Технический
Центр
Интернет

Внедрение системы управления информационной безопасностью (ISO27001)

Валерий Темников

temnikov@tcinet.ru

Технический Центр Интернет

ПЛАН ПРЕЗЕНТАЦИИ

Проект по внедрению СУИБ в ТЦИ

СУИБ в соответствии со стандартом ISO 27001

Основные процессы СУИБ

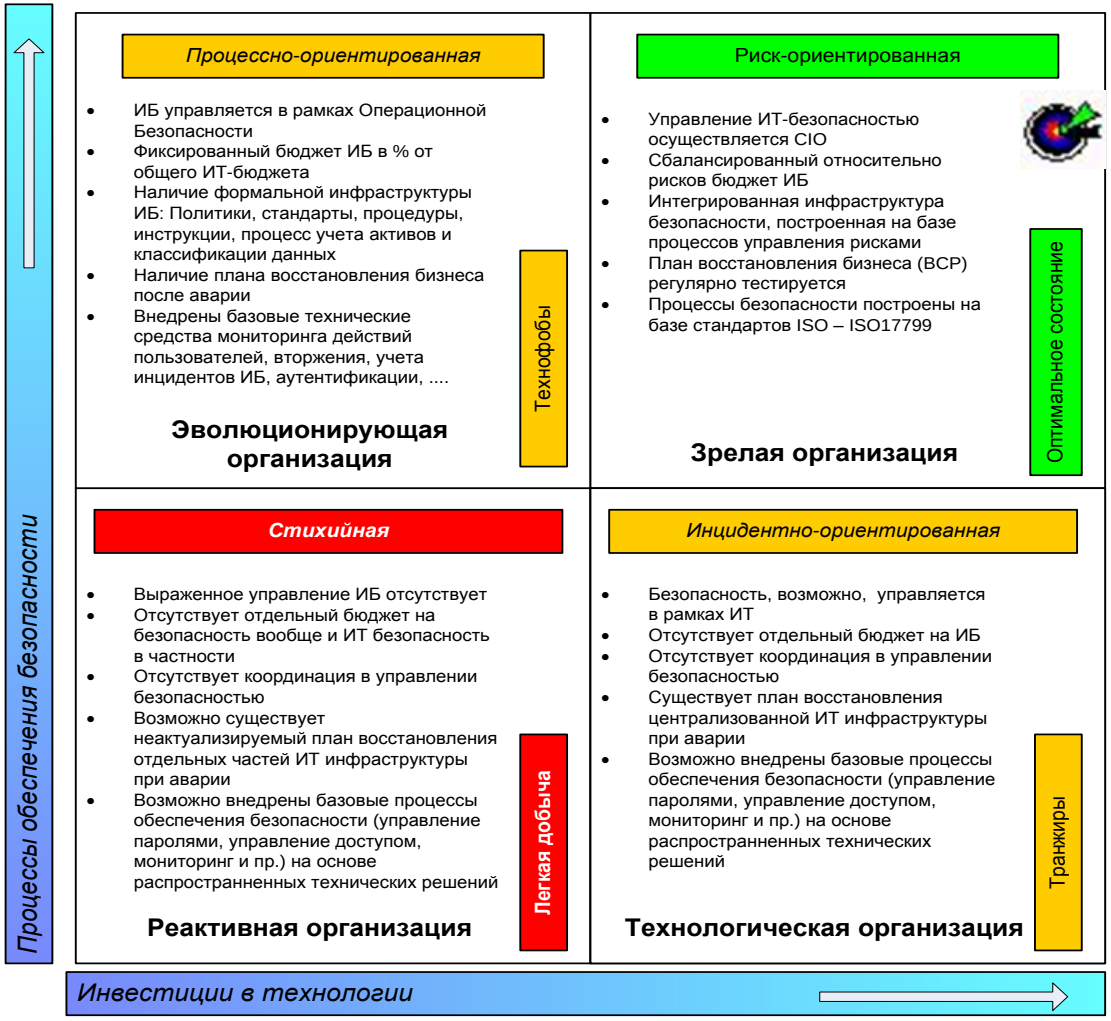
О сертификационном аудите

Технический Центр Интернет

ПРОЕКТ ПО ВНЕДРЕНИЮ СУИБ

Проект по внедрению СУИБ

- Сроки: Июль 2012 – Декабрь 2012
- Инспекционный аудит: май 2014 – август 2014
- Цели:
  - ✓ создание функциональной и организационной модели управления ИБ
  - ✓ создание плана действий по приведению ИТ-инфраструктуры и архитектуры приложений в соответствие требованиям созданной СУИБ
  - ✓ подготовка к сертификации СУИБ по стандарту ISO/IEC 27001:2005



СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ - СУИБ

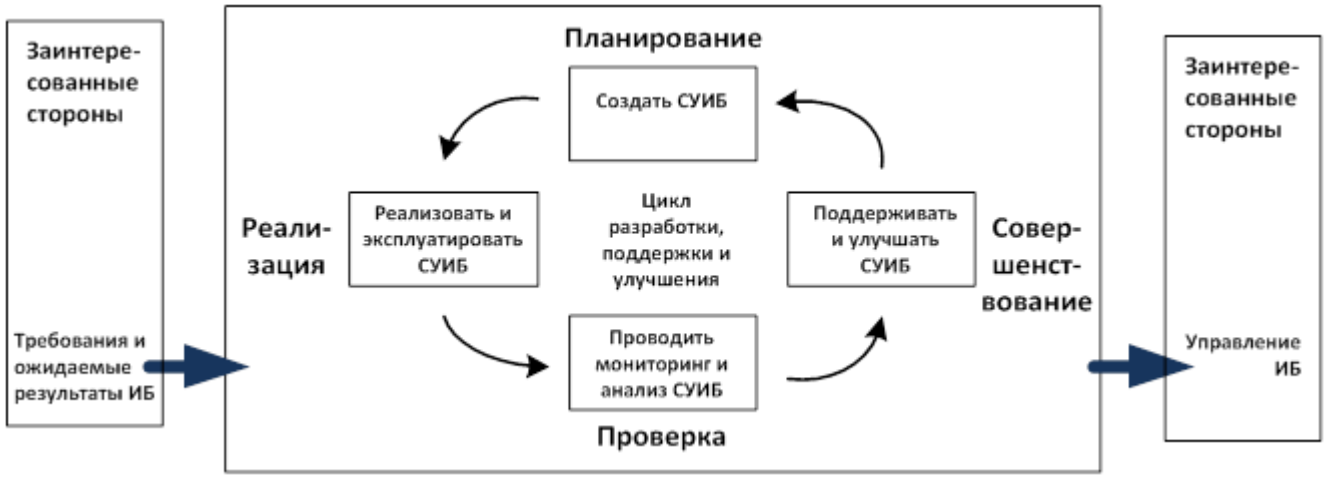
Что такое система управления информационной безопасностью?

- **Система управления информационной безопасностью (СУИБ)** - часть общей системы управления, основанная на управлении бизнес-рисками с целью создания, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности

Состав СУИБ

- Процессы управления ИБ
- Работники, ответственные за обеспечение и организацию управления ИБ
- Комплект документированных политик и процедур
- Механизмы обеспечения ИБ

В основе СУИБ – процессный подход



Технический Центр Интернет

СТАНДАРТ ISO 27001

- Международный стандарт ISO/IEC 27001 - не технический стандарт, это стандарт на систему управления
- Стандарт применим для организаций любого масштаба и отрасли
- Независим от применяемых в организации технологий
- Сертификаты признаются по всему миру
- **Основной акцент стандарта** – защита информации заинтересованных сторон, т.е. клиентов и партнеров
- Стандарт включает в себя основные требования стандарта (обязательные к выполнению), а также требования Приложения А (необходимость выполнения определяется на основе оценки рисков и бизнес-требований)

ОБЛАСТЬ ДЕЯТЕЛЬНОСТИ СУИБ

Бизнес-процессы связанные с обслуживанием Главного реестра

Территориально:

- Центральный офис
- Дополнительный офис
- ЦОД ы

Программные активы:

- Система регистрации доменов
- TRS «HelpDesk»
- Почтовая система
- Системное ПО
- Файлы конфигураций

Подробнее:

- Документ «Область деятельности СУИБ»

Технический Центр Интернет

ПРОЦЕССЫ УПРАВЛЕНИЯ ИБ

УПРАВЛЕНИЕ РИСКАМИ ИБ

Управление рисками ИБ – основополагающий процесс СУИБ

Основные этапы:

- Инвентаризация, оценка ценности активов, идентификация актуальных уязвимостей и угроз
- Анализ и оценка рисков: с учетом вероятности реализации сценариев угроз ИБ и возможного ущерба
- Принятие решения об обработке рисков ИБ
- Обработка рисков ИБ

Величина возможного ущерба	Вероятность реализации сценария угрозы ИБ					
	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	6	8	10
3	0	3	6	9	12	15
4	0	4	8	12	16	20
5	0	5	10	15	20	25
6	0	6	12	18	24	30
7	0	7	14	21	28	35
8	0	8	16	24	32	40
9	0	9	18	27	36	45

Технический Центр Интернет

ОБРАБОТКА РИСКОВ ИБ

Сценарий реализации угрозы ИБ	Нарушаемые свойства информационного актива		
	Конфиденциальность	Целостность	Доступность
Несанкционированный доступ к информационным активам за счет воздействия на ПО специализированными программными средствами (exploits), направленными на активизацию имеющихся уязвимостей ПО, внутренним нарушителем	+	+	+

№	Группа информационных активов	Текущий уровень риска	Механизмы контроля, используемые для уменьшения риска	Статус внедрения механизма контроля	Уровень остаточного риска
1.	Сведения, обрабатываемые в Системе регистрации доменов	Высокий (24)	– определить и регламентировать требования к процессу обеспечения антивирусной защиты; довести требования до пользователей систем под подпись; – использовать антивирусные продукты различных производителей на уровне серверов, рабочих станций и шлюзов; – определить и регламентировать требования к процессу управления уязвимостями; довести требования до пользователей систем под подпись; – внедрить систему анализа защищенности (сканирования уязвимостей в КИС), и проводить регулярное сканирование уязвимостей; – определить и регламентировать требования к процессу управления изменениями; довести требования до пользователей систем под подпись; – регламентировать дисциплинарную ответственность пользователей за нарушение правил ИБ; – проводить систематический контроль знаний работниками требований по обеспечению ИБ;	Планируется к внедрению	Средний (8)
2.	Сведения, обрабатываемые в системе поддержки аккредитованных регистраторов	Средний (6)			Низкий (2)
3.	Исходный код программного обеспечения, разработанного организацией	Средний (12)			Средний (6)

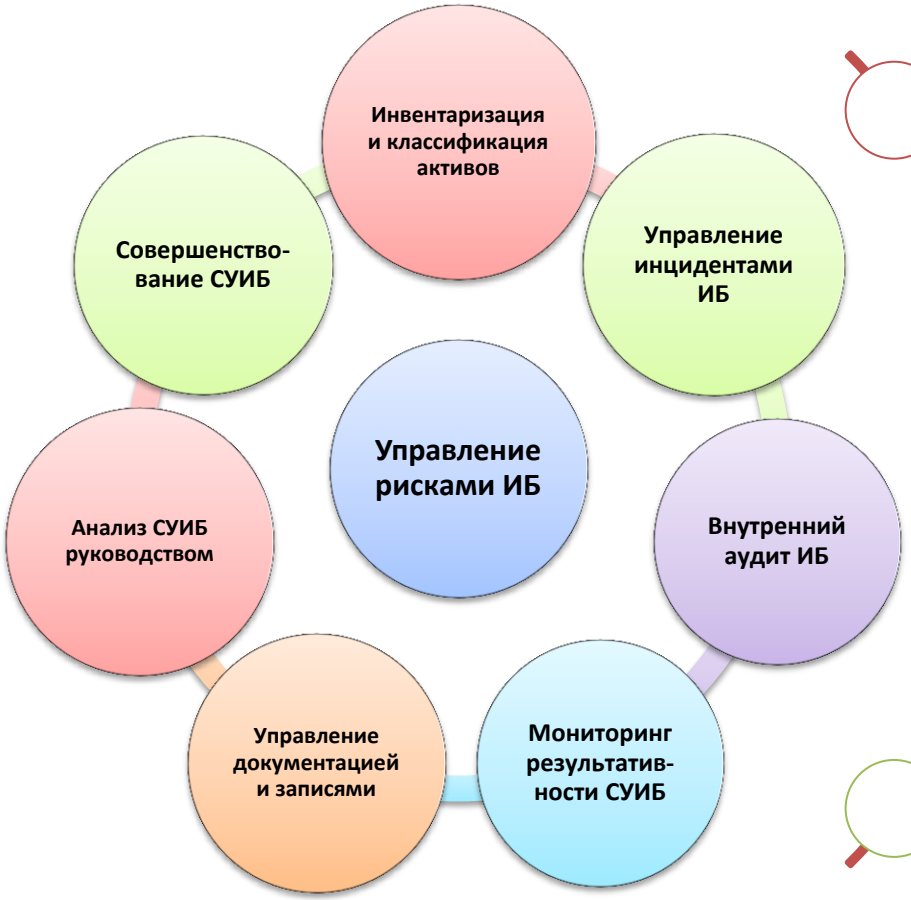
- Обрабатываются риски, превышающие приемлемый уровень
- Руководство определяет приемлемый уровень риска
- Выбор способа обработки: сравнение стоимости обработки и ущерба, учитывается остаточный риск

Способы обработки рисков:

- *уменьшение риска*
- *принятие риска*
- *избежание риска*
- *передача риска*

ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ ИБ

Процессы управления ИБ

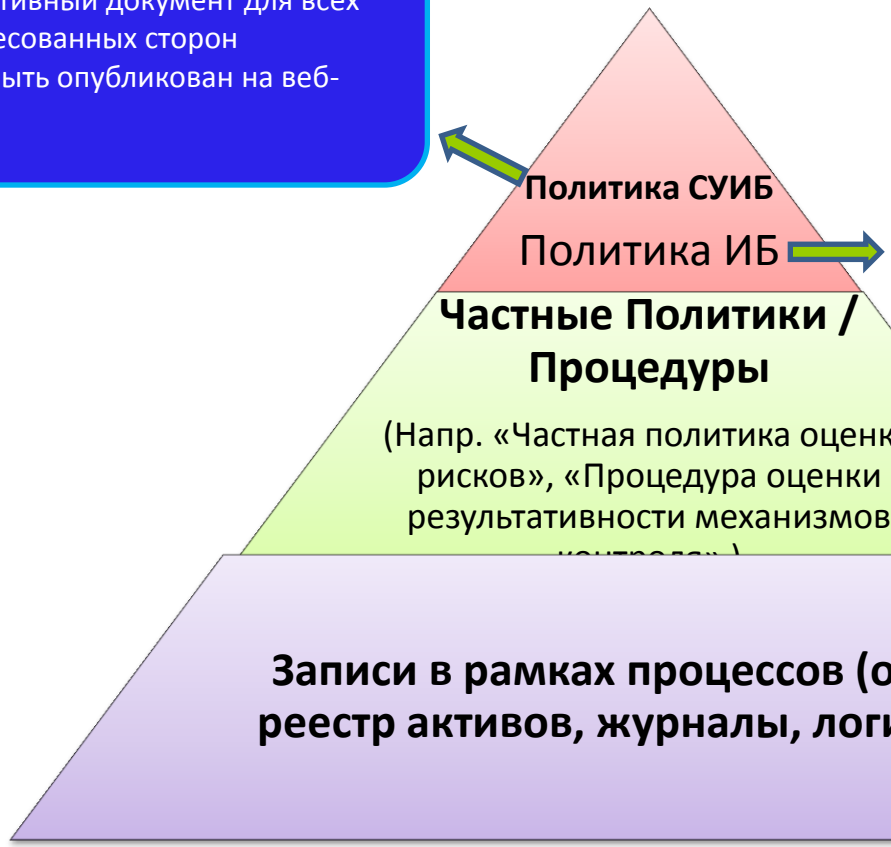


Процессы обеспечения ИБ

- Управление уязвимостями
- Обеспечение ИБ при взаимодействии с персоналом
- Управление доступом к активам
- Управление непрерывностью ИТ-сервисов
- Защита от вредоносного ПО
- Управление сетевой безопасностью
- Контроль соответствия требованиям ИБ

СТРУКТУРА ДОКУМЕНТАЦИИ СУИБ

- Декларативный документ для всех заинтересованных сторон
- Может быть опубликован на веб-сайте



- Определяет основные цели и положения по организации процессов управления и обеспечения ИБ
- Ссылки на все частные политики и процедуры
- Должны знать все работники, входящие в ОД

Разработано 57 организационно – распорядительных документов, всего 131 документ.

Технический Центр Интернет

КОМИТЕТ ИБ

Состав Комитета ИБ

- **Председатель Комитета ИБ** – Генеральный директор
- **Члены Комитета ИБ** (работники, которым присвоены роли в СУИБ или занимающие соответствующие должности):
  - ✓ Технический директор
  - ✓ Начальник отдела ИБ
  - ✓ Руководители ключевых подразделений

Обязанности/Функции

- Обеспечение функционирования процессов управления и обеспечения ИБ
- Выделение необходимых для функционирования процессов управления и обеспечения ИБ ресурсов
- Принятие решения о приемлемом уровне рисков ИБ для Общества
- Принятие решения об обработке рисков ИБ
- Контроль проведения расследования инцидентов ИБ и его результатов
- Принятие решения о привлечении правоохранительных органов к расследованию критичных инцидентов ИБ
- Анализ результатов функционирования процессов управления и обеспечения ИБ

Технический Центр Интернет

О СЕРТИФИКАЦИОННОМ АУДИТЕ

Сертификационный аудит проводился лидером рынка по сертификации систем менеджмента – компанией BSI Russia:

http://www.bsigroup.com/

bsi.

Этапы аудита

- Предсертификационный аудит
- Аудит документации (Этап №1)
- Аудит внедрения (Этап №2)

} Пред-регистрационные этапы

- Инспекционный аудит (1 раз в год)
- Ре-сертификация (1 раз в 3 года)

} После-регистрационные этапы

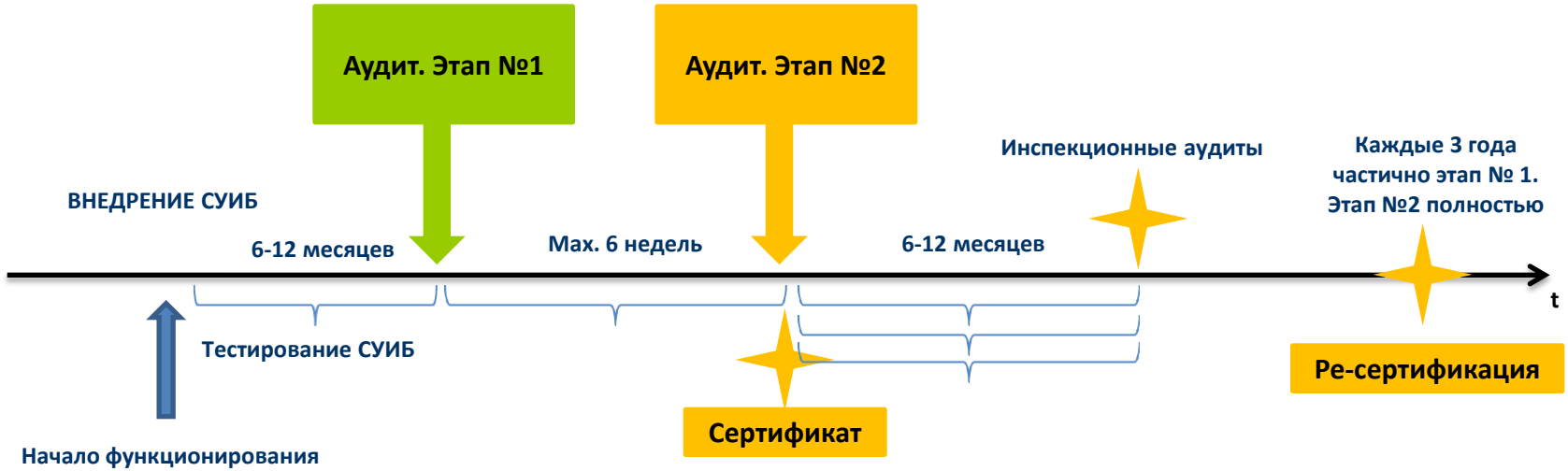
ПРОГРАММА АУДИТА BSI

Этап № 1 – Аудит документации

- Изучение ключевых элементов СУИБ:
  - ✓ Политики, область деятельности
  - ✓ Процессы управления рисками
  - ✓ Декларация о применимости и т.д.
- Как правило, осуществляется на территории Исполнителя (1-2 дня)

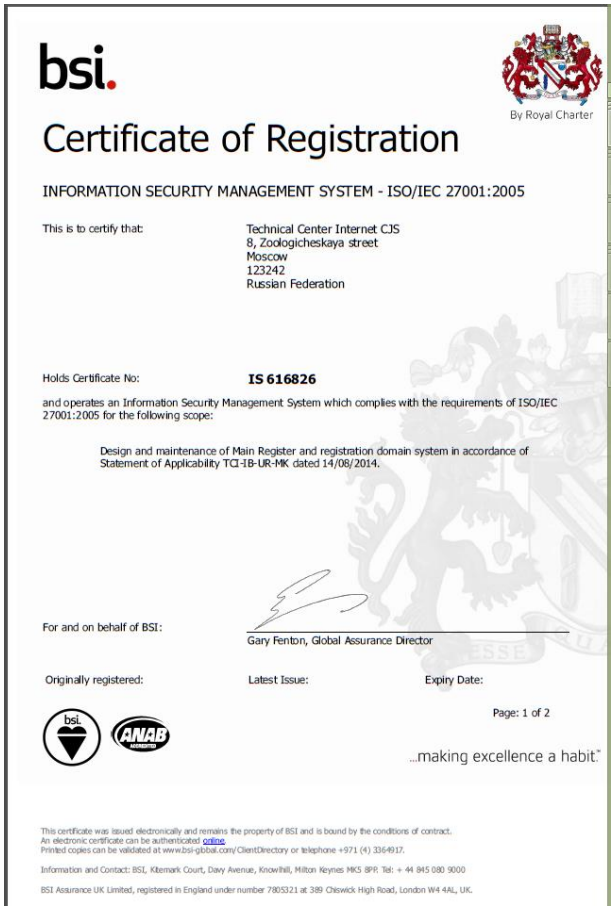
Этап № 2 – Аудит внедрения

- Изучение и анализ результативности политик, процедур и процессов
- Проводится на территории Заказчика (2-5 дней)
- Интервью с руководителями подразделений, опционально – с другими работниками
- Осмотр помещений, наблюдение за действиями работников



Технический Центр Интернет

РЕЗУЛЬТАТ АУДИТА BSI



bsi.

By Royal Charter

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2005

This is to certify that: Technical Center Internet CJS
8, Zoologicheskaya street
Moscow
123242
Russian Federation

Holds Certificate No: **IS 616826**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2005 for the following scope:

Design and maintenance of Main Register and registration domain system in accordance of Statement of Applicability TCI-IB-UR-MK dated 14/08/2014.

For and on behalf of BSI:

Gary Fenton, Global Assurance Director

Originally registered: Latest Issue: Expiry Date:

Page: 1 of 2

...making excellence a habit.

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +971 (4) 3364917.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 845 080 9000

BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.

bsi.

By Royal Charter

Сертификат Регистрации

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ - ISO/IEC 27001:2005

Настоящим удостоверяется, что: ЗАО "Технический центр Интернет"
ул. Зоологическая, д. 8
Москва
123242
Российская Федерация

Выдан Сертификат №: **IS 616826**

о соответствии действующей Системы Управления Информационной Безопасностью требованиям стандарта ISO/IEC 27001:2005 в отношении следующих видов деятельности:

Разработка и техническая поддержка Главного реестра и системы регистрации доменов в соответствии с "Декларацией о применимости механизмов контроля" ТЦИ-ИБ-УР-МК от 14.08.2014.

От имени и по поручению BSI:

Гари Фэнтон, Глобальный директор по сертификации.

Дата первоначальной регистрации: Дата последней выдачи: Действителен до:

Стр.: 1 из 2

...making excellence a habit.

Настоящий сертификат был выпущен в электронной системе BSI и остаётся собственностью BSI;
использование сертификата ограничивается условиями Договора.
Электронный сертификат может быть подтвержден online.
Напечатанные копии могут быть подтверждены на www.bsi-global.com/ClientDirectory.

Контактная информация: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Тел.: +44 845 080 9000
BSI Assurance UK Limited, зарегистрировано в Великобритании за номером 7805321 по адресу 389 Chiswick High Road, London W4 4AL, UK.
Член группы компаний BSI Group.

ЧТО НУЖНО ЗНАТЬ ПРИ ПРОХОЖДЕНИИ АУДИТА

- ✓ Знать Политики ИБ основных процессов, которые функционируют в организации;
- ✓ Понимать область деятельности СУИБ;
- ✓ Знать Дату введения СУИБ в эксплуатацию
- ✓ Понимать назначение, структуру и места хранения документов СУИБ;
- ✓ Знать какие роли исполняет работник в рамках СУИБ и связанные с этой ролью обязанности;
- ✓ Владельцы процессов/активов должны понимать, как проводилась инвентаризация активов;

Всем работникам организации необходимо понимать!

В процессе проверки аудитор может обратиться с вопросом к любому работнику!

Находясь на территории организации аудитор должен быть всегда в сопровождении ответственного сотрудника.

Ваши вопросы

?

Спасибо за внимание

Валерий Темников
temnikov@tcinet.ru