Аудит

Teach
Me
Skills

Собираемся и отмечаемся

Teach
Me
Skills

Вопросы по предыдущим темам или ДЗ

Teach Me Skills

Mini-quize по новой теме:

1. **Что такое аудит ИБ? И для чего он необходим?**
2. **Сертификация, что это такое?**
3. **Что приходится сертифицировать и кто нас обязывает?**
4. **Какие основные стандарты существуют? По отношении к чему они действуют?**
5. **Что такое ISO 27001?**
6. **Как ISO 27001 вписывается и соотносится с ИБ?**

Teach
Me
Skills

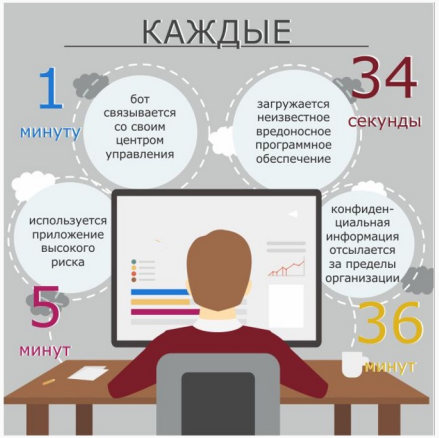
План занятия

1. Рассмотрим основных регуляторов сферы ИБ
2. Изучим НПА в области ИБ
3. Разберемся в отличии сертификации, аудита и аттестации, и зачем нам их проводить или участвовать в них
4. Рассмотри особенности обучения персонала

Аудит ИБ

Teach Me Skills

Аудит информационной безопасности — системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности.



Можно выделить внутренний и внешний аудит информационной безопасности.

- Внутренний аудит регламентируется внутренними документами и уставами компании. Они определяют порядок работы с данными и процессами. Внутренний аудит проводится собственными структурными подразделениями и выполняется на регулярной основе.

- Внешний аудит проводится независимыми экспертами, которым по условиям договоров предоставляется доступ к внутренней сети компании. Он может проводиться по требованию руководства, акционеров и правоохранительных органов. Как правило, привлечение внешних аудиторов ведет к более объективной оценке существующей СУИБ, поскольку такие компании имеют штат квалифицированных аудиторов.

Виды аудита ИБ

Всем организациям необходимо регулярно проводить четыре типа аудита безопасности:
ОЦЕНКА РИСКОВ.
Помогает выявлять, оценивать и расставлять приоритеты для организаций.
ОЦЕНКА УЯЗВИМОСТИ.
Выявляет недостатки в процедурах безопасности, дизайне, реализации или внутреннем контроле, определяя слабые места для нарушения безопасности.
ТЕСТ НА ПРОНИКНОВЕНИЕ.
Определяет потенциальные лазейки в инфраструктуре, облачных технологиях, мобильных платформах и операционных системах.
АУДИТ СООТВЕТСТВИЯ.

Анализ ИБ нацелен на выполнение следующих задач:
• оценку текущего состояния системы ИБ,
• оценку и прогноз уязвимостей,
• повышение уровня ИБ,
• соблюдение требований регуляторов,
• разработку вектора развития для обеспечения необходимого уровня ИБ,
• обоснование финансовых затрат на внесение изменений в систему информационной безопасности компании.

Проведение аудита

Внутренний аудит бывает **повседневным** или **проводимым по заранее согласованному плану** специально определенным подразделением.

За повседневный аудит отвечают сотрудники, связанные с процессом определения негативного воздействия на инфраструктуру организации.

Среди них: инженеры, отвечающие за эксплуатацию инфраструктуры, сотрудники подразделений информационной безопасности, службы мониторинга, защиты активов и другие.
Они отслеживают изменения в основных показателях, присущих информации (целостность, доступность, конфиденциальность).

Глубокий внутренний аудит ИБ — сложное мероприятие, требующее предварительного согласования, разработки регламентирующих документов (плана проверки) и задействования основных ресурсов ИТ/ИБ подразделений и владельцев проверяемых процессов и сервисов.

Проведение аудита

Внешний аудит. Определение требований к аудиту.

Заказчик и исполнитель определяют сферы и направления проверки и ее глубину.
Сбор и систематизация данных.

Формируется перечень источников данных, лиц с правом доступа и с указанием его уровня, и анализируются способы обмена данными, их хранения и использования.

Оценка информационных процессов. Проверяется корректность работы с данными персоналом компании и знание нормативных документов, регламентирующих ИБ. В том числе проверяется механизм распределения прав доступа, эффективность защиты от вредоносного ПО, порядок внутреннего мониторинга ИБ.Формирование заключения по результатам проведенного аудита. В документ вносится информация о выявленных проблемах и недостатках, а также рекомендованные методы их устранения.

Основные стандарты

Что такое стандарт

Национальный стандарт - утвержденный национальным органом по стандартизации стандарт, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг.

Основные стандарты

Что такое стандарт

Стандарт организации - стандарт, утвержденный и применяемый организацией для целей стандартизации, а также для совершенствования производства и обеспечения качества продукции, выполнения работ, оказания услуг, а также для распространения и использования полученных в различных областях знаний результатов исследований (испытаний), измерений и разработок.

Зачем нужны стандарты

При проведении стандартизации решают следующие задачи:

● устанавливают требования к техническому уровню и качеству продукции, а также нормам в области проектирования и производства продукции, которые позволяют ускорить внедрение прогрессивных методов производства продукции высокого качества и ликвидировать нерациональное многообразие видов, марок и размеров, а также обеспечить взаимозаменяемость элементов сложной продукции;

● содействуют взаимопроникновению технологий, знаний и опыта, накопленных в различных отраслях экономики.

Основные стандарты

Кто разрабатывает стандарты

ISO - международная организация по стандартизации, основанная в 1947 году. Совместно с «Международной электротехнической комиссией» (International Electrotechnical Commission, IEC) разработала одну из основополагающих серий стандартов по ИБ – «ISO/IEC 27-ой серии: 27XXX»

Основные стандарты

Кто разрабатывает стандарты

NIST - институт, основанный в 1901 году. Представляет собой подразделение Управления по технологиям США, которое совместно с Американским национальным институтом стандартов США (American national standards institute, ANSI) участвует в разработке стандартов, в том числе и по информационной безопасности.

NIST стандарты

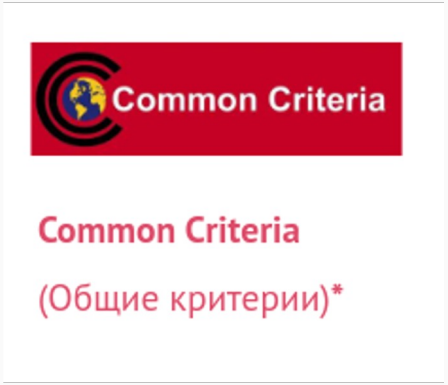
Основные стандарты

Кто разрабатывает стандарты

Общие критерии оценки безопасности информационных технологий
(Common Criteria for Information TechnologySecurity Evaluation) - они же ISO/IEC 15408.

Стандарты устанавливают основные понятия и принципы оценки безопасности ИТ, определяет общую модель оценки, предназначенную для использования в качестве основы при оценке характеристик безопасности продуктов ИТ.

Стандарт формирует методологическую базу в рамках которой разработчики, пользователи и эксперты могут декларировать и проверять свойства безопасности конкретных продуктов. Объектом применения стандарта являются не технологии, как таковые, а конкретные технологии, например ОС Windows 7 или СУБД MS SQL



Основные стандарты

Кто разрабатывает стандарты

Центр безопасности интернета (Center for Internet Security) - некоммерческая организация, разрабатывающая многочисленные стандарты и практики по защите информации. Основана в 2000 году, в основании участвовали такие организации как ISACA, AICPA, IIA, ISC2, SANS Institute. Одни из направлений деятельности разработка лучших практик по ИБ - CIS Controls и CIS benchmarks.

CIS рекомендации

Основные стандарты

Кто разрабатывает стандарты

Open Web Application Security Project - открытый проект, основанный в 2001 году, который направлен на повышение безопасности веб-приложений и мобильных приложений. Проект активно поддерживается множеством участников со всего мира.

OWASP материалы

Open Web Application Security Project*

Основные стандарты

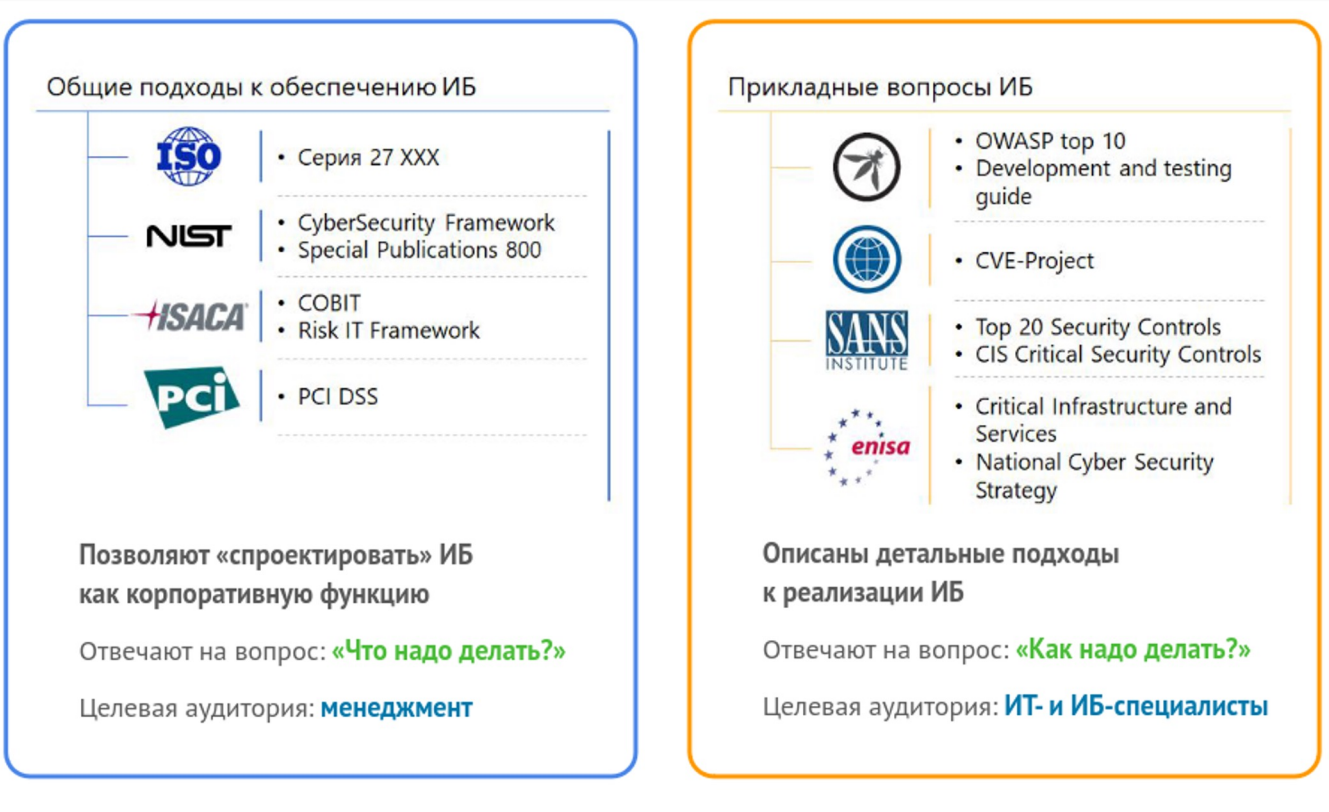
Кто разрабатывает стандарты

Payment Card Industry Security Standards Council,
PCI SSC - совет по стандартам безопасности индустрии платежных карт, учреждённый международными платёжными системами Visa, MasterCard, American Express, JCB и Discover. в 2006 году. Разработчик стандарт по безопасности данных платежных карт PCI DSS Payment Card Industry Data Security Standard

PCI материалы

Основные стандарты

Типы стандартов ИБ



Основные стандарты

Типы стандартов ИБ

* Обязательность или необязательность применения конкретных стандартов очень сильно зависит от организации и отрасли в которой она работает. На данном слайде приведены примеры, для конкретной организации ситуация может сильно отличаться

Как применять стандарты ИБ

Определить перечень нормативных актов, которым должна соответствовать организация.

Определить перечень внешних, обязательных к применению стандартов.

Определить перечень иных внешних обязательных требований (например, требования партнеров или головных организаций).

Провести анализ рисков.

Определить риски, которые “не закрываются” совокупностью обязательных требованиями.

Для этих рисков определить и использовать соответствующие меры.

Основные стандарты

ISO/IEC 27XXX - общее

ISO/IEC 27XXX - семейство стандартов посвященное выстраиванию процессов управления информационной безопасностью. Идеологически являются развитием стандартов BS 7799.

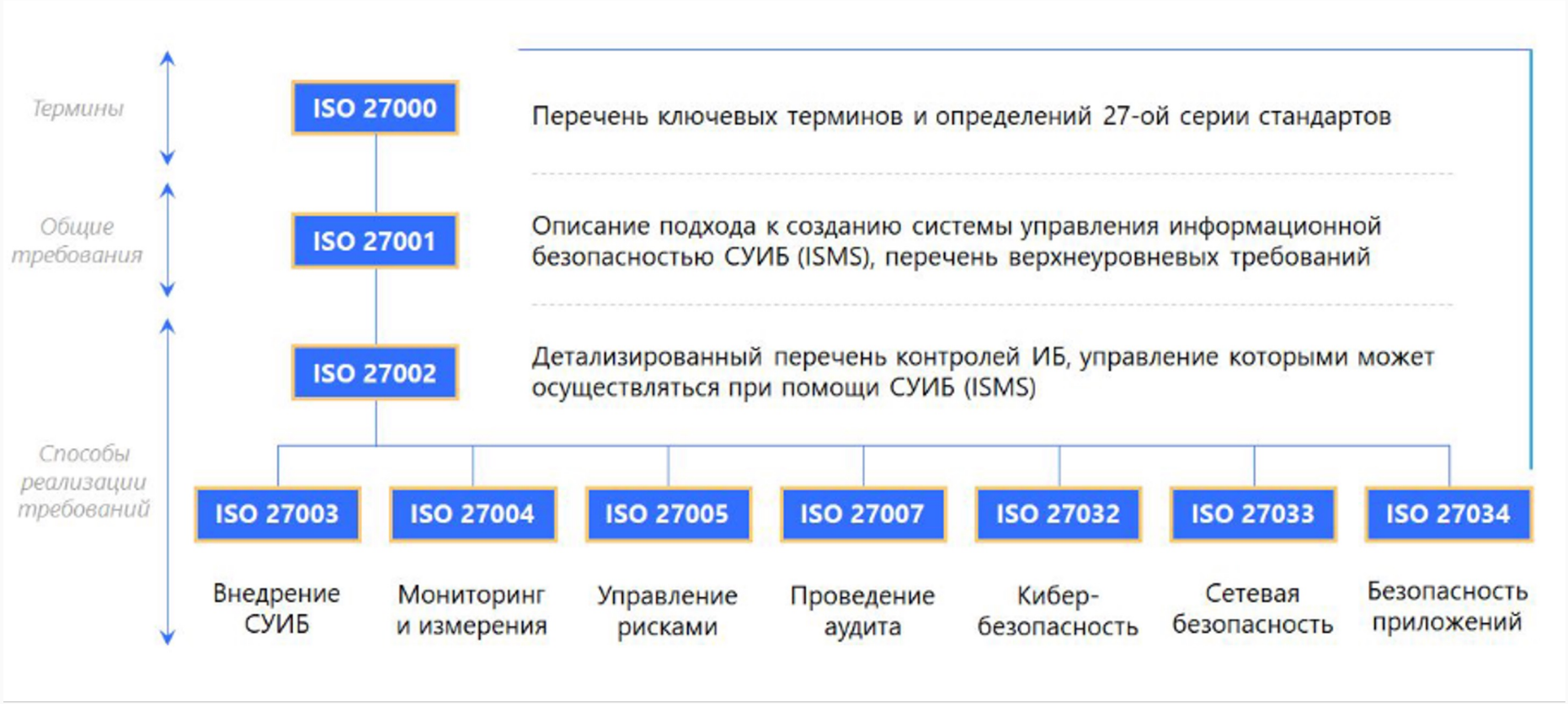
Ключевой идеей является создание СУИБ (системы управления информационной безопасностью) как ключевого элемента процессного подхода, представляющих собой систематический, основанный на управлении рисками, подход к установлению, внедрению, эксплуатации, мониторингу, обзору, поддержанию и улучшению информационной безопасности компании, чтобы достигать ее бизнес-целей.

Основные стандарты

ISO/IEC 27XXX

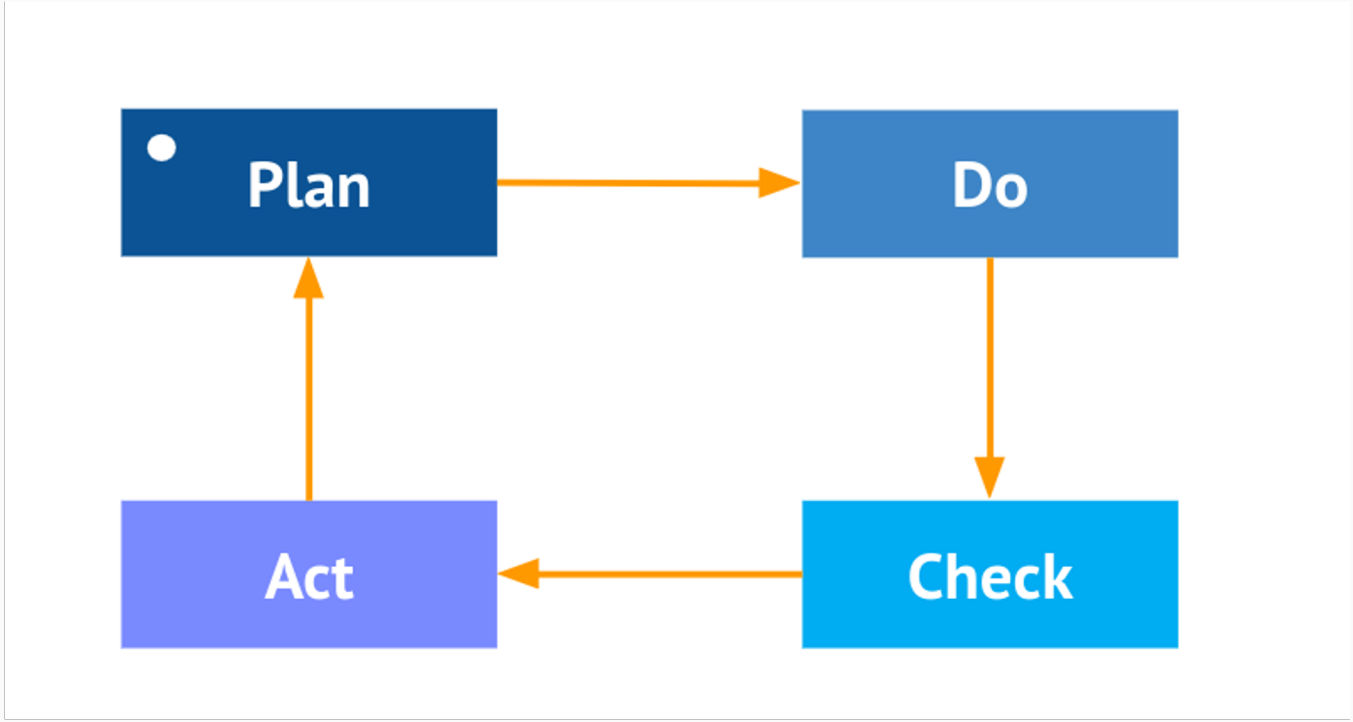
Основные стандарты

ISO/IEC 27XXX



Основные стандарты

Цикл Деминга - непрерывное улучшение



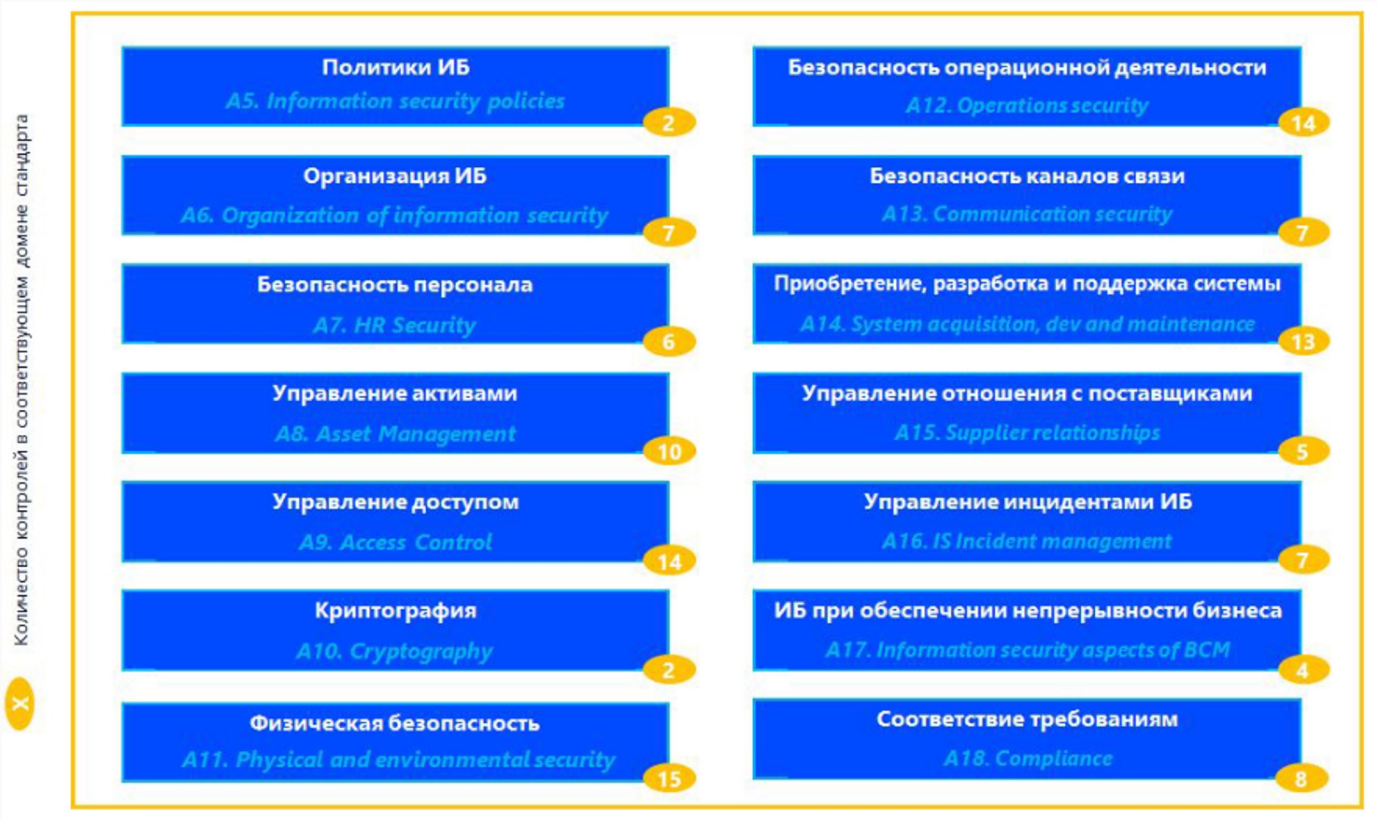
Основные стандарты

ISO/IEC 27001 - “Тело” стандарта

Стадия цикла PDCA				
Plan		**Do**	**Check**	**Act**
Контекст организации • Понимание контекста • Понимание потребностей и ожиданий заинтересованных сторон • Определение области действия и границ СУИБ • Связь СУИБ с циклом PDCA	**Планирование** • Действия по отношению к рискам и возможностям • Цели информационной безопасности и планы по достижению этих целей	**Исполнение** • Операционное планирование и контроль • Оценка рисков информационной безопасности • Обработка оценки риксов информационной безопасности	**Оценивание производительности** • Мониторинг, измерение, анализ и оценивание • Внутренний аудит • Обзор руководством	**Улучшение** • Несоответствия и корректирующие действия • Непрерывное улучшение
Лидерство • Лидерство и приверженность руководства • Политика информационной безопасности • Организационные роли, обязанности и полномочия	**Поддержка** • Ресурсы • Компетенции • Повышение осведомленности • Коммуникации • Документированная информация			

Основные стандарты

ISO/IEC 27001 - Приложение стандарта



Коммерческая тайна

Закон о коммерческой тайне

Закон регулирует отношения, связанные с **установлением, изменением и прекращением режима коммерческой тайны** в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. Закон не может применяться к сведениям, составляющим гостайну.

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ

5 января 2013 г. № 16-З

РФ

98-ФЗ

Коммерческая тайна

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Коммерческая тайна

Информация, составляющая коммерческую тайну - сведения любого характера (производственные, технические, экономические, организационные и другие), к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Коммерческая тайна

К коммерческой тайне не могут быть отнесены сведения

1. содержащиеся в учредительных документах юридического лица и в соответствующих государственных реестрах

2. о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов

3. о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест

4. обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами

Коммерческая тайна

Обладатель информации, доступ к информации

- **Обладатель информации, составляющей коммерческую тайну** - лицо которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

- **Доступ к информации, составляющей коммерческую тайну** - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Коммерческая тайна

Законный vs незаконный доступ

Законный	Незаконный
• информация получена на основании договора; • информация получена на другом законном основании.	• получение информации осуществлялось с умышленным преодолением мер по охране ее конфиденциальности; • получающее информацию лицо знало или предполагало, что информация составляет коммерческую тайну; • лицо, осуществляющее передачу информации, не имеет законного основания на передачу информации.

Коммерческая тайна

Меры по охране информации

1. **Определение перечня информации**, составляющей коммерческую тайну.

2. **Ограничение доступа к информации**, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

3. **Учет лиц, получивших доступ к информации**, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана.

4. **Регулирование отношений по использованию информации**, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.

5. **Нанесение на материальные носители**, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации.

Коммерческая тайна

Меры по охране информации

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных на предыдущем слайде.

Обязательства работодателя

- **Ознакомить под расписку работника с перечнем информации**, составляющей коммерческую тайну.
- **Ознакомить под расписку работника с режимом коммерческой тайны** и с мерами ответственности за его нарушение, которые установил работодатель.
- **Создать работнику необходимые условия** для соблюдения им установленного работодателем режима коммерческой тайны

Коммерческая тайна

Обязательства сотрудника

● **Выполнять установленный работодателем режим коммерческой тайны**.

● **Не разглашать эту информацию**, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима.

● **Возместить причиненные работодателю убытки**, если работник виновен в разглашении информации, составляющей коммерческую тайну.

● **Передать работодателю при прекращении/расторжении трудового договора материальные носители информации**, имеющиеся в пользовании и содержащие информацию, составляющую коммерческую тайну.

Коммерческая тайна

Выводы

1. Нельзя установить режим коммерческой тайны на информацию доступную третьим лицам.

2. Режим коммерческой тайны считается установленным только после выполнения требований, указанных в законе.

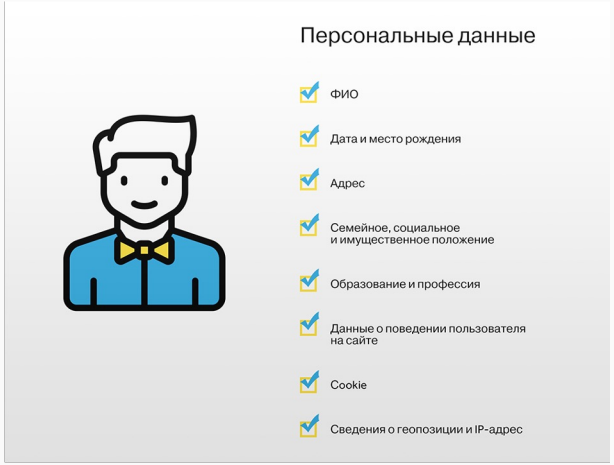
3. Обладатель информации должен выполнять ряд мер для соблюдения режима коммерческой тайны.

4. В случае, если обладатель должным образом не выполнял меры для соблюдения режима коммерческой тайны, он не вправе требовать возмещения убытков.

5. В законе зафиксирован перечень сведений, к которым нельзя применить режим коммерческой тайны.

Персональные данные

Персональные данные — это виды сведений, которые дают возможность косвенно либо напрямую идентифицировать гражданина и в отдельных случаях получить о нем дополнительную информацию.



В контексте проверки согласия и доступности персональных данных (ПДН) можно выделить несколько видов:

Проверка наличия согласия: проверка дачи своего явного или неявного согласия на обработку их персональных данных в соответствии с применимыми законодательными требованиями?

Проверка доступности ПДН: проверка доступа и возможности использования в рамках установленных целей и правил обработки.

Проверка обновления согласия: периодическая проверка наличия актуального согласия субъектов на обработку их персональных данных и обновление этого согласия при необходимости.

Проверка обеспечения прав субъектов данных: проверка того, что субъекты данных имеют доступ к своим персональным данным, могут запросить их исправление, удаление или ограничение обработки в соответствии с применимыми правилами защиты данных.

Закон о персональных данных

Законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой:

- органами власти,
- юридическими лицами,
- физическими лицами*

с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств

Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»

152 ФЗ
О персональных данных

Закон о персональных данных

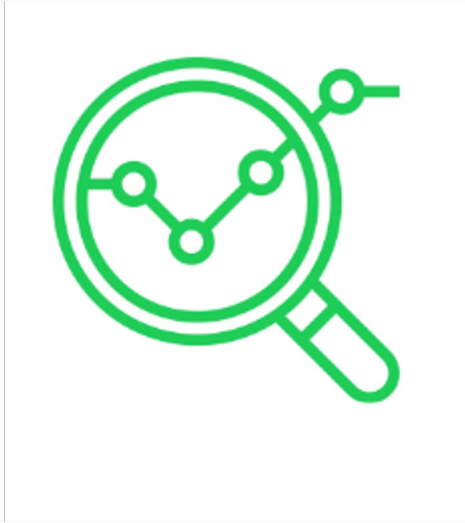
Оператор - государственный, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных.

Оператор определяет: цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных

Обработка персональных данных - любое действие или совокупность действий (операций) с персональными данными, включая сбор, запись, хранение, уточнение, использование, передачу, и т.д.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники (СВТ).



Персональные данные

Блокирование, уничтожение и обезличивание персональных данных

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Под базами данных понимаются в том числе любые файлы, в которых содержатся ПДн.

Трансграничная передача персональных данных

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Защита персональных данных

- В организации должен быть выпущен НПА, закрепляющий цели обработки ПДн.

- Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

- Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

- Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если иное не установлено федеральным законом.

- Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки

Условия обработки ПДн

ПДн могут обрабатываться при условии:

● либо наличия согласия субъекта персональных данных (конкретного человека)

● либо обработки ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн по его просьбе (т.е. человек их сделал общедоступными, например сам опубликовал на странице соц.сети)

● на основании соглашений, в случаях, установленных НПА и т.п

Согласие субъекта ПДн

- Субъект персональных данных принимает решение о предоставлении персональных данных и дает согласие на их обработку.

- Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. Есть прецеденты, когда при подписании договора субъект давал согласие, а затем отзывал его.

- Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в отдельных пунктах закона, возлагается на оператора.

Права субъекта

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- и другие.

Обеспечение безопасности

В законе формулируются требования к оператору ПДн в части обеспечения безопасности:

- определение перечня угроз
- применение орг. и технических мер, обеспечивающих необходимый уровень защищенности
- применение СЗИ, в том числе прошедших оценку соответствия
- оценка эффективности мер
- учет носителей ПДн
- обнаружение фактов несанкционированного доступа (НСД)
- восстановление ПДн, "повреждённых" вследствии НСД
- оценка ущерба
- и другие.

Основные стандарты

Осведомленность пользователей, проведение обучений

- Настройка еженедельной рассылки информации
- Проведение занятий с сотрудниками компании
- Проверка сотрудников с помощью тестовых методов (фишинг, проверка рабочих мест)
- Обучение с помощью специальных программ

Виды тестирования

Нагрузочное тестирование (load testing) — это проверка уровня производительности системы под реальной или смоделированной нагрузкой ожидаемого объема. Т. е. такой анализ направлен на оценку ее поведения в условиях предопределенной нормальной и пиковой нагрузок. Проще говоря, load test показывает, отвечает ли программный продукт предъявленным к нему нефункциональным требованиям: справляется ли с тем объемом работы, на который рассчитан; если справляется, то насколько эффективно; если нет, то почему.

Стресс тестирование (stress testing) — метод нефункционального тестирования ПО, направленный на проверку устойчивости и надежности системы в условиях, которые выходят за рамки обычного функционирования. Stress tests помогают увидеть, как приложение поведет себя при перегрузке или внешних воздействиях: например, при переполнении базы данных, отказе оборудования или атаке злоумышленников. В данном случае целью является поиск пределов работоспособности системы, а кроме того, решаются задачи по оценке ее стойкости, доступности и качества обработки исключений под экстремальной нагрузкой. Стресс-тест также оценивает, как система справляется с отказом отдельных компонентов и есть ли возможность восстановить их полноценную работу после перегрузки.

Backup

Бэкап (backup) — это резервная копия данных, которая содержит всю информацию о сайте или ваших персональных данных. Хранится бэкап на компьютере, сервере или в облачном хранилище.

FTP-бэкапы

FTP-backup — метод, который предназначен для резервного копирования сайтов (или любых других данных). Именно он чаще всего используется хостинг-провайдерами в виде дополнительной услуги, потому что бэкап файлов клиента можно настроить автоматически. Суть этого метода в том, что провайдер выделяет необходимый объём дискового пространства на отдельном FTP-сервере и сохраняет туда данные сайтов своих клиентов.

Облачные бэкапы

Облачное резервное копирование — один из самых удобных способов из бэкапов, который позволяет размещать в своих хранилищах данные любых видов и объёмов: от отдельных файлов до операционных систем, до физических или виртуальных серверов.

Snapshot-бэкап

Снэпшот — снимок сервера, который можно сделать вручную или по API в любой момент. Он используется, если нужно мгновенно сохранить состояние сервера перед внесением изменений или для клонирования сервера. Например, с помощью снэпшота можно сделать снимки системы Linux.

Главное преимущество snapshot — высокая скорость передачи файлов. При нём работа компьютера или другого оборудования приостанавливается буквально на секунду.

HDD-бэкапы

Процесс резервного копирования данных на жёсткий диск HDD При этом устройство может быть как стационарным, так и внешним (съёмным). Выполнять данную операцию можно как в ручном режиме, так и автоматически при помощи специальных программ.

CDP-бэкапы

Технология CDP (Continuous Data Protection) — буквально непрерывная защита данных. Выбирая этот вид резервного копирования, вы можете автоматически сохранять данные при каждом их изменении.

Но для этого нужно установить на сервер специальное ПО — CDP-агент, которое разделяет всю информацию на логические блоки. После чего программа начинёт поблочно передавать файлы в хранилище бэкапов — на CDP-сервер. После первой загрузки программа будет отправлять на сервер только те блоки данных, которые как-либо изменялись, что неплохо сэкономит и место на сервере, и ваше время.

Backup

Proxmox Backup Server

Backup solutions for VMware ESXi

Teach
Me
Skills

Спасибо за внимание!