Международные и отраслевые стандарты

ISO/IEC 27001

Часть 2

Павел Новожилов,
руководитель группы консалтинга

Проверка связи

Если у вас нет звука:

- убедитесь, что на вашем устройстве и на колонках включён звук
- обновите страницу вебинара (или закройте страницу и заново присоединитесь к вебинару)
- откройте вебинар в другом браузере
- перезагрузите компьютер (ноутбук) и заново попытайтесь зайти

Поставьте в чат:

\+ если меня видно и слышно

– если нет

Правила участия

1. Приготовьте блокнот и ручку, чтобы записывать важные мысли и идеи
2. Продолжительность вебинара — 80 минут
3. Вы можете писать вопросы в чате
4. Запись вебинара будет доступна в личном кабинете

Павел Новожилов

О спикере:

- более 14 лет в сфере ИБ
- тимлид команды в области различных регуляторных требований
- более 60 выполненных проектов
- основные направления: 152-ФЗ, 187-ФЗ и различные подзаконные акты, 683-П/716-П/719-П/802-П/821-П, стандарт ГОСТ Р 57580.1-2017, ISO 27001

Вспомним материалы лекций

1. Познакомились с историей и семейством стандартов ISO/IEC 27001
2. Узнали структуру стандарта ISO/IEC 27001
3. Узнали, как самостоятельно подготовиться к международной сертификации СУИБ по стандарту ISO/IEC 27001

Повторим

Вопрос: сколько уровней можно выделить в иерархии документации?

Повторим

Вопрос: сколько уровней можно выделить в иерархии документации?

Ответ: 4 уровня:

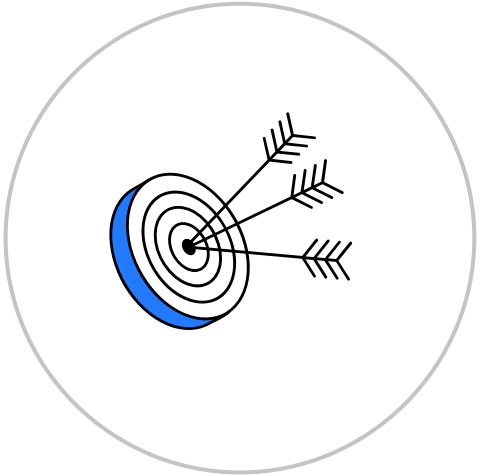
- политика ИБ
- частные политики
- регламенты/инструкции
- свидетельства

Перечислите ключевые элементы процесса управления рисками ИБ

Ваши вопросы?

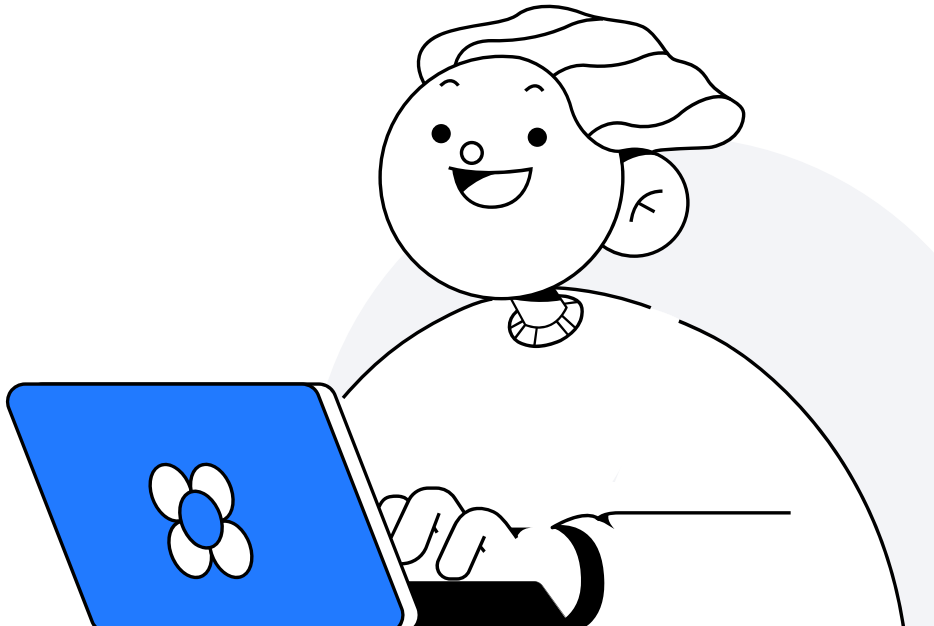
Цель занятия

Узнать, как внедрять контроли ИБ
в соответствии с лучшими практиками ИБ



План занятия

1. Организационные контроли. Часть 2
2. Человеческие контроли
3. Контроли физической безопасности
4. Технологические контроли
5. Итоги
6. Домашнее задание



Организационные контроли

Часть 2

Дайте определение и приведите примеры организационных контролей

Управление инцидентами ИБ

Документирование управления инцидентами ИБ, включая разработку планов реагирования (playbook)

Мониторинг событий ИБ

Реагирование на инциденты ИБ

Регистрация инцидентов ИБ

Расследование инцидентов ИБ

Классификация инцидентов ИБ

Ведение базы инцидентов ИБ

Тестирование разработанных планов реагирования на инциденты (playbook)

Подумайте

Вопрос: чем отличается событие ИБ от инцидента ИБ?

Подумайте

Вопрос: чем отличается событие ИБ от инцидента ИБ?

Ответ:

- **событие ИБ** — идентифицированное появление определённого состояния системы, сервиса или сети, указывающее на возможное нарушение политики ИБ, отказ защитных мер или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности
- **инцидент ИБ** — одно или несколько событий ИБ, которые могут привести к риску нарушения выполнения процессов организации или нарушить безопасность информации

Управление уязвимостями

Документирование процесса управления уязвимостями

Выявление уязвимостей

Устранение уязвимостей

Контроль за устранением выявленных уязвимостей

Управление изменениями

Документирование процесса управления изменениями

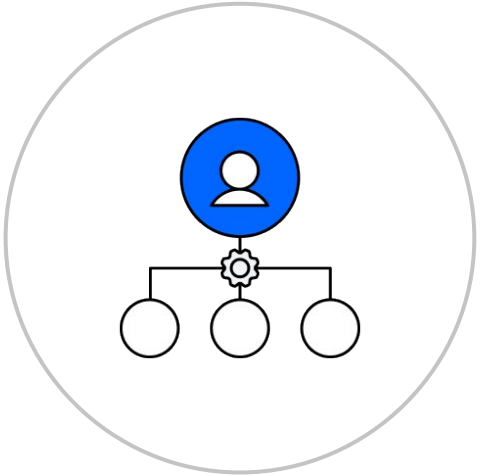
Создание заявки на изменение

Согласование изменений

Приведите примеры изменений в ИТ-инфраструктуре

Управление требованиями в области ИБ

- Определение применимых внешних требований в области ИБ
- Определение требований со стороны сторонних организаций, партнёров, контрагентов
- Учёт применимых внешних требований в области ИБ к организации, например в виде перечня на Confluence



Какие могут быть внешние требования к организации, в которой обрабатываются персональные данные, данные платёжных карт?

Примеры сторонних проверок

Тестирование на проникновение

Экспертный аудит по ИБ

Аудит на соответствие регуляторным требованиям, например 152-ФЗ

Аудит на соответствие требованиям международных стандартов, например стандарту PCI DSS

Выводы

1. Процесс управления инцидентами ИБ, уязвимостями, изменениями должен быть документирован

2. Должен осуществляться учёт внешних требований, в том числе регуляторных, требований международных стандартов, требований сторонних организаций

3. Примерами сторонних проверок могут быть: аудит на соответствие международным требованиям, аудит на соответствие регуляторным требованиям, тестирование на проникновение, экспертные аудиты по ИБ

Ваши вопросы?

Человеческие контроли

2

Приведите примеры человеческих контролей

Человеческие контроли

Проверка персонала

До приёма на работу

Ознакомление с документами по ИБ, подписание NDA (Non-Disclosure Agreement, соглашение о неразглашении)

Повышение осведомлённости в области ИБ

Для новых и действующих работников

Подписание дополнительного NDA

Возврат активов

Отзыв прав доступа

При увольнении работников

Подумайте

Вопрос: какие бывают формы обучения по ИБ?

Подумайте

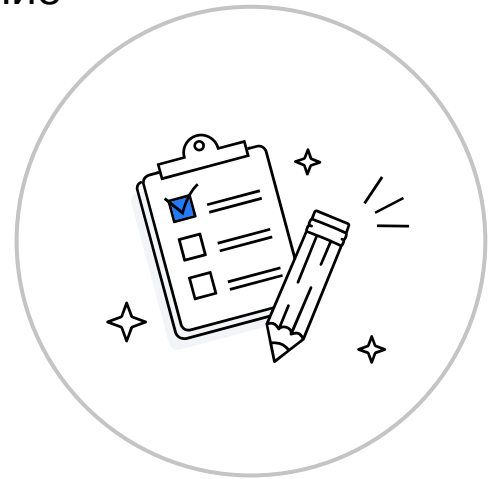
Вопрос: какие бывают формы обучения по ИБ?

Ответ:

- тестовые фишинговые рассылки
- электронный курс + тестирование
- электронный курс в игровой форме
- очное обучение

Выводы

1. Необходимо уделять внимание вопросам ИБ от подбора персонала до увольнения
2. До приёма на работу — проверка персонала
3. При приёме на работу — подписание NDA, ознакомление с документами по ИБ, обучение
4. В течении работы — проведение повышения осведомлённости
5. При увольнении — отзыв прав доступа, возврат активов, например токенов, подписание дополнительного NDA



Ваши вопросы?

Перерыв

5 минут

Контроли физической безопасности

3

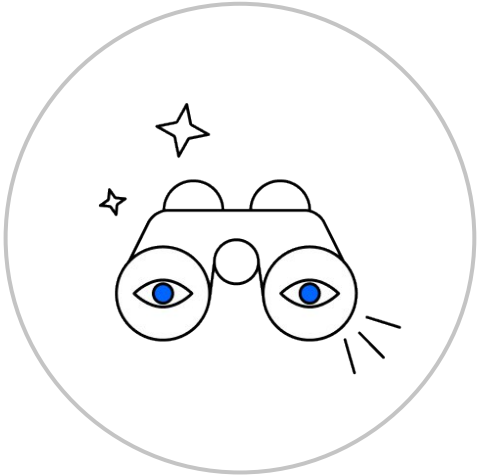
Приведите примеры мер по обеспечению физической безопасности

Физическая безопасность

Пропускной режим

- Организация пропусков для посетителей
- Выдача временных пропусков
- Выдача пропусков работникам
- Технические меры: система контроля и управления доступом (СКУД), охранная сигнализация, система видеонаблюдения, датчики движения и др.

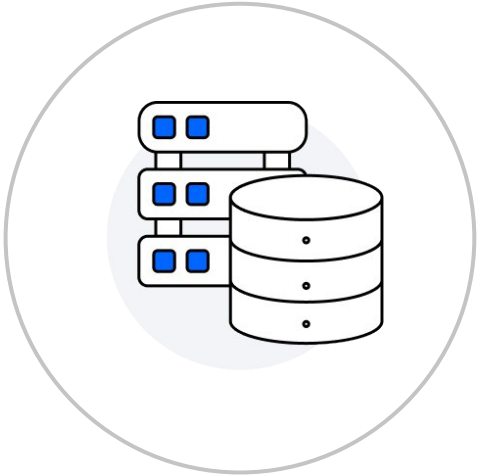
Необходимо помнить про вопросы обработки персональных данных



Физическая безопасность

Внутриобъектовый режим

- Доступ в серверное и кроссовое помещения
- Доступ в помещения, где размещены работники
- Технические меры: СКУД, охранная сигнализация, система видеонаблюдения, датчики движения и др.



Выводы

1. Для пропускного режима необходимо продумать обеспечение доступа для посетителей, работников сторонних организаций, работников самой организации. Также важны вопросы доступа в помещения ограниченного доступа, в том числе серверные помещения

2. К техническим мерам физической безопасности относятся: СКУД, охранная сигнализация, система видеонаблюдения, датчики движения

Ваши вопросы?

Технологические контроли

4

Приведите примеры технических контролей

Основные классы технологических решений ИБ

Антивирусные средства защиты

Средства криптографической защиты информации (СКЗИ)

Межсетевые экраны: FW/NGFW, IPS/IDS

Сканер безопасности

- **FW** — Firewall
- **NGFW** — Next-Generation Firewall
- **IPS** — Intrusion Prevention System
- **IDS** — Intrusion Detection System

Дополнительные классы технологических решений ИБ

Межсетевой экран для веб-приложений
(Web Application Firewall, WAF)

Двухфакторная аутентификация (Two-Factor Authentication, 2FA)

Система сбора и анализа событий ИБ
(Security Information and Event Management, SIEM)

Подумайте

Вопрос: приведите примеры, что можно использовать в качестве второго фактора для аутентификации?

Подумайте

Вопрос: приведите примеры, что можно использовать в качестве второго фактора для аутентификации?

Ответ:

- биометрические персональные данные: отпечаток пальца, рисунок вен и др.
- сертификат на токене
- OTP-код (One-Time Password) в виде SMS-генератора в мобильном приложении

Подумайте, какие объекты можно подключить к SIEM-системе?

Security Information and Event Management,
управление событиями и информацией
о безопасности

Подумайте, какие объекты можно сканировать на выявление уязвимостей?

Безопасность данных

Обезличивание / Маскирование данных

Классификация данных

DLP-система*

Контроль возможных каналов утечки информации:

- съёмные носители
- печать
- мессенджеры
- почта
- интернет

* DLP (Data Loss Prevention) — предотвращение потери данных

Безопасная разработка ПО

Статический анализ кода

Динамический анализ кода

Обучение разработчиков безопасной разработке ПО

Выводы

1. Существуют 4 основных класса средств защиты: антивирусное средство защиты, FW/NGFW и IPS/IDS, СКЗИ, сканер безопасности

2. Дополнительно рекомендуется применять такие СЗИ, как WAF, 2FA, SIEM

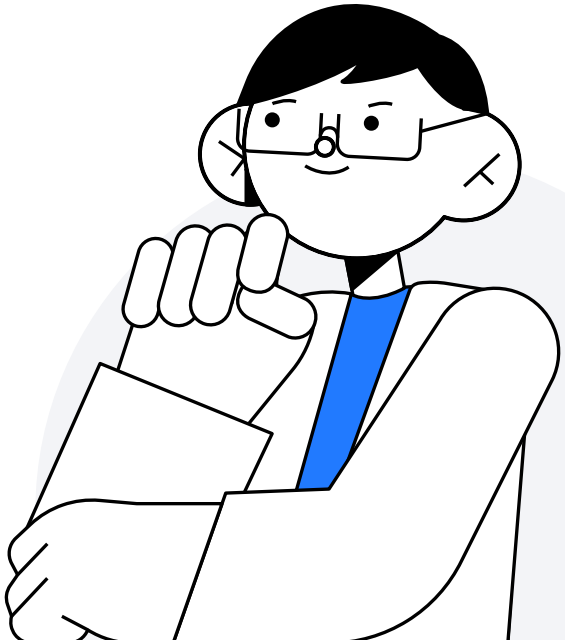
3. В качестве защиты от утечек информации необходимо применять решение класса DLP

4. Для собственной разработки прикладных систем необходимо выполнять анализ кода для выявления уязвимостей

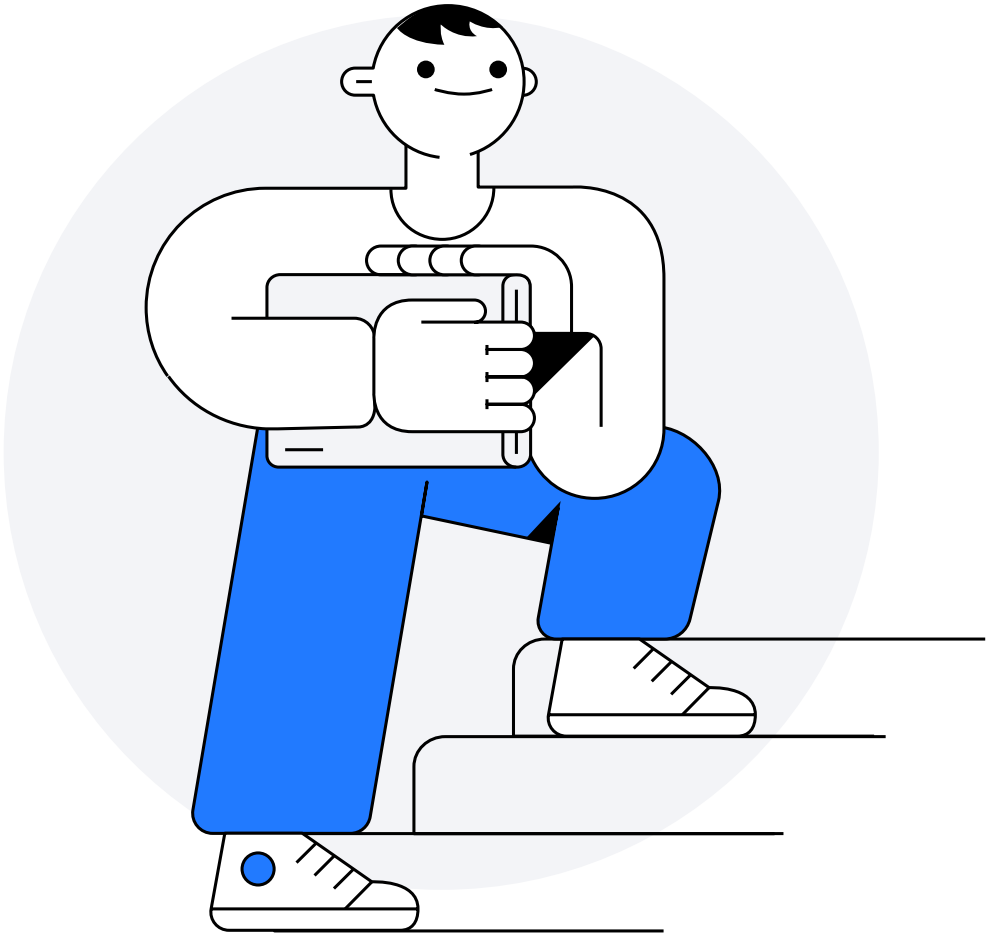
Ваши вопросы?

Итоги занятия

Узнали, как можно внедрять контроли
в соответствии с лучшими практиками
по стандарту ISO/IEC 27002:2022



Домашнее задание



Домашнее задание

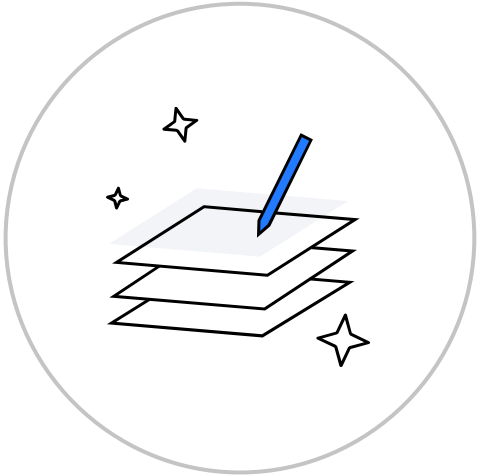
Цель: проверить умение определять несоответствия требованиям стандарта ISO/IEC 27001, используя российский аналог стандарта

Инструменты: Google Документы, стандарт ГОСТ Р ИСО/МЭК 27001-2021 — российский аналог стандарта ISO/IEC 27001

Формат выполнения: файл с заданием

Результат: перечень выявленных несоответствий требованиям стандарта ГОСТ Р ИСО/МЭК 27001-2021 с указанием пунктов стандарта

Описание: исходя из содержания кейса, заполнить по предложенному шаблону описание выявленного несоответствия и дать ссылку на пункт стандарта



Международные и отраслевые стандарты

ISO/IEC 27001. Часть 2

Павел Новожилов,
руководитель группы консалтинга