Стандарты информационной безопасности

Лекция-4.
Стандарт BS 7799

Стандарт BS 7799

Стандарт BS 7799 был разработаны BSI (British Standards Institution).

Они включают следующие три части:

1) **BS 7799-1** «Практические правила управления информационной безопасностью» (1995, 2005 гг.).

2) **BS 7799-2** «Системы управления информационной безопасностью. Спецификация и руководство по применению» (1998, 2002, 2005 гг.).

3) **BS 7799-3** «Руководство по управлению рисками информационной безопасности» (2005 г.).

Стандарты BS 7799

Стандарты являются базовыми для международных стандартов управления информационной безопасностью (СУИБ).

Таблица соответствия стандартов

Британский стандарт	Международный стандарт	Российский стандарт
BS 7799-1:2005	ISO 27002:2007 (ISO 17799:2005)	ГОСТ 17799:2005
BS 7799-2:2005	ISO 27001:2005	ГОСТ 27001:2005
BS 7799-3:2006	ISO 27005	Отсутствует

Стандарт BS 7799-1

Стандарт BS 7799-1 ««Системы управления информационной безопасностью. Спецификация и руководство по применению».

Он описывает 10 областей и 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определенных на основе лучших примеров мирового опыта в данной области.

Стандарт является руководством по созданию СУИБ.

Стандарт в большинстве своем предназначается для определения норм безопасности при ведении коммерческой деятельности.

Стандарт BS 7799-1

Цель ИБ – обеспечение бесперебойной работы организации, предотвращение/минимизация ущерба от нарушений безопасности.

Факторы, значимые для успешной реализации системы информационной безопасности в организации:

– цели безопасности и ее обеспечение должны основываться на производственных задачах и требованиях. Функции управления безопасностью должно взять на себя руководство организации;

– необходима явная поддержка и приверженность к соблюдению режима безопасности со стороны высшего руководства;

– требуется хорошее понимание рисков (как угроз, так и уязвимостей), которым подвергаются активы организации, и адекватное представление о ценности этих активов;

– необходимо ознакомление с системой безопасности всех руководителей и рядовых сотрудников организации.

Стандарт BS 7799-1

Выделяются следующие **регуляторы безопасности**:

– политика безопасности;

– общеорганизационные аспекты защиты;

– классификация активов и управление ими;

– безопасность персонала;

– физическая безопасность и безопасность окружающей среды;

– администрирование систем и сетей;

– управление доступом к системам и сетям;

– разработка и сопровождение информационных систем;

– управление бесперебойной работой организации;

– контроль соответствия требованиям.

Стандарт BS 7799-2

Стандарт BS 7799-2 «Системы управления информационной безопасностью. Спецификация и руководство по применению».

Предметом рассмотрения стандарта является **СУИБ**.

СУИБ должна включать следующие процессы:

– планирование;

– реализация;

– оценка;

– корректировка.

Во второй части стандарта подробно раскрываются регуляторы безопасности, представленные в первой части.

Стандарт BS 7799-2

1. Политика безопасности включает следующие компоненты:

– документально оформленная политика;

– процесс ревизии политики.

Стандарт BS 7799-2

2. Общеорганизационные аспекты включают три подгруппы:

1) инфраструктура ИБ:

– создание сообщества по управлению ИБ;

– меры по координации действий в области информационной безопасности;

– распределение обязанностей в области информационной безопасности;

– утверждение руководством новых средств обработки информации;

– получение рекомендаций специалистов по информационной безопасности;

– сотрудничество с другими организациями (правоохранительными органами, поставщиками информационных услуг и т. д.);

– проведение независимого анализа информационной безопасности.

Стандарт BS 7799-2

2. Общеорганизационные аспекты включают три подгруппы:

2) безопасность доступа сторонних организаций:

– идентификация рисков, связанных с подключениями сторонних организаций, и реализация соответствующих защитных мер;

– выработка требований безопасности для включения в контракты со сторонними организациями.

Стандарт BS 7799-2

2. Общеорганизационные аспекты включают три подгруппы:

3) обеспечение ИБ при использовании услуг внешних организаций.

Необходимо выработать требования безопасности для включения в контракты с поставщиками информационных услуг.

Стандарт BS 7799-2

3. Классификация активов и управление ими

Необходимым условием обеспечения надлежащей защиты активов является их идентификация и классификация.

Должны быть выработаны критерии классификации, в соответствии с которыми активы тем или иным способом получают метки безопасности.

Стандарт BS 7799-2

4. Безопасность персонала

Превентивные меры: документирование ролей и обязанностей в области информационной безопасности при определении требований ко всем должностям, тщательный отбор новых сотрудников.

Меры реагирования:

– уведомления об инцидентах, замеченных уязвимостях, нештатной работе программного обеспечения;

– механизм оценки ущерба от инцидентов и сбоев,

– дисциплинарные наказания виновных сотрудников.

Стандарт BS 7799-2

5. Физическая безопасность и безопасность окружающей среды

1) организация защищенных областей;

2) защита оборудования:

– размещать оборудование в защищенных областях;

– наладить бесперебойное электропитание;

– защитить кабельную разводку;

– организовать обслуживание оборудования;

– перемещать устройства (в том числе за пределы организации) только с разрешения руководства;

– удалять информацию перед выведением из эксплуатации или изменением характера использования оборудования.

3) меры общего характера.

Стандарт BS 7799-2

6. Администрирование систем и сетей

1) операционные процедуры и обязанности;

2) планирование и приемка систем;

3) защита от вредоносного программного обеспечения;

4) повседневное обслуживание;

5) администрирование сетей;

6) безопасное управление носителями;

7) обмен данными и программами с другими организациями.

Стандарт BS 7799-2

7. Управление доступом к системам и сетям

1) производственные требования к управлению доступом;

2) управление доступом пользователей:

– авторизация, выделение и контроль прав в соответствии с политикой безопасности;

– процедуры регистрации пользователей и ликвидации их системных счетов;

– управление привилегиями в соответствии с принципом их минимизации;

– управление паролями пользователей;

– регулярная ревизия прав доступа.

3) обязанности пользователей;

Стандарт BS 7799-2

7. Управление доступом к системам и сетям

4) управление доступом к сетям:

– политика использования сетевых услуг;

– задание маршрута от пользовательской системы до используемых систем (предоставление выделенных линий, недопущение неограниченного перемещения по сети и т. д.);

– аутентификация удаленных пользователей **и** удаленных систем;

– контроль доступа (особенно удаленного) к диагностическим портам;

– сегментация сетей (выделение групп пользователей, информационных сервисов и систем);

– контроль сетевых подключений (услуг и/или времени);

– управление маршрутизацией;

– защита сетевых сервисов (должны быть описаны атрибуты безопасности всех сетевых сервисов, используемых организацией).

Стандарт BS 7799-2

7. Управление доступом к системам и сетям

5) управление доступом средствами операционных систем:

– автоматическая идентификация терминалов;

– безопасные процедуры входа в систему (следует выдавать как можно меньше информации о системе, ограничить разрешаемое количество неудачных попыток, контролировать минимальную и максимальную продолжительность входа и т. и.);

– идентификация и аутентификация пользователей;

– управление паролями, контроль их качества;

– разграничение доступа к системным средствам;

– уведомление пользователей об опасных ситуациях;

– контроль времени простоя терминалов (с автоматическим отключением по истечении заданного периода);

– ограничение времени подключения к критичным приложениям.

Стандарт BS 7799-2

7. Управление доступом к системам и сетям

6) управление доступом к приложениям;

7) контроль за доступом и использованием систем:

– протоколирование событий, относящихся к безопасности;

– отслеживание и регулярный анализ использования средств обработки информации.

8) контроль мобильных пользователей и удаленного доступа.

Стандарт BS 7799-2

8. Разработка и сопровождение информационных систем

1) анализ и задание требований безопасности:

– управление доступом к информации и сервисам;

– протоколирование для повседневного контроля или специальных расследований;

– контроль и поддержание целостности данных на всех или избранных стадиях обработки;

– обеспечение конфиденциальности данных, возможно, с использованием криптографических средств;

– выполнение требований действующего законодательства, договорных требований и т. п.;

– резервное копирование производственных данных;

– восстановление систем после отказов;

– защита систем от несанкционированных модификаций;

– безопасное управление системами и их использование сотрудниками, не являющимися специалистами.

Стандарт BS 7799-2

8. Разработка и сопровождение информационных систем

2) безопасность прикладных систем:

– проверка входных данных;

– встроенные проверки корректности данных в процессе их обработки;

– аутентификация сообщений как элемент контроля их целостности;

– проверка выходных данных.

Стандарт BS 7799-2

8. Разработка и сопровождение информационных систем

3) криптографические регуляторы

Их основой служит документированная политика использования средств криптографии.

Стандартом предусматривается применение шифрования, электронных цифровых подписей, средств управления ключами.

Стандарт BS 7799-2

8. Разработка и сопровождение информационных систем

4) защита системных файлов:

– управление программным обеспечением, находящимся в эксплуатации;

– защита данных систем;

– управление доступом к библиотекам исходных текстов.

Стандарт BS 7799-2

8. Разработка и сопровождение информационных систем

5) безопасность процесса разработки и вспомогательных процессов:

– процедуры управления внесением изменений;

– анализ и тестирование систем после внесения изменений;

– ограничение на внесение изменений в программные пакеты;

– проверка наличия скрытых каналов и троянских программ;

– контроль за разработкой ПО, выполняемой внешними организациями.

Стандарт BS 7799-2

9. Управление бесперебойной работой организации

1) формирование процесса управления бесперебойной работой организации;

2) выработка стратегии обеспечения бесперебойной работы организации;

3) документирование и реализация планов обеспечения бесперебойной работы организации;

4) поддержание единого каркаса для планов обеспечения бесперебойной работы организации, чтобы гарантировать их согласованность и определить приоритетные направления тестирования и сопровождения;

5) тестирование, сопровождение и регулярный пересмотр планов обеспечения бесперебойной работы организации на предмет их эффективности и соответствия текущему состоянию.

Стандарт BS 7799-2

10. Контроль соответствия требованиям

1) регуляторы соответствия законодательству:

– идентификация применимых законов, нормативных актов и т. п.;

– обеспечение соблюдения законодательства по защите интеллектуальной собственности;

– защита деловой документации от утери, уничтожения или фальсификации;

– обеспечение защиты персональных данных;

– предотвращение незаконного использование средств обработки информации;

– обеспечение выполнения законов, касающихся криптографических средств;

– обеспечение сбора свидетельств на случай взаимодействия с правоохранительными органами.

Стандарт BS 7799-2

10. Контроль соответствия требованиям

2) контроль соответствия политике безопасности и техническим требованиям

Руководители всех уровней должны убедиться, что все защитные процедуры, входящие в их зону ответственности, выполняются должным образом и что все такие зоны регулярно анализируются на предмет соответствия политике и стандартам безопасности.

Информационные системы нуждаются в регулярной проверке соответствия стандартам реализации защитных функций.

Стандарт BS 7799-2

10. Контроль соответствия требованиям

3) аудит информационных систем

Цель – максимизация эффективности аудита и минимизация помех, создаваемые процессом аудита.

Ход аудита должен тщательно планироваться, а используемый инструментарий защищаться от несанкционированного доступа.

Лекция-4.
Стандарт BS 7799