.com/ru-ru/library/cc756109(WS.10).aspx.

4. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Электрон. ресурс] / A. Рукхин и др. // NIST Special Publication 800-22 Revision 1a. – 2010. – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

5. Lamport L. Password Authentication with Insecure Communication [Текст] / Leslie Lamport // Communications of the ACM. – 1981. – №11. – С.770-772.

6. Haller N. The S/KEY One-Time Password System [Электрон. ресурс] / N. Haller // RFC 1760, Bellcore. – 1995. – Режим доступа: http://tools.ietf.org/html/rfc1760.

7. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие [Текст] / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.

8. Блэк, У. Интернет: протоколы безопасности. Учебный курс [Текст] / У. Блэк. – СПб.: Питер, 2001. – 288 с.

9. Пидодня, А. Пошаговое руководство по использованию протокола IPSec (Internet Protocol Security) [Электрон. ресурс] / А. Пидодня // OSZone. – 2000. – 17 фев. – Режим доступа: http://www.oszone.net/4158/IPSec.

10. Уваров, А.С. Настраиваем VPN сервер. Часть 4 – PPTP. Платформа Windows. [Электрон. ресурс] / А.С. Уваров // Записки IT специалиста. Технический блог специалистов ООО «Интерфейс». – 2011. – 12 апр. – Режим доступа: http://interface31.ru/tech_it/2011/04/nastraivaem-vpn-server-chast-4-pptp-platforma-windows.html .

11. Уваров, А.С. Настраиваем VPN сервер. Часть 5 – L2TP. Платформа Windows. [Электрон. ресурс] / А.С. Уваров // Записки IT специалиста. Технический блог специалистов ООО «Интерфейс». – 2013. – 4 янв. – Режим доступа: http://interface31.ru/tech_it/2013/01/nastraivaem-vpn-server-chast-5-l2tp-windows.html .

12. Томас Шиндлер, Работа с Windows Server 2008 R2 – установка и создание тестового контроллера домена (часть 1) [Электрон. ресурс] / Томас Шиндлер // OSZone. – 2009. – 27 окт. – Режим доступа: http://www.oszone.net/10457/Windows-Server-2008-R2 .

13. Буланов, Д. Создание учетных записей пользователей в Active Directory [Электрон. ресурс] / Д. Буланов // OSZone. – 2010. – 25 сент. – Режим доступа: http://www.oszone.net/13334/createuser .

14. Протокол SSL. Часть 1 [Электрон. ресурс] // Криптография и защита информации. – 2012. – 29 дек. – Режим доступа: http://mcrypt.ru/protokoly/protokol-ssl-chast-1.html .

15. Протокол SSL. Часть 2 [Электрон. ресурс] // Криптография и защита информации. – 2012. – 29 дек. – Режим доступа: http://mcrypt.ru/protokoly/protokol-ssl-chast-2.html .

16. Уваров, А.С. Windows Server. Создание автономного центра сертификации [Электрон. ресурс] / А.С. Уваров // Записки IT специалиста. Технический блог специалистов ООО «Интерфейс». – 2010. – 19 нояб. – Режим доступа: http://interface31.ru/tech_it/2010/11/windows-server-sozdanie-avtonomnogo-centra-sertifikacii.html .

17. Уваров, А.С. Windows Server. Настраиваем веб-сервер IIS [Электрон. ресурс] / А.С. Уваров // Записки IT специалиста. Технический блог специалистов ООО «Интерфейс». – 2012. – 31 мая – Режим доступа: http://interface31.ru/tech_it/2012/05/windows-server-nastraivaem-veb-server-iis.html.

## ДЛЯ ПОДГОТОВКИ К СЕМИНАРСКИМ ЗАНЯТИЯМ

18. Международный стандарт ISO/IEC 17799-2005 "Информационные технологии - Методы обеспечения безопасности – Практические правила управления информационной безопасностью".

19. A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *Transactions on Dependable and Secure Computing.* 2004, vol 1 (1), pp. 11–33.

20. A. Avizienis, J.-C. Laprie, B. Randell, et al. *Basic concepts and taxonomy of dependable and secure computing, Technical Research Report TR 2004-47.* Institute for Systems Research, the University of Maryland. 2004.

21. *Autonomic Network Architecture Wiki.* 2006. Available at:

http://www.ana- project.org/

22. B. Bhattacharjee, K. Calvert, J. Griffioen, ed al. *Postmodern Internetwork Architecture, Technical Report ITTC- FY2006-TR-45030-01*. Information and Telecommunication Center, 2335 Irving Hill Road, Lawrence, KS 66045-7612. 2006.

23. C. Doerr, J. M. Hernandez, R. Holz, ed al. *Mieghem. Defining metrics for resilient networking (Final). ResumeNet Project Deliverable.* September 2011.

24. C. Landwehr. Computer security. *International Journal of Information Security*. 2001, vol. 1 (1), pp. 3–13.

25. E. Jen. Robust Design: A Repertoire of Biological, Ecological, and Engineering Case Studies. *Oxford University Press.* 2005.

26. F. Foukalas, V. Gazis, N. Alonistioti. Cross-layer design proposals for wireless mobile networks: a survey and taxonomy. *IEEE Communications Surveys Tutorials*. 2008, vol. 10 (1) pp. 70–85. DOI:10.1109/COMST.2008.4483671. ISSN: 1553-877X.

27. *IRIS: Infrastructure for Resilient Internet Systems*. Available at:https://pdos.csail.mit.edu/archive/iris/

28. J. F. Meyer. Model-based evaluation of system resilience. In: *43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*. 2013, pp. 1-7. DOI: 10.1109/DSNW.2013.6615535.

29. J. Meyer. Performability: a retrospective and some pointers to the future. *Performance Evaluation.* 1992, vol. 14 (3–4), pp. 139–156.

30. J. P. G. Sterbenz et al. Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines. *Elsevier Computer Networks, Special Issue on Resilient and Survivable Networks.* 2010, vol.54, no. 8, pp. 1243–1304.

31. J.C. Knight & E.A. Strunk & K.J. Sullivan. Towards a rigorous definition of information system survivability. In: *Proceedings of the DARPA Information Survivability Conference and Exposition DISCEX III.* Washington DC. 2003, pp. 78–89.

32. J.-C. Laprie. Dependability: basic concepts and terminology, Draft. *IFIP Working Group 10.4 – Dependable Computing and Fault Tolerance.* 1994.

33. J.-C. Laprie. From dependability to resilience. In: *Proc. IEEE Int. Conf. on Dependable Systems and Networks.* 2008, vol. Supplemental, pp. G8–G9.

34. J.P.G. Sterbenz, D. Hutchison. ResiliNets: Multilevel Resilient and Survivable Networking Initiative Wiki. 2008. Available at: http://wiki.ittc.ku.edu/resilinets

35. J.P.G. Sterbenz, J.D. Touch. *High-Speed Networking: A Systematic Approach to High-Bandwidth Low-Latency Communication, first ed*. Wiley. 2001.

36. James P.G. Sterbenz and David Hutchison. *ResiliNets: Multilevel Resilient and Survivable Networking Initiative*. Available at: http://www.ittc.ku.edu/resilinets/

37. James P.G. Sterbenz, David Hutchison, Egemen Çetinkaya, et al. Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines. *Computer Networks: Special Issue on Resilient and Survivable Networks (COMNET)*. June 2010, vol.54, iss.8., pp.1245–1265.

38. M. Schöller, J.P.G. Sterbenz, A. Jabbar, D. Hutchison. *First draft of the Resilience and Security Framework.* 2006. Available at: http://www.ana-project.org/deliverables/2006/D.3.2.-Resilience.pdf

39. M. Schöller, P. Smith, C. Rohner, ed at. On realising a strategy for resilience in opportunistic networks. In: *Proceedings of the EU Future Network and Mobile Summit.* Florence, Italy, in press.

40. Merriam-Webster. Dictionary. (2013). Available at: http://www.merriam- webster.com/

41. P. Smith, D. Hutchison, J. P.G. Sterbenz (KU), ed al. *Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation. Final strategy document for resilient Networking.* 2011. 61 p.

42. P.A. Lee, T. *Anderson. Fault Tolerance: Principles and Practice.* Springer-Verlag New York, Inc., Secaucus, NJ, USA. 1990. ISBN:0387820779.

43. Paul Smith, David Hutchison, James P. G. Sterbenz, ed al. Network Resilience: A Systematic Approach. *IEEE Communications Magazine*. 2011, Vol. 49, Issue: 7, pp. 88 – 97. DOI: 10.1109/MCOM.2011.5936160.

44. R. Billinton, R. Allan. *Reliability Evaluation of Engineering Systems.* Plenum Press, New York, 1992.

45. *ResumeNet Wiki.* 2009. Available at: http://www.resumenet.eu/project/index

46. T1A1.2 Working group. *Enhanced network survivability performance, Technical Report T1.TR.68-2001*. Alliance for Telecommunications Industry Solutions (ATIS), 2001.

# АНОТАЦІЯ

УДК 004.056.5+681.324
Ж86

Безпека та резіл’єнтність систем і мереж. Практикум / І.В. Жуковицький, Д.А. Остапець, С.А. Розгонів, А.П. Заєць - За ред. Жуковицького І.В. – Харків: Національний аерокосмічний університет імені М.Є. Жуковського «ХАІ». - 2017. - 131 с.

The material practical part of the course System and Networks Security and Resilience, for undergraduates trained under the project TEMPUS-SEREIN Project Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (543968-TEMPUS-1-2013- 1-EE-TEMPUS-JPCP).

Курс присвячений вивченню сучасних підходів і технологій побудови безпечних і стійких систем і мереж, а також методів і засобів реалізації механізмів захисту систем і мереж.

Метою курсу є забезпечити оволодіння слухачем знаннями в галузі безпеки і стабільності систем і мереж. В результаті студент зможе: ефективно використовувати методи і засоби забезпечення безпеки і стабільності комп'ютерних систем і мереж; оцінити ступінь інформаційної безпеки комп'ютерних систем і мереж, ефективно взаємодіяти з колегами та клієнтами.

Практична частина курсу складається з восьми лабораторних робіт та трьох семінарських занять. Наводиться навчальна програма курсу, перелік запитань та літературних джерел для самостійного вивчення матеріалу курсу.

Для магістрантів університетів, які навчаються за напрямами комп'ютерних наук, комп'ютерної та програмної інженерії, кібербезпеки при вивченні методів і засобів забезпечення безпеки та стійкості комп’ютерних систем та мереж, а також для викладачів дисциплін за відповідними напрямами.

Бібл. – 46 найменувань, рисунків – 45, таблиць – 2

ЗМІСТ

ABSTRACT

UDC 004.056.5+681.324

System and Networks Security and Resilience. Practical workshop / I.V. Zhukovytskyy, D.A. Ostapets, S.A. Razgonov, A.P. Zaec – Ed. Zhukovytskyy I.V. – Kharkov: National Aerospace University named after N.E. Zhukovsky "Khai". – 2017. – xx pp.

The course is devoted to the study of modern approaches and technologies for building safe and resilienable systems and networks, as well as methods and means for implementing mechanisms to protect systems and networks.

Ensure mastery of the listener to the extent necessary knowledge in the field of security and resilience for systems and networks. As a result, the student will be able to: effective use of methods and techniques to ensure the security and resilience of computer systems and networks; assess the degree of information security of computer systems, networks, to communicate effectively with colleagues and clients.

The practical part of the course consists of eight laboratory work and three seminars. The workshop aims to develop students' skills of creating such software, the performance of which the level of electricity consumption is minimal computing device. The curriculum of the course, a list of questions and literary sources for self- study of the course material is given.

For university undergraduates and graduate students who study in areas of computer science, computer and software engineering, cybersecurity, when studying methods and tools to ensure the security and resilience of computer systems and networks, as well as for teachers in chosen disciplines.

Ref. – 46 items, figures – 45, tables – 2.

CONTENT

ПРИЛОЖЕНИЕ А. УЧЕБНАЯ ПРОГРАММА

**DESCRIPTION OF THE MODULE**

| TITLE OF THE MODULE | Code |
|---|---|
| **System and Networks Security and Resilience** | |

| Teacher(s) | Department |
|---|---|
| **Coordinating:** Prof. Zhukovytskyy Igor<br>**Others:** PhD, Associate Professor Ostapec Denis; PhD, Associate Professor Razgonov Sergey | Electronic computers |

| Study cycle | Level of the module | Type of the module |
|---|---|---|
| Master | A | Full-time tuition |

| Form of delivery | Duration | Langage(s) |
|---|---|---|
| Full-time tuition | One semester | English or Ukrain |

| Prerequisites | |
|---|---|
| **Prerequisites:**<br>Probability Theory and Foundations of Mathematic; Foundation of Modeling; Computer Networks; Information Technologies; Computer Systems; Cryptography. | **Co-requisites (if necessary):** |

| Credits of the module | Total student workload | Contact hours | Individual work hours |
|---|---|---|---|
| 4 | 108 | 54 | 54 |

| Aim of the module (course unit): competences foreseen by the study program |
|---|
| Ensure mastery of the listener to the extent necessary knowledge in the field of security and resiliense for systems and networks. As a result, the student will be able to: effective use of methods and techniques to ensure the security and resiliense of computer systems and networks; assess the degree of information security of computer systems, networks, to communicate effectively with colleagues and clients. |

| Learning outcomes of module (course unit) | Teaching/learning methods | Assessment methods |
|---|---|---|
| As a result, the student will receive:<br>1. Theoretical knowledge in the field of security and stability of computer systems and networks. | Interactive lectures,<br>Learning in laboratories,<br>Just-in-Time Teaching | Module Evaluation Questionnaire |
| 2. Practical skills in the use of methods and techniques to ensure the security and stability of computer systems and networks. | Interactive lectures,<br>Learning in laboratories,<br>Just-in-Time Teaching | Module Evaluation Questionnaire |
| 3. Knowledge of the mechanisms of protection services in the network Intrnet. | Interactive lectures,<br>Learning in laboratories,<br>Just-in-Time Teaching | Module Evaluation Questionnaire |
| 4. Knowledge of the international legal framework in the field of information security. | Interactive lectures,<br>Learning in laboratories,<br>Just-in-Time Teaching | Module Evaluation Questionnaire |

| Themes | Contact work hours | | | | | | | Time and tasks for individual work | |
|---|---|---|---|---|---|---|---|---|---|
| | Lectures | Consultations | Seminars | Practical work | Laboratory work | Placements | **Total contact work** | **Individual work** | **Tasks** |
| 1. Information and forms of its features.<br>1.1. General concepts of information and its features.<br>1.2. Limited access information and its properties (integrity, confidentiality, availability).<br>1.3. Forms of information and channels of distribution. | 1 | | | | | | | 2 | 1.4. The history of information security problems.<br>1.5. Information offenses.<br>1.6. Features of information warfare in the modern world. |
| 2. Threats to information security<br>2.1. The concept of automation system (AS) information processing.<br>2.2. Information Security AS.<br>2.3. Threats to information security and their classification in a number of basic features. | 1 | | | | | | | 2 | 2.4. Search for different classifications of information security threats on the Internet |
| 3. Normative and methodological support in protecting information in USA, EU countries, Canada and the Russian federation. | 2 | | 2 | | | | | 3 | 3.5. State Technical guidance documents of RUSSIAN |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3.1. Trusted Computer System Evaluation Criteria (Orange book).<br>3.2. Federal Criteria for Information Technology Security (FCITS).<br>3.3. Information Technology Security Evaluation Criteria (ITSEC)<br>3.4. Canadian security criteria (STSREC)<br>3.5. State Technical guidance documents of RUSSIAN FEDERATION on information protection.<br>3.6. Common Criteria for Information Technology Security Evaluation (ISO / IEC 15408: 1999) | | | | | | | | | FEDERATION on information protection.<br>3.6. Common Criteria for Information Technology Security Evaluation (ISO / IEC 15408: 1999) |
| 4. Regulatory guidance in the field technical information protection in Ukraine<br>4.1. State Service for Special Communication and Information Protection of Ukraine (State Service): history, tasks, rights and obligations.<br>4.2. General provisions for the protection of information in computer systems from unauthorized access.<br>4.3. Criteria for evaluating the security of information in computer systems from unauthorized access .<br>4.4. Classification of automated systems and standard functional profiles manufacturing security information from unauthorized access. | 2 | | 2 | | | | | 5 | 4.4. Classification of automated systems and standard functional profiles manufacturing security information from unauthorized access. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 5. Classification of methods and means of information protection. Services and mechanisms of information protection.<br>5.1. General terms and classification.<br>5.2. Hardware, technical, software, cryptographic, organizational methods and means of information protection.<br>5.3. Main services and mechanisms of information protection.<br>5.4. Threats of information in computer systems. Malware. | 2 | | | | | | | 4 | 5.5. The model of intruder.<br>5.6. Protection against malware. |
| 6. Identification and authentication.<br>6.1. Classification and general characteristics of authentication factors.<br>6.2. Biometrical methods. Biometrical systems. The accuracy of biometrics.<br>6.3. Authentication devices. Active and passive devices.<br>6.4. One-time passwords (OTP). OTP generation devices.<br>6.5. Password protection by using "request - response" method. ANSI/ISO standards.<br>6.5. The attacks on authentication systems. The average space of attack. The passwords strength | 2 | | | | 6 | | | 4 | 6.6. Requirements to reusable passwords. |
| 7. Typical models of authenti- | 2 | | | | | | | 2 | 7.5. The |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| cation.<br>7.1. Local authentication model.<br>7.2. Direct authentication model.<br>7.3. Indirect authentication model.<br>7.4. Autonomous authentication model. | | | | | | | | | principles of use of authentication models. |
| 8. Access control mechanisms.<br>8.1. In access dispatcher. The functional requirements and the requirements of architecture guarantee.<br>8.2. Discretionary access control. Matrix of access. ACLs.<br>8.3. Mandated access control. Security label.<br>8.4. Role based access control. | 2 | | | | | | | 3 | 8.5. The use of access control methods in modern operating systems. |
| 9. General network security issues<br>9.1. Common security issues of TCP/IP networks<br>9.2. Classification of remote attacks on computer network.<br>9.3. An overview of some typical network attacks.<br>9.4. Characteristics and mechanism of implementation of standard remote attacks:<br>9.3.1. Network traffic analysis,<br>9.3.2. The substitution of the trusted object or subject of the distributed operating system,<br>9.3.3. The distributed operat- | 2 | | | | | | | 4 | 9.3.4. Denial of service. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ing system to a false | | | | | | | | | |
| 10. Mechanisms for the implementation of some network attacks<br>10.1. Sniffing.<br>10.1.1. Passive sniffing through the hub.<br>10.1.2. Active sniffing through the switch.<br>10.2. Protection against listening.<br>10.3. Port scanning. Types of scanning.<br>10.4. Protection from scanning. | 2 | | | | 2 | | | 3 | 10.5. Using remote search algorithm shortcomings. False ARP-server. |
| 11. Using Firewall systems of protection for networks.<br>11.1. Structure and Functioning Firewall.<br>11.2. Principles work Firewall.<br>11.3.1. Firewall to filter traffic kachestve.<br>11.3.2. Firewall as the intermediary.<br>11.4. Basic scheme of protection on the basis of Firewall:<br>11.4.1. Firewall - router with filtering packets,<br>11.4.2. Firewall screening on the basis of transport;<br>11.4.3. Firewall on the basis of the applied gate | 2 | | | | 2 | | | 3 | 11.5. Features of gateway shielding at various levels of model OSI |
| 12 Using IDS and IPS of protection for networks.<br>12.1 An Intrusion Detection System (IDS)<br>12.2 An Intrusion Prevention System (IPS) | 2 | | | | | | | 4 | 12.3 New approaches to detection |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 13. Creation of the protected virtual networks at the network layer.<br>13.1. Architecture of IPsec.<br>13.2. Concept of association of safety of IPSec. IPSec modes.<br>13.3. Protocol of authentication of AH (Authentication Header). Header fields in transport and tunnel modes<br>13.4. Protocol of enciphering (Encapsulation Security Payload). Header fields in transport and tunnel modes. | 2 | | | | 2 | | | 4 | 13.5. Management of the protected tunnel. SAD (Security Associated Database) and SPD (Security Policy Database) databases. |
| 14. Creation of the protected virtual networks at the session layer<br>14.1. The SSL protocol - family of protocols.<br>14.2. Purpose of SSL. Architecture of SSL.<br>14.3. Concept of a session of SSL, SSL connection.<br>14.4. Record SSL protocol. General scheme of work of the protocol of the record SSL. Record SSL format.<br>14.5. Protocol of change of parameters of enciphering.<br>14.6. Message protocol. | 2 | | | | 2 | | | 4 | 14.7. Handshake protocol. Scheme of work of the protocol of a handshake. Creation of keys of enciphering of SSL.<br>14.8 OpenVPN protocol |
| 15. Creation of the protected virtual networks at the data link layer<br>15.1. The PPTP protocol<br>15.2. The L2TP protocol | 2 | | | | 2 | | | 2 | |
| 16. resilience mechanisms of systems and networks.<br>16.1 General concepts of resilience | 4 | | 2 | | | | | 5 | 16.5 Resilience metrics framework |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 16.2 Resilience disciplines<br>16.2.1 Challenge tolerance<br>16.2.2 Disciplines relating to trustworthiness<br>16.2.3 Robustness and complexity<br>16.3 ResiliNets framework and strategy<br>16.3.1 Scope and Definition<br>16.3.2 ResiliNets axioms<br>16.3.3 ResiliNets strategy<br>16.3.4 ResiliNets design principles<br>16.4 Framework for resilience<br>16.4.1 The approach to the formation of the framework for resilience structure<br>16.4.2 Resilience control loop | | | | | | | | | 16.6 Understanding challenges and risks<br>16.7 Defense and dynamic adaptation architecture |
| **Iš viso** | **32** | | **6** | | **16** | | | **54** | |

| **Assessment strategy** | **Weight in %** | **Deadlines** | **Assessment criteria** |
|---|---|---|---|
| Lecture activity, including fulfilling special self-tasks | 10 | 7,14 | 85% – 100% Outstanding work, showing a full grasp of all the questions answered.<br>70% – 84% Perfect or near perfect answers to a high proportion of the questions answered. There should be a thorough understanding and appreciation of the material.<br>60% – 69% A very good knowledge of much of the important material, possibly excellent in places, but with a limited account of some significant topics.<br>50% – 59% There should be a good grasp of several important topics, but |

| | | | |
|---|---|---|---|
| | | | with only a limited understanding or ability in places. There may be significant omissions.<br>45% – 49% Students will show some relevant knowledge of some of the issues involved, but with a good grasp of only a minority of the material. Some topics may be answered well, but others will be either omitted or incorrect.<br>40% – 44% There should be some work of some merit. There may be a few topics answered partly or there may be scattered or perfunctory knowledge across a larger range.<br>20% – 39% There should be substantial deficiencies, or no answers, across large parts of the topics set, but with a little relevant and correct material in places.<br>0% – 19% Very little or nothing that is correct and relevant. |
| Learning in laboratories | 30 | 7,14 | 85% – 100% An outstanding piece of work, superbly organised and presented, excellent achievement of the objectives, evidence of original thought.<br>70% – 84% Students will show a thorough understanding and appreciation of the material, producing work without significant error or omission. Objectives achieved well. Excellent organisation and presentation.<br>60% – 69% Students will show a clear understanding of the issues involved and the work should be well written and well organised. Good work towards the objectives.<br>The exercise should show evidence that the student has thought about the topic and has not simply reproduced standard solutions or arguments.<br>50% – 59% The work should show evi- |

| | | | |
|---|---|---|---|
| | | | dence that the student has a reasonable understanding of the basic material. There may be some signs of weakness, but overall the grasp of the topic should be sound. The presentation and organisation should be reasonably clear, and the objectives should at least be partially achieved.<br>45% – 49% Students will show some appreciation of the issues involved. The exercise will indicate a basic understanding of the topic, but will not have gone beyond this, and there may well be signs of confusion about more complex material. There should be fair work towards the laboratory work objectives.<br>40% – 44% There should be some work towards the laboratory work objectives, but significant issues are likely to be neglected, and there will be little or no appreciation of the complexity of the problem.<br>20% – 39% The work may contain some correct and relevant material, but most issues are neglected or are covered incorrectly. There should be some signs of appreciation of the laboratory work requirements.<br>0% – 19% Very little or nothing that is correct and relevant and no real appreciation of the laboratory work requirements. |
| Module Evaluation Quest | 60 | 8,16 | The score corresponds to the percentage of correct answers to the test questions |

| Author | Year of issue | Title | No of periodical or volume | Place of printing. Printing house or intrenet link |
|---|---|---|---|---|
| **Compulsory literature** | | | | |
| | | | | |
| Bill Ballad, Tricia Ballad, Erin K. Banks | 2011 | Access Control, Authentication, And Public Key Infrastructure | | Jones & Bartlett Learning LLC |
| John E. Canavan | 2001 | Fundamentals of Network Security | | http://www.sciencel-ib.net/files/Fundamen-tals%20of%20Network%20Security%20-%20J.%20Canavan%20(Artech%20House,%202001)%20WW.pdf |
| William R. Cheswick and Steven M. Bellovin | 2006 | Firewalls and Internet Security | | http://www.onlineprogram-mingbooks.com/firewalls-and-internet-securi-ty/#sthash.tLhVJjly.dpuf |
| Michael S Collins | 2014 | Network Security Through Data Analysis: Building Situational Awareness Paperback | | http://www.amazon.co.uk/Network-Security-Through-Data-Analy-sis/dp/1449357903/ref=sr_1_1/276-9205023-2672722?ie=UTF8&qid=141068 |

| | | | | |
|---|---|---|---|---|
| | | | | 9889&sr=8-1&keywords=books+on+network+security |
| Ali Ismail Awad Aboul Ella Hassanien Kensuke Baba (Eds.) | 2013 | Advances in Security of Information and Communication Networks | | |
| Christos Kalloniatis | 2012 | Security Enhanced Applications for Information Systems | | |
| Chris McNab | 2007 | Network Security Assessment, 2nd Edition | | http://it-ebooks.info/read/262/ |
| Netkachov, A., Popov, P. T. & Salako, K. | 2014 | Model-based Evaluation of the Resilience of Critical Infrastructures under Cyber Attacks. | | Paper presented at the 9th International Conference on Critical Information Infrastructures Security (CRITIS 2014), 13-10-2014 - 15-10-2014, Limassol, Cyprus. |
| Thomas R Peltier | 2013 | Information Security Fundamentals- Second Edition | | |
| Omar Santos | | End-to-End Network Security. Defense-in-Depth | | http://it-ebooks.info/read/2255/ |

| | | | | |
|---|---|---|---|---|
| M. Schöller, J.P.G. Sterbenz, A. Jabbar, D. Hutchison. | 2006 | First draft of the Resilience and Security Framework | | http://www.ana-pro-ject.org/deliverables/2006/D.3.2.-Resilience.pdf |
| Richard E. Smith | 2002 | Authentication: From Passwords to Public Keys | | Addison-Wesley |
| William Stallings | 2013 | Cryptography and Network Security: Principles and Practice Paperback | | http://faculty.mu.edu.sa/public/uploads/1360993259.0858Cryptography%20and%20Network%20Security%20Principles%20and%20Practice,%205th%20Edition.pdf |
| J. P. G. Sterbenz et al. | 2010 | Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines. | Elsevier Computer Networks, Special Issue on Resilient and Survivable Networks. 2010, vol.54, no. 8, pp. 1243–1304. | |

| | | | | |
|---|---|---|---|---|
| M. Teichmann | 2013 | Human Factors Engineering | | Tallinn University of Technology, Estonia http://www.tpi.ee/digiope/hfe/ |
| Dobromir Todorov | 2007 | Mechanics of User Identification and Authentication: Fundamentals of Identity Management | | Auerbach Publications Taylor & Francis Group |
| Harold F. Tipton | 2012 | Information Security Management Handbook | | |
| | | | | |
| **Additional literature** | | | | |
| | | | | |
| | 1999 | НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в компю'терних системах від несанкціонованого доступу. | | |
| | 1999 | НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. | | |
| | 1999 | НД ТЗІ 2.5- | | |

| | | | | |
|---|---|---|---|---|
| | | 005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу | | |
| Haller N. | 1995 | The S/KEY One-Time Password System. RFC 1760, Bellcore | | http://tools.ietf.org/html/rfc1760 |
| | 2011 | Надежные пароли. Библиотека Microsoft TechNet | | http://technet.microsoft.com/ru/library/cc756109(WS.10).aspx |
| | 2006 | Планирование защиты паролей. Информационный центр IBM DB2 Content Manager Version 8.3 | | http://publib.boulder.ibm.com/infocenter/cmgmt/v8r3m0/index.jsp?topic=%2Fcom.ibm.installingcm.doc%2Ficmpgmst39.htm |

СОДЕРЖАНИЕ