ICORE

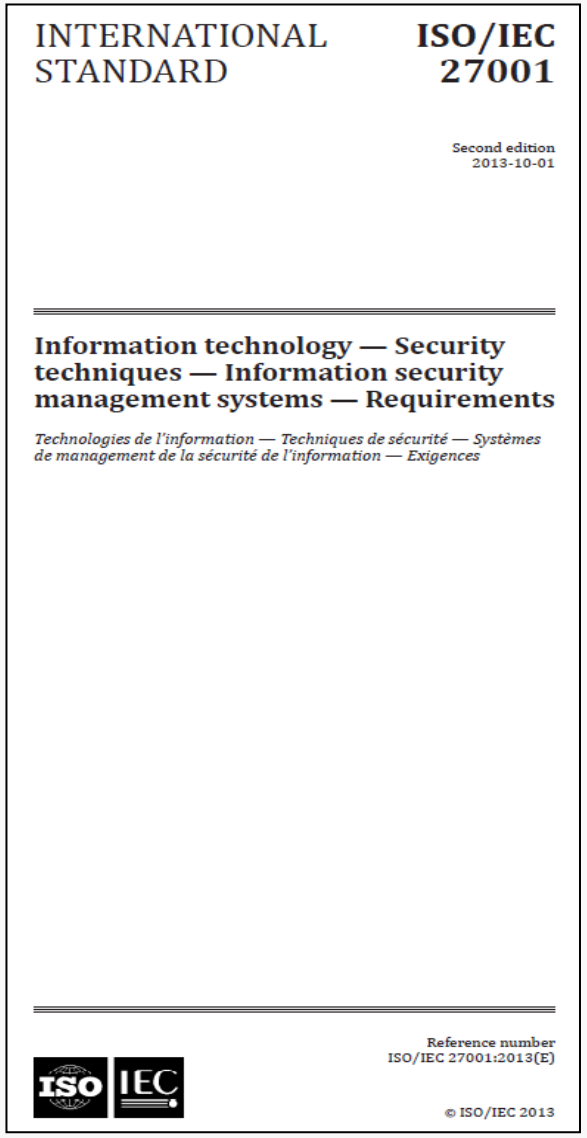
Обследование Системы Управления Информационной Безопасностью (СУИБ)

Содержание

1. Схема внедрения СУИБ
2. Цели, задачи, границы и результаты Услуги
3. Модель Услуги и описание этапов работ, включая разработку/актуализацию ВД

Жизненный цикл СУИБ и структура Стандарта

ISO/IEC 27001:2013


INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Предисловие
0 Введение
1 Область применения
2 Нормативные ссылки
3 Термины и определения

4 Контекст организации
- 4.1 Понимание организации и ее контекста
- 4.2 Понимание ожиданий и потребностей заинтересованных сторон
- 4.3 Определение области применения системы менеджмента информационной безопасности
- 4.4 Система менеджмента информационной безопасности

5 Лидерство
- 5.1 Лидерство и обязательства
- 5.2 Политика
- 5.3 Организационные функции, ответственность и полномочия

6 Планирование
- 6.1 Действия в отношении рисков и потенциальных возможностей
- 6.2 Целевые показатели в сфере информационной безопасности и планирование их достижения

7 Обеспечение
- 7.1 Ресурсы
- 7.2 Компетентность
- 7.3 Осведомленность
- 7.4 Коммуникация
- 7.5 Документированная информация

Plan

8 Функционирование
- 8.1 Планирование и управление функционированием
- 8.2 Оценка рисков информационной безопасности
- 8.3 Обработка рисков информационной безопасности

Do

9 Оценка результатов деятельности
- 9.1 Мониторинг, измерение, анализ и оценка
- 9.2 Внутренний аудит
- 9.3 Анализ системы руководством

Check

10 Улучшение
- 10.1 Несоответствия и корректирующие действия
- 10.2 Непрерывное улучшение

Act

Приложение А (нормативное) Связь задач и средств их реализации
Библиография

Общая схема внедрения СУИБ

I

Обследование ИТ и ИБ

1) Анализ существующей документации
2) Интервью и сбор свидетельств
3) Оценивание ИТ и ИБ инфраструктуры
4) Сканирование на уязвимости и рекомендации

II

Разработка ВНД

1) Разработка системы документации
2) Разработка необходимых процедур HR
3) Разработка модели ролей ИБ в компании
4) Разработка процессов и процедур СМИБ
5) Обучение Рабочей группы СМИБ

III

Анализ, формализация, оптимизация БП

1) Обследование БП (составление Реестра процессов)
2) Категоризация процессов
3) Формализация процессов с учетом Орг.структуры и модели ролей (описание БП)
4) Оптимизация БП
5) Обучение

IV

Работа с активами

1) Разработка документации , всех уровней и форм
2) Разработка Реестра активов
3) Разработка Базы требований
4) Обучение

V

Управление рисками ИБ

1) Разработка документации , всех уровней и форм
2) Разработка и формирование Реестра рисков ИБ , Плана обработки рисков
3) Обучение

VI

Процессы совершенствования СМИБ

1) Разработка процедур анализа и оценивания (МИ и МУ)
2) Разработка программы внутреннего аудита
3) Разработка программы подготовки к внешним аудитам
4) Разработка процессов и процедур совершенствования ИБ

VII

Разработка карты технической защиты

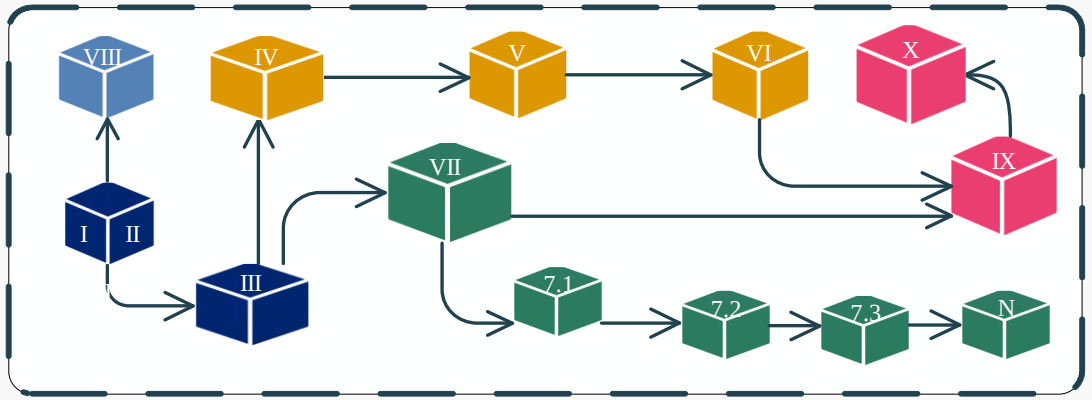
1) Разработка карты Кибер защиты
2) Разработка плана реализации Тех .карты и состава работ

Защита от вредоносного ПО	*Контроль доступа (AC)*	*Инцидент Менеджмент*
Сетевая безопасность	*Удаленный доступ*	*Криптография*
Резервное копирование	*Управление уязвимостями*	*ОЦИБ (SOC)*
Безопасность конечных устройств	*Предотвращение утечек информации (DLP)*	*Управление привилег . пользователями (PAM)*

VIII

Управление человеческими ресурсами и культура ИБ

1) Разработка документации
2) Разработка процедур информирования и поддержания осведомленности
3) Разработка процесса Аттестации
4) Программа обучения
5) Программа оценки уровня лояльности
6) Обучение



X

Автоматизация СМИБ

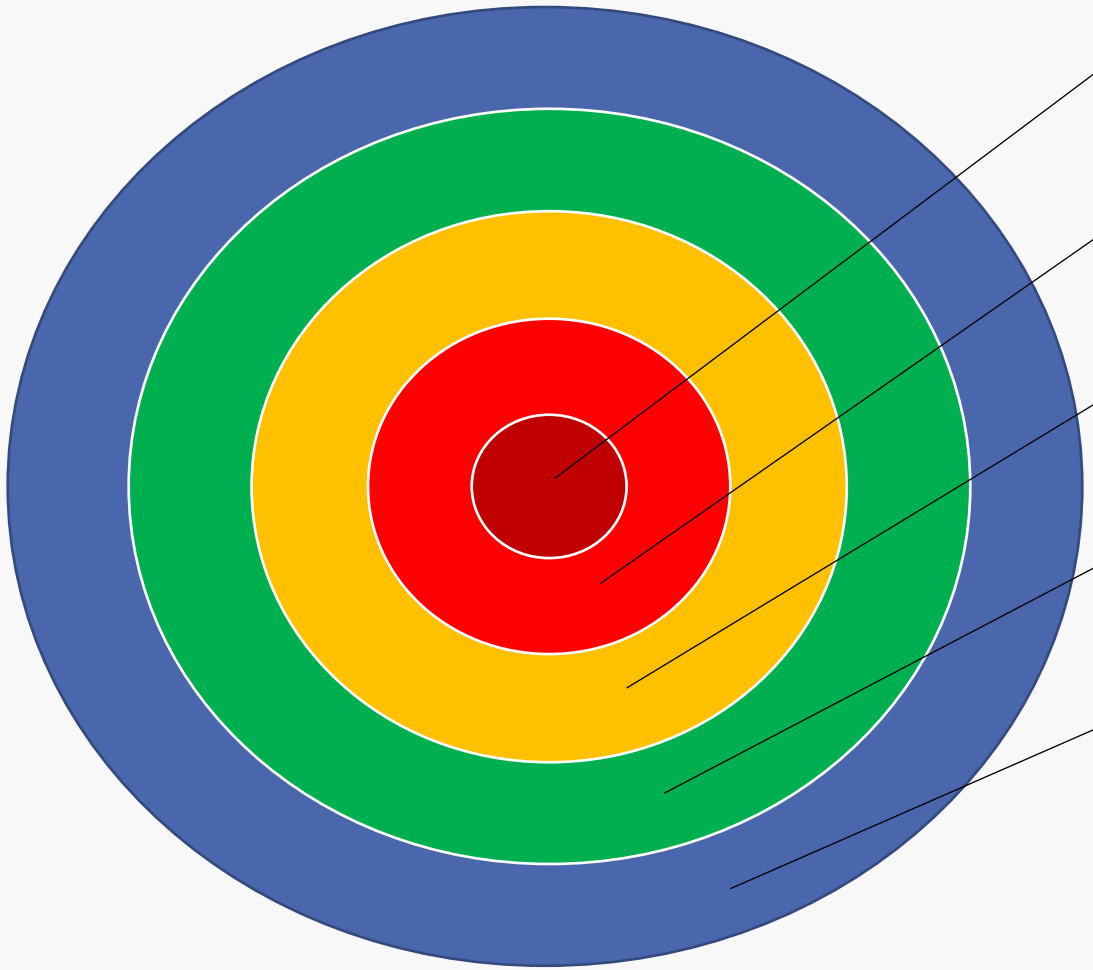
Автоматизация всех процессов ИБ
1)Сбор и анализ информации о ходе выполнения деятельности со всех подразделений компании (испл. класс системы GRC)
2)Агрегация данных и реагирование на инциденты от систем и средств ИБ(испл. системы IRP)
3)Управление доступом и ролями (испл. системы Коргаушы)
4)Обучение

IX

Система отчетности

Разработка системы отчетности ИБ
1)Определение объектов измерения
2)Выбор метрик эффективности ИБ
3)Определение формул измерения
4) Анализ полученных данных и формирование отчета
5) Оценка результативности процессов ИБ
6)Обучение

СУИБ в организации



Формирование бизнес идеи (бизнес-цели)

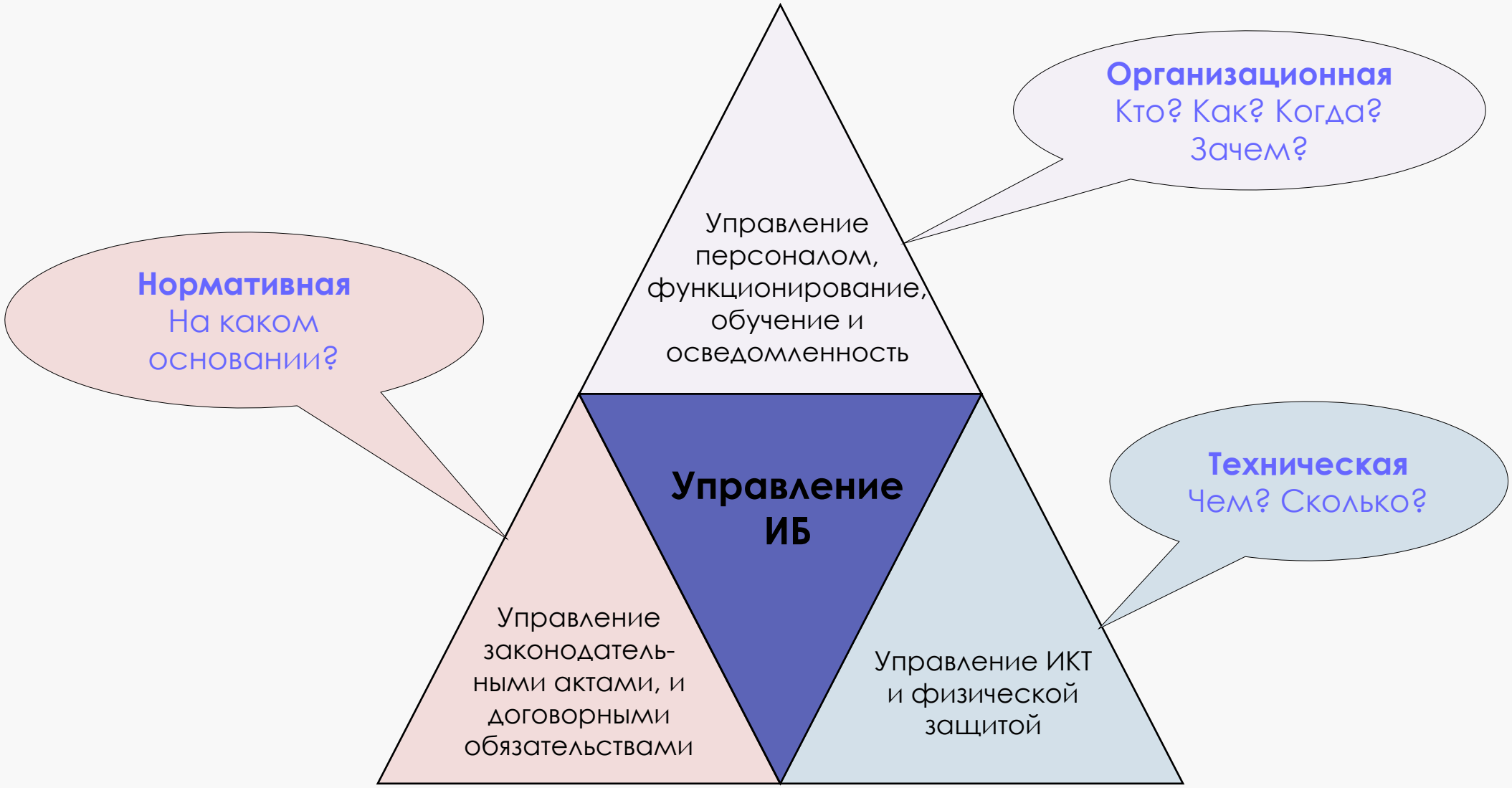
Постановка основных процессов

Автоматизация основных процессов

Формирование информационных активов

Организация информационной безопасности

СУИБ охватывает следующие области:



Обследование или аудит?

Аудит - систематический, независимый и документированный процесс получения свидетельства аудита и объективной его оценки с целью определения степени, с которой выполняются критерии аудита (ISO 27000).

Обследование - оценка текущего уровня ИБ организации с разработкой рекомендаций по реализации комплекса организационных и технических мер, повышающих существующий уровень ИБ.

Цели Услуги и ее ценность для Заказчика

1. Получение объективной независимой экспертной оценки текущего уровня соответствия СУИБ:
- требованиям нормативно-правовых актов Республики Казахстан*;
- положениям международных стандартов в области информационной безопасности**;
- внутренним требованиям организации в области ИБ,

с выявлением несоответствий, «проблемных зон» и выработкой рекомендаций по их устранению

2. Оценка зрелости существующих процессов ИБ в организации

3. Подготовка к внешним аудитам регуляторов или к сертификации на соответствие стандарту ISO 27001

5. Проверка существующих мер (контролей) защиты информации и эффективности работы ключевых участников СУИБ

6. Обоснование инвестиций в направление информационной безопасности

Задачи Услуги

1. Анализ действующих ВД, регламентирующих вопросы ИБ Заказчика, на соответствие требованиям НПА РК и международным стандартам в области ИБ;
2. Интервьюирование с ключевыми лицами ответственными за управление и обеспечение ИТ и ИБ, а также работниками, отобранными для участия в опросах;
3. Инструментальное сканирование компонентов ИТ-инфраструктуры на наличие уязвимостей (опционально);
4. Выработка рекомендаций по устранению выявленных несоответствий по управлению ИБ;
5. Выработка рекомендаций по совершенствованию и автоматизации технических средств обеспечения ИБ;
6. Пакет разработанных/актуализированных ВД по ИБ;
7. Формирование отчетов и рекомендаций по устранению выявленных уязвимостей;
8. Обучение (опционально), повышение осведомленности работников.

Нормативные, регуляторные требования, лучшие практики, которые учитываются при реализации Услуги:

Законы, Указы, Постановления и Приказы в области ИТ и ИБ Республики Казахстан

Государственная техническая служба Комитета Национальной безопасности Республики Казахстан

Постановления Национального Банка РК в области ИТ и ИБ

Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework

ISO27001
ISO27002

PCI DSS v.3.2
PA DSS v.3.2

Национальный институт стандартов и технологий США

Методология управления ИТ, Библиотека инфраструктуры ИТ

Границы Услуги

Формируются на основании:

- информации из первоначального Опросника
- результатов аудитов (при наличии), ИТ обследования

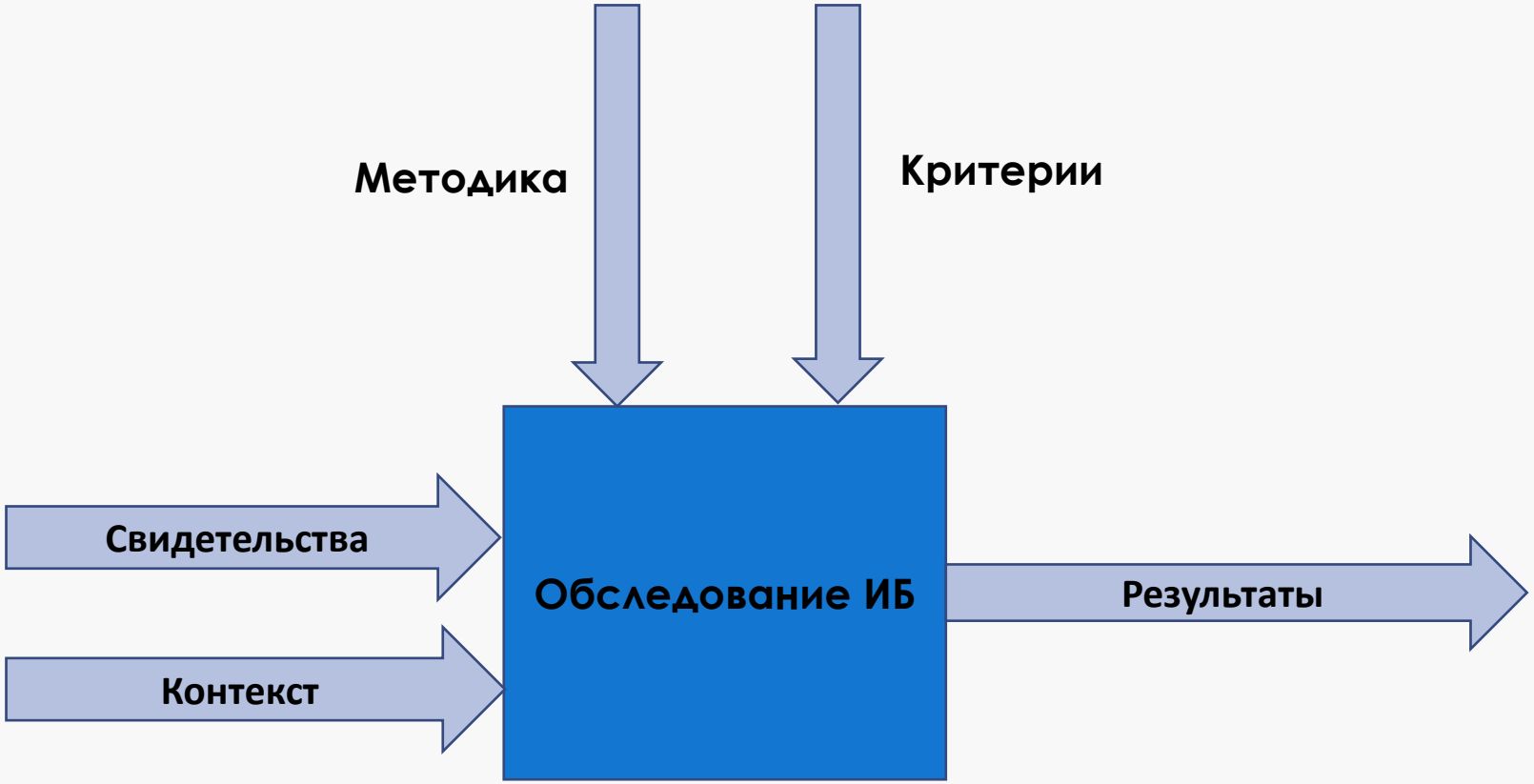
Границами Услуги являются:

- руководители структурных подразделений и работники Заказчика, являющиеся ключевыми участниками СУИБ,
- работники, отобранные для участия в опросах,
- действующие ВД, в том числе организационно-распорядительные, локально-нормативные, справочно-информационные и подтверждающие записи,
- ИТ-инфраструктура.

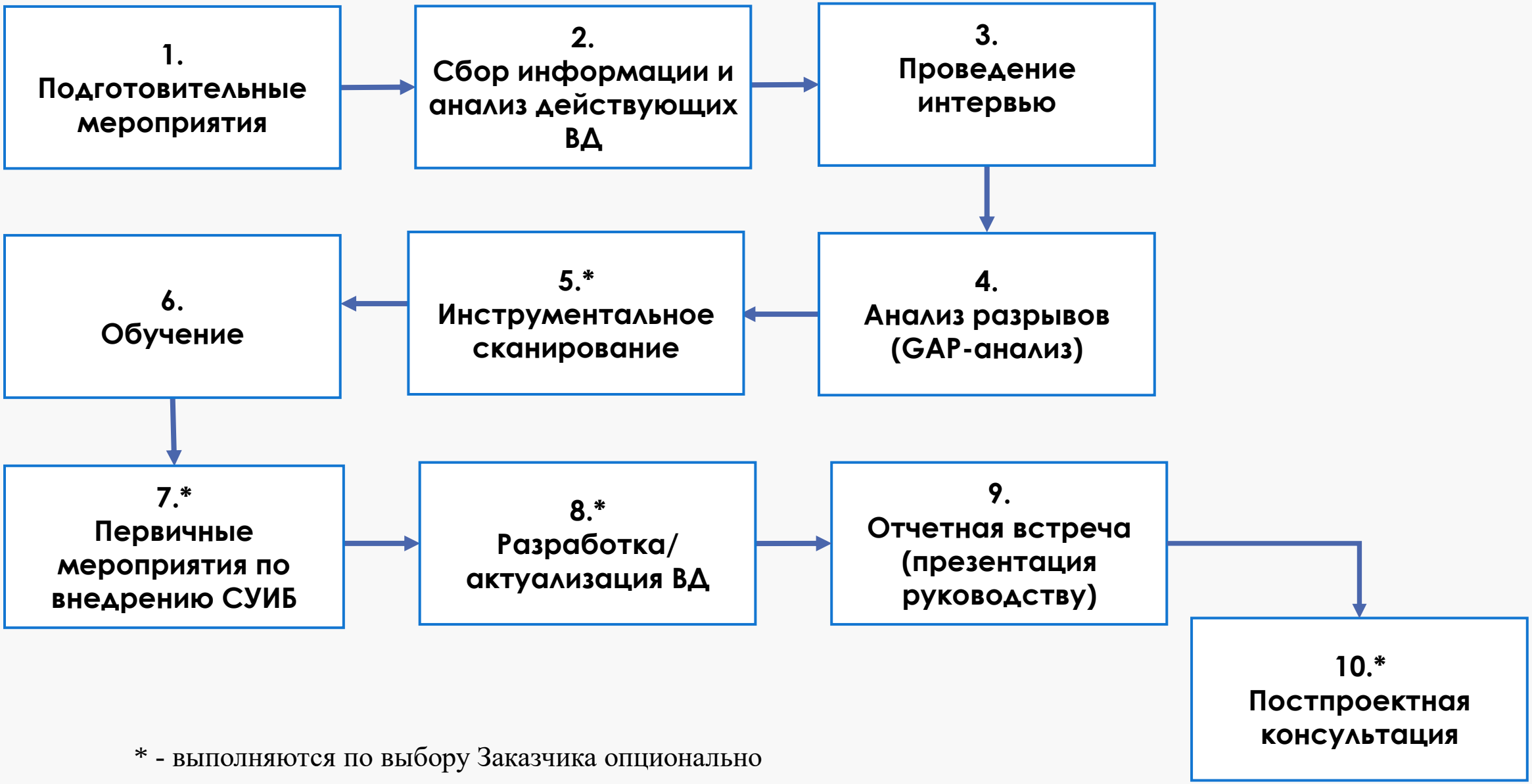
Результаты Услуги:

- Итоговый отчет с оценкой текущего состояния СУИБ, с формированием и ранжированием рекомендаций по организационным и техническим мерам управления ИБ;
- Отчеты по GAP-анализу с определением уровня соответствия требованиям и положениям ЕТ №832 и ISO/IEC 27001, с выработкой детальных рекомендаций по устранению несоответствий и возможностей для улучшения (совершенствования) СУИБ, внедрению технических средств обеспечения ИБ;
- Перечень рекомендуемых к актуализации/разработке ВД с распределением в них пунктов требований и положений ЕТ №832 и ISO/IEC 27001;
- Пакет разработанных/актуализированных ВД;
- Положение о применимости SoA;
- Отчеты о выявленных уязвимостях (отчет, сформированный из автоматизированной системы оценки уязвимостей на английском языке, и отчет, включающий ручной анализ выявленных критичных уязвимостей, с рекомендациями по их устранению на русском языке);
- Стратегический план по внедрению/совершенствованию СУИБ;
- Резюме для высшего руководства в виде слайдов презентации, содержащее краткие итоги работ;
- Сертификаты о прохождении по курсу «Система менеджмента информационной безопасности (ISO/IEC 27001)».

Общая модель Услуги



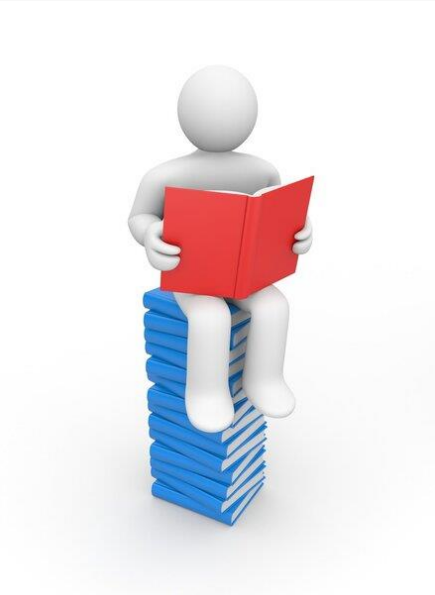
Этапы работ



* - выполняются по выбору Заказчика опционально

1. Подготовительные мероприятия

1. Получение поддержки от руководства Заказчика путем формирования организационно-распорядительного документа (Приказа/Распоряжения) о начале проекта на основании предоставленного Исполнителем шаблона (сроки, ответственный за проект со стороны Заказчика, рабочая группа, их роли);
2. Получение и изучение функционально-организационной схемы Заказчика (оргструктура, штатное расписание, корпоративный телефонный справочник);
3. Составление и согласование формы Протокола разногласий;
4. Получение списка действующих ВД, определение и запрос необходимых для анализа ВД;
5. Формирование и согласование Плана проекта, сроков проведения работ;
6. Определение лиц, ответственных за управление процессами ИБ.



Ответственный за проект работник Заказчика по запросу предоставляет всю необходимую ВД, права доступа и иные необходимые ресурсы для выполнения услуги.

Исполнитель согласует с Заказчиком формы, способы и периодичность предоставления отчетности по статусу выполняемых работ.

2. Сбор информации и анализ действующих ВД

1. Получение необходимых действующих ВД, включая свидетельства (записи), подтверждающих выполнение, для анализа на соответствие требованиям и положениям ЕТ №832 и ISO/IEC 27001;

2. Анализ соответствия отражения в ВД требований и положений ЕТ №832 и ISO/IEC 27001, включая свидетельства (записи), подтверждающие выполнение.

3. Интервью

1. Формирование и согласование с ответственным за проект со стороны Заказчика Методики и Плана-графика проведения интервьюирований с ключевыми участниками СУИБ (ИТ, ИБ, HR, Риски, Аудит, физическая безопасность и комплаенс), с работниками Заказчика, которые будут участвовать в опросах;

2. Проведение интервьюирования с ключевыми участниками СУИБ согласно План-графику на соответствие требованиям и положениям ЕТ №832 и ISO/IEC 27001;

3. Ознакомление и подписание заполненных анкет интервьюированными лицами;

4. Наблюдения и опрос работников Заказчика для подтверждения объективных свидетельств выполнения применимых требований и положений ЕТ №832 и ISO/IEC 27001.

4. Анализ разрывов (GAP-анализ)

Проведение GAP-анализа на основании предоставленных действующих ВД, собранных записей и наблюдений, включающий:

- оценку соответствия требованиям и положениям ЕТ №832 и ISO/IEC 27001,
- перечень собранных подтверждающих записей и наблюдений,
- рекомендации по устранению/минимизации выявленных несоответствий, включая рекомендации по совершенствованию и автоматизации технических средств обеспечения ИБ, а также **Перечень рекомендуемых к актуализации/разработке ВД**.

Форма GAP-анализа

КОНФИДЕНЦИАЛЬНО

	Пункт Требований ISO 27001	Описание требования СТ РК ISO/IEC 27001	Категории оценки соответствия				Свидетельства	Рекомендации по коррекции	Причина несоответствия	Корректирующие действия
			Регламентированность	Выполнение на практике	Оценка соответствия					
4. Организационная среда										
1	4.1	**Анализ деятельности организации и ее рабочей среды** Организация должна установить внешние и внутренние факторы, влияющие на достижение установленных целей её деятельности, а также влияющие на результативность системы менеджмента информационной безопасностью. Примечание – Установление таких факторов влияния заключается в установлении соответствующих внешних и внутренних условий деятельности организации, которые приведены в [5] Раздел 5.3.	да	частично	Частичное соответствие	3		Отразить краткое описание внешнего и внутреннего контекста Компании в одном из документов ИБ верхнего уровня		

5. Инструментальное сканирование*

- Сканирование минимум 2 (двумя) проприетарными автоматизированными системами оценки уязвимостей различных производителей:
  - сканирование внешних IP-адресов (все бизнес-системы, сервисы и сетевые узлы) на наличие уязвимостей и слабых мест доступных с внешнего периметра,
  - сканирование внутренних IP-адресов на наличие уязвимостей и слабых мест во внутренней сети (все бизнес-системы и сервисы, сетевые узлы, сервера и не менее 20% конечных рабочих станций);
- Ручной анализ выявленных уязвимостей и разработка методических указаний по устранению выявленных критичных уязвимостей в ИТ-инфраструктуре.

Критичность найденных слабых мест оценивается качественно по шкалам согласно стандартам CVSS 3.0/ CVSS 2.0.

6. Обучение

1. Повышение осведомленности работников организации (рабочей группы) в процессе реализации Услуги

и/или

2. Обучение руководителей СП

и/или

3. Обучение не менее 2 (двух) работников Заказчика на базе собственного учебного центра Исполнителя по курсу «Система менеджмента информационной безопасности (ISO/IEC 27001)» с выдачей сертификатов

7. Первичные мероприятия по внедрению СУИБ

1. Разработка/актуализация ВД:

- по управлению внутренней документацией (4-х уровневая системы, типы и виды, форма и структура ВД),
- Приказы/Распоряжения по СУИБ (о внедрении, о ролях СУИБ, о создании уполномоченного органа по СУИБ),
- Глоссарий терминов и определений в области ИБ;

2. Согласование разработанных/актуализированных проектов ВД с их бизнес-владельцами.

4-х уровневая системы документации

8. Разработка/актуализация ВД по ИБ

1. Формирование и согласование с ответственным за управление и обеспечение ИБ Перечня действующих и рекомендуемых к созданию ВД;
2. Разработка/актуализация ВД согласно Перечня, определяющих **требования** по вопросам ИБ;
3. Согласование проектов ВД с их бизнес-владельцами;
4. Формирование Положения о применимости (SoA).

ВНД, записи

Исходя из опыта разработки и переработки систем ВНД своих Заказчиков, сформулированы усредненные показатели по количеству требуемых документов для системы документации СУИБ:

Общее количество документов, требуемых согласно стандарту ISO/IEC 27001/27002	Общее количество документов, требуемых согласно ЕТ№832	Общее количество документов, требуемых согласно ПП НБРК №48	Количество свидетельств (записей)
От 40 до 100	От 16 до 74	Более 50	Более 100

Записи - свидетельства выполнения процессов (например, отчеты, планы, приказы, распоряжения, логи ИС, журналы, договора и т.д.)

Примерный список ВНД согласно ISO/IEC 27001

Обязательные документы, требуемые ИСО 27001:2013

1.Область действия СУИБ
2.Политика и цели информационной безопасности
3.Методика оценки и обработки рисков
4.Положение о Применимости
5.Отчет об оценке рисков
6.План обработки рисков
7.Определение ролей и обязанностей в области безопасности (например, оргструктура СУИБ, ДИ, шаблоны ТД)
8.Реестр активов
9.Приемлемое использование активов
10.Политика контроля доступа
11.Рабочие процедуры для ИТ-управления
12.Принципы разработки защищенных систем
13.Политика безопасности в отношении поставщиков
14.Процедура управления инцидентами
15.Положение по управлению инцидентами ИБ
16.Процедуры непрерывности бизнеса
17.Требования законодательства, нормативных документов и контрактов

Обязательные записи, требуемые ИСО 27001:2013

18.Записи об обучении, навыках, опыте и квалификациях
19.Результаты мониторинга и измерений
20.Программа внутреннего аудита
21.Результаты внутренних аудитов
22.Результаты анализа со стороны руководства
23.Результаты корректирующих действий (например, Протокола заседаний Комитета по рискам, Планы мероприятия по управлению рисками)
24.Журналы регистрации действий пользователей, отклонениях от нормы и событиях безопасности

Необязательные (но часто используемые) документы

25.Процедура по контролю документации
26.Средства безопасности для управления записями
27.Процедура внутреннего аудита
28.Процедура корректирующих действий
29.Политика использования собственных устройств
30.Политика использования мобильных устройств и удаленной работы
31.Политика категорирования информации
32.Политика использования паролей
33.Политика размещения и уничтожения
34.Процедуры для работы в зонах безопасности (например, документ об организации пропускного и внутриобъектового режимов, документ о порядке доступа в специализированные помещения)
35.Политика чистого стола и чистого монитора
36.Политика управления изменениями
37.Политика резервного копирования
38.Политика передачи информации
39.Анализ воздействия на бизнес
40.План отработки и тестирования
41.План поддержания и анализа
42.Стратегия непрерывности бизнеса (например, Политика непрерывности бизнеса, Положение по обеспечению непрерывности деятельности ИТ-инфраструктуры)
43.Безопасность кабельного хозяйства
44.Положение о безопасности сети передачи данных

Примерный список ВНД согласно ЕТ №832

1.Политика информационной безопасности
2.Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации
3.Методика оценки рисков информационной безопасности
4.Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации
5.Правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения
6.Правила проведения внутреннего аудита информационной безопасности
7.Правила использования средств криптографической защиты информации
8.Правила разграничения прав доступа к электронным информационным ресурсам
9.Правила использования Интернет и электронной почты
10.Правила организации процедуры аутентификации
11.Правила организации антивирусного контроля
12.Правила использования мобильных устройств и носителей информации
13.Правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов
14.Регламент резервного копирования и восстановления информации
15.Руководство администратора по сопровождению объекта информатизации
16.Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях
17.Приказ об утверждении технической документации по информационной безопасности (ТД ИБ)
18.Реестр активов
19.Расчет класса ИС ОИ
20.Приказ о проведении инвентаризации активов
21.Паспорта на средства вычислительной техники, телекоммуникационного оборудования и ПО
22.Документирование процедуры утилизации и(или) подготовки к повторному использованию серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций, носителей информации (например, акты, приказы или другое)
23.Документирование функционального назначения подразделения ИБ или функциональных обязанностей ответственного за ИБ (например, должностные инструкции)
24.Подтверждение компетентности специалистов в сфере обеспечения ИБ
25.Документирование и функционирование рабочих групп по проведению совещаний в сфере обеспечения ИБ (например, протоколы, приказы и прочее)
26.Документирование взаимодействия с профессиональными сообществами, профессиональными ассоциациями или форумами специалистов по ИБ
27.Листы ознакомления работников, в том числе сторонних организаций, с процедурами обеспечения ИБ описанных в ТД по ИБ и их ответственностью за несоблюдение этих процедур
28.Листы соглашения о конфиденциальности и неразглашении служебной информации
29.Документальная проверка кандидатов при приеме на работу в случае, если работник принимается на должность, связанную с ИБ
30.Документальное подтверждение исполнения процедуры увольнения работников, имеющих обязательства в области обеспечения ИБ
31.Документальное подтверждение предпринятых действий (процедур), которые будут предприняты к нарушителям требований ИБ
32.Документы подтверждающие осведомленность работников и привлекаемых со стороны исполнителей об их обязанностях и ответственности, связанными с обеспечением ИБ в период их занятости, изменений или прекращений трудовых отношений
33.Документы подтверждающие проведение обучения (инструктажа) по вопросам ИБ
34.Утвержденная процедура по реагированию на инциденты ИБ? Ознакомлены ли работники и привлекаемые со стороны исполнители с этой процедурой
35.Документальная стратегия или процесс, обеспечивающий непрерывность ИБ в организации
36.План (процедур и процессов) обеспечения непрерывности ИБ и бизнес-процессов и восстановления после внештатной (кризисной) ситуации
37.Документальное подтверждение тестирования планов (процедур и процессов) обеспечения непрерывности ИБ и бизнес-процессов и восстановления после внештатной (кризисной) ситуации (например, акты, протоколы и прочее)
38.Документы фиксирующие выполнение процедур резервного копирования информации (например, акты, протоколы и прочее)
39.Документы фиксирующие тестирование резервных копий (например, акты, протоколы и прочее)
40.Утвержденный перечень портов управления сетевого оборудования
41.Документальное подтверждение на получение доступа к сетевым ресурсам и сервисам
42.Документированная утвержденная схема локальной сети
43.Документирование каталога угроз (рисков) активов, связанных со средствами обработки информации
44.Документирование утвержденного плана обработки рисков
45.Документирование матрицы доступа
46.Документирование окончания срока трудового соглашения
47.Документирование процесса применения утилит с привилегированными правами в ОИ
48.Документируется ли процесс обслуживания и копирования исходных кодов в ОИ
49.Документирование проведения работ в серверном помещении
50.Регламентирование проведения регламентных работ, действия в аварийных ситуациях, доступ в серверные помещения (физический и организационный), вопросы охраны труда при проведении работ
51.Документирование о фактических неисправностях оборудования и видах восстановительных работ
52.Документально подтверждение компетентности работников, осуществляющих техническое обслуживание оборудования (например, сертификаты, дипломы и прочее)
53.Документированная схема ведомственной (корпоративной) сети телекоммуникаций
54.Документирование кабельных соединений
55.Документированные процедуры установки (обновления) (ПО (прикладного и системного)) в эксплуатируемых ОИ (например, акты, журналы, реестры и прочее)
56.Документирование процесса перевода ПО из среды разработки, в среду тестирования и в среду эксплуатации (например, акты, журналы, реестры и прочее)
57.Документирование перечня интернет-ресурсов, доступ к которым должен быть ограничен
58.Документирование процедуры, реализующих соответствие законодательным, нормативным и договорным требованиям, связанным с правами на интеллектуальную собственность ПО или информационных продуктов и сервисов
59.Листы ознакомления системных администраторов и пользователей ОИ с политикой организации в отношении соблюдения прав интеллектуальной собственности
60.Документирование процедуры безопасной утилизации (или передачи) лицензионного ПО
61.Документирование свидетельства обладания лицензиями ПО
62.Документирование методов защиты конфиденциальных и персональных данных, соответствующих нормам законодательства
63.Документирование анализа ОИ на предмет соответствия требованиям законодательства, стандартов и технической документации по ИБ
64.Документирование результата анализа ОИ на предмет соответствия требованиям законодательства, стандартов и технической документации по ИБ
65.Документирование процедур регламентирующих безопасную разработку (модернизацию) ПО, интеграцию ОИ
66.Документирование в технической документации на создание и модернизацию ОИ требования по ИБ
67.Задокументированная процедура управления изменениями ПО (системного и прикладного) для эксплуатируемых систем
68.Документирование осведомленности работников владельца (собственника) ОИ с содержанием документа, регламентирующего вопросы безопасной разработки ПО
69.Договор на разработку ПО в случае, если процесс разработки ПО осуществляется сторонней организацией
70.Договор на техническое сопровождение ПО в случае, если процесс разработки ПО осуществляется сторонней организацией
71.Приказ о назначении ответственного за ИБ
72.Положения о службе и должностные инструкции ответственного за ИБ
73.Должностные инструкции администраторов ОИ
74.Договор аренды серверного помещения/коллокейшн (при необходимости)

Примерный список ВНД согласно ПП НБРК №48

ВНД:

1.Организационная структура
2.Правила управления документацией
3.Политика ИБ и Область действия СУИБ
4.Реестр информационных активов
5.Перечень критичных ИА
6.Правила работы с защищаемой информацией (допустимого использования)
7.Правила категорирования
8.Политика по управлению рисками ИБ
9.Правила использования мобильных устройств и носителей информации
10.Инструкция по удаленному доступу к корпоративным сервисам
11.Кадровая политика
12.Правила внутреннего трудового распорядка
13.Регламент приема и увольнения персонала
14.Правила обучения, развития и осведомленности персонала по вопросам информационной безопасности
15.Памятка по соблюдению политик ИБ
16.Журнал о прохождении вводного инструктажа
17.Соглашение о принятии документов СМИБ
18.Обязательство о неразглашении защищаемой информации с работником
19.Шаблон ТД
20.Положение о Правлении
21.Положение о СД
22.Положение об уполномоченном органе по ИБ
23.Положение о СП по ИБ
24.Положение о СП по IT
25.Положение о СП по работе с персоналом
26.Положение о СП по безопасности
27.Положение о юридическом СП
28.Положение о СП комплаенс-контроля
29.Положение о СП внутреннего аудита
30.Положение о СП по управлению рисками ИБ
31.Правила проведения внутреннего аудита СМИБ
32.Регламент корректирующих действий
33.Правила разграничения прав доступа к электронным информационным ресурсам
34.Правила организации процедуры аутентификации
35.Правила использования средств криптографической защиты информации
36.Положение о пропускном и внутриобъектовом режиме
37.Правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов
38.Регламент по работе в защищенных помещениях
39.Правила утилизации и уничтожения носителей информации
40.Правила организации антивирусного контроля
41.Правила управления изменениями
42.Регламент резервного копирования и восстановления информации
43.Правила использования Интернет и электронной почты
44.Регламент обеспечения сетевой безопасности
45.Правила безопасной разработки ИС
46.Правила безопасности при работе с Поставщиками
47. Правила осуществления закупок
48. Типовой Договор
49. Политика управления инцидентами
50. Правила мониторинга событий ИБ
51. Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях

Записи:

47. Приказ о внедрении СМИБ (в т.ч. Модель ролей с описанием, КИБ, Раб.группы)
48. Приказ о создании уполномоченного органа по СМИБ
49. Перечень ответственных администраторов узлов информационной инфраструктуры (телекоммуникационных устройств, серверов и размещенных на них ОС, СУБД и приложений)
50. Перечень программного обеспечения и оборудования, разрешенных к использованию
51. Журнал учета приема-передачи внешних носителей и мобильных устройств
52. Годовой План обучения по ИБ
53. Программа обучения и осведомленности персонала по вопросам ИБ
54. План проведения тестирования по ИБ
55. Тестовые вопросы для проведения аттестации работников по ИБ
56. Отчет по внутреннему аудиту СМИБ
57. Отчет о проведении оценки уязвимости сетевых ресурсов
58. Перечень групп пользователей, которым предоставляются права локального администратора или аналогичные права
59. Перечень технологических учетных записей (для каждой информационной системы с указанием лиц, персонально ответственных за их использование и актуальность)
60. Перечень пользователей информационных систем, имеющих доступ к данным информационной системы напрямую, минуя приложение
61. Перечень применяемых средств криптографической защиты информации (с указанием их назначения, реализованных в них криптоалгоритмов, наименования ИС, владельца ИС, использующей СКЗИ)
62. Перечень лиц, допущенных к администрированию средства криптографической защиты информации и управлению ключевой информацией
63. Перечень лиц, допущенных к работе со средствами криптографической защиты информации в качестве пользователей
64. Перечень лиц, имеющих доступ в защищенные помещения (в т.ч. ЦОД-ы)
65. Перечень администраторов средств обеспечения безопасности периметра защиты
66. Журнал регистрации инцидентов ИБ и учета внештатных ситуаций
67. Каталог типовых событий ИБ, подлежащих мониторингу
68. Отчет по мониторингу событий ИБ

9. Отчетная встреча

- Формирование презентации с результатами Обследования
- Определение даты, времени проведения встречи
- Проведение презентации

10. Постпроектная консультация

- Консультирование Ответственных работников Заказчика по вопросам организации и управление процессами ИБ в течении 3-х месяцев с момента подписания акта выполненных работ,

- Консультирование бизнес-владельцев разработанных/актуализированных проектов ВД в процессе согласования ВД с заинтересованными структурными подразделениями Заказчика.

Почему стоит работать с ICORE?

1. При оказании услуг, высококвалифицированные специалисты «ICORE-Consulting» придерживаются процессного, риск-ориентированного подходов, стандартов по управлению проектами и качеством (ISO 31000, ISO 21500, ISO 10005, ISO 9001).
2. Безопасный портал для отчетности и отслеживания проекта
3. Собственная команда квалифицированных аудиторов и отраслевых экспертов-консультантов
4. Строгая политика конфиденциальности
5. Независимая от поставщиков компания
6. Политика отсутствия аутсорсинга
7. Строгие сроки с четко определенным планом проекта и SLA
8. Прозрачность в рабочем процессе
9. Так как информационная безопасность является динамично развивающейся областью, наши специалисты постоянно в курсе современных угроз, уязвимостей и ситуации в бизнес-процессах и технологиях
10. Более 10 лет опыта и знаний в отрасли, более 30 успешно реализованных проектов по консалтингу
11. Сочетание отличного качества и приемлемой стоимости

Спасибо!