

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра управления в технических системах

УТВЕРЖДАЮ:

Проректор по учебной работе
Е.И. Луковникова

мая 2020 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ

ФТД.В.02

НАПРАВЛЕНИЕ ПОДГОТОВКИ

27.03.04 Управление в технических системах

ПРОФИЛЬ ПОДГОТОВКИ

Управление и информатика в технических системах

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 27.03.04 Управление в технических системах от 20.10.2015 г № 1171 и учебным планом ФГБОУ ВО «БрГУ» от 03.02.2020 г № 46 для очной формы обучения, заочно - ускоренной формы обучения для набора 2020 года

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	3
3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ	4
3.1 Распределение объёма дисциплины по формам обучения.....	4
3.2 Распределение объёма дисциплины по видам учебных занятий и трудоемкости	4
4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	5
4.1 Распределение разделов дисциплины по видам учебных занятий	5
4.2 Содержание дисциплины, структурированное по разделам и темам	11
4.3 Лабораторные работы.....	64
4.4 Практические занятия.....	64
4.5. Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат	64
5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	65
6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ	66
7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	66
8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО – ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ	66
9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ.....	67
9.1. Методические указания для обучающихся по выполнению лабораторных работ/ практических работ	67
10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	76
11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	77
Приложение 1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	78
Приложение 2. Аннотация рабочей программы дисциплины	83
Приложение 3. Протокол о дополнениях и изменениях в рабочей программе	84
Приложение 4. Фонд оценочных средств для текущего контроля успеваемости по дисциплине.....	84

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Вид деятельности выпускника

Дисциплина охватывает круг вопросов, относящихся к научно-исследовательскому виду профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Формирование у обучаемых знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и системах связи.

Задачи дисциплины

Заложить методически правильные основы знаний, необходимые будущим специалистам по инфокоммуникационным технологиям и системам связи в области информационной безопасности.

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ПК-2	Способность проводить вычислительные эксперименты с использованием стандартных программных средств с целью получения математических моделей процессов и объектов автоматизации и управления	знать: - Основные термины, используемые в научно-технической литературе по информационной безопасности. уметь: - формулировать основные технические требования к телекоммуникационным сетям и систем. владеть: - Основными требованиями информационной безопасности.
ОПК-9	Способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности	знать: - основы цифровой вычислительной техники, структуры и функционирование локальных вычислительных сетей и глобальной сети Интернет, основные закономерности передачи информации в инфокоммуникационных системах, основные виды сигналов, используемых в телекоммуникационных системах, особенности передачи различных сигналов по каналам и тракам телекоммуникационных систем; уметь: - оценивать основные проблемы, связанные с эксплуатацией и внедрением новой вычислительной техники; владеть: - начальными навыками разработки и отладки с использованием соответствующих отладочных средств программного обеспечения сигнальных процессов и микроконтроллеров.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина ФТД.В.2 Основы информационной безопасности сетей и систем относится к факультативным дисциплинам

Дисциплина основы информационной безопасности сетей и систем базируется на знаниях, полученных при изучении дисциплин Б1.Б.12 Информационные технологии, Б1.В.ОД.7 Информатика.

Основываясь на изучении перечисленных дисциплин, основы информационной безопасности сетей и систем представляет основу для Б1.В.ОД.16 Системы управления базами данных.

Такое системное междисциплинарное изучение направлено на достижение требуемого ФГОС уровня подготовки по квалификации бакалавр.

3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ

3.1. Распределение объема дисциплины по формам обучения

Форма обучения	Курс	Семестр	Трудоемкость дисциплины в часах						Контрольная работа	Вид промежуточной аттестации
			Всего часов (с экз.)	Аудиторных часов	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа		
1	2	3	4	5	6	7	8	9	10	11
Очная	3	5	108	51	17	17	17	57	-	зачет
Заочная	3	-	108	10	4	4	2	98	-	зачет
Заочная (ускоренное обучение)	1	-	108	6	2	2	2	102	-	зачет
Очно-заочная	-	-	-	-	-	-	-	-	-	-

3.2. Распределение объема дисциплины по видам учебных занятий и трудоемкости

Вид учебных занятий	Трудоемкость (час.)	в т.ч. в интерактивной, активной, инновационной формах, (час.)	Распределение по семестрам, час
			5
1	2	3	4
I. Контактная работа обучающихся с преподавателем (всего)	51	6	51
Лекции (Лк)	17	2	17
Лабораторные работы (ЛР)	17	2	17
Практические работы (ПР)	17	2	17
Индивидуальные (групповые) консультации	+	-	+
II. Самостоятельная работа обучающихся (СР)	57	-	57

Подготовка к лабораторным работам	19	-	19
Подготовка к практическим работам	19		19
Подготовка к зачету в течение семестра	19	-	19
III. Промежуточная аттестация зачет	+	-	+
Общая трудоемкость дисциплины час. зач. ед.	108	-	108
	3	-	3

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий - для очной формы обучения:

№ раз- дела и темы	Наименование раздела и тема дисциплины	Трудоем- кость, (час.)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)			
			учебные занятия			самостоя тельная работа обучаю- щихся
			лекции	лабораторные работы	практиче ские работы	
1	2	3	4	5	6	7
1.	Введение в информационную безопасность.	11	5	-	-	6
1.1.	Понятие информационной безопасности	1,5	1	-	-	0,5
1.2.	Основные составляющие информационной безопасности	1,5	1	-	-	0,5
1.3.	Важность и сложность проблемы информационной безопасности	1	0,5	-	-	0,5
1.4.	Основные определения и критерии классификации угроз	1	0,5	-	-	0,5
1.5.	Некоторые примеры угроз доступности	1,5	0,5	-	-	1
1.6.	Вредоносное программное обеспечение	1,5	0,5	-	-	1
1.7.	Основные угрозы целостности	1,5	0,5	-	-	1
1.8.	Основные угрозы конфиденциальности	1,5	0,5	-	-	1
2.	Уровни информационной безопасности.	11	5	-	-	6
2.1.	Законодательный уровень информационной безопасности	0,84	0,5	-	-	0,34
2.2.	Обзор российского законодательства в области информационной безопасности	0,83	0,5	-	-	0,33

2.3.	Обзор зарубежного законодательства в области информационной безопасности	0,83	0,5	-	-	0,33
2.4.	Административный уровень информационной безопасности	1	0,5	-	-	0,5
2.5.	Политика безопасности	1	0,5	-	-	0,5
2.6.	Программа безопасности	1	0,5	-	-	0,5
2.7.	Синхронизация программы безопасности с жизненным циклом систем	1	0,5	-	-	0,5
2.8.	Процедурный уровень информационной безопасности	0,84	0,34	-	-	0,5
2.9.	Управление персоналом	0,83	0,33	-	-	0,5
2.10.	Физическая защита	0,83	0,33	-	-	0,5
2.11.	Поддержание работоспособности	0,83	0,33	-	-	0,5
2.12.	Реагирование на нарушения режима безопасности	0,83	0,33	-	-	0,5
2.13.	Планирование восстановительных работ	0,84	0,34	-	-	0,5
3.	Основные программно-технические меры информационной безопасности сетей и систем	86	7	17	17	45
3.1.	Основные понятия программно-технического уровня информационной безопасности	2,5	0,5	-	-	2
3.2.	Особенности современных информационных систем, существенные с точки зрения безопасности	2,5	0,5	-	-	2
3.3.	Архитектурная безопасность	2,5	0,5	-	-	2
3.4.	Идентификация и аутентификация	7,5	0,5	2	2	3
3.5.	Управление доступом	8,5	0,5	2	3	3
3.6.	Протоколирование и аудит	8,5	0,5	2	3	3
3.7.	Активный аудит	8,5	0,5	2	3	3
3.8.	Шифрование	8,5	0,5	2	3	3
3.9.	Контроль целостности	8,5	0,5	2	3	3
3.10.	Экранирование	5,5	0,5	2	-	3
3.11.	Анализ защищенности	5,33	0,33	2	-	3
3.12.	Обеспечение высокой доступности	5,33	0,33	2	-	3
3.13.	Основы мер обеспечения высокой доступности	4,33	0,33	1	-	3

3.14.	Отказоустойчивость и зона риска	2,33	0,33	-	-	3
3.15.	Программное обеспечение промежуточного слоя	3,34	0,34	-	-	3
3.16.	Обеспечение обслуживаемости	3,34	0,34	-	-	3
	ИТОГО	108	17	17	17	57

- для заочной формы обучения:

№ раздела и темы	Наименование раздела и тема дисциплины	Трудоемкость, (час.)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)			
			учебные занятия			самостоятельная работа обучающихся
			лекции	лабораторные работы	практические работы	
1	2	3	4	5	6	7
1.	Введение в информационную безопасность.	31	1	-	-	30
1.1.	Понятие информационной безопасности	3,33	0,33	-	-	3
1.2.	Основные составляющие информационной безопасности	3,33	0,33	-	-	3
1.3.	Важность и сложность проблемы информационной безопасности	4,34	0,34	-	-	4
1.4.	Основные определения и критерии классификации угроз	4	-	-	-	4
1.5.	Некоторые примеры угроз доступности	4	-	-	-	4
1.6.	Вредоносное программное обеспечение	4	-	-	-	4
1.7.	Основные угрозы целостности	4	-	-	-	4
1.8.	Основные угрозы конфиденциальности	4	-	-	-	4
2.	Уровни информационной безопасности.	31	1	-	-	30
2.1.	Законодательный уровень информационной безопасности	2,33	0,33	-	-	2
2.2.	Обзор российского законодательства в области информационной безопасности	2,33	0,33	-	-	2
2.3.	Обзор зарубежного законодательства в области информационной безопасности	2,34	0,34	-	-	2
2.4.	Административный	2	-	-	-	2

	уровень информационной безопасности					
2.5.	Политика безопасности	2	-	-	-	2
2.6.	Программа безопасности	2	-	-	-	2
2.7.	Синхронизация программы безопасности с жизненным циклом систем	2	-	-	-	2
2.8.	Процедурный уровень информационной безопасности	2	-	-	-	2
2.9.	Управление персоналом	2	-	-	-	2
2.10.	Физическая защита	3	-	-	-	3
2.11.	Поддержание работоспособности	3	-	-	-	3
2.12.	Реагирование на нарушения режима безопасности	3	-	-	-	3
2.13.	Планирование восстановительных работ	3	-	-	-	3
3.	Основные программно-технические меры информационной безопасности сетей и систем	42	2	4	2	34
3.1.	Основные понятия программно-технического уровня информационной безопасности	2,33	0,33	-	-	2
3.2.	Особенности современных информационных систем, существенные с точки зрения безопасности	2,33	0,33	-	-	2
3.3.	Архитектурная безопасность	2,34	0,34	-	-	2
3.4.	Идентификация и аутентификация	5,33	0,33	1	1	3
3.5.	Управление доступом	5,33	0,33	1	1	3
3.6.	Протоколирование и аудит	3,34	0,34	1	-	2
3.7.	Активный аудит	3	-	1	-	2
3.8.	Шифрование	2	-	-	-	2
3.9.	Контроль целостности	2	-	-	-	2
3.10.	Экранирование	2	-	-	-	2
3.11.	Анализ защищенности	2	-	-	-	2
3.12.	Обеспечение высокой доступности	2	-	-	-	2
3.13.	Основы мер обеспечения высокой доступности	2	-	-	-	2
3.14.	Отказоустойчивость и зона риска	2	-	-	-	2
3.15.	Программное обеспечение промежуточного слоя	2	-	-	-	2
3.16.	Обеспечение	2	-	-	-	2

	обслуживаемости					
	ИТОГО	104	4	4	2	94

- для заочной формы обучения (ускоренное обучение):

№ раздела и темы	Наименование раздела и тема дисциплины	Трудоемкость, (час.)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)			
			учебные занятия			самостоятельная работа обучающихся
			лекции	лабораторные работы	практические работы	
1	2	3	4	5	6	7
1.	Введение в информационную безопасность.	33	1	-	-	32
1.1.	Понятие информационной безопасности	4,33	0,33	-	-	4
1.2.	Основные составляющие информационной безопасности	4,33	0,33	-	-	4
1.3.	Важность и сложность проблемы информационной безопасности	4,34	0,34	-	-	4
1.4.	Основные определения и критерии классификации угроз	4	-	-	-	4
1.5.	Некоторые примеры угроз доступности	4	-	-	-	4
1.6.	Вредоносное программное обеспечение	4	-	-	-	4
1.7.	Основные угрозы целостности	4	-	-	-	4
1.8.	Основные угрозы конфиденциальности	4	-	-	-	4
2.	Уровни информационной безопасности.	33	1	-	-	32
2.1.	Законодательный уровень информационной безопасности	2,33	0,33	-	-	2
2.2.	Обзор российского законодательства в области информационной безопасности	2,33	0,33	-	-	2
2.3.	Обзор зарубежного законодательства в области информационной безопасности	2,34	0,34	-	-	2
2.4.	Административный уровень информационной безопасности	2	-	-	-	2
2.5.	Политика безопасности	2	-	-	-	2

2.6.	Программа безопасности	2	-	-	-	2
2.7.	Синхронизация программы безопасности с жизненным циклом систем	2	-	-	-	2
2.8.	Процедурный уровень информационной безопасности	3	-	-	-	3
2.9.	Управление персоналом	3	-	-	-	3
2.10.	Физическая защита	3	-	-	-	3
2.11.	Поддержание работоспособности	3	-	-	-	3
2.12.	Реагирование на нарушения режима безопасности	3	-	-	-	3
2.13.	Планирование восстановительных работ	3	-	-	-	3
3.	Основные программно-технические меры информационной безопасности сетей и систем	38	-	2	2	34
3.1.	Основные понятия программно-технического уровня информационной безопасности	2	-	-	-	2
3.2.	Особенности современных информационных систем, существенные с точки зрения безопасности	1	-	-	-	1
3.3.	Архитектурная безопасность	1	-	-	-	1
3.4.	Идентификация и аутентификация	3	-	1	1	1
3.5.	Управление доступом	3	-	1	1	1
3.6.	Протоколирование и аудит	2	-	-	-	2
3.7.	Активный аудит	2	-	-	-	2
3.8.	Шифрование	2	-	-	-	2
3.9.	Контроль целостности	2	-	-	-	2
3.10.	Экранирование	2	-	-	-	2
3.11.	Анализ защищенности	2	-	-	-	2
3.12.	Обеспечение высокой доступности	2	-	-	-	2
3.13.	Основы мер обеспечения высокой доступности	2	-	-	-	2
3.14.	Отказоустойчивость и зона риска	2	-	-	-	2
3.15.	Программное обеспечение промежуточного слоя	2	-	-	-	2
3.16.	Обеспечение обслуживаемости	2	-	-	-	2
	ИТОГО	104	2	2	2	98

4.2. Содержание дисциплины, структурированное по разделам и темам

РАЗДЕЛ №1: ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ.

1.1. Понятие информационной безопасности

Словосочетание "информационная безопасность" в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин "информационная безопасность" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе РФ "Об участии в международном информационном обмене" информационная безопасность определяется аналогичным образом - как состояние защищенности информационной среды общества, обеспечивающее деформирование, использование и развитие в интересах граждан, организаций, государства.

В данном курсе наше внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, на каком языке (русском или каком-либо ином), она закодирована, кто или что является ее источником, и какое психологическое воздействие она оказывает на людей. Поэтому термин "информационная безопасность" будет использоваться в узком смысле, так, как это принято, например, в англоязычной литературе.

Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. (Чуть дальше мы поясним, что следует понимать под поддерживающей инфраструктурой.)

Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности. Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности - это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

- Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации учебные институты. В первом случае "пусть лучше все сломается, чем враг узнает хоть один секретный бит", во втором - "да нет у нас никаких секретов, лишь бы все работало".
- Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Возвращаясь к вопросам терминологии, отметим, что термин "компьютерная безопасность" (как эквивалент или заменитель ИБ) представляется нам слишком узким. Компьютеры - только одна из составляющих информационных систем, и хотя наше внимание будет сосредоточено в первую очередь на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на "горчичнике", прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций. Обратим внимание, что в определении ИБ перед существительным "ущерб" стоит прилагательное "неприемлемый". Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

1.2. Основные составляющие информационной безопасности

Информационная безопасность - многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Иногда в число основных составляющих ИБ включают защиту от несанкционированного копирования информации, но, на наш взгляд, это слишком специфический аспект с сомнительными шансами на успех, поэтому мы не станем его выделять.

Поясним понятия доступности, целостности и конфиденциальности

Доступность - это возможность за приемлемое время получить требуемую информационную услугу. Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Наконец, конфиденциальность - это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если потом или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления - производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия - и материальные, имморальные - может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит "руководством к действию". Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса - все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации. Конфиденциальность - самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, набути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, то реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность, - какой смысл в информационной услуге, если она содержит искаженные сведения?

Наконец, конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

1.3. Важность и сложность проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю - национальном, отраслевом, корпоративном или персональном.

Для иллюстрации этого положения ограничимся несколькими примерами.

В Доктрине информационной безопасности Российской Федерации (здесь, подчеркнем, термин "информационная безопасность" используется в широком смысле) защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере.

По распоряжению президента США Клинтона (от 15 июля 1996 года, номер 13010) была создана Комиссия по защите критически важной инфраструктуры, как от физических нападений, так и от атак, предпринятых с помощью информационного оружия. В начале октября 1997 года при подготовке доклада президенту глава вышеупомянутой комиссии Роберт Марш заявил, что в настоящее время ни правительство, ни частный сектор не располагают средствами защиты от компьютерных атак, способных вывести из строя коммуникационные сети и сети энергоснабжения.

Американский ракетный крейсер "Йорктаун" был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (Government Computer News, июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения с целью снижения стоимости военной техники. Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, AP, 17 сентября 1996 года).

Как сообщил журнал Internet Week от 23 марта 1998 года, потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности. Согласно результатам совместного исследования Института информационной безопасности и ФБР, в 1997 году ущерб от компьютерных преступлений достиг 136 миллионов долларов, что на 36% больше, чем в 1996 году. Каждое компьютерное преступление наносит ущерб примерно в 200 тысяч долларов.

В середине июля 1996 года корпорация General Motors отозвала 292860 автомобилей марки Pontiac, Oldsmobile и Buick моделей 1996 и 1997 годов, поскольку ошибка в программном обеспечении двигателя могла привести к пожару. В феврале 2001 года двое бывших сотрудников компании Commerce One, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом.

Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.

Понятно, что подобных примеров множество, можно вспомнить и другие случаи - недостатка в нарушениях ИБ нет и не предвидится. Много стоит одна только "Проблема 2000" - стыд и позор программистского сообщества! При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий - области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует быстрому развитию средств обеспечения ИБ. Следует исходить из того, что необходимо конструировать надежные системы (информационной безопасности) с привлечением ненадежных компонентов (программ). В принципе, это возможно, но требует соблюдения определенных архитектурных принципов и контроля состояния защищенности на всем протяжении жизненного цикла ИС.

Приведем еще несколько цифр. В марте 1999 года был опубликован очередной, четвертый по счету, годовой отчет «Компьютерная преступность и безопасность-1999: проблемы и тенденции» (Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey). В отчете отмечается резкий рост числа обращений в правоохранительные органы по поводу компьютерных преступлений (32% из числа опрошенных); 30% респондентов сообщили о том, что их информационные системы были взломаны внешними злоумышленниками; атакам через Internet подвергались 57% опрошенных; в 55% случаях отмечались нарушения со стороны собственных сотрудников. Примечательно, что 33% респондентов на вопрос "были ли взломаны ваши Web-серверы и системы электронной коммерции за последние 12 месяцев?" ответили "не знаю".

В аналогичном отчете, опубликованном в апреле 2002 года, цифры изменились, но тенденция осталась прежней: 90% респондентов (преимущественно из крупных компаний и правительственных структур) сообщили, что за последние 12 месяцев в их организациях имели место нарушения информационной безопасности; 80% констатировали финансовые потери от этих нарушений; 44% (223 респондента) смогли и/или захотели оценить потери количественно, общая сумма составила более 455 млн. долларов. Наибольший ущерб нанесли кражи и подлоги (более 170 и 115 млн. Долларов соответственно).

Столь же тревожные результаты содержатся в обзоре InformationWeek, опубликованном 12 июля 1999 года. Лишь 22% респондентов заявили об отсутствии нарушений информационной безопасности. Наряду с распространением вирусов отмечается резкий рост числа внешних атак.

Увеличение числа атак - еще не самая большая неприятность. Хуже то, что постоянно обнаруживаются новые уязвимые места в программном обеспечении (выше мы указывали на ограниченность современной технологии программирования) и, как следствие, появляются новые виды атак.

Так, в информационном письме Национального центра защиты инфраструктуры США (National Infrastructure Protection Center, NIPC) от 21 июля 1999 года сообщается, что за период с 3 по 16 июля 1999 года выявлено девять проблем с ПО, риск использования которых оценивается как средний или высокий (общее число обнаруженных уязвимых мест равно 17). Среди "пострадавших" операционных платформ - почти все разновидности ОС Unix, Windows, MacOS, так что никто не может чувствовать себя спокойно, поскольку новые ошибки тут же начинают активно использоваться злоумышленниками.

В таких условиях системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание уязвимых мест ведется медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение всех составляющих ИБ - доступности, целостности или конфиденциальности

1.4. Основные определения и критерии классификации угроз

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, - злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

- должно стать известно о средствах использования пробела в защите;
- должны быть выпущены соответствующие заплатки;
- заплатки должны быть установлены в защищаемой ИС.

Мы уже указывали, что новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат - как можно более оперативно.

Отметим, что некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания. Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы. Иметь представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Слишком много мифов существует в сфере информационных технологий (вспомним все ту же "Проблему 2000"), поэтому незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

Подчеркнем, что само понятие "угроза" в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнута открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Мы попытаемся взглянуть на предмет с точки зрения типичной (на наш взгляд) организации. Впрочем, многие угрозы (например, пожар) опасны для всех.

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).
- В качестве основного критерия мы будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные.
- Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь - следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками - максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.)

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при (пере)конфигурировании системы;

- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые "обиженные" сотрудники - нынешние и бывшие. Как правило, они стремятся нанести вред организации-"обидчику", например:

- испортить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия, - пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных "злоумышленников" (среди которых самый опасный - перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

1.5. Некоторые примеры угроз доступности

Угрозы доступности могут выглядеть грубо - как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего - грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования - не редкость.

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно сгенерировать и искусственным образом - с помощью так называемых высокоэнергетических радиочастотных пушек.

Но, наверное, в наших условиях подобную угрозу следует все же признать надуманной. Действительно опасны протечки водопровода и отопительной системы. Часто организации, чтобы сэкономить на арендной плате, снимают помещения в домах старой постройки, делают косметический ремонт, но не меняют ветхие трубы. Автору курса довелось быть свидетелем ситуации, когда прорвало трубу с горячей водой, и системный блок компьютера (это была рабочая станция производства Sun Microsystems) оказался заполнен кипятком. Когда кипяток вылили, а компьютер просушили, он возобновил нормальную работу, но лучше таких опытов не ставить...

Летом, в сильную жару, норовят сломаться кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием. В результате значительный ущерб наносится и репутации, и кошельку организации.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранят небрежно (к этому мы еще вернемся при обсуждении угроз конфиденциальности), не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Перейдем теперь к угрозам доступности, которые будут похитрее засоров канализации. Речь пойдет о программных атаках на доступность.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно - полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника угрозы такое потребление подразделяется на локальное и удаленное. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов - атака, получившая наименование "SYN-наводнение". Она представляет собой попытку переполнить таблицу "полуоткрытых" TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая атака по меньшей мере затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

По отношению к атаке "Papa Smurf" уязвимы сети, воспринимающие ping-пакеты с широкоэвещательными адресами. Ответы на такие пакеты "съедают" полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме - как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание. Временем начала "моды" на подобные атаки можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее - владельцы и пользователи систем). Отметим, что если имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных атак на доступность крайне трудно.

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentium I дает возможность локальному пользователю путем выполнения определенной команды "подвесить" компьютер, так что помогает только аппаратный RESET.

Программа "Teardrop" удаленно "подвешивает" компьютеры, эксплуатируя ошибку в сборке фрагментированных IP- пакетов.

1.6. Вредоносное программное обеспечение

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Мы выделим следующие грани вредоносного ПО:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Часть, осуществляющую разрушительную функцию, будем называть "бомбой" (хотя, возможно, более удачными терминами были бы "заряд" или "боеголовка"). Вообще говоря, спектр вредоносных функций неограничен, поскольку "бомба", как и любая другая программа, может обладать сколь угодно сложной логикой, но обычно "бомбы" предназначаются для:

- внедрения другого вредоносного ПО;
- получения контроля над атакуемой системой;
- агрессивного потребления ресурсов;
- изменения или разрушения программ и/или данных.

По механизму распространения различают:

- вирусы - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- "черви" - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. "Черви", напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, "черви" "съедают" полосу пропускания сети и ресурсы почтовых систем. По этой причине для атак на доступность они не нуждаются во встраивании специальных "бомб".

Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Отметим, что данные нами определения и приведенная классификация вредоносного ПО отличаются от общепринятых. Например, в ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения" содержится следующее определение:

"Программный вирус - это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах".

На наш взгляд, подобное определение неудачно, поскольку в нем смешаны функциональные и транспортные аспекты. Окно опасности для вредоносного ПО появляется с выпуском новой разновидности "бомб", вирусов и/или "червей" и перестает существовать с обновлением базы данных антивирусных программ и наложением других необходимых заплат.

По традиции из всего вредоносного ПО наибольшее внимание общественности приходится на долю вирусов. Однако до марта 1999 года с полным правом можно было утверждать, что "несмотря на экспоненциальный рост числа известных вирусов, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. Соблюдение несложных правил "компьютерной гигиены" практически сводит риск заражения к нулю. Там, где работают, а не играют, число зараженных компьютеров составляет лишь доли процента".

В марте 1999 года, с появлением вируса "Melissa", ситуация кардинальным образом изменилась. "Melissa" - это макровирус для файлов MS-Word, распространяющийся посредством электронной почты в присоединенных файлах. Когда такой (зараженный) присоединенный файл открывают, он рассылает свои копии по первым 50 адресам из адресной книги Microsoft Outlook. В результате почтовые серверы подвергаются атаке на доступность.

В данном случае нам хотелось бы отметить два момента.

- Как уже говорилось, пассивные объекты отходят в прошлое; так называемое активное содержимое становится нормой. Файлы, которые по всем признакам должны были бы относиться к данным (например, документы в форматах MS-Word или Postscript, тексты почтовых сообщений), способны содержать интерпретируемые компоненты, которые могут запускаться неявным образом при открытии файла. Как и всякое в целом прогрессивное явление, такое "повышение активности данных" имеет свою обратную сторону (в рассматриваемом случае - отставание в разработке механизмов безопасности и ошибки в их реализации).

Обычные пользователи еще не скоро научатся применять интерпретируемые компоненты "в мирных целях" (или хотя бы узнают об их существовании), а перед злоумышленниками открылось по существу неограниченное поле деятельности. Как ни банально это звучит, но если для стрельбы по воробьям выкатывается пушка, то пострадает в основном стреляющий.

• Интеграция разных сервисов, наличие среди них сетевых, всеобщая связность многократно увеличивают потенциал для атак на доступность, облегчают распространение вредоносного ПО (вирус "Melissa" - классический тому пример). Образно говоря, многие информационные системы, если не принять защитных мер, оказываются "в одной лодке" (точнее - в корабле без переборок), так что достаточно одной пробоины, чтобы "лодка" тут же пошла ко дну.

Как это часто бывает, вслед за "Melissa" появилась на свет целая серия вирусов, "червей" и их комбинаций: "Explorer.zip" (июнь 1999), "Bubble Boy" (ноябрь 1999), "ILOVEYOU" (май 2000) и т.д. Не то что бы от них был особенно большой ущерб, но общественный резонанс они вызвали немалый.

Активное содержимое, помимо интерпретируемых компонентов документов и других файлов данных, имеет еще одно популярное обличье - так называемые мобильные агенты. Это программы, которые загружаются на другие компьютеры и там выполняются. Наиболее известные примеры мобильных агентов - Java-апплеты, загружаемые на пользовательский компьютер и интерпретируемые Internet-навигаторами. Оказалось, что разработать для них модель безопасности, оставляющую достаточно возможностей для полезных действий, не так-то просто; еще сложнее реализовать такую модель без ошибок. В августе 1999 года стали известны недочеты в реализации технологий ActiveX и Java в рамках Microsoft Internet Explorer, которые давали возможность размещать на Web-серверах вредоносные апплеты, позволяющие получать полный контроль над системой-визитером.

Для внедрения "бомб" часто используются ошибки типа "переполнение буфера", когда программа, работая с областью памяти, выходит за границы допустимого и записывает в нужные злоумышленнику места определенные данные. Так действовал еще в 1988 году знаменитый "червь Морриса"; в июне 1999 года хакеры нашли способ использовать аналогичный метод по отношению к Microsoft Internet Information Server (IIS), чтобы получить контроль над Web-сервером. Окно опасности охватило сразу около полутора миллионов серверных систем... Не забыты современными злоумышленниками и испытанные троянские программы. Например, "троянцы" Back Orifice и Netbus позволяют получить контроль над пользовательскими системами с различными вариантами MSWindows.

Таким образом, действие вредоносного ПО может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности.

1.7. Основные угрозы целостности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. Можно предположить, что реальный ущерб был намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты; не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Ранее мы проводили различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

Иногда изменяются содержательные данные, иногда - служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее начальником президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что в указанное время он разговаривал по мобильному телефону, находясь вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние "файл против файла". Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарша знала пароль вице-президента, поскольку ей было поручено его менять), и иск был отвергнут...

(Теоретически возможно, что оба фигурировавших на суде файла были подлинными, корректными с точки зрения целостности, а письмо отправили пакетными средствами, однако, на наш взгляд, это было бы очень странное для вице-президента действие.)

Из приведенного случая можно сделать вывод не только об угрозах нарушения целостности, но и об опасности слепого доверия компьютерной информации. Заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль отправителя (мы приводили соответствующие примеры). Отметим, что последнее возможно даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов информационной безопасности: если нарушена конфиденциальность, может пострадать целостность.

Еще один урок: угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить "неотказуемость", компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение рассмотренного выше вредоносного ПО - пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

1.8. Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многозначные пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности - частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую - и не может быть обеспечена) необходимая защита. Угроза же состоит в том, что кто-то не откажется узнать секреты, которые сами просятся в руки. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна - осуществить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Весьма опасной угрозой являются... выставки, на которые многие организации, не долго думая, отправляют оборудование из производственной сети, со всеми хранящимися на них данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде. Это плохо даже в пределах защищенной сети организации; в объединенной сети выставки - это слишком суровое испытание честности всех участников.

Еще один пример изменения, о котором часто забывают, - хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Перехват данных - очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют. Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие как маскарад - выполнение действий под видом лица, обладающего полномочиями для доступа к данным (см., например, статью Айрэ Винклера "Задание: шпионаж" в Jet Info, 1996, 19).

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример - нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Таковы основные угрозы, которые наносят наибольший ущерб субъектам информационных отношений.

РАЗДЕЛ №2: УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

2.1. Законодательный уровень информационной безопасности

В деле обеспечения информационной безопасности успех может принести только комплексный подход. Мы уже указывали, что для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Мы будем различать на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их мерами ограничительной направленности);
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но нам хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Самое важное (и, вероятно, самое трудное) на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

2.2. Обзор российского законодательства в области информационной безопасности

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 - право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

В Гражданском кодексе Российской Федерации (в своем изложении мы опираемся на редакцию от 15 мая 2001 года) фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Весьма продвинутом в плане информационной безопасности является Уголовный кодекс Российской Федерации (редакция от 14 марта 2002 года). Глава 28 - "Преступления в сфере компьютерной информации" - содержит три статьи:

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Первая имеет дело с посягательствами на конфиденциальность, вторая - с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе "О государственной тайне" (с изменениями и дополнениями от 6 октября 1997 года). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения.

Закон "Об информации, информатизации и защите информации"

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В нем даются основные определения и намечаются направления развития законодательства в данной области.

Процитируем некоторые из этих определений: •

информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

- документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- информационные процессы - процессы сбора, обработки, накопления, хранения, поиска и распространения информации;
- информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;
- информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
- конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;
- пользователь (потребитель) информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Мы, разумеется, не будем обсуждать качество данных в Законе определений. Обратим лишь внимание на гибкость определения конфиденциальной информации, которая не сводится к сведениям, составляющим государственную тайну, а также на понятие персональных данных, закладывающее основу защиты последних.

Закон выделяет следующие цели защиты информации:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Отметим, что Закон на первое место ставит сохранение конфиденциальности информации. Целостность представлена также достаточно полно, хотя и на втором месте. О доступности ("предотвращение несанкционированных действий по ... блокированию информации") сказано довольно мало.

Продолжим цитирование:

"Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу".

По сути, это положение констатирует, что защита информации направлена на обеспечение интересов субъектов информационных отношений.

Далее. "Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";
- в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;

- в отношении персональных данных - федеральным законом."

Здесь явно выделены три вида защищаемой информации, ко второму из которых принадлежит, в частности, коммерческая информация. Поскольку защите подлежит только документированная информация, необходимым условием является фиксация коммерческой информации на материальном носителе и снабжение ее реквизитами. Отметим, что в данном месте Закона речь идет только о конфиденциальности; остальные аспекты ИБ забыты.

Обратим внимание, что защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники.

Как же защищать информацию? В качестве основного закон предлагает для этой цели мощные универсальные средства: лицензирование и сертификацию. Прочитируем статью 19.

Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".

Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.

Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

Здесь трудно удержаться от риторического вопроса: а есть ли в России информационные системы без импортной продукции? Получается, что на защите интересов потребителей стоит в данном случае только таможня...

И еще несколько пунктов, теперь из статьи 22:

Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

Из пункта 5 следует, что должны обнаруживаться все (успешные) атаки на ИС. Вспомним в этой связи один из результатов опроса (см. лекцию 1): около трети респондентов-американцев не знали, были ли взломаны их ИС за последние 12 месяцев. По нашему законодательству их можно было бы привлечь к ответственности...

Далее, статья 23 "Защита прав субъектов в сфере информационных процессов и информатизации" содержит следующий пункт:

Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба. Очень важными являются пункты статьи 5, касающиеся юридической силы электронного документа и электронной цифровой подписи:

Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Таким образом, Закон предлагает действенное средство контроля целостности и решения проблемы "неотказуемости" (невозможности отказаться от собственной подписи).

Таковы важнейшие, на наш взгляд, положения Закона "Об информации, информатизации и защите информации". На следующей странице будут рассмотрены другие законы РФ в области информационной безопасности.

Другие законы и нормативные акты

Следуя логике Закона "Об информации, информатизации и защите информации", мы продолжим наш обзор Законом "О лицензировании отдельных видов деятельности" от 8 августа 2001 года номер 128-ФЗ (Принят Государственной Думой 13 июля 2001 года). Начнем с основных определений.

- "Лицензия - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю
- Лицензируемый вид деятельности - вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.
- Лицензирование - мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением и возобновлением действия лицензий, аннулированием лицензий и контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.
- Лицензирующие органы - федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом.
- Лицензиат - юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности."

Статья 17 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Нас будут интересовать следующие виды:

- распространение шифровальных (криптографических) средств;
- техническое обслуживание шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;
- выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и (или) производство средств защиты конфиденциальной информации;
- техническая защита конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

- деятельность, связанная с защитой государственной тайны;
- деятельность в области связи;
- образовательная деятельность.

Подчеркнем в этой связи, что данный Закон не препятствует организации Интернет-Университетом учебных курсов по информационной безопасности (не требует получения специальной лицензии; ранее подобная лицензия была необходима). В свою очередь, Федеральный Закон "Об образовании" не содержит каких-либо специальных положений, касающихся образовательной деятельности в области ИБ.

Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации (ФАПСИ) и Гостехкомиссия России. ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. Эти же организации возглавляют работы по сертификации средств соответствующей направленности. Кроме того, ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ. Все эти вопросы регламентированы соответствующими указами Президента и постановлениями Правительства РФ, которые мы здесь перечислять не будем.

В эпоху глобальных коммуникаций важную роль играет Закон "Об участии в международном информационном обмене" от 4 июля 1996 года номер 85-ФЗ (принят Государственной Думой 5 июня 1996 года). В нем, как и в Законе "Об информации...", основным защитным средством являются лицензии и сертификаты. Протицируем несколько пунктов из статьи 9.

Защита конфиденциальной информации государством распространяется только на ту деятельность по международному информационному обмену, которую осуществляют физические и юридические лица, обладающие лицензией на работу с конфиденциальной информацией и использующие сертифицированные средства международного информационного обмена.

Выдача сертификатов и лицензий возлагается на Комитет при Президенте Российской Федерации по политике информатизации, Государственную техническую комиссию при Президенте Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации. Порядок выдачи сертификатов и лицензий устанавливается Правительством Российской Федерации

При обнаружении нештатных режимов функционирования средств международного информационного обмена, то есть возникновения ошибочных команд, а также команд, вызванных несанкционированными действиями обслуживающего персонала или иных лиц, либо ложной информацией собственник или владелец

этих средств должен своевременно сообщить об этом в органы контроля за осуществлением международного информационного обмена и собственнику или владельцу взаимодействующих средств международного информационного обмена, в противном случае он несет ответственность за причиненный ущерб.

При желании здесь можно усмотреть обязательность выявления нарушителя информационной безопасности - положение, вне всяких сомнений, очень важное и прогрессивное. Еще одна цитата - теперь из статьи 17 того же Закона.

Статья 17: "Сертификация информационных продуктов, информационных услуг, средств международного информационного обмена.

При ввозе информационных продуктов, информационных услуг в Российскую Федерацию импортер представляет сертификат, гарантирующий соответствие данных продуктов и услуг требованиям договора. В случае невозможности сертификации ввозимых на территорию Российской Федерации информационных продуктов, информационных услуг ответственность за использование данных продуктов и услуг лежит на импортере.

Средства международного информационного обмена, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих средств подлежат обязательной сертификации.

Сертификация сетей связи производится в порядке, определяемом Федеральным законом "О связи".

" Читая пункт 2, трудно удержаться от вопроса: "А нужно ли сертифицировать средства защиты средств защиты этих средств?" Ответ, конечно, положительный...

10 января 2002 года Президентом был подписан очень важный закон "Об электронной цифровой подписи" номер 1-ФЗ (принят Государственной Думой 13 декабря 2001 года), развивающий и конкретизирующий приведенные выше положения закона "Об информации...". Его роль поясняется в статье 1.

Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Закон вводит следующие основные понятия:

- Электронный документ - документ, в котором информация представлена в электронно-цифровой форме.
- Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.
- Владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).
- Средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.
- Сертификат средств электронной цифровой подписи - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.
- Закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
- Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе
- Сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Информационная система общего пользования - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Корпоративная информационная система - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Пересказать такие определения своими словами невозможно... Обратим внимание на неоднозначное использование термина "сертификат", которое, впрочем, не должно привести к путанице. Кроме того, данное здесь определение электронного документа слабее, чем в Законе "Об информации...", поскольку нет упоминания реквизитов.

Согласно Закону, электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
 - подтверждена подлинность электронной цифровой подписи в электронном документе;
 - электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.
- Закон определяет сведения, которые должен содержать сертификат ключа подписи:
 - уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
 - фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима запись об этом вносится удостоверяющим центром в сертификат ключа подписи;
 - открытый ключ электронной цифровой подписи;
 - наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
 - наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
 - сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Интересно, много ли Федеральных законов, содержащих такое количество технической информации и столь зависимых от конкретной технологии?

На этом мы заканчиваем обзор законов РФ, относящихся к информационной безопасности.

2.3. Обзор зарубежного законодательства в области информационной безопасности

Конечно, излишняя амбициозность заголовка очевидна. Разумеется, мы лишь пунктиром очертим некоторые законы нескольких стран (в первую очередь - США), поскольку только в США таких законодательных актов около 500.

Ключевую роль играет американский "Закон об информационной безопасности" (Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988). Его цель - реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

Характерно, что уже в начале Закона называется конкретный исполнитель - Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и подлогов, выполняемых с помощью компьютеров. Таким образом, имеется в виду как регламентация действий специалистов, так и повышение информированности всего общества.

Согласно Закону, все операторы федеральных ИС, содержащих конфиденциальную информацию, должны сформировать планы обеспечения ИБ. Обязательным является и периодическое обучение всего персонала таких ИС. НИСТ, в свою очередь, обязан проводить исследования природы и масштаба уязвимых мест, вырабатывать экономически оправданные меры защиты. Результаты исследований рассчитаны на применение не только в государственных системах, но и в частном секторе.

Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерство обороны, Министерство энергетики, Агентство национальной безопасности (АНБ) и т.д., чтобы избежать дублирования и несовместимости

Помимо регламентации дополнительных функций НИСТ, Закон предписывает создать при Министерстве торговли комиссию по информационной безопасности, которая должна:

- выявлять перспективные управленческие, технические, административные и физические меры, способствующие повышению ИБ;
- выдавать рекомендации Национальному институту стандартов и технологий, доводить их до сведения всех заинтересованных ведомств.

С практической точки зрения важен раздел 6 Закона, обязывающий все правительственные ведомства сформировать план обеспечения информационной безопасности, направленный на то, чтобы компенсировать

риски и предотвратить возможный ущерб от утери, неправильного использования, несанкционированного доступа или модификации информации в федеральных системах. Копии плана направляются в НИСТ и АНБ.

В 1997 году появилось продолжение описанного закона - законопроект "О совершенствовании информационной безопасности" (Computer Security Enhancement Act of 1997, H.R. 1903), направленный на усиление роли Национального института стандартов и технологий и упрощение операций с криптосредствами.

В законопроекте констатируется, что частный сектор готов предоставить криптосредства для обеспечения конфиденциальности и целостности (в том числе аутентичности) данных, что разработка и использование шифровальных технологий должны происходить на основании требований рынка, а не распоряжений правительства. Кроме того, здесь отмечается, что за пределами США имеются сопоставимые и общедоступные криптографические технологии, и это следует учитывать при выработке экспортных ограничений, чтобы не снижать конкурентоспособность американских производителей аппаратного и программного обеспечения.

Для защиты федеральных ИС рекомендуется более широко применять технологические решения, основанные на разработках частного сектора. Кроме того, предлагается оценить возможности общедоступных зарубежных разработок.

Очень важен раздел 3, в котором от НИСТ требуется по запросам частного сектора готовить добровольные стандарты, руководства, средства и методы для инфраструктуры открытых ключей (см. выше Закон РФ об ЭЦП), позволяющие сформировать негосударственную инфраструктуру, пригодную для взаимодействия с федеральными ИС.

В разделе 4 особое внимание обращается на необходимость анализа средств и методов оценки уязвимых мест других продуктов частного сектора в области ИБ.

Приветствуется разработка правил безопасности, нейтральных по отношению к конкретным техническим решениям, использование в федеральных ИС коммерческих продуктов, участие в реализации шифровальных технологий, позволяющее в конечном итоге сформировать инфраструктуру, которую можно рассматривать как резервную для федеральных ИС.

Важно, что в соответствии с разделами 10 и далее предусматривается выделение конкретных (и немалых) сумм, называются точные сроки реализации программ партнерства и проведения исследований инфраструктуры с открытыми ключами, национальной инфраструктуры цифровых подписей. В частности, предусматривается, что для удостоверяющих центров должны быть разработаны типовые правила и процедуры, порядок лицензирования, стандарты аудита.

В 2001 году был одобрен Палатой представителей и передан в Сенат новый вариант рассмотренного законопроекта - Computer Security Enhancement Act of 2001 (H.R. 1259 RFS). В этом варианте примечательно как то, что, по сравнению с предыдущей редакцией, было убрано, так и то, что добавилось.

За четыре года (1997-2001 гг.) на законодательном и других уровнях информационной безопасности США было сделано многое. Смягчены экспортные ограничения на криптосредства (в январе 2000 г.). Сформирована инфраструктура с открытыми ключами. Разработано большое число стандартов (например, новый стандарт электронной цифровой подписи - FIPS 186-2, январь 2000 г.). Все это позволило не заострять более внимания на криптографии как таковой, а сосредоточиться на одном из ее важнейших приложений - аутентификации, рассматривая ее по отработанной на криптосредствах методике. Очевидно, что, независимо от судьбы законопроекта, в США будет сформирована национальная инфраструктура электронной аутентификации. В данном случае законодательная деятельность идет в ногу с прогрессом информационных технологий.

Программа безопасности, предусматривающая экономически оправданные защитные меры и синхронизированная с жизненным циклом ИС, упоминается в законодательстве США неоднократно. Согласно пункту 3534 ("Обязанности федеральных ведомств") подглавы II ("Информационная безопасность") главы 35 ("Координация федеральной информационной политики") рубрики 44 ("Общественные издания и документы"), такая программа должна включать:

- периодическую оценку рисков с рассмотрением внутренних и внешних угроз целостности, конфиденциальности и доступности систем, а также данных, ассоциированных с критически важными операциями и ресурсами;
- правила и процедуры, позволяющие, опираясь на проведенный анализ рисков, экономически оправданным образом уменьшить риски до приемлемого уровня;
- обучение персонала с целью информирования о существующих рисках и об обязанностях, выполнение которых необходимо для их (рисков) нейтрализации;
- периодическую проверку и (пере)оценку эффективности правил и процедур;
- действия при внесении существенных изменений в систему; процедуры выявления нарушений информационной безопасности и реагирования на них; эти процедуры должны помочь уменьшить риски, избежать крупных потерь; организовать взаимодействие с правоохранительными органами.
- Конечно, в законодательстве США имеются в достаточном количестве и положения ограничительной направленности, и директивы, защищающие интересы таких ведомств, как Министерство обороны, АНБ, ФБР, ЦРУ, но мы не будем на них останавливаться. Желаящие могут прочитать раздел "Законодательная база в области защиты информации" в превосходной статье О. Беззубцева и А. Ковалева "О лицензировании и сертификации в области защиты информации" (Jet Info, 1997, 4).

В законодательстве ФРГ выделим весьма развернутый (44 раздела) Закон о защите данных (Federal Data Protection Act of December 20, 1990 (BGBl. I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)). Он целиком посвящен защите персональных данных.

Как, вероятно, и во всех других законах аналогичной направленности, в данном случае устанавливается приоритет интересов национальной безопасности над сохранением тайны частной жизни. В остальном права

личности защищены весьма тщательно. Например, если сотрудник фирмы обрабатывает персональные данные в интересах частных компаний, он дает подписку о неразглашении, которая действует и после перехода на другую работу.

Государственные учреждения, хранящие и обрабатывающие персональные данные, несут ответственность за нарушение тайны частной жизни "субъекта данных", как говорится в Законе. В материальном выражении ответственность ограничена верхним пределом в 250 тысяч немецких марок.

Из законодательства Великобритании упомянем семейство так называемых добровольных стандартов BS 7799, помогающих организациям на практике сформировать программы безопасности. В последующих лекциях мы еще вернемся к рассмотрению этих стандартов; здесь же отметим, что они действительно работают, несмотря на "добровольность" (или благодаря ей?).

В современном мире глобальных сетей законодательная база должна быть согласована с международной практикой. В этом плане поучителен пример Аргентины. В конце марта 1996 года компетентными органами Аргентины был арестован Хулио Цезар Ардита, 21 года, житель Буэнос-Айреса, системный оператор электронной доски объявлений "Крик", известный в компьютерном подполье под псевдонимом "El Griton". Ему вменялись в вину систематические вторжения в компьютерные системы ВМС США, НАСА, многих крупнейших американских университетов, а также в компьютерные системы Бразилии, Чили, Кореи, Мексики и Тайваня. Однако, несмотря на тесное сотрудничество компетентных органов Аргентины и США, Ардита был отпущен без официального предъявления обвинений, поскольку по аргентинскому законодательству вторжение в компьютерные системы не считается преступлением. Кроме того, в силу принципа "двойной криминальности", действующего в международных правовых отношениях, Аргентина не может выдать хакера американским властям. Дело Ардита показывает, каким может быть будущее международных компьютерных вторжений при отсутствии всеобщих или хотя бы двусторонних соглашений о борьбе с компьютерной преступностью. О текущем состоянии российского законодательства в области информационной безопасности

Как уже отмечалось, самое важное (и, вероятно, самое трудное) на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Пока такого механизма нет и, увы, не предвидится. Сейчас бессмысленно задаваться вопросом, чего не хватает российскому законодательству в области ИБ, это все равно что интересоваться у пунктирного отрезка, чего тому не хватает, чтобы покрыть всю плоскость. Даже чисто количественное сопоставление с законодательством США показывает, что наша законодательная база явно неполна.

Справедливости ради необходимо отметить, что ограничительная составляющая в российском законодательстве представлена существенно лучше, чем координирующая и направляющая. Глава 28 Уголовного кодекса достаточно полно охватывает основные аспекты информационной безопасности, однако обеспечить реализацию соответствующих статей пока еще сложно.

Положения базового Закона "Об информации, информатизации и защите информации" носят весьма общий характер, а основное содержание статей, посвященных информационной безопасности, сводится к необходимости использовать исключительно сертифицированные средства, что, в общем, правильно, но далеко не достаточно. Характерно, что Закон разъясняет вопросы ответственности в случае использования несертифицированных средств, но что делать, если нарушение ИБ произошло в системе, построенной строго по правилам? Кто возместит ущерб субъектам информационных отношений? Поучителен в этом отношении рассмотренный выше закон ФРГ о защите данных.

Законодательством определены органы, ведающие лицензированием и сертификацией. (Отметим в этой связи, что Россия - одна из немногих стран (в список еще входят Вьетнам, Китай, Пакистан), сохранивших жесткий государственный контроль за производством и распространением внутри страны средств обеспечения ИБ, в особенности продуктов криптографических технологий.) Но кто координирует, финансирует и направляет проведение исследований в области ИБ, разработку отечественных средств защиты, адаптацию зарубежных продуктов? Законодательством США определена главная ответственная организация - НИСТ, которая исправно выполняет свою роль. В Великобритании имеются содержательные добровольные стандарты ИБ, помогающие организациям всех размеров и форм собственности. У нас пока ничего такого нет.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи очень важны Руководящие документы Гостехкомиссии России, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно выделим утвержденный в июле 1997 года Руководящий документ по межсетевым экранам, вводящий в официальную сферу один из самых современных классов защитных средств.

В современном мире глобальных сетей нормативно-правовая база должна быть согласована с международной практикой. Особое внимание следует обратить на то, что желательно привести российские стандарты и сертификационные нормативы в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности. Есть целый ряд оснований для того, чтобы это сделать. Одно из них - необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских компаний. Второе (более существенное) - доминирование аппаратно-программных продуктов зарубежного производства.

На законодательном уровне должен быть решен вопрос об отношении к таким изделиям. Здесь необходимо выделить два аспекта: независимость в области информационных технологий и информационную безопасность. Использование зарубежных продуктов в некоторых критически важных системах (в первую очередь, военных), в принципе, может представлять угрозу национальной безопасности (в том числе информационной), поскольку нельзя исключить вероятности встраивания закладных элементов. В то же время,

в подавляющем большинстве случаев потенциальные угрозы информационной безопасности носят исключительно внутренний характер. В таких условиях незаконность использования зарубежных разработок (ввиду сложностей с их сертификацией) при отсутствии отечественных аналогов затрудняет (или вообще делает невозможной) защиту информации без серьезных на то оснований.

Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно сложна, однако, как показывает опыт европейских стран, решить ее можно. Сложившаяся в Европе система сертификации по требованиям информационной безопасности позволила оценить операционные системы, системы управления базами данных и другие разработки американских компаний. Вхождение России в эту систему и участие российских специалистов в сертификационных испытаниях в состоянии снять имеющееся противоречие между независимостью в области информационных технологий и информационной безопасностью без какого-либо ущерба для национальной безопасности.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

разработка новых законов с учетом интересов всех категорий субъектов информационных отношений; обеспечение баланса созидательных и ограничительных (в первую очередь преследующих цель наказать виновных) законов;

интеграция в мировое правовое пространство;

учет современного состояния информационных технологий

2.4: Административный уровень информационной безопасности

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации.

Главная цель мер административного уровня - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Термин "политика безопасности" является не совсем точным переводом английского словосочетания "security policy", однако в данном случае калька лучше отражает смысл этого понятия, чем лингвистически более верные "правила безопасности". Мы будем иметь в виду не отдельные правила или их наборы (такого рода решения выносятся на процедурный уровень, речь о котором впереди), а стратегию организации в области информационной безопасности. Для выработки стратегии и проведения ее в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под политикой безопасности мы будем понимать совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Такая трактовка, конечно, гораздо шире, чем набор правил разграничения доступа (именно это означал термин "security policy" в "Оранжевой книге" и в построенных на ее основе нормативных документах других стран).

ИС организации и связанные с ней интересы субъектов - это сложная система, для рассмотрения которой необходимо применять объектно-ориентированный подход и понятие уровня детализации. Целесообразно выделить, по крайней мере, три таких уровня, что мы уже делали в примере и сделаем еще раз далее.

Чтобы рассматривать ИС предметно, с использованием актуальных данных, следует составить карту информационной системы. Эта карта, разумеется, должна быть изготовлена в объектно-ориентированном стиле, с возможностью варьировать не только уровень детализации, но и видимые грани объектов. Техническим средством составления, сопровождения и визуализации подобных карт может служить свободно распространяемый каркас какой-либо системы управления.

2.5. Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь,

повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносятся управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий вопросы физической защиты;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов - отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отличаться.

Роли и обязанности. В "политический" документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно "точкой контакта" служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта - цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

2.6. Программа безопасности

После того, как сформулирована политика безопасности, можно приступить к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней - верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

- управление рисками (оценка рисков, выбор эффективных средств защиты);
- координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- стратегическое планирование;
- контроль деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определенный штат и бюджет.

Цель программы нижнего уровня - обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

2.7. Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее. То же справедливо и для информационной безопасности.

В жизненном цикле информационного сервиса можно выделить следующие этапы:

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

Выведение из эксплуатации. Происходит переход на новый сервис.

Рассмотрим действия, выполняемые на каждом из этапов, более подробно.

На этапе инициации оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

- какого рода информация предназначена для обслуживания новым сервисом?
- каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?
- каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?
- есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?
- каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?
- каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его жизненного цикла

Этап закупки - один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Подчеркнем также, что нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо установить. Несмотря на кажущуюся простоту, установка является очень ответственным делом. Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоемким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей и т.п.

После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности эксплуатации в штатном режиме.

Период эксплуатации - самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось; на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При выведении из эксплуатации затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

При выведении данных из эксплуатации их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи. Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных

2.8. Процедурный уровень информационной безопасности

Мы приступаем к рассмотрению мер безопасности, которые ориентированы на людей, а не на технические средства. Именно люди формируют режим информационной безопасности и они же оказываются главной угрозой, поэтому "человеческий фактор" заслуживает первостепенного внимания.

В отечественных организациях накоплен богатый опыт регламентирования и реализации процедурных (организационных) мер, однако проблема состоит в том, что они пришли из докомпьютерного прошлого, поэтому нуждаются в существенном пересмотре.

Следует осознать ту степень зависимости от компьютерной обработки данных, в которую попало современное общество. Без всякого преувеличения, нужна информационная гражданская оборона. Спокойно, без нагнетания страстей, нужно разъяснять обществу не только преимущества, но и опасности, вытекающие из использования информационных технологий. Акцент следует делать не на военной или криминальной стороне дела, а на чисто гражданских аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

На процедурном уровне можно выделить следующие классы мер:

- управление персоналом;
 - физическая защита;
 - поддержание работоспособности;
 - реагирование на нарушения режима безопасности;
 - планирование восстановительных работ.
- Перейдем к детальному рассмотрению выделенных классов.

2.9. Управление персоналом

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше - с составления описания должности. Уже на этом этапе желательно привлечение специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

- разделение обязанностей;
- минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, нежелательна ситуация, когда крупные платежи от имени организации выполняет один человек. Надежнее поручить одному сотруднику оформлять заявки на подобные платежи, а другому - заверять эти заявки. Другой пример - процедурные ограничения действий суперпользователя. Можно искусственно "расщепить" пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую - другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоем, что снижает вероятность ошибок и злоупотреблений.

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно - уменьшить ущерб от случайных или умышленных некорректных действий пользователей.

Предварительное составление описания должности позволяет оценить ее критичность и спланировать процедуру проверки и отбора кандидатов. Чем критичнее должность, тем тщательнее нужно проверять кандидатов: навести о них справки, быть может, побеседовать с бывшими сослуживцами и т.д. Подобная процедура может быть длительной и дорогой, поэтому нет смысла усложнять ее сверх необходимого. В то же время, неразумно и совсем отказываться от предварительной проверки, рискуя принять на работу человека с уголовным прошлым или с душевными болезнями.

Когда кандидат отобран, он, вероятно, должен пройти обучение; по крайней мере, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до заведения его системного счета с входным именем, паролем и привилегиями.

С момента заведения системного счета начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности и т.п. Все это требует соответствующего изменения привилегий. Техническую сложность составляют временные перемещения сотрудника, выполнение им обязанностей взамен лица, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала дать, а через некоторое время взять обратно. В такие периоды профиль активности пользователя резко меняется, что создает трудности при выявлении подозрительных ситуаций. Определенную аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая изымать старые права доступа.

Ликвидация системного счета пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно (в идеале - одновременно с извещением о наказании или увольнении). Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять все его компьютерное хозяйство и, в частности, криптографические ключи, если использовались средства шифрования.

К управлению сотрудниками примыкает администрирование лиц, работающих по контракту (например, специалистов фирмы-поставщика, помогающих запустить новую систему). В соответствии с принципом минимизации привилегий, им нужно выделить ровно столько прав, сколько необходимо, и изъять эти права сразу по окончании контракта. Проблема, однако, состоит в том, что на начальном этапе внедрения "внешние" сотрудники будут администрировать "местных", а не наоборот. Здесь на первый план выходит квалификация

персонала организации, его способность быстро обучаться, а также оперативное проведение учебных курсов. Важны и принципы выбора деловых партнеров.

Иногда внешние организации принимают на обслуживание и администрирование ответственные компоненты компьютерной системы, например, сетевое оборудование. Нередко администрирование выполняется в удаленном режиме. Вообще говоря, это создает в системе дополнительные уязвимости, которые необходимо компенсировать усиленным контролем средств удаленного доступа или, опять-таки, обучением собственных сотрудников.

Мы видим, что проблема обучения - одна из центральных с точки зрения информационной безопасности. Если сотрудник не знаком с политикой безопасности своей организации, он не может стремиться к достижению сформулированных в ней целей. Если он не знает мер безопасности, он не сможет их соблюдать. Напротив, если сотрудник знает, что его действия протоколируются, он, возможно, воздержится от нарушений.

2.10. Физическая защита

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных.

Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как "непрерывность защиты в пространстве и времени". Ранее мы рассматривали понятие окна уязвимости. Для физической защиты таких окон быть не должно.

Мы кратко рассмотрим следующие направления физической защиты:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры;
- защита от перехвата данных;
- защита мобильных систем.

Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может все здание организации и, кроме того, отдельные помещения, например, те, где расположены серверы, коммуникационная аппаратура и т.п.

При проектировании и реализации мер физического управления доступом целесообразно применять объектный подход. Во-первых, определяется периметр безопасности, ограничивающий контролируемую территорию. На этом уровне детализации важно продумать внешний интерфейс организации - порядок входа/выхода штатных сотрудников и посетителей, вноса/выноса техники. Все, что не входит во внешний интерфейс, должно быть инкапсулировано, то есть защищено от нелегальных проникновений.

Во-вторых, производится декомпозиция контролируемой территории, выделяются (под)объекты и связи (проходы) между ними. При такой, более глубокой детализации следует произвести приоритизацию подобъектов, выделить среди них наиболее критичные с точки зрения безопасности и обеспечить им повышенное внимание. Декомпозиция должна быть семантически оправданной, обеспечивающей разграничение разнородных сущностей, таких как оборудование разных владельцев или персонал, работающий с данными разной степени критичности. Важно в максимальной степени разграничить компьютеры и поток посетителей или, в крайнем случае, позаботиться о том, чтобы от окон и дверей не просматривались экраны мониторов и принтеры. Необходимо, чтобы посетители отличались от штатных сотрудников. Если отличие состоит в том, что посетителям выдаются идентификационные карточки, а сотрудники ходят "без опознавательных знаков", злоумышленнику достаточно снять карточку, чтобы его считали "своим". Очевидно, карточки разных видов нужны всем.

Средства физического управления доступом известны давно. Это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое. Для выбора оптимального (по критерию стоимость/эффективность) средства целесообразно провести анализ рисков (к этому соображению мы еще вернемся). Кроме того, есть смысл периодически отслеживать появление технических новинок в данной области, стремясь к максимальной автоматизации физической защиты.

Более подробно данная тема рассмотрена в статье В. Барсукова "Физическая защита информационных систем" (Jet Info, 1997, 1).

Профессия пожарника - одна из древнейших, но пожары по-прежнему случаются и наносят большой ущерб. Мы не собираемся цитировать параграфы противопожарных инструкций или изобретать новые методы борьбы с огнем - для этого есть профессионалы. Отметим лишь крайнюю желательность установки противопожарной сигнализации и автоматических средств пожаротушения. Обратим также внимание на то, как защитные меры могут создавать новые слабости. Если на работу взят новый охранник, это, вероятно, улучшает физическое управление доступом. Если же он по ночам курит и пьет, то повышенная пожарная опасность делает его скорее врагом, чем другом организации.

К поддерживающей инфраструктуре можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций. В принципе, к ним применимы те же требования целостности и доступности, что и к информационным системам. Для обеспечения целостности нужно защищать оборудование от краж и повреждений. Для поддержания доступности целесообразно выбирать оборудование с максимальным временем наработки на отказ, дублировать ответственные узлы, всегда иметь под рукой запчасти.

Отдельную проблему составляют аварии водопровода. Они происходят нечасто, но чреваты серьезными материальными потерями. При размещении компьютеров разумно принять во внимание расположение водопроводных и канализационных труб и постараться держаться от них подальше. Сотрудники должны знать, куда следует обращаться при обнаружении протечек.

Перехват данных (о чем мы уже писали) может осуществляться самыми разными способами: подсматриванием за экраном монитора, чтением пакетов, передаваемых по сети, анализом побочных электромагнитных излучений и наводок (ПЭМИН) и т.д. Остается уповать на повсеместное использование криптографии (что, впрочем, сопряжено у нас в стране со множеством технических и законодательных проблем), стараться в максимально возможной степени расширить контролируемую территорию, разместившись в тихом особняке, поодаль от других домов, пытаться держать под контролем линии связи (например, заключать их в надувную оболочку с обнаружением прокалывания), но главное, вероятно, состоит в том, что нужно по возможности избавиться от паранойи и осознать, что для коммерческих систем обеспечение конфиденциальности не является главной задачей.

Желающим подробнее ознакомиться с данной тематикой мы рекомендуем статью В. Барсукова "Блокирование технологических каналов утечки информации" (Jet Info, 1998, 5-6).

Мобильные и портативные компьютеры - заманчивый объект кражи. Их довольно часто оставляют без присмотра, в автомобиле или на работе, и унести и спрятать такой компьютер весьма несложно. Довольно часто средства массовой информации сообщают о том, что какой-нибудь офицер английской разведки или американский военный лишился таким образом движимого имущества. Следует настоятельно рекомендовать шифрование данных на жестких дисках подобных компьютеров.

Вообще говоря, при выборе средств физической защиты следует производить анализ рисков. Так, принимая решение о закупке источника бесперебойного питания, необходимо учесть качество электропитания в здании, занимаемом организацией (впрочем, почти наверняка оно окажется плохим), характер и длительность нарушений питания, стоимость доступных источников и возможные потери от аварий (выход из строя техники, приостановка работы организации и т.п.) (см. также статью В. Барсукова "Защита компьютерных систем от силовых деструктивных воздействий" в Jet Info, 2000, 2). В то же время, во многих случаях решения очевидны. Меры противопожарной безопасности обязательны для всех организаций. Стоимость реализации многих мер (например, установка обычного замка на дверь серверной комнаты) пренебрежимо мала, другие имеют хоть и заметную стоимость, но все же явно меньшую, чем возможный ущерб. К числу последних можно отнести регулярное копирование больших баз данных. Физическая защита, как и другие области информационной безопасности, должна базироваться на здравом смысле, который подскажет большинство решений.

2.11. Поддержание работоспособности

Мы переходим к рассмотрению рутинных действий, направленных на поддержание работоспособности информационных систем. Именно здесь таится наибольшая опасность. Нечаянные ошибки системных администраторов и пользователей грозят повреждением аппаратуры, разрушением программ и данных; "в лучшем случае" создаются уязвимости, делающие возможной реализацию угроз.

Недооценка факторов безопасности в повседневной работе - ахиллесова пята многих организаций. Дорогие средства безопасности теряют смысл, если они плохо документированы, конфликтуют с другим программным обеспечением, а пароль системного администратора не менялся с момента установки.

Можно выделить следующие направления повседневной деятельности:

- поддержка пользователей;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Поддержка пользователей состоит прежде всего в консультировании и в оказании помощи при решении разного рода проблем. Иногда в организациях создают для этой цели специальный "стол справок"; чаще от пользователей отбивается системный администратор. Очень важно в потоке вопросов, умных и не очень, уметь выявлять проблемы, связанные с информационной безопасностью. Так, многие трудности пользователей, работающих на персональных компьютерах, могут быть следствием заражения вирусами. Целесообразно фиксировать вопросы пользователей, чтобы выявлять их типичные ошибки и выпускать памятки с рекомендациями для распространенных ситуаций.

Поддержка программного обеспечения - одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо контролировать, какое программное обеспечение выполняется на компьютерах. Если пользователи могут устанавливать программы по своему усмотрению, это чревато заражением вирусами, а также появлением утилит, действующих в обход защитных средств. Вполне вероятно также, что самостоятельность пользователей постепенно приведет к хаосу на их компьютерах, а исправлять ситуацию придется системному администратору.

Второй аспект поддержки программного обеспечения - контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Сюда же можно отнести поддержание эталонных копий программных систем. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и поддержания целостности.

Конфигурационное управление позволяет контролировать и фиксировать изменения, вносимые в программную конфигурацию. Прежде всего, необходимо застраховаться от случайных или непродуманных модификаций, уметь как минимум возвращаться к прошлой, работающей версии. Фиксация изменений позволит легко восстановить текущую версию после аварии.

Лучший способ уменьшить количество ошибок в рутинной работе - в максимальной степени автоматизировать ее. Правы "ленивые" программисты и системные администраторы, которые, поглядев на море

однообразных задач, говорят: "Я ни за что не буду делать этого; я напишу программу, которая сделает все за меня". Автоматизация и безопасность - родные сестры; тот, кто заботится в первую очередь об облегчении собственного труда, на самом деле оптимальным образом формирует режим информационной безопасности.

Резервное копирование необходимо для восстановления программ и данных после аварий. И здесь целесообразно автоматизировать работу, как минимум сформировав компьютерное расписание выполнения полных и инкрементальных копий, а как максимум воспользовавшись соответствующими программными продуктами (см., например, Jet Info, 2000, 12). Нужно также наладить размещение копий в безопасном месте, защищенном от несанкционированного доступа, пожаров, протечек, то есть от всего, что чревато кражей или повреждением носителей. Целесообразно иметь несколько экземпляров резервных копий и часть из них хранить вне территории организации, защищаясь таким образом от крупных аварий и аналогичных инцидентов.

Время от времени в тестовых целях следует проверять возможность восстановления информации с копий.

Управление носителями служит для обеспечения физической защиты и учета дискет, лент, печатных выдач и т.п.

Управление носителями должно обеспечить конфиденциальность, целостность и доступность информации, хранящейся вне компьютерных систем. Под физической защитой здесь понимается не только отражение попыток несанкционированного доступа, но и предохранение от вредных влияний окружающей среды (жары, холода, влаги, магнетизма). Управление носителями должно охватывать весь жизненный цикл - от закупки до выведения из эксплуатации.

Документирование - неотъемлемая часть информационной безопасности. В виде документов оформляется почти все - от политики безопасности до журнала учета носителей. Важно, чтобы документация была актуальной, отражала текущее, а не прошлое, состояние дел, причем отражала в непротиворечивом виде.

К хранению некоторых документов (содержащих, например, анализ системных уязвимостей и угроз) применимы требования обеспечения конфиденциальности, к другим, таким как план восстановления после аварий - требования целостности и доступности (в критической ситуации план необходимо найти и прочитать).

Регламентные работы - очень серьезная угроза безопасности. Лицо, осуществляющее регламентные работы, получает исключительный доступ к системе, и на практике очень трудно проконтролировать, какие именно действия совершаются. Здесь на первый план выходит степень доверия к тем, кто выполняет работы.

2.12. Реагирование на нарушения режима безопасности

Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- прослеживание нарушителя;
- недопущение повторных нарушений.

В организации должен быть человек, доступный 24 часа в сутки (лично, по телефону, пейджеру или электронной почте), отвечающий за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В общем, нужно действовать, как при пожаре: знать, куда звонить, и что делать до приезда пожарной команды.

Важность быстрой и скоординированной реакции можно продемонстрировать на следующем примере. Пусть локальная сеть предприятия состоит из двух сегментов, администрируемых разными людьми. Пусть, далее, в один из сегментов был внесен вирус. Почти наверняка через несколько минут (или, в крайнем случае, несколько десятков минут) вирус распространится и на другой сегмент. Значит, меры нужны немедленные. Далее, вычищать вирус нужно одновременно в обоих сегментах; в противном случае сегмент, вычищенный первым, заразится от другого, а затем вирус вернется и во второй сегмент.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием проследить нарушителя. В политике безопасности организации должны быть заранее расставлены приоритеты. Поскольку, как показывает практика, на успешное прослеживание не так уж много шансов, на наш взгляд, в первую очередь следует заботиться об уменьшении ущерба.

Для прослеживания нарушителя нужно заранее выяснить контактные координаты поставщика сетевых услуг и договориться с ним о самой возможности и порядке выполнения соответствующих действий. Более подробно данная тема освещена в статье Н. Браунли и Э. Гатмэна "Как реагировать на нарушения информационной безопасности (RFC 2350, BCP 21)" (Jet Info, 2000, 5).

Для недопущения повторных нарушений необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику. Каковы источники вредоносного ПО? Какие пользователи имеют обыкновение выбирать слабые пароли? На подобные вопросы и должны дать ответ результаты анализа.

Необходимо отслеживать появление новых уязвимостей и как можно оперативнее ликвидировать ассоциированные с ними окна опасности. Кто-то в организации должен курировать этот процесс, принимать краткосрочные меры и корректировать программу безопасности для принятия долгосрочных мер.

2.13. Планирование восстановительных работ

Ни одна организация не застрахована от серьезных аварий, вызванных естественными причинами, чьим-то злым умыслом, халатностью или некомпетентностью. В то же время, у каждой организации есть функции, которые она считает критически важными, выполнение которых она хотела бы продолжать, несмотря ни на что. Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объеме.

Отметим, что меры информационной безопасности можно разделить на три группы, в соответствии с тем, направлены ли они на предупреждение, обнаружение или ликвидацию последствий атак. Большинство мер носят предупредительный характер. Оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения (так называемый активный аудит) служат для обнаружения и отражения атак. Планирование восстановительных работ, очевидно, можно отнести к последней из трех перечисленных групп.

Процесс планирования восстановительных работ можно подразделить на следующие этапы:

- выявление критически важных функций организации, установление приоритетов;
- идентификация ресурсов, необходимых для выполнения критически важных функций;
- определение перечня возможных аварий;
- разработка стратегии восстановительных работ;
- подготовка к реализации выбранной стратегии;
- проверка стратегии.

Планируя восстановительные работы, следует отдавать себе отчет в том, что полностью сохранить функционирование организации не всегда возможно. Необходимо выявить критически важные функции, без которых организация теряет свое лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить деятельность после аварии.

Идентифицируя ресурсы, необходимые для выполнения критически важных функций, следует помнить, что многие из них имеют некомпьютерный характер. На этом этапе желательно привлечение специалистов разного профиля, способных в совокупности охватить все аспекты проблемы. Критичные ресурсы обычно относятся к одной из следующих категорий:

- персонал,
- информационная инфраструктура,
- физическая инфраструктура.

Составляя списки критически важных специалистов, следует учитывать, что некоторые из них могут напрямую пострадать от аварии (например, от пожара), кто-то может находиться в состоянии стресса, часть сотрудников, возможно, будет лишена возможности попасть на работу (например, в случае массовых беспорядков). Желательно иметь некоторый резерв специалистов или заранее определить каналы, по которым можно на время привлечь дополнительный персонал.

Информационная инфраструктура включает в себя следующие элементы:

- компьютеры,
- программы и данные,
- информационные сервисы внешних организаций,
- документацию.

Нужно подготовиться к тому, что на "запасном аэродроме", куда организация будет эвакуирована после аварии, аппаратная платформа может отличаться от исходной. Соответственно, следует продумать меры поддержания совместимости по программам и данным.

Среди внешних информационных сервисов для коммерческих организаций, вероятно, важнее всего получение оперативной информации и связь с государственными службами, курирующими данный сектор экономики.

Документация важна хотя бы потому, что не вся информация, с которой оперирует организация, представлена в электронной форме. Скорее всего, план восстановительных работ напечатан на бумаге.

К физической инфраструктуре относятся здания, инженерные коммуникации, средства связи, оргтехника и многое другое. Компьютерная техника не может работать в плохих условиях, без нормального электропитания и т.п.

Анализируя критичные ресурсы, целесообразно учесть временной профиль их использования. Большинство ресурсов нужны постоянно, но в некоторых случаях потребность может возникать только в определенные периоды (например, в конце месяца или года при составлении отчета).

При определении перечня возможных аварий нужно попытаться разработать их сценарии. Как будут развиваться события? Каковы могут оказаться масштабы бедствия? Что произойдет с критичными ресурсами? Например, смогут ли люди попасть на работу? Будут ли выведены из строя компьютеры? Возможны ли случаи саботажа? Будет ли работать связь? Пострадает ли здание организации? Можно ли будет найти и прочитать необходимые бумаги?

Стратегия восстановительных работ должна базироваться на наличных ресурсах и быть не слишком накладной для организации. При разработке стратегии целесообразно провести анализ рисков, которым подвержены критичные функции, и попытаться выбрать наиболее экономичное решение.

Стратегия должна предусматривать не только работу по временной схеме, но и возвращение к нормальному функционированию.

Подготовка к реализации выбранной стратегии состоит в проработке детального плана действий в экстренных ситуациях и по их окончании, а также в обеспечении некоторой избыточности критичных ресурсов. Последнюю цель можно достичь без большого расхода средств, если заключить с одной или несколькими организациями соглашения о взаимной поддержке в случае аварий - тот, кто не пострадал, предоставляет часть своих ресурсов во временное пользование менее удачливым партнерам.

Избыточность обеспечивается также мерами резервного копирования, хранением копий в нескольких местах, представлением информации в разных видах (на бумаге и в файлах) и т.д.

Разумно заключить соглашение с поставщиками информационных услуг о первоочередном обслуживании в критических ситуациях или иметь соглашения с несколькими поставщиками. Правда, эти меры могут потребовать определенных расходов.

Проверка стратегии производится путем анализа подготовленного плана, принятых и намеченных мер.

Просмотр и обсуждение фильма о различных уровнях информационной безопасности (2 часа).

РАЗДЕЛ №3: ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И систем

3.1. Основные понятия программно-технического уровня информационной безопасности

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей - оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности. Напомним, что основную часть ущерба наносят действия легальных пользователей, по отношению к которым процедурные регуляторы не могут дать решающего эффекта. Главные враги - некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

Компьютеры помогли автоматизировать многие области человеческой деятельности. Вполне естественным представляется желание возложить на них и обеспечение собственной безопасности. Даже физическую защиту все чаще поручают не охранникам, а интегрированным компьютерным системам, что позволяет одновременно отслеживать перемещения сотрудников и по пространству организации, и по информационному пространству. Это вторая причина, объясняющая важность программно-технических мер.

Следует, однако, учитывать, что быстрое развитие информационных технологий не только дает новые возможности обороняющимся, но и объективно затрудняет обеспечение надежной защиты, если опираться исключительно на меры программно-технического уровня. Причин тому несколько:

- повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет методом грубой силы преодолевать барьеры (прежде всего криптографические), ранее казавшиеся неприступными;
- развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют число злоумышленников, имеющих техническую возможность организовывать атаки;
- появление новых информационных сервисов ведет и к появлению новых уязвимостей как "внутри" сервисов, так и на их стыках;
- конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки, что ведет к снижению качества тестирования и выпуску продуктов с дефектами защиты;
- навязываемая потребителям парадигма постоянного наращивания аппаратного и программного обеспечения не позволяет долго оставаться в рамках надежных, апробированных конфигураций и, кроме того, вступает в конфликт с бюджетными ограничениями, из-за чего снижается доля ассигнований на безопасность.
- Перечисленные соображения лишней раз подчеркивают важность комплексного подхода к информационной безопасности, а также необходимость динамичной позиции при выборе и сопровождении программно-технических регуляторов.

Центральным для программно-технического уровня является понятие сервиса безопасности.

Следуя объектно-ориентированному подходу, при рассмотрении информационной системы с единичным уровнем детализации мы увидим совокупность предоставляемых ею информационных сервисов. Назовем их основными. Чтобы они могли функционировать и обладали требуемыми свойствами, необходимо несколько уровней дополнительных (вспомогательных) сервисов - от СУБД и мониторов транзакций до ядра операционной системы и оборудования.

В число вспомогательных входят сервисы безопасности (мы уже сталкивались с ними при рассмотрении стандартов и спецификаций в области ИБ); среди них нас в первую очередь будут интересовать универсальные, высокоуровневые, допускающие использование различными основными и вспомогательными сервисами. Далее будут изучены:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

Будут описаны требования к сервисам безопасности, их функциональность, возможные методы реализации, место в общей архитектуре.

Если сопоставить приведенный перечень сервисов с классами функциональных требований "Общих критериев", то бросается в глаза их существенное несовпадение. Мы отказались от рассмотрения вопросов, связанных с приватностью, по следующей причине. На наш взгляд, сервис безопасности, хотя бы частично, должен находиться в распоряжении того, кого он защищает. В ситуации с приватностью это не так: критически важные компоненты сосредоточены не на клиентской, а на серверной стороне, так что приватность по существу оказывается свойством предлагаемой информационной услуги (в простейшем случае приватность достигается сохранением конфиденциальности серверной регистрационной информации и защитой от перехвата данных, для чего достаточно перечисленных нами сервисов безопасности).

С другой стороны, наш перечень шире, чем в "Общих критериях", поскольку в него входят экранирование, анализ защищенности и туннелирование. Мы покажем, что эти сервисы имеют важное самостоятельное значение и, кроме того, могут комбинироваться с другими сервисами для получения таких необходимых защитных средств, как, например, виртуальные собственные сети.

Совокупность перечисленных выше сервисов безопасности мы будем называть полным набором. Согласно современным воззрениям, он в принципе достаточен для построения надежной защиты на программно-техническом уровне, правда, при соблюдении целого ряда дополнительных условий (отсутствие уязвимостей, безопасное администрирование и т.д., и т.п.).

Для проведения классификации сервисов безопасности и определения их места в общей архитектуре целесообразно подразделить меры безопасности на следующие виды:

- превентивные, препятствующие нарушениям ИБ;
- меры обнаружения нарушений;
- локализирующие, сужающие зону воздействия нарушений;
- меры по прослеживанию нарушителя;
- меры восстановления режима безопасности.

Большинство сервисов безопасности попадает в число превентивных, и это, безусловно, правильно. Аудит и контроль целостности способны помочь в обнаружении нарушений; активный аудит, кроме того, позволяет запрограммировать реакцию на нарушение с целью локализации и/или прослеживания. Направленность сервисов отказоустойчивости и безопасного восстановления очевидна. Наконец, управление играет инфраструктурную роль, обслуживая все аспекты ИС.

3.2. Особенности современных информационных систем, существенные с точки зрения безопасности

Информационная система типичной современной организации является весьма сложным образованием, построенным в многоуровневой архитектуре клиент/сервер, пользующимся многочисленными внешними сервисами и, в свою очередь, предоставляющим собственные сервисы вовне. Даже сравнительно небольшие магазины, обеспечивающие расчет с покупателями по пластиковым картам (и, конечно, имеющие внешний Web-сервер), критическим образом зависят от своих информационных систем и, в частности (и вместе с покупателями), - от защищенности всех компонентов систем и коммуникаций между ними.

С точки зрения безопасности наиболее существенными представляются следующие аспекты современных ИС:

- корпоративная сеть имеет несколько территориально разнесенных частей (поскольку организация располагается на нескольких производственных площадках), связи между которыми находятся в ведении внешнего поставщика сетевых услуг, выходя за пределы зоны, контролируемой организацией;
- корпоративная сеть имеет одно или несколько подключений к Интернет;
- на каждой из производственных площадок могут находиться критически важные серверы, в доступе к которым нуждаются работники, базирующиеся на других площадках, мобильные работники и, возможно, сотрудники сторонних организаций и другие внешние пользователи;
- для доступа пользователей могут применяться не только компьютеры, но и потребительские устройства, использующие, в частности, беспроводную связь;
- в течение одного сеанса работы пользователю приходится обращаться к нескольким информационным сервисам, опирающимся на разные аппаратно-программные платформы;
- к доступности информационных сервисов предъявляются жесткие требования, обычно выражающиеся в необходимости круглосуточного функционирования с максимальным временем простоя порядка минут или десятков минут;
- информационная система представляет собой сеть с активными агентами, то есть в процессе работы программные компоненты, такие как апплеты или сервлеты, передаются с одной машины на другую и выполняются в целевой среде, поддерживая связь с удаленными компонентами;
- не все пользовательские системы контролируются сетевыми и/или системными администраторами организации;
- программное обеспечение, особенно полученное по сети, не может считаться доверенным, в нем могут присутствовать зловредные элементы или ошибки, создающие уязвимости в защите;
- конфигурация информационной системы постоянно изменяется на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привилегии, версии программ, появляются новые сервисы, новая аппаратура и т.п.).

Следует учитывать еще по крайней мере два момента. Во-первых, для каждого сервиса основные грани ИБ (доступность, целостность, конфиденциальность) трактуются по-своему. Целостность с точки зрения системы управления базами данных и с точки зрения почтового сервера - вещи принципиально разные. Бессмысленно говорить о безопасности локальной или иной сети вообще, если сеть включает в себя разнородные компоненты. Следует анализировать защищенность сервисов, функционирующих в сети. Для разных сервисов и защиту строят по-разному. Во-вторых, основная угроза информационной безопасности организаций по-прежнему исходит не от внешних злоумышленников, а от собственных сотрудников, по той или иной причине не являющихся лояльными.

В силу изложенных причин далее будут рассматриваться распределенные, разнородные, многосервисные, эволюционирующие системы. Соответственно, нас будут интересовать решения, ориентированные на подобные конфигурации.

3.3. Архитектурная безопасность

Сервисы безопасности, какими бы мощными и стойкими они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. Только разумная, проверенная архитектура способна сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

Теоретической основой решения проблемы архитектурной безопасности является следующее фундаментальное утверждение, которое мы уже приводили при рассмотрении Интерпретации "Оранжевой книги" для сетевых конфигураций:

Утверждение. Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Пусть, далее, каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы проводят в жизнь согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации.

Обратим внимание на три принципа, содержащиеся в приведенном утверждении:

- необходимость выработки и проведения в жизнь единой политики безопасности;
- необходимость обеспечения конфиденциальности и целостности при сетевых взаимодействиях;
- необходимость формирования составных сервисов по содержательному принципу, чтобы каждый полученный таким образом компонент обладал полным набором защитных средств и с внешней точки зрения представлял собой единое целое (не должно быть информационных потоков, идущих к незащищенным сервисам).

Если какой-либо (составной) сервис не обладает полным набором защитных средств (состав полного набора описан выше), необходимо привлечение дополнительных сервисов, которые мы будем называть экранирующими. Экранирующие сервисы устанавливаются на путях доступа к недостаточно защищенным элементам; в принципе, один такой сервис может экранировать (защищать) сколь угодно большое число элементов.

С практической точки зрения наиболее важными являются следующие принципы архитектурной безопасности:

- непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;
- следование признанным стандартам, использование апробированных решений;
- иерархическая организация ИС с небольшим числом сущностей на каждом уровне;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы.

Поясним смысл перечисленных принципов. Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Определенные выше экранирующие сервисы должны исключить подобную возможность. Следование признанным стандартам, использование апробированных решений повышает надежность ИС, уменьшает вероятность попадания в тупиковую ситуацию, когда обеспечение безопасности потребует непомерно больших затрат и принципиальных модификаций.

Иерархическая организация ИС с небольшим числом сущностей на каждом уровне необходима по технологическим соображениям. При нарушении данного принципа система станет необозримой и, следовательно, обеспечить ее безопасность будет невозможно.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. (Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.)

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

Применительно к программно-техническому уровню принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа - уменьшить ущерб от случайных или умышленных некорректных действий пользователей и администраторов.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите по заказу злоумышленников. Соблюдение данного принципа особенно важно, чтобы предотвратить злонамеренные или некачественные действия системного администратора.

Принцип эшелонированной обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические

средства, заидентификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (например, таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и плохо управляемой.

Для обеспечения высокой доступности (непрерывности функционирования) необходимо соблюдать следующие принципы архитектурной безопасности:

- Внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.).
- Наличие средств обнаружения нештатных ситуаций.
- Наличие средств реконфигурирования для восстановления, изоляции и/или замены компонентов, отказавших или подвергшихся атаке на доступность.
- Рассредоточенность сетевого управления, отсутствие единой точки отказа.
- Выделение подсетей и изоляция групп пользователей друг от друга. Данная мера, являющаяся обобщением разделения процессов на уровне операционной системы, ограничивает зону поражения при возможных нарушениях информационной безопасности.

Еще одним важным архитектурным принципом следует признать минимизацию объема защитных средств, выносимых на клиентские системы. Причин тому несколько:

- для доступа в корпоративную сеть могут использовать потребительские устройства с ограниченной функциональностью;
- конфигурацию клиентских систем трудно или невозможно контролировать.

К необходимому минимуму следует отнести реализацию сервисов безопасности на сетевом и транспортном уровнях и поддержку механизмов аутентификации, устойчивых к сетевым угрозам.

3.4. Идентификация и аутентификация

Основные понятия

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация - это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

(Заметим в скобках, что происхождение русскоязычного термина "аутентификация" не совсем понятно. Английское "authentication" скорее можно прочесть как "аутентикация"; трудно сказать, откуда в середине взялось еще "фи" - может, из идентификации? Тем не менее, термин устоялся, он закреплен в Руководящих документах Гостехкомиссии России, использован в многочисленных публикациях, поэтому исправить его уже невозможно.)

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации - процедура входа пользователя в систему.

В сетевой среде, когда стороны идентификации/аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

- что служит аутентификатором (то есть используется для подтверждения подлинности субъекта);
- как организован (и защищен) обмен данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);
- нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения и/или воспроизведения данных. Передача

паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

Надежная идентификация и аутентификация затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства идентификации-аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

Любопытно отметить, что сервис идентификации/аутентификации может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

Парольная аутентификация

Главное достоинство парольной аутентификации - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Известна классическая история про советского разведчика Рихарда Зорге, объект внимания которого через слово говорил "карамба"; разумеется, этим же словом открывался сверхсекретный сейф.

Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Ввод пароля можно подсмотреть. Иногда для подглядывания используются даже оптические приборы.

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

Пароль можно угадать "методом грубой силы", используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен).

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");
- обучение пользователей;
- использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

Одноразовые пароли

Рассмотренные выше пароли можно назвать многоразовыми; их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются одноразовые пароли.

Наиболее известным программным генератором одноразовых паролей является система S/KEY компании Bellcore. Идея этой системы состоит в следующем. Пусть имеется односторонняя функция f (то есть функция, вычислить обратную которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и серверу аутентификации. Пусть, далее, имеется секретный ключ K , известный только пользователю.

На этапе начального администрирования пользователя функция f применяется к ключу K n раз, после чего результат сохраняется на сервере. После этого процедура проверки подлинности пользователя выглядит следующим образом:

- сервер присылает на пользовательскую систему число $(n-1)$;
- пользователь применяет функцию f к секретному ключу K $(n-1)$ раз и отправляет результат по сети на сервер аутентификации;

- сервер применяет функцию f к полученному от пользователя значению и сравнивает результат с ранее сохраненной величиной. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик (n).

На самом деле реализация устроена чуть сложнее (кроме счетчика, сервер посылает затравочное значение, используемое функцией f), но для нас сейчас это не важно. Поскольку функция f необратима, перехват пароля, равно как и получение доступа к серверу аутентификации, не позволяют узнать секретный ключ K и предсказать следующий одноразовый пароль.

Система S/KEY имеет статус Internet-стандарта (RFC 1938).

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или специальные интеллектуальные карты (с практической точки зрения такие пароли можно считать одноразовыми). Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронизированы.

Сервер аутентификации Kerberos

Kerberos - это программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

Kerberos предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены субъекты - пользователи, а также клиентские и серверные программные системы. Каждый субъект обладает секретным ключом. Чтобы субъект C мог доказать свою подлинность субъекту S (без этого S не станет обслуживать C), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. C не может просто послать S свой секретный ключ, во-первых, потому, что сеть открыта (доступна для пассивного и активного прослушивания), а, во-вторых, потому, что S не знает (и не должен знать) секретный ключ C . Требуется менее прямолинейный способ демонстрации знания секретного ключа.

Система Kerberos представляет собой доверенную третью сторону (то есть сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности. Чтобы с помощью Kerberos получить доступ к S (обычно это сервер), C (как правило - клиент) посылает Kerberos запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ Kerberos возвращает так называемый билет, зашифрованный секретным ключом сервера, и копию части информации из билета, зашифрованную секретным ключом клиента. Клиент должен расшифровать вторую порцию данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом. Совпадение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные (ведь содержимое билета никому, кроме сервера и Kerberos, недоступно), то есть продемонстрировал знание секретного ключа. Значит, клиент - именно тот, за кого себя выдает. Подчеркнем, что секретные ключи в процессе проверки подлинности не передавались по сети (даже в зашифрованном виде) - они только использовались для шифрования. Как организован первоначальный обмен ключами между Kerberos и субъектами и как субъекты хранят свои секретные ключи - вопрос отдельный.

Проиллюстрируем описанную процедуру.

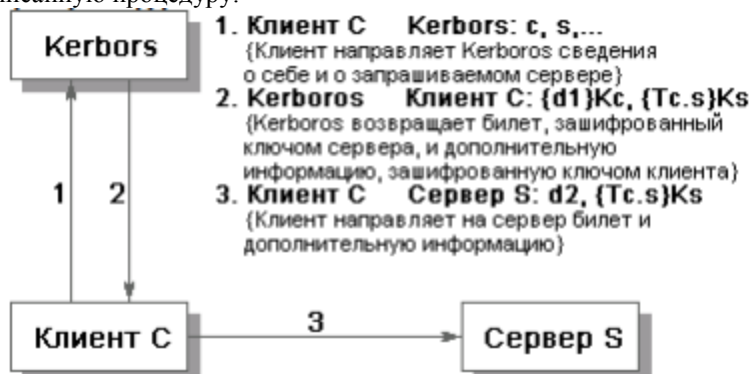


Рис. 7.1. Проверка сервером S подлинности клиента C . Здесь c и s - сведения (например, имя), соответственно, о клиенте и сервере, $d1$ и $d2$ - дополнительная (по отношению к билету) информация, $Tc.s$ - билет для клиента C на обслуживание у сервера S , K_c и K_s - секретные ключи клиента и сервера, $\{info\}K$ - информация $info$, зашифрованная ключом K .

Приведенная схема - крайне упрощенная версия реальной процедуры проверки подлинности. Более подробное рассмотрение системы Kerberos можно найти, например, в статье В. Галатенко "Сервер аутентификации Kerberos (Jet Info, 1996, 12-13). Нам же важно отметить, что Kerberos не только устойчив к сетевым угрозам, но и поддерживает концепцию единого входа в сеть.

Идентификация/аутентификация с помощью биометрических данных

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

Биометрией во всем мире занимаются очень давно, однако долгое время все, что было связано с ней, отличалось сложностью и дороговизной. В последнее время спрос на биометрические продукты, в первую очередь в связи с развитием электронной коммерции, постоянно и весьма интенсивно растет. Это понятно, поскольку с точки зрения пользователя гораздо удобнее предъявить себя самого, чем что-то запоминать. Спрос рождает предложение, и на рынке появились относительно недорогие аппаратно-программные продукты, ориентированные в основном на распознавание отпечатков пальцев.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

Обычно биометрию применяют вместе с другими аутентификаторами, такими, например, как интеллектуальные карты. Иногда биометрическая аутентификация является лишь первым рубежом защиты и служит для активизации интеллектуальных карт, хранящих криптографические секреты; в таком случае биометрический шаблон хранится на той же карте.

Активность в области биометрии очень велика. Организован соответствующий консорциум (см. <http://www.biometrics.org>), активно ведутся работы по стандартизации разных аспектов технологии (формата обмена данными, прикладного программного интерфейса и т.п.), публикуется масса рекламных статей, в которых биометрия преподносится как средство обеспечения сверхбезопасности, ставшее доступным широким массам.

На наш взгляд, к биометрии следует относиться весьма осторожно. Необходимо учитывать, что она подвержена тем же угрозам, что и другие методы аутентификации. Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти. Во-вторых, биометрические методы не более надежны, чем база данных шаблонов. В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в "полевых" условиях, когда, например к устройству сканирования роговицы могут поднести муляж и т.п. В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

Но главная опасность состоит в том, что любая "пробоина" для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей системы.

3.5. Управление доступом

Основные понятия

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). В данном разделе речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах - объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа. Фрагмент матрицы может выглядеть, например, так:

Табл. 7.1. Фрагмент матрицы доступа

	Файл	Программа	Линия связи	Реляционная таблица
Пользователь 1	огв с системной консоли	e	гв с 8:00 до 18:00	
Пользователь 2				a

"o" - обозначает разрешение на передачу прав доступа другим пользователям,

"r" - чтение,
"w" - запись,
"e" - выполнение,
"a" - добавление информации

Тема логического управления доступом - одна из сложнейших в области информационной безопасности. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные операционные системы могут поддерживать и другие объекты.

Для систем управления реляционными базами данных объект - это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа.

Разнообразие объектов и применимых к ним операций приводит к принципиальной децентрализации логического управления доступом. Каждый сервис должен сам решать, позволить ли конкретному субъекту ту или иную операцию. Теоретически это согласуется с современным объектно-ориентированным подходом, на практике же приводит к значительным трудностям. Главная проблема в том, что ко многим объектам можно получить доступ с помощью разных сервисов (возможно, при этом придется преодолеть некоторые технические трудности). Так, до реляционных таблиц можно добраться не только средствами СУБД, но и путем непосредственного чтения файлов или дисковых разделов, поддерживаемых операционной системой (разобравшись предварительно в структуре хранения объектов базы данных). В результате при задании матрицы доступа нужно принимать во внимание не только принцип распределения привилегий для каждого сервиса, но и существующие связи между сервисами (приходится заботиться о согласованности разных частей матрицы). Аналогичная трудность возникает при экспорте/импорте данных, когда информация о правах доступа, как правило, теряется (поскольку на новом сервисе она не имеет смысла). Следовательно, обмен данными между различными сервисами представляет особую опасность с точки зрения управления доступом, а при проектировании и реализации разнородной конфигурации необходимо позаботиться о согласованном распределении прав доступа субъектов к объектам и о минимизации числа способов экспорта/импорта данных.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

- идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой произвольного (или дискреционного) управления доступом;
- атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности - основа принудительного (мандатного) управления доступом.

Матрицу доступа, ввиду ее разреженности (большинство клеток - пустые), неразумно хранить в виде двумерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Элементами списков могут быть имена групп и шаблоны субъектов, что служит большим подспорьем администратору. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится нечасто.

Списки доступа - исключительно гибкое средство. С их помощью легко выполнить требование о гранулярности прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.

Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления - гибкость. Вообще говоря, для каждой пары "субъект-объект" можно независимо задавать права доступа (особенно легко это делать, если используются списки управления доступом). К сожалению, у "произвольного" подхода есть ряд недостатков. Рассредоточенность управления доступом ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной информацией, эту информацию могут узнать и все остальные пользователи. Следовательно, произвольность управления должна быть дополнена жестким контролем за реализацией избранной политики безопасности.

Второй недостаток, который представляется основным, состоит в том, что права доступа существуют отдельно от данных. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту ее "тройным" аналогом. Подобная "разделенность" прав и данных существенно осложняет проведение несколькими системами согласованной политики безопасности и, главное, делает практически невозможным эффективный контроль согласованности.

Возвращаясь к вопросу представления матрицы доступа, укажем, что для этого можно использовать также функциональный способ, когда матрицу не хранят в явном виде, а каждый раз вычисляют содержимое соответствующих клеток. Например, при принудительном управлении доступом применяется сравнение меток безопасности субъекта и объекта.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход

обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек, таких как `restricted shell` в ОС Unix.

В заключение подчеркнем важность управления доступом не только на уровне операционной системы, но и в рамках других сервисов, входящих в состав современных приложений, а также, насколько это возможно, на "стыках" между сервисами. Здесь на первый план выходит существование единой политики безопасности организации, а также квалифицированное и согласованное системное администрирование. Ролевое управление доступом При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить. Таким решением является ролевое управление доступом (РУД). Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности - роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (см. рис. 7.2).



Рис. 7.2. Пользователи, объекты и роли.

Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно.

Ролевой доступ развивается более 10 лет (сама идея ролей, разумеется, значительно старше) как на уровне операционных систем, так и в рамках СУБД и других информационных сервисов. В частности, существуют реализации ролевого доступа для Web-серверов.

В 2001 году Национальный институт стандартов и технологий США предложил проект стандарта ролевого управления доступом (см. <http://csrc.nist.gov/rbac/>), основные положения которого мы и рассмотрим.

Ролевое управление доступом оперирует следующими основными понятиями: • пользователь (человек, интеллектуальный автономный агент и т.п.);

- сеанс работы пользователя;
- роль (обычно определяется в соответствии с организационной структурой);
- объект (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);
- операция (зависит от объекта; для файлов ОС - чтение, запись, выполнение и т.п.; для таблиц СУБД - вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными);
- право доступа (разрешение выполнять определенные операции над определенными объектами).

Ролям приписываются пользователи и права доступа; можно считать, что они (роли) именуют отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многие пользователи; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов.

Между ролями может быть определено отношение частичного порядка, называемое наследованием. Если роль r_2 является наследницей r_1 , то все права r_1 приписываются r_2 , а все пользователи r_2 приписываются r_1 . Очевидно, что наследование ролей соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям - объекты (экземпляры) классов.

Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить себе формирование иерархии ролей, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), вплоть до роли "руководитель" (что, впрочем, не значит, что руководителю предоставляются неограниченные права; как и другим ролям, в соответствии с принципом минимизации привилегий, этой роли целесообразно разрешить только то, что необходимо для выполнения служебных обязанностей). Фрагмент подобной иерархии ролей показан на рис. 7.3.



Рис. 7.3. Фрагмент иерархии ролей.

Для реализации еще одного упоминавшегося ранее важного принципа информационной безопасности вводится понятие разделения обязанностей, причем в двух видах: статическом и динамическом.

Статическое разделение обязанностей налагает ограничения на приписывание пользователей ролям. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей. В общем случае данное ограничение задается как пара "множество ролей - число" (где множество состоит, по крайней мере, из двух ролей, а число должно быть больше 1), так что никакой пользователь не может быть приписан указанному (или большему) числу ролей из заданного множества. Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях (здесь число=3). При наличии наследования ролей ограничение приобретает несколько более сложный вид, но суть остается простой: при проверке членства в ролях нужно учитывать приписывание пользователей ролям-наследникам.

Динамическое разделение обязанностей отличается от статического только тем, что рассматриваются роли, одновременно активные (быть может, в разных сеансах) для данного пользователя (а не те, которым пользователь статически приписан). Например, один пользователь может играть роль и кассира, и контролера, но не одновременно; чтобы стать контролером, он должен сначала закрыть кассу. Тем самым реализуется так называемое временное ограничение доверия, являющееся аспектом минимизации привилегий.

Рассматриваемый проект стандарта содержит спецификации трех категорий функций, необходимых для администрирования РУД:

1. Административные функции (создание и сопровождение ролей и других атрибутов ролевого доступа): создать/удалить роль/пользователя, приписать пользователя/право роли или ликвидировать существующую ассоциацию, создать/удалить отношение наследования между существующими ролями, создать новую роль и сделать ее наследницей/предшественницей существующей роли, создать/удалить ограничения для статического/динамического разделения обязанностей.

2. Вспомогательные функции (обслуживание сеансов работы пользователей): открыть сеанс работы пользователя с активацией подразумеваемого набора ролей; активировать новую роль, деактивировать роль; проверить правомерность доступа.

3. Информационные функции (получение сведений о текущей конфигурации с учетом отношения наследования). Здесь проводится разделение на обязательные и необязательные функции. К числу первых принадлежат получение списка пользователей, приписанных роли, и списка ролей, которым приписан пользователь.

Все остальные функции отнесены к разряду необязательных. Это получение информации о правах, приписанных роли, о правах заданного пользователя (которыми он обладает как член множества ролей), об активных в данный момент сеансах ролях и правах, об операциях, которые роль/пользователь правомочны совершить над заданным объектом, о статическом/динамическом разделении обязанностей. Можно надеяться, что предлагаемый стандарт поможет сформировать единую терминологию и, что более важно, позволит оценивать РУД-продукты с единых позиций, по единой шкале.

Управление доступом в Java-среде

Java - это объектно-ориентированная система программирования, поэтому и управление доступом в ней спроектировано и реализовано в объектном стиле. По этой причине рассмотреть Java-среду для нас очень важно. Подробно о Java-технологии и безопасности Java-среды рассказано в статье А. Таранова и В. Цишевского "Java в три года" (Jet Info, 1998, 11-12). С разрешения авторов далее используются ее фрагменты.

Прежде всего, остановимся на эволюции модели безопасности Java. В JDK 1.0 была предложена концепция "песочницы" (sandbox) - замкнутой среды, в которой выполняются потенциально ненадежные программы (апплеты, поступившие по сети). Программы, располагающиеся на локальном компьютере, считались абсолютно надежными, и им было доступно все, что доступно виртуальной Java-машине.

В число ограничений, налагаемых "песочницей", входит запрет на доступ к локальной файловой системе, на сетевое взаимодействие со всеми хостами, кроме источника апплета, и т.п. Независимо от уровня достигаемой при этом безопасности (а проблемы возникали и с разделением свой/чужой, и с определением источника апплета), наложенные ограничения следует признать слишком обременительными: возможности для содержательных действий у апплетов почти не остается.

Чтобы справиться с этой проблемой, в JDK 1.1 ввели деление источников (точнее, распространителей) апплетов на надежные и ненадежные (источник определялся по электронной подписи). Надежные апплеты приравнивались в правах к "родному" коду. Сделанное послабление решило проблемы тех, кому прав не хватало, но защита осталась нешелонирующей и, следовательно, неполной.

В JDK 1.2 сформировалась модель безопасности, используемая и в Java 2. От модели "песочницы" отказались. Оформились три основных понятия:

- источник программы;
- право и множество прав;
- политика безопасности.

Источник программы определяется парой (URL, распространители программы). Последние задаются набором цифровых сертификатов.

Право - это абстрактное понятие, за которым, как и положено в объектной среде, стоят классы и объекты. В большинстве случаев право определяется двумя цепочками символов - именем ресурса и действием. Например, в качестве ресурса может выступать файл, а в качестве действия - чтение. Важнейшим методом "правовых" объектов является `implies()`. Он проверяет, следует ли одно право (запрашиваемое) из другого (имеющегося).

Политика безопасности задает соответствие между источником и правами поступивших из него программ (формально можно считать, что каждому источнику соответствует своя "песочница"). В JDK 1.2 "родные" программы не имеют каких-либо привилегий в плане безопасности, и политика по отношению к ним может быть любой. В результате получился традиционный для современных ОС и СУБД механизм прав доступа со следующими особенностями:

- Java-программы выступают не от имени пользователя, их запустившего, а от имени источника программы. (Это весьма глубокая и прогрессивная трактовка, если ее правильно развить, см. следующий раздел);
- нет понятия владельца ресурсов, который мог бы менять права; последние задаются исключительно политикой безопасности (формально можно считать, что владельцем всего является тот, кто формирует политику);
- механизмы безопасности снабжены объектной оберткой.

Весьма важным понятием в модели безопасности JDK 1.2 является контекст выполнения. Когда виртуальная Java-машина проверяет права доступа объекта к системному ресурсу, она рассматривает не только текущий объект, но и предыдущие элементы стека вызовов. Доступ предоставляется только тогда, когда нужным правом обладают все объекты в стеке. Разработчики Java называют это реализацией принципа минимизации привилегий.

На первый взгляд, учет контекста представляется логичным. Нельзя допускать, чтобы вызов какого-либо метода расширял права доступа хотя бы по той причине, что доступ к системным ресурсам осуществляется не напрямую, а с помощью системных объектов, имеющих все права.

К сожалению, подобные доводы противоречат одному из основных принципов объектного подхода - принципу инкапсуляции. Если объект А обращается к объекту В, он не может и не должен знать, как реализован В и какими ресурсами он пользуется для своих целей. Если А имеет право вызывать какой-либо метод В с некоторыми значениями аргументов, В обязан обслужить вызов. В противном случае при формировании политики безопасности придется учитывать возможный граф вызовов объектов, что, конечно же, нереально.

Разработчики Java осознали эту проблему. Чтобы справиться с ней, они ввели понятие привилегированного интервала программы. При выполнении такого интервала контекст игнорируется. Привилегированная программа отвечает за себя, не интересуясь предысторией. Аналогом привилегированных программ являются файлы с битами переустановки идентификатора пользователя/группы в ОС Unix, что лишний раз подтверждает традиционность подхода, реализованного в JDK 1.2. Известны угрозы безопасности, которые приносят подобные файлы. Теперь это не лучшее средство ОС Unix перекочевало в Java.

Рассмотрим дисциплину контроля прав доступа более формально.

Класс `AccessController` (встроенный менеджер безопасности) предоставляет единый метод для проверки заданного права в текущем контексте - `checkPermission(Permission)`. Это лучше (по причине параметризуемости), чем множество методов вида `checkXXX`, присутствующих в `SecurityManager` - динамически изменяемом менеджере безопасности из ранних версий JDK.

Пусть текущий контекст выполнения состоит из N стековых фреймов (верхний соответствует методу, вызвавшему `checkPermission(p)`). Метод `checkPermission` реализует следующий алгоритм (см. Листинг 7.1).

```
i = N
; while (i > 0) {
  if (метод, породивший i-й фрейм, не имеет проверяемого
  права) {
    throw AccessControlException
  } else if (i-й фрейм помечен как привилегированный) {
    return;
  }
  i = i - 1;
};
// Выясним, есть ли проверяемое право у унаследованного контекста
inheritedContext.checkPermission (p);
```

Листинг 7.1. Алгоритм работы метода `checkPermission` класса `AccessController`.

Сначала в стеке ищется фрейм, не обладающий проверяемым правом. Проверка производится до тех пор, пока либо не будет исчерпан стек, либо не встретится "привилегированный" фрейм, созданный в результате обращения к методу `doPrivileged(PrivilegedAction)` класса `AccessController`. Если при порождении текущего потока выполнения был сохранен контекст `inheritedContext`, проверяется и он. При положительном результате

проверки метод `checkPermission(p)` возвращает управление, при отрицательном возникает исключительная ситуация `AccessControlException`.

Выбранный подход имеет один недостаток - тяжеловесность реализации. В частности, при порождении нового потока управления с ним приходится ассоциировать зафиксированный "родительский" контекст и, соответственно, проверять последний в процессе контроля прав доступа.

Отметим, что этот подход не распространяется на распределенный случай (хотя бы потому, что контекст имеет лишь локальный смысл, как, впрочем, и политика безопасности).

В целом средства управления доступом в JDK 1.2 можно оценить как "наполовину объектные". Реализация оформлена в виде интерфейсов и классов, однако по-прежнему разграничивается доступ к необъектным сущностям - ресурсам в традиционном понимании. Не учитывается семантика доступа. Имеют место и другие отмеченные выше концептуальные проблемы.

Возможный подход к управлению доступом в распределенной объектной среде

Представляется, что в настоящее время проблема управления доступом существует в трех почти не связанных между собой проявлениях:

- традиционные модели (дискреционная и мандатная);
- модель "песочница" (предложенная для Java-среды и близкой ей системы Safe-Tcl);
- модель фильтрации (используемая в межсетевых экранах).

На наш взгляд, необходимо объединить существующие подходы на основе их развития и обобщения.

Формальная постановка задачи разграничения доступа может выглядеть следующим образом.

Рассматривается множество объектов (в смысле объектно-ориентированного программирования). Часть объектов может являться контейнерами, группирующими объекты-компоненты, задающими для них общий контекст, выполняющими общие функции и реализующими перебор компонентов. Контейнеры либо вложены друг в друга, либо не имеют общих компонентов.

С каждым объектом ассоциирован набор интерфейсов, снабженных дескрипторами (ДИ). К объекту можно обратиться только посредством ДИ. Разные интерфейсы могут предоставлять разные методы и быть доступными для разных объектов.

Каждый контейнер позволяет опросить набор ДИ объектов-компонентов, удовлетворяющих некоторому условию. Возвращаемый результат в общем случае зависит от вызывающего объекта.

Объекты изолированы друг от друга. Единственным видом межобъектного взаимодействия является вызов метода. Предполагается, что используются надежные средства аутентификации и защиты коммуникаций. В плане разграничения доступа локальные и удаленные вызовы не различаются.

Предполагается также, что разрешение или запрет на доступ не зависят от возможного параллельного выполнения методов (синхронизация представляет отдельную проблему, которая здесь не рассматривается).

Разграничивается доступ к интерфейсам объектов, а также к методам объектов (с учетом значений фактических параметров вызова). Правила разграничения доступа (ПРД) задаются в виде предикатов над объектами.

Рассматривается задача разграничения доступа для выделенного контейнера СС, компонентами которого должны являться вызывающий и/или вызываемый объекты. ДИ этого контейнера полагается общеизвестным. Считается также, что между внешними по отношению к выделенному контейнеру объектами возможны любые вызовы.

Выполнение ПРД контролируется монитором обращений.

При вызове метода мы будем разделять действия, производимые вызывающим объектом (инициация вызова) и вызываемым методом (прием и завершение вызова).

При инициации вызова может производиться преобразование ДИ фактических параметров к виду, доступному вызываемому методу ("трансляция интерфейса"). Трансляция может иметь место, если вызываемый объект не входит в тот же контейнер, что и вызывающий.

Параметры методов могут быть входными и/или выходными. При приеме вызова возникает информационный поток из входных параметров в вызываемый объект. В момент завершения вызова возникает информационный поток из вызываемого объекта в выходные параметры. Эти потоки могут фигурировать в правилах разграничения доступа. Структурируем множество всех ПРД, выделив четыре группы правил:

- политика безопасности контейнера;

- ограничения на вызываемый метод;
- ограничения на вызывающий метод;
- добровольно налагаемые ограничения.

Правила, общие для всех объектов, входящих в контейнер С, назовем политикой безопасности данного контейнера.

Пусть метод М1 объекта О1 в точке Р1 своего выполнения должен вызвать метод М объекта О. Правила, которым должен удовлетворять М, можно разделить на три следующие подгруппы:

- правила, описывающие требования к формальным параметрам вызова;
- правила, описывающие требования к семантике М;
- реализационные правила, накладывающие ограничения на возможные реализации М;
- правила, накладывающие ограничения на вызываемый объект О.

Метод М объекта О, потенциально доступный для вызова, может предъявлять к вызываемому объекту следующие группы требований:

- правила, описывающие требования к фактическим параметрам вызова;
- правила, накладывающие ограничения на вызывающий объект.

Можно выделить три разновидности предикатов, соответствующих семантике и/или особенностям реализации методов:

- утверждения о фактических параметрах вызова метода М в точке Р1;
- предикат, описывающий семантику метода М;
- предикат, описывающий особенности реализации метода М.

Перечисленные ограничения можно назвать добровольными, поскольку они соответствуют реальному поведению объектов и не связаны с какими-либо внешними требованиями.

Предложенная постановка задачи разграничения доступа соответствует современному этапу развития программирования, она позволяет выразить сколь угодно сложную политику безопасности, найти баланс между богатством выразительных возможностей и эффективностью работы монитора обращений.

3.6. *Протоколирование и аудит*

Основные понятия

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

Аудит - это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Протоколирование требует для своей реализации здравого смысла. Какие события регистрировать? С какой степенью детализации? На подобные вопросы невозможно дать универсальные ответы. Необходимо следить за тем, чтобы, с одной стороны, достигались перечисленные выше цели, а, с другой, расход ресурсов оставался в пределах допустимого. Слишком обширное или подробное протоколирование не только снижает производительность сервисов (что отрицательно сказывается на доступности), но и затрудняет аудит, то есть не увеличивает, а уменьшает информационную безопасность.

Разумный подход к упомянутым вопросам применительно к операционным системам предлагается в "Оранжевой книге", где выделены следующие события:

- вход в систему (успешный или нет);
- выход из системы;
- обращение к удаленной системе;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).

При протоколировании события рекомендуется записывать, по крайней мере, следующую информацию:

- дата и время события;
- уникальный идентификатор пользователя - инициатора действия;
- тип события;
- результат действия (успех или неудача);
- источник запроса (например, имя терминала);
- имена затронутых объектов (например, открываемых или удаляемых файлов);
- описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

Еще одно важное понятие, фигурирующее в "Оранжевой книге", - выборочное протоколирование, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Характерная особенность протоколирования и аудита - зависимость от других средств безопасности. Идентификация и аутентификация служат отправной точкой подотчетности пользователей, логическое управление доступом защищает конфиденциальность и целостность регистрационной информации. Возможно, для защиты привлекаются и криптографические методы.

Возвращаясь к целям протоколирования и аудита, отметим, что обеспечение подотчетности важно в первую очередь как сдерживающее средство. Если пользователи и администраторы знают, что все их действия фиксируются, они, возможно, воздержатся от незаконных операций. Очевидно, если есть основания подозревать какого-либо пользователя в нечестности, можно регистрировать все его действия, вплоть до каждого нажатия клавиши. При этом обеспечивается не только возможность расследования случаев нарушения режима безопасности, но и откат некорректных изменений (если в протоколе присутствуют данные до и после модификации). Тем самым защищается целостность информации.

Реконструкция последовательности событий позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе.

Обнаружение попыток нарушений информационной безопасности - функция активного аудита, о котором пойдет речь в следующем разделе. Обычный аудит позволяет выявить подобные попытки с опозданием, но и это оказывается полезным. В свое время поимка немецких хакеров, действовавших по заказу КГБ, началась с выявления подозрительного расхождения в несколько центов в ежедневном отчете крупного вычислительного центра.

Выявление и анализ проблем могут помочь улучшить такой параметр безопасности, как доступность. Обнаружив узкие места, можно попытаться переконфигурировать или перенастроить систему, снова измерить производительность и т.д.

Непросто осуществить организацию согласованного протоколирования и аудита в распределенной разнородной системе. Во-первых, некоторые компоненты, важные для безопасности (например, маршрутизаторы), могут не обладать своими ресурсами протоколирования; в таком случае их нужно экранировать другими сервисами, которые возьмут протоколирование на себя. Во-вторых, необходимо увязывать между собой события в разных сервисах.

3.7. Активный аудит

Основные понятия

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Задача активного аудита - оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее.

Активность, не соответствующую политике безопасности, целесообразно разделить на атаки, направленные на незаконное получение полномочий, и на действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности.

Атаки нарушают любую осмысленную политику безопасности. Иными словами, активность атакующего является разрушительной независимо от политики. Следовательно, для описания и выявления атак можно применять универсальные методы, инвариантные относительно политики безопасности, такие как сигнатуры и их обнаружение во входном потоке событий с помощью аппарата экспертных систем.

Сигнатура атаки - это совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию. Простейший пример сигнатуры - "зафиксированы три последовательные неудачные попытки входа в систему с одного терминала", пример ассоциированной реакции - блокирование терминала до прояснения ситуации.

Действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности, мы будем называть злоупотреблением полномочиями. Злоупотребления полномочиями возможны из-за неадекватности средств разграничения доступа выбранной политике безопасности. Простейшим примером злоупотреблений является неэтичное поведение суперпользователя, просматривающего личные файлы других пользователей. Анализируя регистрационную информацию, можно обнаружить подобные события и сообщить о них администратору безопасности, хотя для этого необходимы соответствующие средства выражения политики безопасности.

Выделение злоупотреблений полномочиями в отдельную группу неправомерных действий, выявляемых средствами активного аудита, не является общепринятым, однако, на наш взгляд, подобный подход имеет право на существование и мы будем его придерживаться, хотя наиболее радикальным решением было бы развитие средств разграничения доступа (см. "Возможный подход к управлению доступом в распределенной объектной среде").

Нетипичное поведение выявляется статистическими методами. В простейшем случае применяют систему порогов, превышение которых является подозрительным. (Впрочем, "пороговый" метод можно трактовать и как вырожденный случай сигнатуры атаки, и как тривиальный способ выражения политики безопасности.) В более развитых системах производится сопоставление долговременных характеристик работы (называемых долгосрочным профилем) с краткосрочными профилями. (Здесь можно усмотреть аналогию биометрической аутентификации по поведенческим характеристикам.)

Применительно к средствам активного аудита различают ошибки первого и второго рода: пропуск атак и ложные тревоги, соответственно. Нежелательность ошибок первого рода очевидна; ошибки второго рода не менее неприятны, поскольку отвлекают администратора безопасности от действительно важных дел, косвенно способствуя пропуску атак.

Достоинства сигнатурного метода - высокая производительность, малое число ошибок второго рода, обоснованность решений. Основной недостаток - неумение обнаруживать неизвестные атаки и вариации известных атак.

Основные достоинства статистического подхода - универсальность и обоснованность решений, потенциальная способность обнаруживать неизвестные атаки, то есть минимизация числа ошибок первого рода. Минусы заключаются в относительно высокой доле ошибок второго рода, плохой работе в случае, когда неправомерное поведение является типичным, когда типичное поведение плавно меняется от легального к неправомерному, а также в случаях, когда типичного поведения нет (как показывает статистика, таких пользователей примерно 5-10%).

Средства активного аудита могут располагаться на всех линиях обороны информационной системы. На границе контролируемой зоны они могут обнаруживать подозрительную активность в точках подключения к внешним сетям (не только попытки нелегального проникновения, но и действия по "прощупыванию" сервисов безопасности). В корпоративной сети, в рамках информационных сервисов и сервисов безопасности, активный аудит в состоянии обнаружить и пресечь подозрительную активность внешних и внутренних пользователей, выявить проблемы в работе сервисов, вызванные как нарушениями безопасности, так и аппаратно-программными ошибками. Важно отметить, что активный аудит, в принципе, способен обеспечить защиту от атак на доступность.

К сожалению, формулировка "в принципе, способен обеспечить защиту" не случайна. Активный аудит развивается более десяти лет, и первые результаты казались весьма многообещающими. Довольно быстро удалось реализовать распознавание простых типовых атак, однако затем было выявлено множество проблем, связанных с обнаружением заранее неизвестных атак, атак распределенных, растянутых во времени и т.п. Было бы наивно ожидать полного решения подобных проблем в ближайшее время. (Оперативное пополнение базы сигнатур атак таким решением, конечно, не является.) Тем не менее, и на нынешней стадии развития активный аудит полезен как один из рубежей (вернее, как набор прослоек) эшелонированной обороны.

Функциональные компоненты и архитектура

В составе средств активного аудита можно выделить следующие функциональные компоненты:

- компоненты генерации регистрационной информации. Они находятся на стыке между средствами активного аудита и контролируруемыми объектами;
- компоненты хранения сгенерированной регистрационной информации;
- компоненты извлечения регистрационной информации (сенсоры). Обычно различают сетевые и хостовые сенсоры, имея в виду под первыми выделенные компьютеры, сетевые карты которых установлены в режим прослушивания, а под вторыми - программы, читающие регистрационные журналы операционной системы. На наш взгляд, с развитием коммутационных технологий это различие постепенно стирается, так как сетевые сенсоры приходится устанавливать в активном сетевом оборудовании и, по сути, они становятся частью сетевой ОС;
- компоненты просмотра регистрационной информации. Могут помочь при принятии решения о реагировании на подозрительную активность;
- компоненты анализа информации, поступившей от сенсоров. В соответствии с данным выше определением средств активного аудита, выделяют пороговый анализатор, анализатор нарушений политики безопасности, экспертную систему, выявляющую сигнатуры атак, а также статистический анализатор, обнаруживающий нетипичное поведение;
- компоненты хранения информации, участвующей в анализе. Такое хранение необходимо, например, для выявления атак, протяженных во времени;
- компоненты принятия решений и реагирования ("решатели"). "Решатель" может получать информацию не только от локальных, но и от внешних анализаторов, проводя так называемый корреляционный анализ распределенных событий;
- компоненты хранения информации о контролируемых объектах. Здесь могут храниться как пассивные данные, так и методы, необходимые, например, для извлечения из объекта регистрационной информации или для реагирования;
- компоненты, играющие роль организующей оболочки для менеджеров активного аудита, называемые мониторами и объединяющие анализаторы, "решатели", хранилище описаний объектов и интерфейсные компоненты. В число последних входят компоненты интерфейса с другими мониторами, как равноправными, так и входящими в иерархию. Такие интерфейсы необходимы, например, для выявления распределенных, широкомасштабных атак;
- компоненты интерфейса с администратором безопасности.

Средства активного аудита строятся в архитектуре менеджер/агент. Основными агентскими компонентами являются сенсоры. Анализ, принятие решений - функции менеджеров. Очевидно, между менеджерами и агентами должны быть сформированы доверенные каналы.

Подчеркнем важность интерфейсных компонентов. Они полезны как с внутренней для средств активного аудита точки зрения (обеспечивают расширяемость, подключение компонентов различных производителей), так и с внешней точки зрения. Между менеджерами (между компонентами анализа и "решателями") могут существовать горизонтальные связи, необходимые для анализа распределенной активности. Возможно также формирование иерархий средств активного аудита с вынесением на верхние уровни информации о наиболее масштабной и опасной активности.

Обратим также внимание на архитектурную общность средств активного аудита и управления, являющуюся следствием общности выполняемых функций. Продуманные интерфейсные компоненты могут существенно облегчить совместную работу этих средств.

3.8. Шифрование

Мы приступаем к рассмотрению криптографических сервисов безопасности, точнее, к изложению элементарных сведений, помогающих составить общее представление о компьютерной криптографии и ее месте в общей архитектуре информационных систем.

Криптография необходима для реализации, по крайней мере, трех сервисов безопасности:

- шифрование;
- контроль целостности;
- аутентификация (этот сервис был рассмотрен нами ранее).

Шифрование - наиболее мощное средство обеспечения конфиденциальности. Во многих отношениях оно занимает центральное место среди программно-технических регуляторов безопасности, являясь основой реализации многих из них, и в то же время последним (а подчас и единственным) защитным рубежом. Например, для портативных компьютеров только шифрование позволяет обеспечить конфиденциальность данных даже в случае кражи.

В большинстве случаев и шифрование, и контроль целостности играют глубоко инфраструктурную роль, оставаясь прозрачными и для приложений, и для пользователей. Типичное место этих сервисов безопасности - на сетевом и транспортном уровнях реализации стека сетевых протоколов.

Различают два основных метода шифрования: симметричный и асимметричный. В первом из них один и тот же ключ (хранящийся в секрете) используется и для зашифрования, и для расшифрования данных. Разработаны весьма эффективные (быстрые и надежные) методы симметричного шифрования. Существует и национальный стандарт на подобные методы - ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это создает новую проблему распространения ключей. С другой стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно.

В асимметричных методах используются два ключа. Один из них, несекретный (он может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой (секретный, известный только получателю) - для расшифрования. Самым популярным из асимметричных является метод RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (скажем, 100-значными) простыми числами и их произведениями. Проиллюстрируем использование асимметричного шифрования (см. рис. 8.1).



Рис. 8.1. Использование асимметричного метода шифрования

Существенным недостатком асимметричных методов шифрования является их низкое быстродействие, поэтому данные методы приходится сочетать с симметричными (асимметричные методы на 3 - 4 порядка медленнее). Так, для решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Рис. 8.2 иллюстрирует эффективное шифрование, реализованное путем сочетания симметричного и асимметричного методов.

На рис. 8.3 показано расшифрование эффективно зашифрованного сообщения.

Отметим, что асимметричные методы позволили решить важную задачу совместной выработки секретных ключей (это существенно, если стороны не доверяют друг другу), обслуживающих сеанс взаимодействия, при изначальном отсутствии общих секретов. Для этого используется алгоритм Диффи-Хелмана.



Рис. 8.2. Эффективное шифрование сообщения.

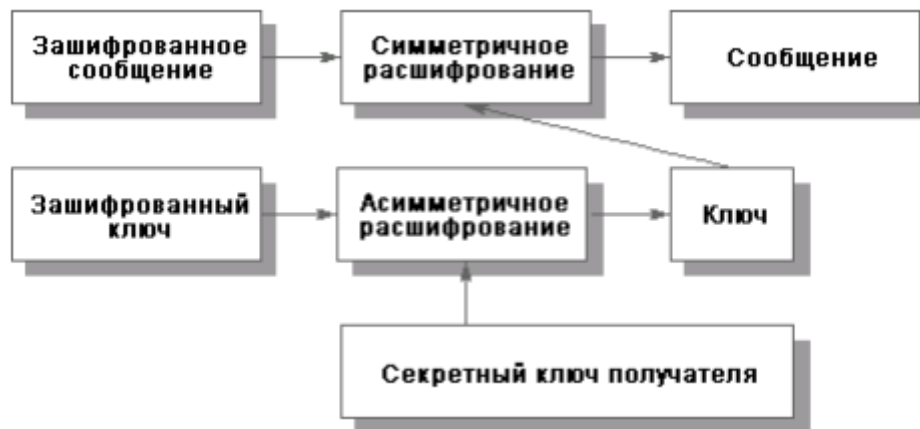


Рис. 8.3. Расшифрование эффективно зашифрованного сообщения.

Определенное распространение получила разновидность симметричного шифрования, основанная на использовании составных ключей. Идея состоит в том, что секретный ключ делится на две части, хранящиеся отдельно. Каждая часть сама по себе не позволяет выполнить расшифрование. Если у правоохранительных органов появляются подозрения относительно лица, использующего некоторый ключ, они могут в установленном порядке получить половинки ключа и дальше действовать обычным для симметричного расшифрования образом.

Порядок работы с составными ключами - хороший пример следования принципу разделения обязанностей. Он позволяет сочетать права на разного рода тайны (персональную, коммерческую) с возможностью эффективно следить за нарушителями закона, хотя, конечно, здесь очень много тонкостей и технического, и юридического плана.

Многие криптографические алгоритмы в качестве одного из параметров требуют псевдослучайное значение, в случае предсказуемости которого в алгоритме появляется уязвимость (подобное уязвимое место было обнаружено в некоторых вариантах Web-навигаторов). Генерация псевдослучайных последовательностей - важный аспект криптографии, на котором мы, однако, останавливаться не будем.

Более подробную информацию о компьютерной криптографии можно почерпнуть из статьи Г. Семенова "Не только шифрование, или Обзор криптотехнологий" (Jet Info, 2001, 3).

3.9. Контроль целостности

Криптографические методы позволяют надежно контролировать целостность как отдельных порций данных, так и их наборов (таких как поток сообщений); определять подлинность источника данных; гарантировать невозможность отказать от совершенных действий ("неотказуемость").

В основе криптографического контроля целостности лежат два понятия:

- хэш-функция;
- электронная цифровая подпись (ЭЦП).

Хэш-функция - это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Пусть имеются данные, целостность которых нужно проверить, хэш-функция и ранее вычисленный результат ее применения к исходным данным (так называемый дайджест). Обозначим хэш-функцию через h , исходные данные - через T , проверяемые данные - через T' . Контроль целостности данных сводится к проверке равенства $h(T') = h(T)$. Если оно выполнено, считается, что $T' = T$. Совпадение дайджестов для различных данных называется коллизией. В принципе, коллизии, конечно, возможны, поскольку мощность множества дайджестов меньше, чем мощность множества хэшируемых данных, однако то, что h есть функция односторонняя, означает, что за приемлемое время специально организовать коллизию невозможно.

Рассмотрим теперь применение асимметричного шифрования для выработки и проверки электронной цифровой подписи. Пусть $E(T)$ обозначает результат зашифрования текста T с помощью открытого ключа, а $D(T)$ - результат расшифрования текста T (как правило, зашифрованного) с помощью секретного ключа. Чтобы асимметричный метод мог применяться для реализации ЭЦП, необходимо выполнение тождества $E(D(T)) = D(E(T)) = T$

На рис. 8.4 показана процедура выработки электронной цифровой подписи, состоящая в шифровании преобразованием D дайджеста $h(T)$



Рис. 8.4. Выработка электронной цифровой подписи

Проверка ЭЦП может быть реализована так, как показано на рис. 8.5.



Рис. 8.5. Проверка электронной цифровой подписи.

Из равенства $E(S') = h(T')$ следует, что $S' = D(h(T'))$ (для доказательства достаточно применить к обеим частям преобразование D и вычеркнуть в левой части тождественное преобразование $D(E())$). Таким образом, электронная цифровая подпись защищает целостность сообщения и удостоверяет личность отправителя, то есть защищает целостность источника данных и служит основой неотказуемости.

Два российских стандарта, ГОСТ Р 34.10-94 "Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма" и ГОСТ Р 34.8-94 "Функция хэширования", объединенные общим заголовком "Информационная технология. Криптографическая защита информации", регламентируют вычисление дайджеста и реализацию ЭЦП. В сентябре 2001 года был утвержден, а 1 июля 2002 года вступил в силу новый стандарт ЭЦП - ГОСТ Р 34.10-2001, разработанный специалистами ФАПСИ.

Для контроля целостности последовательности сообщений (то есть для защиты от кражи, дублирования и переупорядочения сообщений) применяют временные штампы и нумерацию элементов последовательности, при этом штампы и номера включают в подписываемый текст.

Цифровые сертификаты

При использовании асимметричных методов шифрования (и, в частности, электронной цифровой подписи) необходимо иметь гарантию подлинности пары (имя пользователя, открытый ключ пользователя). Для решения этой задачи в спецификациях X.509 вводятся понятия цифрового сертификата и удостоверяющего центра.

Удоверяющий центр - это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится удоверяющими центрами в виде цифровых сертификатов, имеющих следующую структуру:

- порядковый номер сертификата;
- идентификатор алгоритма электронной подписи;
- имя удоверяющего центра;
- срок годности;
- имя владельца сертификата (имя пользователя, которому принадлежит сертификат);
- открытые ключи владельца сертификата (ключей может быть несколько);
- идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;
- электронная подпись, сгенерированная с использованием секретного ключа удоверяющего центра (подписывается результат хэширования всей информации, хранящейся в сертификате).

Цифровые сертификаты обладают следующими свойствами:

- любой пользователь, знающий открытый ключ удоверяющего центра, может узнать открытые ключи других клиентов центра и проверить целостность сертификата;
- никто, кроме удоверяющего центра, не может модифицировать информацию о пользователе без нарушения целостности сертификата.

В спецификациях X.509 не описывается конкретная процедура генерации криптографических ключей и управления ими, однако даются некоторые общие рекомендации. В частности, оговаривается, что пары ключей могут порождаться любым из следующих способов.

- ключи может генерировать сам пользователь. В таком случае секретный ключ не попадает в руки третьих лиц, однако нужно решать задачу безопасной связи с удостоверяющим центром;
- ключи генерирует доверенное лицо. В таком случае приходится решать задачи безопасной доставки секретного ключа владельцу и предоставления доверенных данных для создания сертификата;
- ключи генерируются удостоверяющим центром. В таком случае остается только задача безопасной передачи ключей владельцу.

Цифровые сертификаты в формате X.509 версии 3 стали не только формальным, но и фактическим стандартом, поддерживаемым многочисленными удостоверяющими центрами.

3.10. Экранирование

Основные понятия

Формальная постановка задачи экранирования состоит в следующем. Пусть имеется два множества информационных систем. Экран - это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем (рис. 9.1). Контроль потоков состоит в их фильтрации, возможно, с выполнением некоторых преобразований.

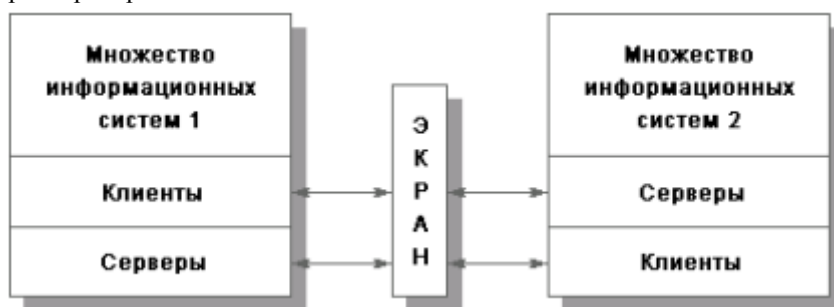


Рис. 9.1. Экран как средство разграничения доступа.

На следующем уровне детализации экран (полупроницаемую мембрану) удобно представлять как последовательность фильтров. Каждый из фильтров, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за экран. Кроме того, допускается преобразование данных, передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю (рис. 9.2).



Рис. 9.2. Экран как последовательность фильтров.

Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны (МЭ) (предложенный автором перевод английского термина firewall) чаще всего устанавливаются для защиты корпоративной сети организации, имеющей выход в Internet (см. следующий раздел).

Экранирование помогает поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности в ИС организации. Подчеркнем, что экранирование может использоваться как сервис безопасности не только в сетевой, но и в любой другой среде, где происходит обмен сообщениями. Важнейший пример подобной среды - объектно-

ориентированные программные системы, когда для активизации методов объектов выполняется (по крайней мере, в концептуальном плане) передача сообщений. Весьма вероятно, что в будущих объектно-ориентированных средах экранирование станет одним из важнейших инструментов разграничения доступа к объектам.

Экранирование может быть частичным, защищающим определенные информационные сервисы. Экранирование электронной почты описано в статье "Контроль над корпоративной электронной почтой: система "Дозор-Джет"" (Jet Info, 2002, 5).

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый пользователь видит лишь то, что ему положено видеть. Можно провести аналогию между динамически формируемыми гипертекстовыми документами и представлениями в реляционных базах данных, с той существенной оговоркой, что в случае Web возможности существенно шире.

Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, например таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация данных.

Архитектурные аспекты

Бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС - это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для нелегального получения привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений. Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.). Единственный перспективный путь связан с разработкой специализированных сервисов безопасности, которые в силу своей простоты допускают формальную или неформальную верификацию.

Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов. Межсетевой экран располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети). В первом случае говорят о внешнем МЭ, во втором - о внутреннем. В зависимости от точки зрения, внешний межсетевой экран можно считать первой или последней (но никак не единственной) линией обороны. Первой - если посмотреть на мир глазами внешнего злоумышленника. Последней - если стремиться к защищенности всех компонентов корпоративной сети и пресечению неправомерных действий внутренних пользователей.

Межсетевой экран - идеальное место для встраивания средств активного аудита. С одной стороны, и на первом, и на последнем защитном рубеже выявление подозрительной активности по-своему важно. С другой стороны, МЭ способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой. Правда, нужно отдавать себе отчет в том, что соединение двух сервисов безопасности в принципе может создать брешь, способствующую атакам на доступность.

На межсетевой экран целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

В силу принципов эшелонированности обороны для защиты внешних подключений обычно используется двухкомпонентное экранирование (см. рис. 9.3). Первичная фильтрация (например, блокирование пакетов управляющего протокола SNMP, опасного атаками на доступность, или пакетов с определенными IP-адресами, включенными в "черный список") осуществляется граничным маршрутизатором (см. также следующий раздел), за которым располагается так называемая демилитаризованная зона (сеть с умеренным доверием безопасности, куда выносятся внешние информационные сервисы организации - Web, электронная почта и т.п.) и основной МЭ, защищающий внутреннюю часть корпоративной сети.

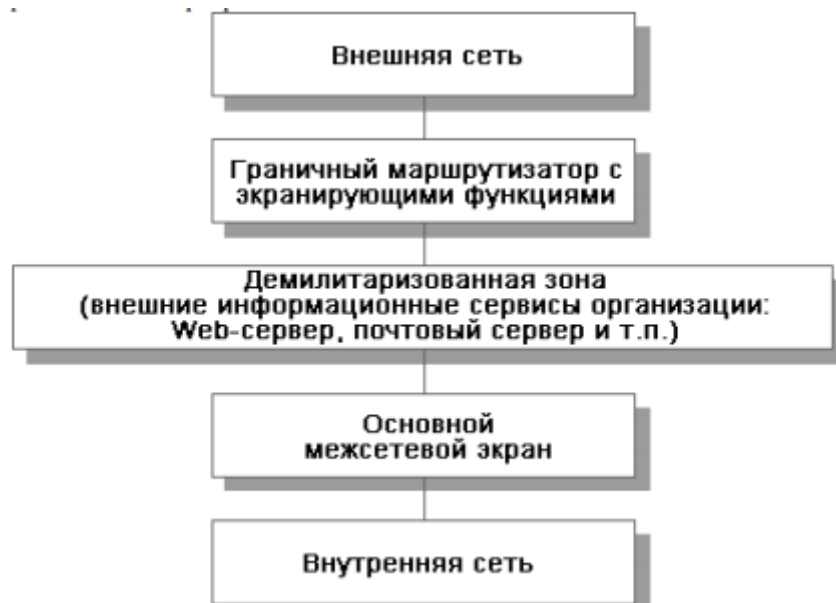


Рис. 9.3. Двухкомпонентное экранирование с демилитаризованной зоной.

Теоретически межсетевой экран (особенно внутренний) должен быть многопротокольным, однако на практике доминирование семейства протоколов TCP/IP столь велико, что поддержка других протоколов представляется излишеством, вредным для безопасности (чем сложнее сервис, тем он более уязвим).

Вообще говоря, и внешний, и внутренний межсетевой экран может стать узким местом, поскольку объем сетевого трафика имеет тенденцию быстрого роста. Один из подходов к решению этой проблемы предполагает разбиение МЭ на несколько аппаратных частей и организацию специализированных серверов-посредников. Основной межсетевой экран может проводить грубую классификацию входящего трафика по видам и передоверять фильтрацию соответствующим посредникам (например, посреднику, анализирующему HTTP-трафик). Исходящий трафик сначала обрабатывается сервером-посредником, который может выполнять и функционально полезные действия, такие как кэширование страниц внешних Web-серверов, что снижает нагрузку на сеть вообще и основной МЭ в частности.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, являются скорее исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к Internet. В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний межсетевой экран является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

Противоположностью составным корпоративным МЭ (или их компонентами) являются персональные межсетевые экраны и персональные экранирующие устройства. Первые являются программными продуктами, которые устанавливаются на персональные компьютеры и защищают только их. Вторые реализуются на отдельных устройствах и защищают небольшую локальную сеть, такую как сеть домашнего офиса.

При развертывании межсетевых экранов следует соблюдать рассмотренные нами ранее принципы архитектурной безопасности, в первую очередь позаботившись о простоте и управляемости, об эшелонированности обороны, а также о невозможности перехода в небезопасное состояние. Кроме того, следует принимать во внимание не только внешние, но и внутренние угрозы.

Классификация межсетевых экранов

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. Межсетевые экраны также целесообразно классифицировать по уровню фильтрации - каналному, сетевому, транспортному или прикладному. Соответственно, можно говорить об экранирующих концентраторах (мостах, коммутаторах) (уровень 2), маршрутизаторах (уровень 3), о транспортном экранировании (уровень 4) и о прикладных экранах (уровень 7). Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

Фильтрация информационных потоков осуществляется межсетевыми экранами на основе набора правил, являющихся выражением сетевых аспектов политики безопасности организации. В этих правилах, помимо информации, содержащейся в фильтруемых потоках, могут фигурировать данные, полученные из окружения, например, текущее время, количество активных соединений, порт, через который поступил сетевой запрос, и т.д. Таким образом, в межсетевых экранах используется очень мощный логический подход к разграничению доступа.

Возможности межсетевого экрана непосредственно определяются тем, какая информация может использоваться в правилах фильтрации и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует МЭ, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее он может быть сконфигурирован.

Экранирующие маршрутизаторы (и концентраторы) имеют дело с отдельными пакетами данных, поэтому иногда их называют пакетными фильтрами. Решения о том, пропустить или задержать данные, принимаются для каждого пакета независимо, на основании анализа адресов и других полей заголовков сетевого (канального)

и, быть может, транспортного уровня. Еще один важный компонент анализируемой информации - порт, через который поступил пакет.

Экранирующие концентраторы являются средством не столько разграничения доступа, сколько оптимизации работы локальной сети за счет организации так называемых виртуальных локальных сетей. Последние можно считать важным результатом применения внутреннего межсетевого экранирования.

Современные маршрутизаторы позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе, так и на выходе. В принципе, в качестве пакетного фильтра может использоваться и универсальный компьютер, снабженный несколькими сетевыми картами.

Основные достоинства экранирующих маршрутизаторов - доступная цена (на границе сетей маршрутизатор нужен практически всегда, вопрос лишь в том, как задействовать его экранирующие возможности) и прозрачность для более высоких уровней модели OSI. Основным недостатком - ограниченность анализируемой информации и, как следствие, относительная слабость обеспечиваемой защиты.

Транспортное экранирование позволяет контролировать процесс установления виртуальных соединений и передачу информации по ним. С точки зрения реализации экранирующей транспорт представляет собой довольно простую, а значит, надежную программу.

По сравнению с пакетными фильтрами, транспортное экранирование обладает большей информацией, поэтому соответствующий МЭ может осуществлять более тонкий контроль за виртуальными соединениями (например, он способен отслеживать количество передаваемой информации и разрывать соединения после превышения определенного порога, препятствуя тем самым несанкционированному экспорту информации). Аналогично, возможно накопление более содержательной регистрационной информации. Главный недостаток - сужение области применения, поскольку вне контроля остаются датаграммные протоколы. Обычно транспортное экранирование применяют в сочетании с другими подходами, как важный дополнительный элемент.

Межсетевой экран, функционирующий на прикладном уровне, способен обеспечить наиболее надежную защиту. Как правило, подобный МЭ представляет собой универсальный компьютер, на котором функционируют экранирующие агенты, интерпретирующие протоколы прикладного уровня (HTTP, FTP, SMTP, telnet и т.д.) в той степени, которая необходима для обеспечения безопасности.

При использовании прикладных МЭ, помимо фильтрации, реализуется еще один важнейший аспект экранирования. Субъекты из внешней сети видят только шлюзовую компьютер; соответственно, им доступна только та информация о внутренней сети, которую он считает нужным экспортировать. Прикладной МЭ на самом деле экранирует, то есть заслоняет, внутреннюю сеть от внешнего мира. В то же время, субъектам внутренней сети кажется, что они напрямую общаются с объектами внешнего мира. Недостаток прикладных МЭ - отсутствие полной прозрачности, требующее специальных действий для поддержки каждого прикладного протокола.

Если организация располагает исходными текстами прикладного МЭ и в состоянии эти тексты модифицировать, перед ней открываются чрезвычайно широкие возможности по настройке экрана с учетом собственных нужд. Дело в том, что при разработке систем клиент/сервер в многозвенной архитектуре появляются специфические прикладные протоколы, нуждающиеся в защите не меньше стандартных. Подход, основанный на использовании экранирующих агентов, позволяет построить такую защиту, не снижая безопасности и эффективности других приложений и не усложняя структуру связей в межсетевом экране.

Комплексные межсетевые экраны, охватывающие уровни от сетевого до прикладного, соединяют в себе лучшие свойства "одноуровневых" МЭ разных видов. Защитные функции выполняются комплексными МЭ прозрачным для приложений образом, не требуя внесения каких-либо изменений ни в существующее программное обеспечение, ни в действия, ставшие для пользователей привычными.

Комплексность МЭ может достигаться разными способами: "снизу вверх", от сетевого уровня через накопление контекста к прикладному уровню, или "сверху вниз", посредством дополнения прикладного МЭ механизмами транспортного и сетевого уровней.

Помимо выразительных возможностей и допустимого количества правил, качество межсетевого экрана определяется еще двумя очень важными характеристиками - простотой использования и собственной защищенностью. В плане простоты использования первостепенное значение имеют наглядный интерфейс при определении правил фильтрации и возможность централизованного администрирования составных конфигураций. В свою очередь, в последнем аспекте хотелось бы выделить средства централизованной загрузки правил фильтрации и проверки набора правил на непротиворечивость. Важен и централизованный сбор и анализ регистрационной информации, а также получение сигналов о попытках выполнения действий, запрещенных политикой безопасности.

Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. Имеется в виду физическая защита, идентификация и аутентификация, разграничение доступа, контроль целостности, протоколирование и аудит. При выполнении централизованного администрирования следует также позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность. Крайне важно оперативное наложение заплат, ликвидирующих выявленные уязвимые места МЭ.

Хотелось бы подчеркнуть, что природа экранирования как сервиса безопасности очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Мощным методом сокрытия информации является трансляция "внутренних" сетевых адресов, которая попутно решает проблему расширения адресного пространства, выделенного организации.

Отметим также следующие дополнительные возможности межсетевых экранов:

- контроль информационного наполнения (антивирусный контроль "на лету", верификация Java-апплетов, выявление ключевых слов в электронных сообщениях и т.п.);
- выполнение функций ПО промежуточного слоя.

Особенно важным представляется последний из перечисленных аспектов. ПО промежуточного слоя, как и традиционные межсетевые экраны прикладного уровня, скрывает информацию о предоставляемых услугах. За счет этого оно может выполнять такие функции, как маршрутизация запросов и балансировка нагрузки. Представляется вполне естественным, чтобы эти возможности были реализованы в рамках межсетевого экрана. Это существенно упрощает действия по обеспечению высокой доступности экспортируемых сервисов и позволяет осуществлять переключение на резервные мощности прозрачным для внешних пользователей образом. В результате к услугам, традиционно предоставляемым межсетевыми экранами, добавляется поддержка высокой доступности сетевых сервисов.

Пример современного межсетевого экрана представлен в статье "Z-2 - универсальный межсетевой экран высшего уровня защиты" (Jet Info, 2002, 5).

3.11. Анализ защищенности

Сервис анализа защищенности предназначен для выявления уязвимых мест с целью их оперативной ликвидации. Сам по себе этот сервис ни от чего не защищает, но помогает обнаружить (и устранить) пробелы в защите раньше, чем их сможет использовать злоумышленник. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а "оперативные" бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Системы анализа защищенности (называемые также сканерами защищенности), как и рассмотренные выше средства активного аудита, основаны на накоплении и использовании знаний. В данном случае имеются в виду знания о пробелах в защите: о том, как их искать, насколько они серьезны и как их устранять.

Соответственно, ядром таких систем является база уязвимых мест, которая определяет доступный диапазон возможностей и требует практически постоянной актуализации.

В принципе, могут выявляться бреши самой разной природы: наличие вредоносного ПО (в частности, вирусов), слабые пароли пользователей, неудачно сконфигурированные операционные системы, небезопасные сетевые сервисы, неустановленные заплатки, уязвимости в приложениях и т.д. Однако наиболее эффективными являются сетевые сканеры (очевидно, в силу доминирования семейства протоколов TCP/IP), а также антивирусные средства. Антивирусную защиту мы причисляем к средствам анализа защищенности, не считая ее отдельным сервисом безопасности.

Сканеры могут выявлять уязвимые места как путем пассивного анализа, то есть изучения конфигурационных файлов, задействованных портов и т.п., так и путем имитации действий атакующего. Некоторые найденные уязвимые места могут устраняться автоматически (например, лечение зараженных файлов), о других сообщается администратору.

Системы анализа защищенности снабжены традиционным "технологическим сахаром": автообнаружением компонентов анализируемой ИС и графическим интерфейсом (помогающим, в частности, эффективно работать с протоколом сканирования).

С возможностями свободно распространяемого сканера Nessus можно ознакомиться, прочитав статью "Сканер защищенности Nessus: уникальное предложение на российском рынке" (Jet Info, 2000, 10).

Контроль, обеспечиваемый системами анализа защищенности, носит реактивный, запаздывающий характер, он не защищает от новых атак, однако следует помнить, что оборона должна быть эшелонированной, и в качестве одного из рубежей контроль защищенности вполне адекватен. Отметим также, что подавляющее большинство атак носит рутинный характер; они возможны только потому, что известные бреши в защите годами остаются неустраненными.

3.12. Обеспечение высокой доступности

Основные понятия

Информационная система предоставляет своим пользователям определенный набор услуг (сервисов). Говорят, что обеспечен нужный уровень доступности этих сервисов, если следующие показатели находятся в заданных пределах:

Эффективность услуг. Эффективность услуги определяется в терминах максимального времени обслуживания запроса, количества поддерживаемых пользователей и т.п. Требуется, чтобы эффективность не опускалась ниже заранее установленного порога.

Время недоступности. Если эффективность информационной услуги не удовлетворяет наложенным ограничениям, услуга считается недоступной. Требуется, чтобы максимальная продолжительность периода недоступности и суммарное время недоступности за некоторый период (месяц, год) не превышали заранее заданных пределов.

В сущности, требуется, чтобы информационная система почти всегда работала с нужной эффективностью. Для некоторых критически важных систем (например, систем управления) время недоступности должно быть нулевым, без всяких "почти". В таком случае говорят о вероятности возникновения ситуации недоступности и требуют, чтобы эта вероятность не превышала заданной величины. Для решения данной задачи создавались и создаются специальные отказоустойчивые системы, стоимость которых, как правило, весьма высока.

К подавляющему большинству коммерческих систем предъявляются менее жесткие требования, однако современная деловая жизнь и здесь накладывает достаточно суровые ограничения, когда число обслуживаемых пользователей может измеряться тысячами, время ответа не должно превышать нескольких секунд, а время недоступности - нескольких часов в год.

Задачу обеспечения высокой доступности необходимо решать для современных конфигураций, построенных в технологии клиент/сервер. Это означает, что в защите нуждается вся цепочка - от пользователей (возможно, удаленных) до критически важных серверов (в том числе серверов безопасности). Основные угрозы доступности были рассмотрены нами ранее.

В соответствии с ГОСТ 27.002, под отказом понимается событие, которое заключается в нарушении работоспособности изделия. В контексте данной работы изделие - это информационная система или ее компонент. В простейшем случае можно считать, что отказы любого компонента составного изделия ведут к общему отказу, а распределение отказов во времени представляет собой простой пуассоновский поток событий. В таком случае вводят понятие интенсивности отказов и среднего времени наработки на отказ, которые связаны между собой соотношением

$$T_i = 1/\lambda_i$$

где

i - номер компонента,

λ_i

- интенсивность отказов,

T_i

- среднее время наработки на отказ.

Интенсивности отказов независимых компонентов складываются:

$$\lambda = \lambda_1 + \dots + \lambda_n$$

а среднее время наработки на отказ для составного изделия задается соотношением

$$T = 1/\lambda$$

Уже эти простейшие выкладки показывают, что если существует компонент, интенсивность отказов которого много больше, чем у остальных, то именно он определяет среднее время наработки на отказ всей информационной системы. Это является теоретическим обоснованием принципа первоочередного укрепления самого слабого звена.

Пуассоновская модель позволяет обосновать еще одно очень важное положение, состоящее в том, что эмпирический подход к построению систем высокой доступности не может быть реализован за приемлемое время. При традиционном цикле тестирования/отладки программной системы по оптимистическим оценкам каждое исправление ошибки приводит к экспоненциальному убыванию (примерно на половину десятичного порядка) интенсивности отказов. Отсюда следует, что для того, чтобы на опыте убедиться в достижении необходимого уровня доступности, независимо от применяемой технологии тестирования и отладки, придется потратить время, практически равное среднему времени наработки на отказ. Например, для достижения среднего времени наработки на отказ 105 часов потребуется более 104,5 часов, что составляет более трех лет. Значит, нужны иные методы построения систем высокой доступности, методы, эффективность которых доказана аналитически или практически за более чем пятьдесят лет развития вычислительной техники и программирования.

Пуассоновская модель применима в тех случаях, когда информационная система содержит одиночные точки отказа, то есть компоненты, выход которых из строя ведет к отказу всей системы. Для исследования систем с резервированием применяется иной формализм

В соответствии с постановкой задачи будем считать, что существует количественная мера эффективности предоставляемых изделием информационных услуг. В таком случае вводятся понятия показателей эффективности отдельных элементов и эффективности функционирования всей сложной системы.

В качестве меры доступности можно принять вероятность приемлемости эффективности услуг, предоставляемых информационной системой, на всем протяжении рассматриваемого отрезка времени. Чем большим запасом эффективности располагает система, тем выше ее доступность.

При наличии избыточности в конфигурации системы вероятность того, что в рассматриваемый промежуток времени эффективность информационных сервисов не опустится ниже допустимого предела, зависит не только от вероятности отказа компонентов, но и от времени, в течение которого они остаются неработоспособными, поскольку при этом суммарная эффективность падает, и каждый следующий отказ может стать фатальным. Чтобы максимально увеличить доступность системы, необходимо минимизировать время неработоспособности каждого компонента. Кроме того, следует учитывать, что, вообще говоря, ремонтные работы могут потребовать понижения эффективности или даже временного отключения работоспособных компонентов; такого рода влияние также необходимо минимизировать.

Несколько терминологических замечаний. Обычно в литературе по теории надежности вместо доступности говорят о готовности (в том числе о высокой готовности). Мы предпочли термин "доступность", чтобы подчеркнуть, что информационный сервис должен быть не просто "готов" сам по себе, но доступен для своих пользователей в условиях, когда ситуации недоступности могут вызываться причинами, на первый взгляд не имеющими прямого отношения к сервису (пример - отсутствие консультационного обслуживания).

Далее, вместо времени недоступности обычно говорят о коэффициенте готовности. Нам хотелось обратить внимание на два показателя - длительность однократного простоя и суммарную продолжительность простоев, поэтому мы предпочли термин "время недоступности" как более емкий.

3.13. Основы мер обеспечения высокой доступности

Основной мер повышения доступности является применение структурированного подхода, нашедшего воплощение в объектно-ориентированной методологии. Структуризация необходима по отношению ко всем аспектам и составным частям информационной системы - от архитектуры до административных баз данных, на всех этапах ее жизненного цикла - от инициации до выведения из эксплуатации. Структуризация, важная сама по себе, является одновременно необходимым условием практической реализуемости прочих мер повышения доступности. Только маленькие системы можно строить и эксплуатировать как угодно. У больших систем свои законы, которые, как мы уже указывали, программисты впервые осознали более 30 лет назад.

При разработке мер обеспечения высокой доступности информационных сервисов рекомендуется руководствоваться следующими архитектурными принципами, рассматривавшимися ранее:

- апробированность всех процессов и составных частей информационной системы;
- унификация процессов и составных частей;
- управляемость процессов, контроль состояния частей;
- автоматизация процессов;
- модульность архитектуры;
- ориентация на простоту решений.

Доступность системы в общем случае достигается за счет применения трех групп мер, направленных на повышение:

- безотказности (под этим понимается минимизация вероятности возникновения какого-либо отказа; это элемент пассивной безопасности, который дальше рассматриваться не будет);
- отказоустойчивости (способности к нейтрализации отказов, "живучести", то есть способности сохранять требуемую эффективность, несмотря на отказы отдельных компонентов);
- обслуживаемости (под обслуживаемостью понимается минимизация времени простоя отказавших компонентов, а также отрицательного влияния ремонтных работ на эффективность информационных сервисов, то есть быстрое и безопасное восстановление после отказов).

Главное при разработке и реализации мер обеспечения высокой доступности - полнота и систематичность. В этой связи представляется целесообразным составить (и поддерживать в актуальном состоянии) карту информационной системы организации (на что мы уже обращали внимание), в которой фигурировали бы все объекты ИС, их состояние, связи между ними, процессы, ассоциируемые с объектами и связями. С помощью подобной карты удобно формулировать намечаемые меры, контролировать их исполнение, анализировать состояние ИС.

3.14. Отказоустойчивость и зона риска

Информационную систему можно представить в виде графа сервисов, ребра в котором соответствуют отношению "сервис А непосредственно использует сервис В".

Пусть в результате осуществления некоторой атаки (источником которой может быть как человек, так и явление природы) выводится из строя подмножество сервисов S_1 (то есть эти сервисы в результате нанесенных повреждений становятся неработоспособными). Назовем S_1 зоной поражения.

В зону риска S мы будем включать все сервисы, эффективность которых при осуществлении атаки падает ниже допустимого предела. Очевидно, S_1 - подмножество S . S строго включает S_1 , когда имеются сервисы, непосредственно не затронутые атакой, но критически зависящие от пораженных, то есть неспособные переключиться на использование эквивалентных услуг либо в силу отсутствия таковых, либо в силу невозможности доступа к ним. Например, зона поражения может сводиться к одному порту концентратора, обслуживающему критичный сервер, а зона риска охватывает все рабочие места пользователей сервера.

Чтобы система не содержала одиночных точек отказа, то есть оставалась "живучей" при реализации любой из рассматриваемых угроз, ни одна зона риска не должна включать в себя предоставляемые услуги. Нейтрализацию отказов нужно выполнять внутри системы, незаметно для пользователей, за счет размещения достаточного количества избыточных ресурсов.

С другой стороны, естественно соизмерять усилия по обеспечению "живучести" с рассматриваемыми угрозами. Когда рассматривается набор угроз, соответствующие им зоны поражения могут оказаться вложенными, так что "живучесть" по отношению к более серьезной угрозе автоматически влечет за собой и "живучесть" в более легких случаях. Следует учитывать, однако, что обычно стоимость переключения на резервные ресурсы растет вместе с увеличением объема этих ресурсов. Значит, для наиболее вероятных угроз целесообразно минимизировать зону риска, даже если предусмотрена нейтрализация объемлющей угрозы. Нет смысла переключаться на резервный вычислительный центр только потому, что у одного из серверов вышел из строя блок питания.

Зону риска можно трактовать не только как совокупность ресурсов, но и как часть пространства, затрагиваемую при реализации угрозы. В таком случае, как правило, чем больше расстояние дублирующего ресурса от границ зоны риска, тем выше стоимость его поддержания, поскольку увеличивается протяженность линий связи, время переброски персонала и т.п. Это еще один довод в пользу адекватного противодействия угрозам, который следует принимать во внимание при размещении избыточных ресурсов и, в частности, при организации резервных центров.

Введем еще одно понятие. Назовем зоной нейтрализации угрозы совокупность ресурсов, вовлеченных в нейтрализацию отказа, возникшего вследствие реализации угрозы. Имеются в виду ресурсы, режим работы которых в случае отказа изменяется. Очевидно, зона риска является подмножеством зоны нейтрализации. Чем меньше разность между ними, тем экономичнее данный механизм нейтрализации.

Все, что находится вне зоны нейтрализации, отказа "не чувствует" и может трактовать внутренность этой зоны как безотказную. Таким образом, в иерархически организованной системе грань между "живучестью" и

обслуживаемостью, с одной стороны, и безотказностью, с другой стороны, относительно. Целесообразно конструировать целостную информационную систему из компонентов, которые на верхнем уровне можно считать безотказными, а вопросы "живучести" и обслуживаемости решать в пределах каждого компонента.

Обеспечение отказоустойчивости

Основным средством повышения "живучести" является внесение избыточности в конфигурацию аппаратных и программных средств, поддерживающей инфраструктуры и персонала, резервирование технических средств и тиражирование информационных ресурсов (программ и данных).

Меры по обеспечению отказоустойчивости можно разделить на локальные и распределенные. Локальные меры направлены на достижение "живучести" отдельных компьютерных систем или их аппаратных и программных компонентов (в первую очередь с целью нейтрализации внутренних отказов ИС). Типичные примеры подобных мер - использование кластерных конфигураций в качестве платформы критичных серверов или "горячее" резервирование активного сетевого оборудования с автоматическим переключением на резерв.

Если в число рассматриваемых рисков входят серьезные аварии поддерживающей инфраструктуры, приводящие к выходу из строя производственной площадки организации, следует предусмотреть распределенные меры обеспечения живучести, такие как создание или аренда резервного вычислительного центра. При этом, помимо дублирования и/или тиражирования ресурсов, необходимо предусмотреть средства автоматического или быстрого ручного переконфигурирования компонентов ИС, чтобы обеспечить переключение с основной площадки на резервную.

Аппаратура - относительно статичная составляющая, однако было бы ошибкой полностью отказываться ей в динамичности. В большинстве организаций информационные системы находятся в постоянном развитии, поэтому на протяжении всего жизненного цикла ИС следует соотносить все изменения с необходимостью обеспечения "живучести", не забывая "тиражировать" новые и модифицированные компоненты.

Программы и данные более динамичны, чем аппаратура, и резервироваться они могут постоянно, при каждом изменении, после завершения некоторой логически замкнутой группы изменений или по истечении определенного времени.

Резервирование программ и данных может выполняться многими способами - за счет зеркалирования дисков, резервного копирования и восстановления, репликации баз данных и т.п. Будем использовать для всех перечисленных способов термин "тиражирование".

Выделим следующие классы тиражирования:

- Симметричное/асимметричное. Тиражирование называется симметричным, если все серверы, предоставляющие данный сервис, могут изменять принадлежащую им информацию и передавать изменения другим серверам. В противном случае тиражирование называется асимметричным.

- Синхронное/асинхронное. Тиражирование называется синхронным, если изменение передается всем экземплярам сервиса в рамках одной распределенной транзакции. В противном случае тиражирование называется асинхронным.

- Осуществляемое средствами сервиса, хранящего информацию/внешними средствами.

Рассмотрим, какие способы тиражирования предпочтительнее.

Безусловно, следует предпочесть стандартные средства тиражирования, встроенные в сервис.

Асимметричное тиражирование теоретически проще симметричного, поэтому целесообразно выбрать асимметрию.

Труднее всего выбрать между синхронным и асинхронным тиражированием. Синхронное идейно проще, но его реализация может быть тяжеловесной и сложной, хотя это внутренняя сложность сервиса, невидимая для приложений. Асинхронное тиражирование устойчивее к отказам в сети, оно меньше влияет на работу основного сервиса.

Чем надежнее связь между серверами, вовлеченными в процесс тиражирования, чем меньше время, отводимое на переключение с основного сервера на резервный, чем жестче требования к актуальности информации, тем более предпочтительным оказывается синхронное тиражирование.

С другой стороны, недостатки асинхронного тиражирования могут компенсироваться процедурными и программными мерами, направленными на контроль целостности информации в распределенной ИС. Сервисы, входящие в состав ИС, в состоянии обеспечить ведение и хранение журналов транзакций, с помощью которых можно выявлять операции, утерянные при переключении на резервный сервер. Даже в условиях неустойчивой связи с удаленными филиалами организации подобная проверка в фоновом режиме займет не более нескольких часов, поэтому асинхронное тиражирование может использоваться практически в любой ИС.

Асинхронное тиражирование может производиться на сервер, работающий в режиме "горячего" резерва, возможно, даже обслуживающего часть пользовательских запросов, или на сервер, работающий в режиме "теплого" резерва, когда изменения периодически "накапываются", но сам резервный сервер запросов не обслуживает.

Достоинство "теплого" резервирования в том, что его можно реализовать, оказывая меньшее влияние на основной сервер. Это влияние вообще может быть сведено к нулю, если асинхронное тиражирование осуществляется путем передачи инкрементальных копий с основного сервера (резервное копирование необходимо выполнять в любом случае).

Основной недостаток "теплого" резерва состоит в длительном времени включения, что может быть неприемлемо для "тяжелых" серверов, таких как кластерная конфигурация сервера СУБД. Здесь необходимо проводить измерения в условиях, близких к реальным.

Второй недостаток "теплого" резерва вытекает из опасности малых изменений. Может оказаться, что в самый нужный момент срочный перевод резерва в штатный режим невозможен.

Учитывая приведенные соображения, следует в первую очередь рассматривать возможность "горячего" резервирования, либо тщательно контролировать использование "теплого" резерва и регулярно (не реже одного раза в неделю) проводить пробные переключения резерва в "горячий" режим.

3.15. Программное обеспечение промежуточного слоя

С помощью программного обеспечения промежуточного слоя (ПО ПС) можно для произвольных прикладных сервисов добиться высокой "живучести" с полностью прозрачным для пользователей переключением на резервные мощности.

О возможностях и свойствах ПО промежуточного слоя можно прочитать в статье Ф. Бернштейна "Middleware: модель сервисов распределенной системы" (Jet Info, 1997, 11).

Перечислим основные достоинства ПО ПС, существенные для обеспечения высокой доступности.

- ПО ПС уменьшает сложность создания распределенных систем. Подобное ПО берет на себя часть функций, которые в локальном случае выполняют операционные системы;

- ПО ПС берет на себя маршрутизацию запросов, позволяя тем самым обеспечить "живучесть" прозрачным для пользователей образом;

- ПО ПС осуществляет балансировку загрузки вычислительных мощностей, что также способствует повышению доступности данных;

- ПО ПС в состоянии осуществлять тиражирование любой информации, а не только содержимого баз данных. Следовательно, любое приложение можно сделать устойчивым к отказам серверов;

- ПО ПС в состоянии отслеживать состояние приложений и при необходимости тиражировать и перезапускать программы, что гарантирует "живучесть" программных систем;

- ПО ПС дает возможность прозрачным для пользователей образом выполнять переконфигурирование (и, в частности, наращивание) серверных компонентов, что позволяет масштабировать систему, сохраняя инвестиции в прикладные системы. Стабильность прикладных систем - важный фактор повышения доступности данных.

Ранее мы упоминали о достоинствах использования ПО ПС в рамках межсетевых экранов, которые в таком случае становятся элементом обеспечения отказоустойчивости предоставляемых информационных сервисов.

3.16. Обеспечение обслуживаемости

Меры по обеспечению обслуживаемости направлены на снижение сроков диагностирования и устранения отказов и их последствий.

Для обеспечения обслуживаемости рекомендуется соблюдать следующие архитектурные принципы:

- ориентация на построение информационной системы из унифицированных компонентов с целью упрощения замены отказавших частей;

- ориентация на решения модульной структуры с возможностью автоматического обнаружения отказов, динамического переконфигурирования аппаратных и программных средств и замены отказавших компонентов в "горячем" режиме.

Динамическое переконфигурирование преследует две основные цели:

- изоляция отказавших компонентов;

- сохранение работоспособности сервисов.

Изолированные компоненты образуют зону поражения реализованной угрозы. Чем меньше соответствующая зона риска, тем выше обслуживаемость сервисов. Так, при отказах блоков питания, вентиляторов и/или дисков в современных серверах зона риска ограничивается отказавшим компонентом; при отказах процессорных модулей весь сервер может потребовать перезагрузки (что способно вызвать дальнейшее расширение зоны риска). Очевидно, в идеальном случае зоны поражения и риска совпадают, и современные серверы и активное сетевое оборудование, а также программное обеспечение ведущих производителей весьма близки к этому идеалу.

Возможность программирования реакции на отказ также повышает обслуживаемость систем. Каждая организация может выбрать свою стратегию реагирования на отказы тех или иных аппаратных и программных компонентов и автоматизировать эту реакцию. Так, в простейшем случае возможна отправка сообщения системному администратору, чтобы ускорить начало ремонтных работ; в более сложном случае может быть реализована процедура "мягкого" выключения (переключения) сервиса, чтобы упростить обслуживание.

Возможность удаленного выполнения административных действий - важное направление повышения обслуживаемости, поскольку при этом ускоряется начало восстановительных мероприятий, а в идеале все работы (обычно связанные с обслуживанием программных компонентов) выполняются в удаленном режиме, без перемещения квалифицированного персонала, то есть с высоким качеством и в кратчайшие сроки. Для современных систем возможность удаленного администрирования - стандартное свойство, но важно позаботиться о его практической реализуемости в условиях разнородности конфигураций (в первую очередь клиентских). Централизованное распространение и конфигурирование программного обеспечения, управление компонентами информационной системы и диагностирование - надежный фундамент технических мер повышения обслуживаемости. Существенный аспект повышения обслуживаемости - организация консультационной службы для пользователей (обслуживаемость пользователей), внедрение программных систем для работы этой службы, обеспечение достаточной пропускной способности каналов связи с пользователями, в том числе в режиме пиковых нагрузок.

4.3. Лабораторные работы

<i>№ п/п</i>	<i>Номер раздела дисциплины</i>	<i>Наименование лабораторной работы</i>	<i>Объем (час.)</i>	<i>Вид занятия в интерактивной, активной, инновационной формах, (час.)</i>
1	3.	Программирование арифметических алгоритмов	3	Работа в малых группах (2 часа)
2		Программирование алгебраических алгоритмов	3	-
3		Защита от закладок при разработке программ	3	-
4		Программирование алгоритмов криптосистем с открытым ключом	4	-
5		Профилактика заражения вирусами компьютерных систем	4	-
ИТОГО			17	2

4.4. Практические занятия

<i>№ п/п</i>	<i>Номер раздела дисциплины</i>	<i>Наименование практической работы</i>	<i>Объем (час.)</i>	<i>Вид занятия в интерактивной, активной, инновационной формах, (час.)</i>
1	3.	Криптографические методы защиты	3	Работа в малых группах (2 часа)
2		Шифрование методом IDEA	3	-
3		Шифрование методом RC6	3	-
4		Шифрование методом Джиффорда	3	-
5		Шифрование методом аналитических преобразований	3	-
6		Соккрытие информации методом стеганографии	2	-
ИТОГО			17	2

4.5. Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат:

Учебным планом не предусмотрено

5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

<i>№, наименование разделов дисциплины</i>	<i>Кол-во часов</i>	<i>Компетенции</i>		<i>Σ комп.</i>	<i>t_{ср}, час</i>	<i>Вид учебных занятий</i>	<i>Оценка результатов</i>
		<i>ПК</i>	<i>ОПК</i>				
		<i>2</i>	<i>9</i>				
1	2	3	4	5	6	7	8
1. Введение в информационную безопасность.	11	+	+	2	11	Лк, СРС	ЗАЧЕТ
2. Уровни информационной безопасности.	11	+	+	2	11	Лк, СРС	ЗАЧЕТ
3. Основные программно-технические меры информационной безопасности сетей и систем.	86	+	+	2	86	Лк, ЛР, ПЗ, СРС	ЗАЧЕТ
<i>всего часов</i>	108	54	54	2	108		

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Степанов, Е. А. Информационная безопасность и защита информации : учебное пособие / Е. А. Степанов, И. К. Корнеев. - Москва : Инфра-М, 2001. - 304 с.
2. Информационные технологии : учебник / Под ред. В. В. Трофимова. - Москва : Юрайт, 2011. - 624 с.

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№	<i>Наименование издания</i>	<i>Вид занятия</i> (ЛК, ЛР, ПЗ, КП, КР, кр)	<i>Количество экземпляров в библиотеке, шт.</i>	<i>Обеспеченность, (экз./ чел.)</i>
1	2	3	4	5
Основная литература				
1.	Правовое обеспечение информационной безопасности : учебное пособие для вузов / Под ред. С. Я. Казанцева. - 2-е изд., испр. и доп. - Москва : Академия, 2007. - 240 с.	ЛК, ЛР, ПЗ	15	1
2.	Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.	ЛК, ЛР, ПЗ, кр	31	1
3	Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=363040 (11.04.2017).	ЛК, ЛР, ПЗ	ЭР	1
4	Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.	ЛК, ЛР, ПЗ, кр	16	1
Дополнительная литература				
5	Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия- Телеком, 2012. - 320 с.	ЛК, ЛР, ПЗ, кр	5	0,3
6	Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.	ЛК, ЛР, ПЗ, кр	5	0,3

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронный каталог библиотеки БрГУ
[http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=.](http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=)
2. Электронная библиотека БрГУ
<http://ecat.brstu.ru/catalog>.
3. Электронно-библиотечная система «Университетская библиотека online»
<http://biblioclub.ru>.
4. Электронно-библиотечная система «Издательство «Лань»
<http://e.lanbook.com>.
5. Информационная система "Единое окно доступа к образовательным ресурсам"
<http://window.edu.ru>.
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>.
7. Университетская информационная система РОССИЯ (УИС РОССИЯ)
<https://uisrussia.msu.ru/>.
8. Национальная электронная библиотека НЭБ
<http://xn--90ax2c.xn--p1ai/how-to-search/>.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

9.1. Методические указания для обучающихся по выполнению лабораторных работ/практических работ

Лабораторная работа №1

Программирование арифметических алгоритмов

Цель работы:

Исследование и разработка основных методов симметричных криптосистем.

Задание:

1. Изучить основы криптографии
2. Познакомиться с некоторыми арифметическими алгоритмами криптографии.

Порядок выполнения:

1. Изучить теоретические основы.
2. Изучить шифр перестановки.
3. Изучить шифр одиночной перестановки.
4. Изучить шифр двойной перестановки.
5. Изучить шифрование при помощи магического квадрата.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной

дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.
3. Правовое обеспечение информационной безопасности : учебное пособие для вузов / Под ред. С. Я. Казанцева. - 2-е изд., испр. и доп. - Москва : Академия, 2007. - 240 с.

Дополнительная литература

1. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. В чем заключается главная задача криптографии?
2. В чем особенность шифра перестановки?
3. В чем особенность шифра одиночной перестановки?
4. В чем особенность шифра двойной перестановки?
5. В чем особенность шифрования при помощи магического квадрата?

Лабораторная работа №2

Программирование алгебраических алгоритмов

Цель работы:

Исследование и разработка классических методов симметричных криптосистем

Задание:

1. Изучить принцип работы симметричных криптосистем.
2. Познакомиться с некоторыми алгебраическими способами криптографии..

Порядок выполнения:

1. Изучить теоретические основы
2. Изучить шифр простой замены. Система шифрования Цезаря.
3. Изучить шифр сложной замены. Шифр Гронсфелда.
4. Изучить шифр многоалфавитной замены.
5. Изучить способ Гаммирования

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр.

и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия-Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Шифр Гронсфельда.
2. Шифры двойной перестановки. Шифрование с помощью магического квадрата.
3. Шифр многоалфавитной замены и алгоритм его реализации.

Лабораторная работа №3

Защита от закладок при разработке программ

Цель работы:

Исследование и анализ служебных программ Windows для повышения эффективности работы компьютера.

Задание:

1. Установите проверку подлинности доступа к ресурсам компьютера из локальной сети. Запретите доступ к ресурсам вашего компьютера из Интернета.
2. Разрешить удаленный доступ к ресурсам вашего компьютера.
3. Использование удаленного доступа к сетевым ресурсам.
4. Защита и восстановление данных на компьютере.

Порядок выполнения:

1. Установите проверку подлинности доступа к ресурсам компьютера из локальной сети. Запретите доступ к ресурсам вашего компьютера из Интернета.
2. Разрешить удаленный доступ к ресурсам вашего компьютера.
3. Использование удаленного доступа к сетевым ресурсам.
4. Защита и восстановление данных на компьютере.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.
3. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А.

Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.

Контрольные вопросы для самопроверки

1. Почему при эксплуатации компьютерной системы важно знать ее параметры?
2. Какие стандартные средства Windows XP обеспечивают пользователю возможность определения параметров компьютерной системы?
3. Почему обеспечение бесперебойной работы дисковой системы компьютера является одной из основных мер обеспечения информационной безопасности?
4. Опишите причины нарушений в работе магнитных дисков.
5. Почему необходима процедура очистки диска?
6. Что такое фрагментация файла? Почему она возникает и как влияет на скорость операций чтения информации с диска?
7. В каких случаях рекомендуется выполнить дефрагментацию диска?
8. С какой целью выполняется архивация данных компьютера?
9. Что такое дискета аварийного восстановления? Какой программой она создается?

Лабораторная работа №4

Программирование алгоритмов криптосистем с открытым ключом

Цель работы:

Исследование и анализ основных методов асимметричных криптосистем

Задание:

1. Изучить шифрования Эль Гамала.
2. Изучить шифрование данных RSA.

Порядок выполнения:

1. Зашифровать простое сообщение способом Эль Гамала.
2. Зашифровать текст при помощи шифрования данных RSA.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия-Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Алгоритм шифрации двойным квадратом. Шифр Enigma.
2. Алгоритм шифрования DES.
3. Алгоритм шифрования ГОСТ 28147-89.
4. Алгоритм шифрования RSA.
5. Алгоритм шифрования Эль Гамала.
6. Задачи и алгоритмы электронной подписи.
7. Задачи распределения ключей.

Лабораторная работа №5

Профилактика заражения вирусами компьютерных систем

Цель работы:

Анализ и исследование антивирусных программ.

Задание:

1. Познакомиться с работой антивирусных программ.

Порядок выполнения:

1. Изучить теоретические основы.
2. Ознакомится с энциклопедией компьютерных вирусов на сайте лаборатории Касперского.
3. Проверить на присутствие вирусов всех критических областей компьютера.
4. Поиск вирусов на вашем компьютере с тщательной проверкой всех подключенных дисков, памяти, файлов .
5. Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.
6. Поиск на компьютере руткитов, обеспечивающих сокрытие вредоносных программ в операционной системе.
7. Изучить дополнительные возможности программы Norton AntiVirus по защите данных.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.

2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия-Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы?
2. По каким признакам классифицируют компьютерные вирусы? Перечислите типы вирусов.
3. Какие вирусы называются резидентными и в чем особенность таких вирусов?
4. Каковы отличия вирусов-репликаторов, стелс - вирусов, мутантов и «тройных» программ?
5. Опишите схему функционирования загрузочного вируса.
6. Опишите схему функционирования файлового вируса.
7. Опишите схему функционирования загрузочно-файловых вирусов.
8. Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным?

Практическое занятие №1

Криптографические методы защиты

Цель работы:

Познакомиться с криптографическими методами защиты.

Задание:

1. Изучить классификацию криптографических методов защиты.
2. Изучить основные определения.

Порядок выполнения:

Изучить теоретические данные. Изучить классификацию криптографических методов защиты. Изучить основные определения.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Изучение новейших методов криптографической защиты информации.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.
3. Правовое обеспечение информационной безопасности : учебное пособие для вузов / Под ред. С. Я. Казанцева. - 2-е изд., испр. и доп. - Москва : Академия, 2007. - 240 с.

Дополнительная литература

1. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Что такое шифрование?
2. Чем отличается открытый ключ от закрытого?
3. Дать определение стеганографии.

Практическое занятие №2 **Шифрование методом IDEA**

Цель работы:

Приобрести навыки работы с методом шифрования IDEA.

Задание:

1. Изучить методом шифрования IDEA.

Порядок выполнения:

Изучить теоретические данные. Изучить описание алгоритма. Познакомиться с блок-схемой метода.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Найти современные области применения данного способа шифрования.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия- Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Что является входной информацией для шифра IDEA?
2. Сколько нужно циклов шифрования для достаточной степени сокрытия информации?
3. На сколько блоков делится входная информация?

Практическое занятие №3 **Шифрование методом RC6**

Цель работы:

Приобрести навыки работы с методом шифрования RC6.

Задание:

1. Познакомиться с шифрованием методом RC6.

Порядок выполнения:

Изучить теоретические данные. Изучить описание алгоритма. Познакомиться с блок-схемой метода. Изучить процедуры: шифрования, дешифрования и генерации ключа.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Найти современные области применения данного способа шифрования.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Что является входной информацией для шифра RC6?
2. Сколько нужно циклов шифрования для достаточной степени сокрытия информации?
3. На сколько блоков делиться входная информация?

Практическое занятие №4

Шифрование методом Джиффорда.

Приобрести навыки работы с методом шифрования Джиффорда

Задание:

1. Познакомиться с шифрованием методом Джиффорда.

Порядок выполнения:

Изучить теоретические данные. Изучить описание алгоритма. Познакомиться с блок-схемой метода.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Найти современные области применения данного способа шифрования.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной

дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.
3. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с

Дополнительная литература

1. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Принцип действия метода шифрования Джибфорда?
2. Для каких целей использовался данный метода шифрования?
3. В каком году он был взломан?

Практическое занятие №5

Шифрование методом аналитических преобразований.

Цель работы:

Познакомиться с методами аналитически преобразования для сокрытия информации..

Задание:

1. Познакомиться с методами аналитических преобразований.

Порядок выполнения:

Изучить теоретические данные. Изучить описание алгоритмов.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Найти современные области применения данного способа шифрования.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия- Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Дать определение аналитическим преобразованиям.
2. В каких случаях могут быть использованы аналитические преобразования?
3. К какой информации этот вид шифрования может быть применим?

Практическое занятие №6

Соккрытие информации методом стеганографии

Цель работы:

Познакомиться с методами стеганографии.

Задание:

1. Познакомиться с методами аналитических преобразований.

Порядок выполнения:

Изучить теоретические данные. Изучить описание современных методов стеганографии.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Найти современные области применения данного способа шифрования.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия- Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. В чем главный принцип стенографии?
2. В каких «контейнерах» может быть спрятано зашифрованное сообщение?
3. Привести примеры стеганографии древних времён.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Информационно-коммуникационные технологии (ИКТ) – преподаватель использует для:

- получения информации при подготовке к занятиям,
- создания презентационного сопровождения лекций;
- интерактивного общения;
- ОС Windows 7 Professional;
- Microsoft Office 2007 Russian Academic OPEN No Level ;
- Антивирусное программное обеспечение Kaspersky Security

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

<i>Вид занятия</i>	<i>Наименование аудитории</i>	<i>Перечень основного оборудования</i>	<i>№ ЛР или ПЗ</i>
1	2	3	4
ЛР	Лекционный кабинет/дисплейный класс	Персональные компьютеры	ЛР 1-5
ПЗ	Лекционный кабинет/дисплейный класс	Персональные компьютеры	ПЗ 1-6
СР	ЧЗЗ	-	-

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-2	Способностью проводить вычислительные эксперименты с использованием стандартных программных средств с целью получения математических моделей процессов и объектов автоматизации и управления	1. Введение в информационную безопасность.	1.1. Понятие информационной безопасности	Вопросы к зачету 1.1
			1.3. Важность и сложность проблемы информационной безопасности	Вопросы к зачету 1.3
			1.5. Некоторые примеры угроз доступности	Вопросы к зачету 1.5
			1.7. Основные угрозы целостности	Вопросы к зачету 1.7
		2. Уровни информационной безопасности.	2.1. Законодательный уровень информационной безопасности	Вопросы к зачету 2.1
			2.3. Обзор зарубежного законодательства в области информационной безопасности	Вопросы к зачету 2.3
			2.5. Политика безопасности	Вопросы к зачету 2.5
			2.7. Синхронизация программы безопасности с жизненным циклом систем	Вопросы к зачету 2.7.
			2.9. Управление персоналом	Вопросы к зачету 2.9.
			2.11. Поддержание работоспособности	Вопросы к зачету 2.11
			2.13. Планирование восстановительных работ	Вопросы к зачету 2.13
			3. Основные программно-технические меры информационной безопасности сетей и систем	3.1. Основные понятия программно-технического уровня информационной безопасности
		3.3. Архитектурная безопасность		Вопросы к зачету 3.3
		3.5. Управление доступом		Вопросы к зачету 3.5
		3.7. Активный аудит		Вопросы к зачету 3.7
		3.9. Контроль целостности		Вопросы к зачету 3.9
		3.11. Анализ защищенности		Вопросы к зачету 3.11
		3.13. Основы мер обеспечения высокой доступности		Вопросы к зачету 3.13
		ОПК-9	Способность использовать	1. Введение в

навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности	информационную безопасность.	1.4. Основные определения и критерии классификации угроз	Вопросы к зачету 1.4
		1.6. Вредоносное программное обеспечение	Вопросы к зачету 1.6
		1.8. Основные угрозы конфиденциальности	Вопросы к зачету 1.8
	2. Уровни информационной безопасности	2.2. Обзор российского законодательства в области информационной безопасности	Вопросы к зачету 2.2
		2.4. Административный уровень информационной безопасности	Вопросы к зачету 2.4
		2.6. Программа безопасности	Вопросы к зачету 2.6
		2.8. Процедурный уровень информационной безопасности	Вопросы к зачету 2.8
		2.10. Физическая защита	Вопросы к зачету 2.10
		2.12. Реагирование на нарушения режима безопасности	Вопросы к зачету 2.12
		3. Основные программно-технические меры информационной безопасности сетей и систем	3.2. Особенности современных информационных систем, существенные с точки зрения безопасности
	3.4. Идентификация и аутентификация		Вопросы к зачету 3.4
	3.6. Протоколирование и аудит		Вопросы к зачету 3.6
	3.8. Шифрование		Вопросы к зачету 3.8
	3.10. Экранирование		Вопросы к зачету 3.10
	3.12. Обеспечение высокой доступности		Вопросы к зачету 3.12
	3.14. Отказоустойчивость и зона риска		Вопросы к зачету 3.14
3.16. Обеспечение обслуживаемости	Вопросы к зачету 3.16		

2. Вопросы к зачету

№ п/п	Компетенции		ВОПРОСЫ К ЗАЧЕТУ	№ и наименование раздела
	Код	Определение		
1	2	3	4	5
1	ПК-2	Способность проводить вычислительные эксперименты с использованием стандартных программных средств с целью получения	1.1. Понятие информационной безопасности	1. Введение в информационную безопасность.
			1.3. Важность и сложность проблемы информационной безопасности	
			1.5. Некоторые примеры угроз доступности	
			1.7. Основные угрозы целостности	
			2.1. Законодательный уровень информационной безопасности	2. Уровни информационной

		математических моделей процессов и объектов автоматизации и управления	<p>2.3. Обзор зарубежного законодательства в области информационной безопасности</p> <p>2.5. Политика безопасности</p> <p>2.7. Синхронизация программы безопасности с жизненным циклом систем</p> <p>2.9. Управление персоналом</p> <p>2.11. Поддержание работоспособности</p> <p>2.13. Планирование восстановительных работ</p>	безопасности.
			<p>3.1. Основные понятия программно-технического уровня информационной безопасности</p> <p>3.3. Архитектурная безопасность</p> <p>3.5. Управление доступом</p> <p>3.7. Активный аудит</p> <p>3.9. Контроль целостности</p> <p>3.11. Анализ защищенности</p> <p>3.13. Основы мер обеспечения высокой доступности</p> <p>3.15. Программное обеспечение промежуточного слоя</p>	3. Основные программно-технические меры информационной безопасности сетей и систем
2	ОПК-9	Способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности	1.2. Основные составляющие информационной безопасности	1. Введение в информационную безопасность.
			1.4. Основные определения и критерии классификации угроз	
			1.6. Вредоносное программное обеспечение	
			1.8. Основные угрозы конфиденциальности	2. Уровни информационной безопасности.
			2.2. Обзор российского законодательства в области информационной безопасности	
			2.4. Административный уровень информационной безопасности	
			2.6. Программа безопасности	
			2.8. Процедурный уровень информационной безопасности	
			2.10. Физическая защита	
			2.12. Реагирование на нарушения режима безопасности	
			3.2. Особенности современных информационных систем, существенные с точки зрения безопасности	3. Основные программно-технические меры информационной безопасности сетей и систем
			3.4. Идентификация и аутентификация	
			3.6. Протоколирование и аудит	
			3.8. Шифрование	
3.10. Экранирование				

			3.12. Обеспечение высокой доступности	
			3.14. Отказоустойчивость и зона риска	
			3.16. Обеспечение обслуживаемости	

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
<p>Знать (ПК-2):</p> <ul style="list-style-type: none"> – Основные термины, используемые в научно-технической литературе по информационной безопасности. <p>(ОПК-9)</p> <ul style="list-style-type: none"> – основы цифровой вычислительной техники, структуры и функционирование локальных вычислительных сетей и глобальной сети Интернет, основные закономерности передачи информации в инфокоммуникационных системах, основные виды сигналов, используемых в телекоммуникационных системах, особенности передачи различных сигналов по каналам и тракам телекоммуникационных систем; <p>Уметь (ПК-2):</p> <ul style="list-style-type: none"> – формулировать основные технические требования к телекоммуникационным сетям и систем, оценивать основные проблемы, связанные с эксплуатацией и внедрением новой телекоммуникационной техники; <p>(ОПК-9)</p> <ul style="list-style-type: none"> – оценивать основные проблемы, связанные с эксплуатацией и внедрением новой вычислительной техники; <p>Владеть (ПК-2):</p> <ul style="list-style-type: none"> – начальными навыками разработки и отладки с использованием соответствующих отладочных средств программного обеспечения сигнальных процессов и микроконтроллеров. <p>(ОПК-9)</p> <ul style="list-style-type: none"> – начальными навыками разработки и отладки с использованием соответствующих отладочных средств программного обеспечения сигнальных процессов и микроконтроллеров. 	<p>Зачтено</p>	<p>Студент должен во время ответа показать знания: информационной безопасности, основные критерии защищённости, ключевые этапы обеспечения надежности сетей и систем, основных терминов используемые в научно-технической литературе по информационной безопасности. Студент должен иметь навыки владения: использования универсальных программных продуктов на ПК, понимания материала и способности высказывания мыслей на научно-техническом языке. Студент во время ответа должен продемонстрировать умения: использования навыков анализа основных аспектов и критериев защищенности.</p>
	<p>Не зачтено</p>	<p>На оба вопроса студент отвечает неубедительно. На дополнительные вопросы преподавателя также не может ответить.</p>

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Дисциплина основы информационной безопасности сете и систем направлена на ознакомление с информационной безопасностью, и её практическим применением в современных системах телекоммуникаций; на получение теоретических знаний и практических навыков различной работы с различными способами шифрования и

организации систем информационной безопасности для их дальнейшего использования в практической деятельности.

Изучение дисциплины информатика предусматривает:

- лекции,
- лабораторные работы,
- практические занятия,
- самостоятельную работу студента,
- зачет.

В ходе освоения раздела 1 «Введение в информационную безопасность» студенты должны изучить: понятие информационной безопасности, основные составляющие информационной безопасности, важность и сложность проблемы информационной безопасности, основные определения и критерии классификации угроз, некоторые примеры угроз доступности, вредоносное программное обеспечение, основные угрозы целостности, основные угрозы конфиденциальности.

В ходе освоения раздела 2 «Уровни информационной безопасности» студенты должны изучить: законодательный уровень информационной безопасности, обзор российского законодательства в области информационной безопасности, обзор зарубежного законодательства в области информационной безопасности, административный уровень информационной безопасности, политика безопасности, программа безопасности, синхронизация программы безопасности с жизненным циклом систем, процедурный уровень информационной безопасности, управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ.

В ходе освоения раздела 3 «Основные программно-технические меры информационной безопасности сетей и систем» студенты должны изучить: основные понятия программно-технического уровня информационной безопасности, особенности современных информационных систем, существенные с точки зрения безопасности, архитектурная безопасность, идентификация и аутентификация, управление доступом, протоколирование и аудит, активный аудит, шифрование, контроль целостности, экранирование, анализ защищенности, обеспечение высокой доступности, основы мер обеспечения высокой доступности, отказоустойчивость и зона риска, программное обеспечение промежуточного слоя, обеспечение обслуживаемости

В процессе проведения лабораторных работ происходит закрепление знаний, формирование умений и навыков реализации представления об различных способах шифрования информации.

В процессе проведения практических работ происходит закрепление знаний, формирование умений и навыков использования продвинутых методов шифрования и сокрытия информации

При подготовке к зачету рекомендуется особое внимание уделить следующим вопросам: законодательный уровень обеспечения безопасности, идентификация и аутентификация.

Работа с литературой является важнейшим элементом в получении знаний по дисциплине. Прежде всего, необходимо воспользоваться списком рекомендуемой по данной дисциплине литературой. Дополнительные сведения по изучаемым темам можно найти в периодической печати и Интернете.

АННОТАЦИЯ
рабочей программы дисциплины
Основы информационной безопасности сетей и систем

1. Цель и задачи дисциплины

Целью изучения дисциплины является: формирование у обучающихся знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и системах связи.

Задачей изучения дисциплины является: заложить методически правильные основы знаний, необходимые будущим специалистам по инфокоммуникационным технологиям и системам связи в области информационной безопасности.

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: Лк – 17 часов, ЛР – 17 часов, ПЗ – 17 часов, СРС – 57 часов.

Общая трудоемкость дисциплины составляет 108 часов, 3 зачетных единиц

2.2 Основные разделы дисциплины:

- 1 - Введение в информационную безопасность
- 2 - Различные уровни информационной безопасности
- 3 - Основные программно-технические меры информационной безопасности сетей и систем

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующей компетенции:

ПК-2 - Способность проводить вычислительные эксперименты с использованием стандартных программных средств с целью получения математических моделей процессов и объектов автоматизации и управления

ОПК-9 - Способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности.

4. Вид промежуточной аттестации: зачет

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО
КОНТРОЛЯ УСПЕВАЕМОСТИ ПО ДИСЦИПЛИНЕ**

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-2	Способность проводить вычислительные эксперименты с использованием стандартных программных средств с целью получения математических моделей процессов и объектов автоматизации и управления	3. Основные программно-технические меры информационной безопасности сетей и систем	3.5. Управление доступом	Отчеты по лабораторным работам
			3.7. Активный аудит	Отчеты по лабораторным работам
			3.9. Контроль целостности	Отчеты по лабораторным работам
			3.11. Анализ защищенности	Отчеты по лабораторным работам
			3.13. Основы мер обеспечения высокой доступности	Отчеты по лабораторным работам
ОПК-9	Способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности.	3. Основные программно-технические меры информационной безопасности сетей и систем	3.4. Идентификация и аутентификация	Отчеты по лабораторным работам
			3.6. Протоколирование и аудит	Отчеты по лабораторным работам
			3.8. Шифрование	Отчеты по лабораторным работам
			3.10. Экранирование	Отчеты по лабораторным работам
			3.12. Обеспечение высокой доступности	Отчеты по лабораторным работам

2. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
<p>Знать (ПК-2):</p> <ul style="list-style-type: none"> – Основные термины, используемые в научно-технической литературе по информационной безопасности. <p>(ОПК-9)</p> <ul style="list-style-type: none"> – основы цифровой вычислительной техники, структуры и функционирование локальных вычислительных сетей и глобальной сети Интернет, основные закономерности передачи информации в инфокоммуникационных системах, основные виды сигналов, используемых в телекоммуникационных системах, особенности передачи различных сигналов по каналам и тракам телекоммуникационных систем; 	<p>зачтено</p>	<p>Во время защиты лабораторных работ студент ответил на поставленные преподавателем вопросы. Студент показал знание терминов, основы функционирования локальных вычислительных сетей. Продемонстрировал владение навыками разработки и отладки программного обеспечения.</p>
<p>Уметь (ПК-2):</p> <ul style="list-style-type: none"> – формулировать основные технические требования к телекоммуникационным сетям и систем, оценивать основные проблемы, связанные с эксплуатацией и внедрением новой телекоммуникационной техники; <p>(ОПК-9)</p> <ul style="list-style-type: none"> – оценивать основные проблемы, связанные с эксплуатацией и внедрением новой вычислительной техники; <p>Владеть (ПК-2):</p> <ul style="list-style-type: none"> – начальными навыками разработки и отладки с использованием соответствующих отладочных средств программного обеспечения сигнальных процессов и микроконтроллеров. <p>(ОПК-9)</p> <ul style="list-style-type: none"> – начальными навыками разработки и отладки с использованием соответствующих отладочных средств программного обеспечения сигнальных процессов и микроконтроллеров. 		<p>не зачтено</p>